Thematic Investing

You've Been Hacked! – Global Cybersecurity Primer

Primer

Bank of America Merrill Lynch

Equity | 03 September 2015

A Transforming World: Cybersecurity

As part of our work on A Transforming World, we introduce a new Innovation-focused theme with this Primer, setting out the challenges and opportunities offered by cybersecurity, as well as a Primer Picks report.

One of the top global risks today: 90mn+ attacks per year

There are 80-90mn+ cybersecurity events per year, with close to 400 new threats every minute, and up to 70% of attacks going undetected. All companies are being hit: finance & insurance is the most targeted sector, followed by ICT, manufacturing and retail. Cybersecurity has become a homeland security threat with rapid growth in attacks against critical infrastructure and manufacturing. Americans worry about falling victim to cyberattacks more than any other type of crime – with 1bn data records compromised in the US alone in 2014. We believe cybersecurity poses a key threat to the three pillars of creative disruption: the Internet of Things (IoT), the Sharing Economy and Online Services.

"Cybergeddon": up to US$3tn in economic impacts

The average cost of cybercrimes for US companies reached a record US$12.7mn in 2014, with cybercrime costing the global economy up to US$575bn annually. Cyberattacks are the #1 source of economic assaults against governments, and the #1 source of IP theft for corporates. The rise in disruptive technologies – including IoT with 50bn+ devices connected to the internet by 2020 – means that we are facing a potential worst-case "Cybergeddon" scenario where the 'bad guy' has the permanent advantage. Cybercrime extracts up to 20% of the value created by the internet, meaning that as much as US$3tn of global economic value could be at risk by 2020E.

Solutions market: US$75bn today & US$170bn by 2020E

The global cybersecurity solutions market is estimated at US$75-77bn in 2015 and forecast to reach US$170bn by 2020E. Drivers include: the increase in the number, sophistication, scope and impact of attacks; IoT creating new security threats; increased spending on cybersecurity by corporates and governments; and the emergence of regulation.

Multiple entry points for investors: next-gen technologies

We highlight multiple entry points for investors wishing to play the Cybersecurity theme and anticipate fast growth for the likes of: analytics, APTs, automated incident response, biometrics, cloud security, cognitive security, consulting, critical infrastructure & homeland security, e-commerce & payments, endpoint security for IoT, encryption, mobile security, next-gen firewalls, network security, PAM, and threat intelligence, among other areas.

BofAML Stocks with Cybersecurity Exposure & Primer Picks

We present a list of c50 global stocks covered by BofAML that have exposure to cybersecurity-related solutions. Our Buy-rated stocks with material exposure to the theme are detailed in an accompanying Primer Picks document, as is our full stock list.

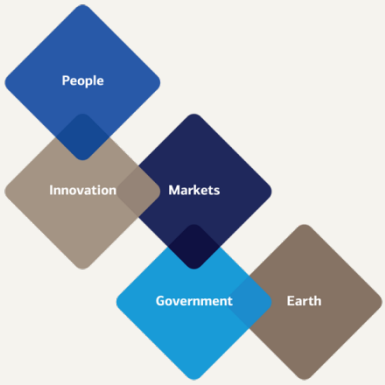
Global
Thematic Investing

Sarbjit Nahal >>
Equity Strategist
MLI (UK)
+44 20 7996 8031
sarbjit.nahal@baml.com

Beijia Ma, CFA >>
Equity Strategist
MLI (UK)
+44 20 7996 9070
beijia.ma@baml.com

Felix Tran >>
Equity Strategist
MLI (UK)
+44 20 7996 7010
felix.tran@baml.com

A Transforming World



>> Employed by a non-US affiliate of MLPF&S and is not registered/qualified as a research analyst under the FINRA rules.

Refer to "Other Important Disclosures" for information on certain BofA Merrill Lynch entities that take responsibility for this report in particular jurisdictions.

BofA Merrill Lynch does and seeks to do business with companies covered in its research reports. As a result, investors should be aware that the firm may have a conflict of interest that could affect the objectivity of this report. Investors should consider this report as only a single factor in making their investment decision.

Refer to important disclosures on page 194 to 195.

11549547

Unauthorized redistribution of this report is prohibited. This report is intended for kegan.lovely@baml.com.

Contents

Cybersecurity - Introduction	3
BofAML Global Cybersecurity stock list	4
Cyber 101: insecurity is the new normal	6
Threatscape: the "bad guy" is already on the inside	46
Costs: US$575bn today; US$3tn at risk	82
Homeland security & cyber war: governments & infrastructure under attack	89
Cybersecurity opportunities: US$75bn market today to US$170bn by 2020E	107
Solutions: next-gen technologies & the road to resilience	122
Good governance: boardroom engagement, insurance & global governance	157
Regulations: early days but still a long way to go	170
Skills & talent crisis: closing the gap	179
Appendix – Cybersecurity Glossary	186

Cybersecurity - Introduction

Please see: You've Been Hacked! - Cybersecurity Primer Picks for a list of our Primer Picks and the full list of BofAML cybersecurity stocks.

Cybersecurity is one of the top global risks today. There have been 80-90mn+ cybersecurity events per year, or up to 250k attacks per day in recent years - with 70% of attacks thought to be going undetected. 100% of major companies are being hit with finance & insurance the most targeted industry, followed by ICT, manufacturing and retail. Cybersecurity has become a homeland security threat, and Americans worry about falling victim to cybercrime more than any other type of crime – with 1bn data records compromised in 2014.

The average cost of cybercrimes for US companies reached a record US$12.7mn in 2014, with cybercrime costing the global economy up to US$575bn annually. Cyberattacks are the #1 source of economic attacks against governments and the #1 source of IP theft for corporates. US$3tn of global economic value could be at risk if companies and governments are unable to successfully combat cyber threats.

Multiple major entry points for investors

The global cybersecurity solutions market continues to grow and is estimated at US$75-77bn in 2015 – and is expected to grow to US$170bn by 2020E. We highlight multiple entry points for investors wishing to play the Cybersecurity theme and anticipate fast growth for the likes of: analytics, APTs, automated incident response, biometrics, cloud security, cognitive security, consulting, critical infrastructure & homeland security, eCommerce & payments, endpoint security for IoT, encryption, mobile security, nextgen firewalls, network security, PAM, and threat intelligence, among other areas.

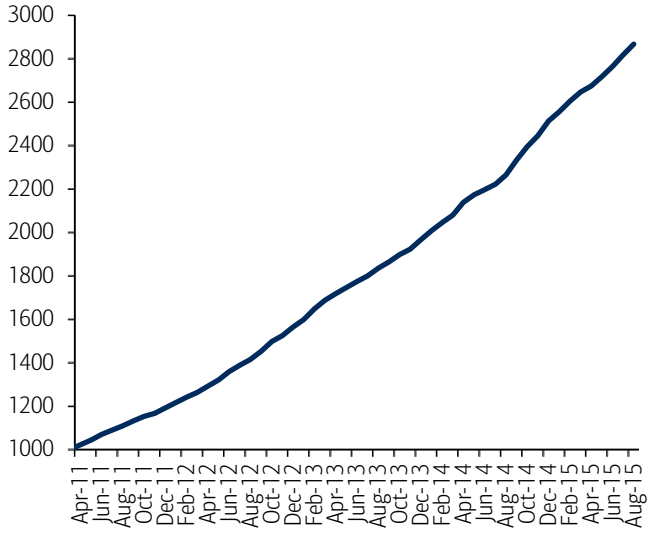
BofAML Stocks with Cybersecurity Expsoure & Primer Picks

We present a list of c50 global stocks covered by BofAML that have exposure to cybersecurity-related solutions. Our Buy-rated stocks with material exposure to the theme are detailed in an accompanying Primer Picks document, as is our full list of stocks with exposure.

Chart 1: ISE Cyber Security Index vs S&P500 Index relative performance

Source: Bloomberg
Rebased to 100 as on 31-Dec-2010

Chart 2: Index of Cybersecurity



Source: Cybersecurity Index. * A sentiment-based measure of perceived risk vis-a-vis cyber threats to the corporate, industrial and governmental information infrastructure ** (base = 1000, March 2011)

BofAML Global Cybersecurity Stocks

The BofAML Global Cybersecurity screen is not a recommended list either individually or as a group of stocks. Investors should consider the fundamentals of the companies and their own individual circumstances / objectives before making any investment decisions.

We have mapped cybersecurity opportunities across multiple entry points for investors wishing to access the Cybersecurity theme: including analytics, APTs, automated incident response, biometrics, cloud security, cognitive security, consulting, critical infrastructure & homeland security, eCommerce & payments, endpoint security for IoT, encryption, mobile security, nextgen firewalls, network security, PAM, and threat intelligence, among other areas

We outline these areas in much greater detail throughout the report. For each company, we have estimated the level and materiality of companies' exposure to cybersecurity-related themes – and the role of cybersecurity as a long-term growth driver. For each company, we have characterised their cybersecurity exposure as follows:

- **Low** – Cybersecurity-related products, technologies, services, and solutions are not material to global revenues and/or growth but are one factor, among others, for the business model, strategy & R&D of the company.
- **Medium** – Cybersecurity-related products, technologies, services, and solutions are an important factor for the business model, strategy and R&D of the company; material to sales and/or growth.
- **High** – Cybersecurity-related technologies, services, and solutions are core to the business model, strategy and R&D of the company; material sales and/or growth driver; pure play (i.e., 100% of sales).

Although it is difficult to accurately gauge the link between such exposure and share price performance (as many factors outside the scope of this analysis are likely to play a role in short- and long-term price development), we still consider cybersecurity exposure as an important and positive point to track given that cybersecurity is a global "Transforming World" theme with a long lifespan.

The aim of our Global Cybersecurity Exposure stock list and its eight underlying themes is to provide investors with information to identify company and sub-sector specific risks and opportunities that are inherent in the cybersecurity theme.

BofAML Global stocks with Cybersecurity exposure

We present a list of stocks that have exposure to cybersecurity-related themes and that we consider should benefit long-term from efforts to promote cybersecurity. The aim of this screen is to provide investors with information to understand company and sub-sector specific risks and opportunities inherent in the cybersecurity theme.

Table 1: Stocks with exposure to the BofAML Cybersecurity theme

BBG Ticker	Company	Location	Mkt Cap US$mn	BofAML Ticker	QRQ	Cybersecurity Sub-Sector	Cybersecurity Exposure
CHKP US	Check Point	Israel	14,485	CHKP	C-1-9	Enterprise/Network	High
ATEN US	A10 Networks, Inc.	United States	338	ATEN	C-1-9	Enterprise/Network	Medium
CSCO US	Cisco Systems	United States	143,650	CSCO	B-1-7	Enterprise/Network	Medium
FFIV US	F5 Networks	United States	8,591	FFIV	C-2-9	Enterprise/Network	Medium
GIMO US	Gigamon	United States	1,160	GIMO	C-2-9	Enterprise/Network	Medium
JNPR US	Juniper Networks	United States	12,609	JNPR	C-1-7	Enterprise/Network	Medium
BBRY US	BlackBerry	Canada	4,869	BBRY	C-3-9	Enterprise/Network	Low
CTXS US	Citrix	United States	14,408	CTXS	B-1-9	Enterprise/Network	Low
IBM US	IBM	United States	170,576	IBM	B-2-7	Enterprise/Network	Low
ST SP	Singtel	Singapore	45,837	SNGNF	B-1-7	Enterprise/Network	Low
SAP US	SAP	Germany	92,532	SAP	A-1-7	Enterprise/Network	Low
SAP GR	SAP	Germany	92,532	SAPGF	A-1-7	Enterprise/Network	Low
EXPN LN	Experian	United Kingdom	17,998	EXPGF	B-1-7	Identity, Payments & Components	High
EXPGY US	Experian	United Kingdom	17,998	EXPGY	B-1-7	Identity, Payments & Components	High
GTO NA	Gemalto N.V.	Netherlands	6,390	GTOFF	C-2-7	Identity, Payments & Components	High
ING FP	Ingenico S.A.	France	7,356	INGIF	C-1-7	Identity, Payments & Components	Medium
LOCK US	LifeLock	United States	864	LOCK	C-2-9	Identity, Payments & Components	Medium
NXPI US	NXP	Netherlands	23,546	NXPI	C-1-9	Identity, Payments & Components	Medium
002456 CH	O-film	China	4,774	XSZHF	C-1-7	Identity, Payments & Components	Medium
IFX GR	Infineon	Germany	12,966	IFNNF	B-2-7	Identity, Payments & Components	Low
IFNNY US	Infineon	Germany	12,966	IFNNY	B-2-7	Identity, Payments & Components	Low
STM FP	STMicroelectronics	France	7,253	STMEF	B-2-7	Identity, Payments & Components	Low
STM US	STMicroelectronics	France	7,253	STM	B-2-7	Identity, Payments & Components	Low
SPLK US	Splunk	United States	8,456	SPLK	C-1-9	Cloud, Data & Threat Intelligence	High
VMW US	VMware Inc	United States	36,110	VMW	C-1-9	Cloud, Data & Threat Intelligence	High
EMC US	EMC Corp.	United States	50,100	EMC	B-1-7	Cloud, Data & Threat Intelligence	Low
HPQ US	Hewlett-Packard	United States	49,586	HPQ	B-1-7	Cloud, Data & Threat Intelligence	Low
9613 JP	NTT DATA	Japan	12,636	NTTDF	A-1-7	Cloud, Data & Threat Intelligence	Low
ORCL US	Oracle	United States	202,207	ORCL	B-1-7	Cloud, Data & Threat Intelligence	Low
CUDA US	Barracuda	United States	2,112	CUDA	C-1-9	Threat Protection	High
CYBR US	CYBR	Israel	1,858	CYBR	C-1-9	Threat Protection	High
FEYE US	FireEye	United States	7,282	FEYE	C-1-9	Threat Protection	High
FTNT US	Fortinet	United States	7,471	FTNT	C-1-9	Threat Protection	High
PANW US	Palo Alto Networks	United States	15,386	PANW	C-2-9	Threat Protection	High
QIHU US	Qihoo	China	7,257	QIHU	C-1-9	Threat Protection	High
SYMC US	Symantec	United States	14,771	SYMC	B-3-7	Threat Protection	High
4704 JP	Trend Micro	Japan	5,159	TMICF	C-1-7	Threat Protection	High
TMICY US	Trend Micro	Japan	5,159	TMICY	C-1-7	Threat Protection	High
INTC US	Intel	United States	141,231	INTC	A-1-7	Threat Protection	Low
MSFT US	Microsoft Corp	United States	389,422	MSFT	B-3-7	Threat Protection	Low
BAH US	Booz Allen Hamilton	United States	4,209	BAH	B-1-8	Homeland & Critical Infrastructure	Medium
LLL US	L-3 Comm	United States	10,175	LLL	B-3-7	Homeland & Critical Infrastructure	Medium
ULE LN	Ultra Electronics	United Kingdom	1,898	UEHPF	B-3-7	Homeland & Critical Infrastructure	Medium
ATO FP	Atos	France	7,850	AEXAF	C-3-7	Homeland & Critical Infrastructure	Low
BA/ LN	BAE SYSTEMS	United Kingdom	22,082	BAESF	A-1-7	Homeland & Critical Infrastructure	Low
BAESY US	BAE SYSTEMS	United Kingdom	22,082	BAESY	A-1-7	Homeland & Critical Infrastructure	Low
FNC IM	Finmeccanica	Italy	8,539	FINMF	B-2-9	Homeland & Critical Infrastructure	Low
GD US	General Dynamics	United States	49,366	GD	B-1-7	Homeland & Critical Infrastructure	Low
ITRI US	Itron	United States	1,213	ITRI	B-3-9	Homeland & Critical Infrastructure	Low
LMT US	Lockheed Martin	United States	64,055	LMT	B-1-7	Homeland & Critical Infrastructure	Low
NOC US	Northrop Grumman	United States	33,218	NOC	B-2-7	Homeland & Critical Infrastructure	Low
QQ/ LN	QinetiQ	United Kingdom	2,288	QNTQF	B-1-7	Homeland & Critical Infrastructure	Low
RTN US	Raytheon Co.	United States	31,895	RTN	A-1-7	Homeland & Critical Infrastructure	Low
SAF FP	Safran SA	France	31,697	SAFRF	B-1-7	Homeland & Critical Infrastructure	Low
SMIN LN	Smiths Group	United Kingdom	7,198	SMGKF	A-3-7	Homeland & Critical Infrastructure	Low
SMGZY US	Smiths Group	United Kingdom	7,198	SMGZY	A-3-7	Homeland & Critical Infrastructure	Low
HO FP	THALES	France	13,088	THLEF	C-1-7	Homeland & Critical Infrastructure	Low

Source: BofA Merrill Lynch Global Research

Cyber 101: insecurity is the new normal

The current escalation in cybersecurity risks is a harbinger of the new normal, in our view. There have been 80-90mn+ cybersecurity events per year between 2013-14, with close to 400 new threats every minute. Worryingly, 70% of attacks are going undetected and 100% of major companies are being hit – with finance and insurance, ICT, manufacturing and retail the most targeted sectors. Cybersecurity is also a homeland security threat, with rapid growth in attacks against critical infrastructure and manufacturing.

Cybercrime cost the average US company a record US$12.7mn in 2014 and the global economy up to US$575bn. Cyberattacks are the no.1 source both of economic attacks against governments and of IP theft for corporates. The rise in disruptive technologies – including the IoT with 50bn+ devices connected to the internet by 2020 – means that we are facing a potential 'Cybergeddon' scenario where the 'bad guy' has a persistent advantage . Cybercrime extracts up to 20% of the value created by the internet, meaning that up to US$3tn of global economic value could be at risk by 2020E.

The global cybersecurity solutions market continues to grow and is estimated at US$75-77bn in 2015 and expected to reach US$170bn by 2020E. Drivers include a rise in the number, sophistication, scope and impact of attacks; the IoT creating new security threats; increased spending on cybersecurity by corporates and governments; and the emergence of regulation. We anticipate fast growth for the likes of: analytics, APTs, automated incident response, biometrics, cloud security, cognitive security, consulting, critical infrastructure & homeland security, e-commerce & payments, endpoint security for IoT, encryption, mobile security, next-gen firewalls, network security, PAM, and threat intelligence, among other areas.

> "There are two types of companies: those who have been hacked, and those who don't yet know they've been hacked." – John Chambers, CEO of Cisco

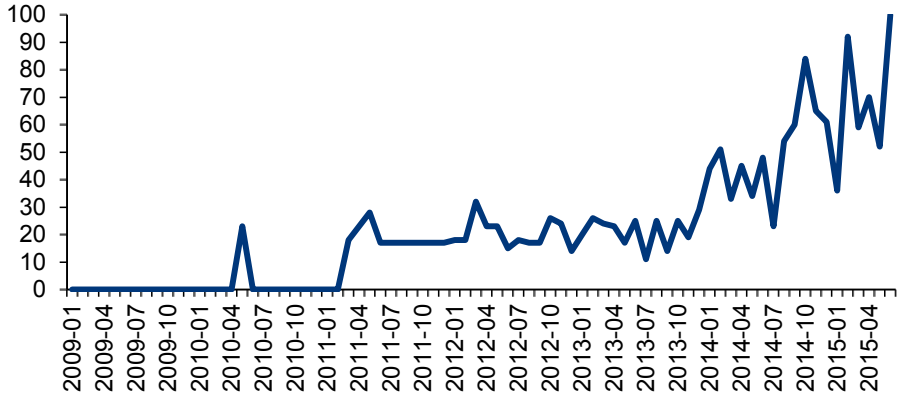
Cybersecurity: a definition

Cybersecurity is commonly defined as security applied to computers, computer networks, and the information and data stored and transmitted over them.

- **It covers all the processes and mechanisms by which digital equipment, information and services are protected** from unintended or unauthorised access, change or destruction and the process of applying security measures to ensure confidentiality, integrity, and availability of data both in transit and at rest.

- **The field is of growing importance due to the increasing reliance on ICT systems in most societies**. ICT systems now include a very wide variety of 'smart' devices, eg, smartphones, televisions and tiny devices as part of the Internet of Things (IoT), and networks include not only the internet and private data networks, but also Bluetooth, Wi-Fi and other wireless networks.

Chart 3: "Cyber breach" as a search term has skyrocketed on Google Trends



Source: Google, BofA Merrill Lynch Global Research

Cyber threatscape is changing fast

The rapid expansion of cyberspace is having a major impact on cybersecurity risk, with threats becoming increasingly interconnected with other global risks. Cyber threat actors are exploiting ICT networks for an ever-widening array of economic and political objectives, which are increasingly targeted and sophisticated in nature.

Table 2: Cyber threatscape

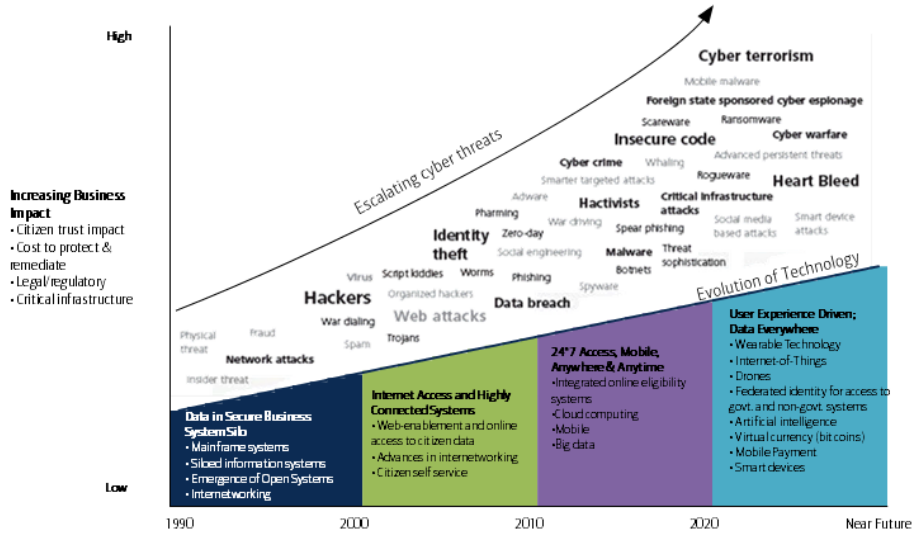
	NUISANCE	DATA THEFT	CYBER CRIME	HACKTIVISM	DESTRUCTIVE ATTACK
Objective	Access & Propagation	Economic, Political Advantage	Financial Ga in	Defamation, Press & Policy	Disrupt Operations
Example	Botnets & Spam	Advanced Persistent Threat Groups	Credit Card Theft	Website Defacements	Delete Data
Targeted	✗	✓	✓	✓	✓
Character	Often Automated	Persistent	Frequently Opportunistic	Conspicuous	Conflict Driven

Source: Mandiant

The 'bad guy' always has the advantage

Cyberattacks take place in an ICT environment that favours attackers. ICT infrastructure was designed for openness and interoperability rather than cybersecurity, meaning that offensive actions have an advantage over defensive actions. There are also lower barriers to criminal entry than in the physical world and a weak government monopoly on the use of force. This allows the 'bad guy' – whether with limited or abundant resources – to carry out disruptive actions with considerable, and often unpredictable, outcomes (source: ESADEgeo-Zurich Insurance).

Exhibit 1: Evolving technology and rapidly escalating cyber threats

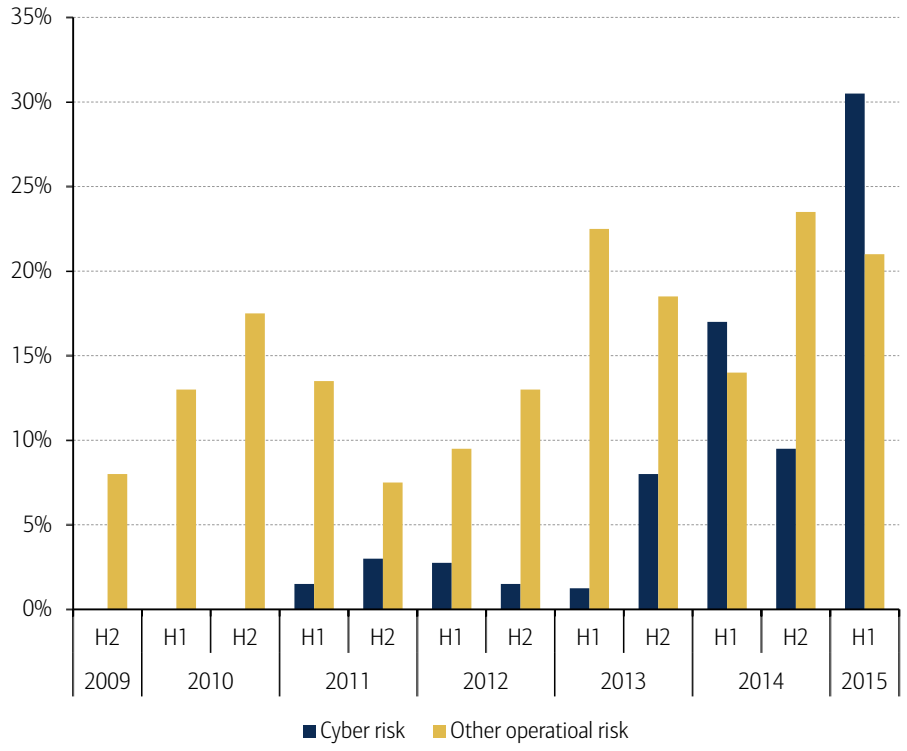


Source: Deloitte

One of the most likely high-impact global risks

Cyber threats have emerged as one of the top 10 global risks today, and among the most likely high-impact risks (source: WEF). The perceived risk of cyberattacks on financial systems has also reached record levels in the Bank of England's Systemic Risk Survey (+20 percentage points to 30% in H1 2015).

Chart 4: Concern about cyber risk continues to grow



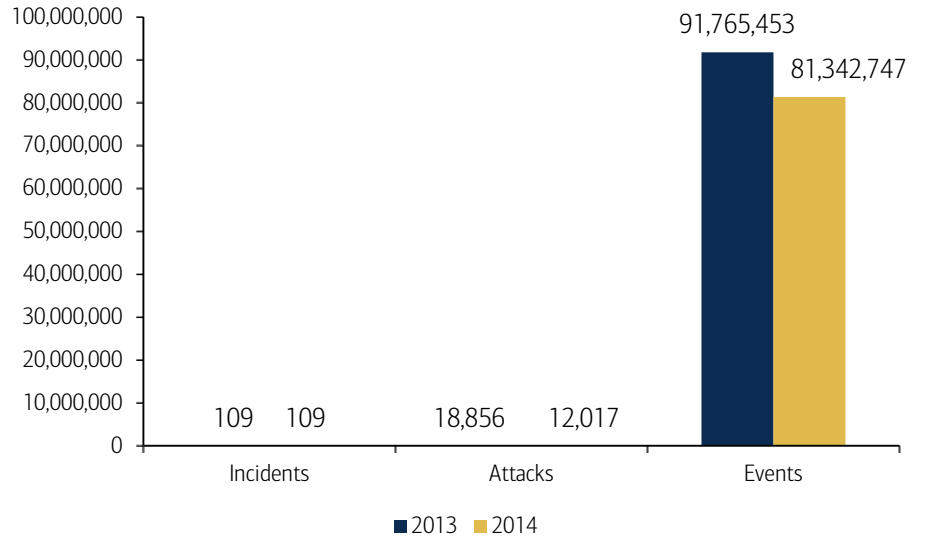
Source: Bank of England

Bank of America Merrill Lynch

80-90mn+ attacks per year

It is difficult to estimate the exact number of cybersecurity incidents given the deficiencies in detection and reporting, and the proliferation in ICT (devices, infrastructure, data, IoT). However, it is clear that cyberattacks are becoming one of the largest risks for corporates today. According to IBM Security Services, the organisations it monitored experienced 81-91mn cybersecurity incidents per year in 2013 and 2014. That is the equivalent of 222,856-251,415 incoming attacks per day, every day.

Chart 5: Average annual cybersecurity events, attacks and incidents



Source: IBM

100+ "real cause" incidents per year for companies

In 2014 and 2015, there has been a significant increase in high-profile, major attacks against corporates including Albertsons, Anthem, Ashley Madison, Dairy Queen, Home Depot, JPMorgan, Sony, and Target. IBM estimates that the average company experienced 109 security incidents in 2014 – i.e, attacks large enough to be considered a real cause for concern. The number of malicious attacks aiming to collect, disrupt, deny, degrade or destroy information system resources or the information itself was estimated to be around 12,000 in 2014 (source: IBM).

Exhibit 2: The cyber risk universe

Source: Ernst & Young, BofA Merrill Lynch Global Research

+66% CAGR in detected attacks 2009-14

PWC's Global State of Information Security Survey 2015 showed a 66% CAGR in detected incidents from 2009-14. The actual number of incidents is bound to be significantly higher given that industry data refers only to those detected and reported.

> Global news report references to cybercrime have increased by 600% in the last decade vs. 80% for homicides (source: UNODC, Dow Jones Factiva)

Advanced attacks going undetected for a median of 205 days

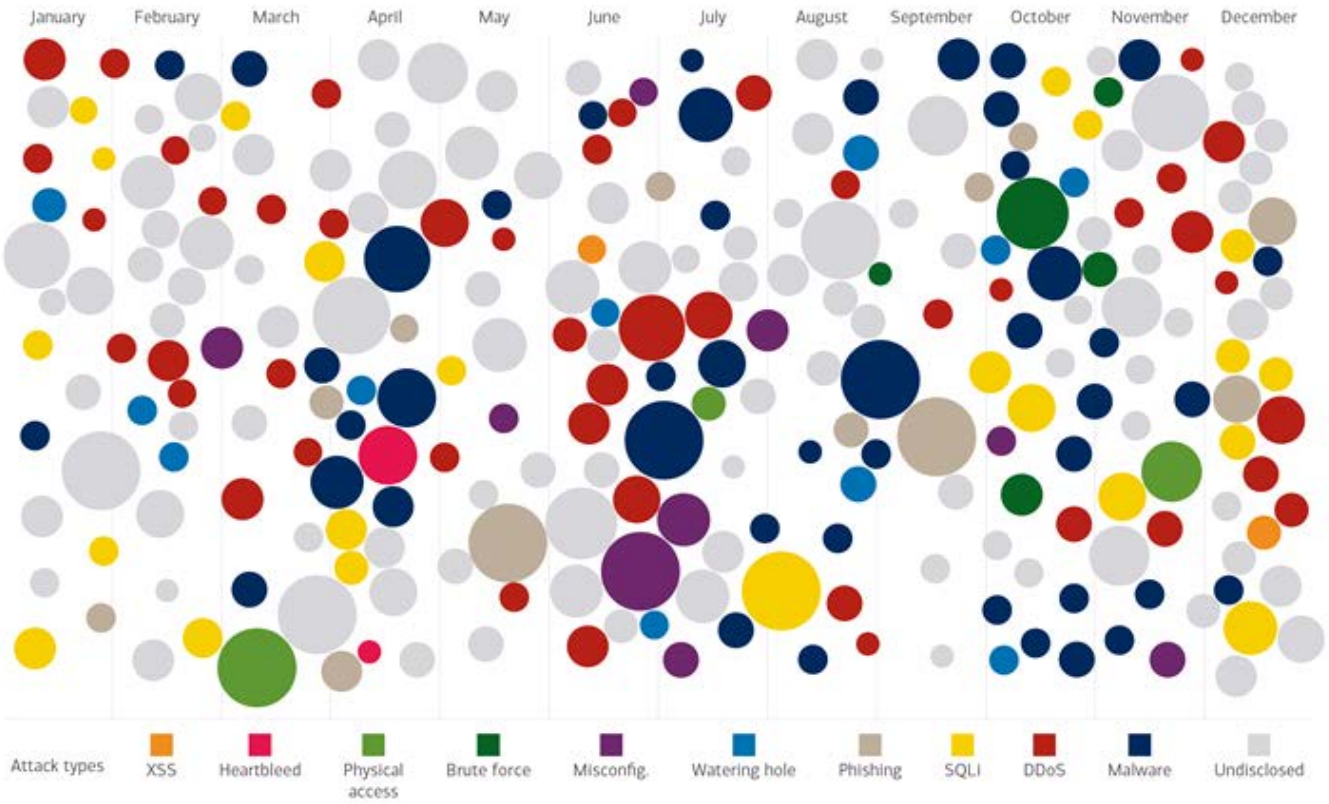
Advanced cyberattacks on organisations are going undetected for a median of 205 days in 2014 – i.e. the average number of days attackers were present on a victim's network before being discovered (source: Mandiant). While this was 24 less days than 2013, the longest presence was 2,982 days.

> As many as 71% of compromises of cybersecurity go undetected (source: Trustwave)

Only 31% of companies are discovering breaches internally

A worryingly small number of organisations – only 31% – are discovering these intrusions on their own, while 69% learned of the breach from an outside entity such as law enforcement, up from 67% in 2013 and 63% in 2012 (source: Mandiant).

Exhibit 3: Sampling of cybersecurity incidents by attack type, time and impact in 2014



Source: IBM X-Force. The size of circle estimates the relative impact of incident in terms of cost to business (based on publicly disclosed information regarding leaked records and financial losses).

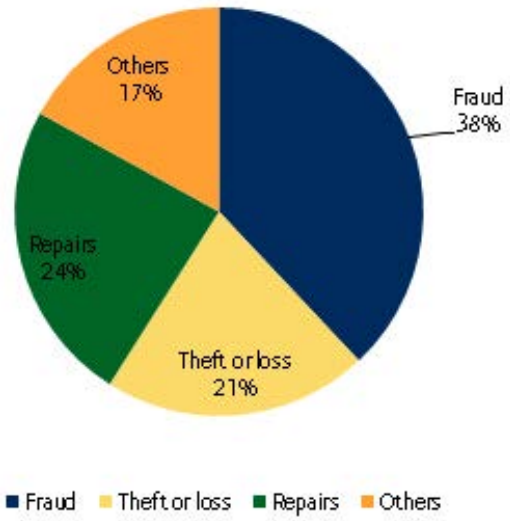
Hitting home: consumers #1 fear is being hacking

One telling indication of the growing importance of the cybersecurity theme is how it is resonating with the average consumer in light of major attacks against companies that resonate in their everyday lives such as Home Depot, JPMorgan, Neiman Marcus, Sony, Target, or in some cases Ashley Madison.

Fundamental change in consumer behaviour

Consumer behaviour continues to undergo a fundamental change including: accessing information, products and services on-line, using connected devices in every aspect of their lives, and a move away from cash to mobile and electronic payments. Unfortunately, this rapid transformation has resulted in consumer complacency towards potential cyber threats, in our view. Nearly 50% of mobile device owners don't use basic precautions such as passwords or security software. As a result 38% experience mobile cybercrime every year (source: Norton).

Exhibit 4: Consumer cybercrime by segment



Source: Norton

69% worry about being hacked vs. 18% about getting murdered

According to a 2014 Gallup poll, the #1 crime that Americans fear is having their credit card information stolen by hackers. 69% of U.S. residents worry "frequently" or "occasionally" about computer hackers stealing their credit card information from stores. The #2 most-feared crime in the U.S; is having a phone or computer hacked to steal personal information (at 62%).

Table 3: Top crimes that have Americans "occasionally" or "frequently" worried (%)

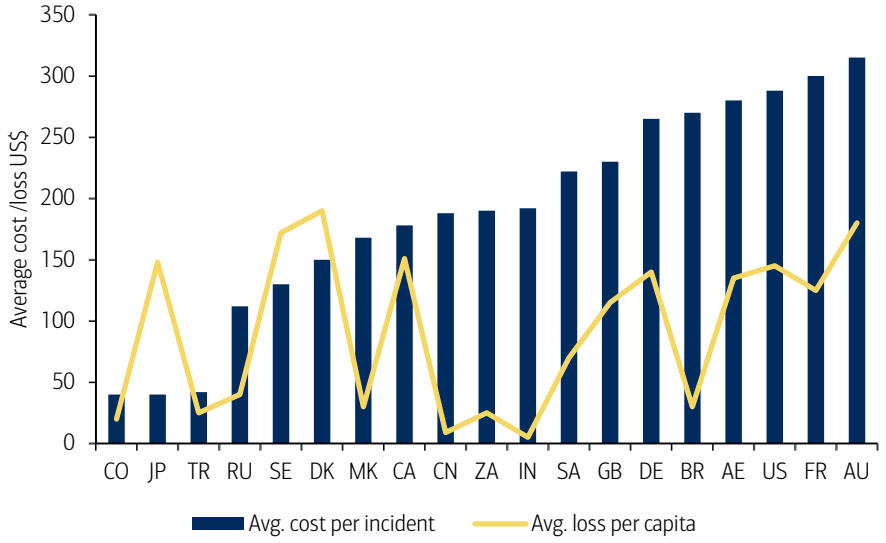
Having the credit card information you have used at stores stolen by computer hackers	69
Having your computer or smartphone hacked and the information stolen by unauthorized persons	62
Your home being burglarized when you are not there	45
Having your car stolen or broken into	42
Having a school-aged child physically harmed attending school	31
Getting mugged	31
Your home being burglarized when you are there	30
Being the victim of terrorism	28
Being attacked while driving your car	20
Being a victim of a hate crime	18
Being sexually assaulted	18
Getting murdered	18
Being assaulted/killed by a co-worker/employee where you work	7

Source: Gallup

Paying the price: US113bn/year+ hit for consumers

Globally, consumer cybercrime accounts for US$113bn every year or an average of nearly US$300 per victim (source: Norton). Fraud is the #1 cause of consumer cybercrime (38%) followed by repairs (24%) and theft/loss (21%). By region, consumers in the US ($38bn) and China ($37bn) are the leading targets of cybercrime.

Chart 6: Estimated costs of consumer cybercrime by country



Source: Norton, UNODC, Anderson et al

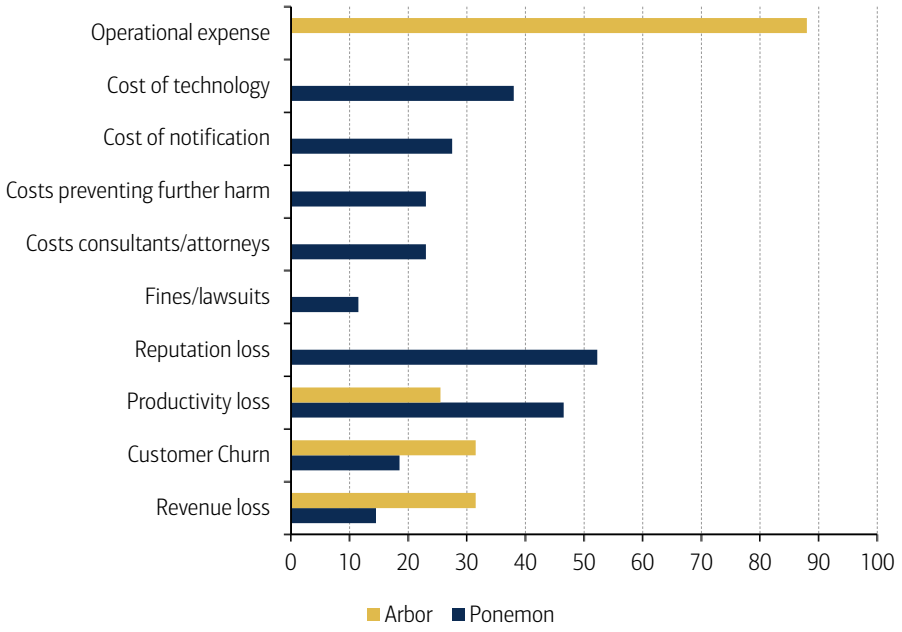
Identity theft, $25bn loss every year in US

Identity theft has been the #1 reported complaint in the US during the past 15 years (source: Federal Trade Commission). Every year 26 million Americans are victims of identity theft where every 2 seconds someone is a victim of this crime (source: Forrester, LifeLock). Overall the total cost of identity theft in the US amounts to $25bn every year (source: Bureau of Justice). Despite 78mn Americans being concerned about security only c30mn are doing something about this, according to a survey conducted by LifeLock.

Data breaches: nothing is secure

Data breaches have perhaps drawn the greatest amount of attention in recent times due to the widespread impact it has had vis-à-vis on companies. 2014 in particular was dubbed the year of the "data breach" or "mega breach" as hundreds of millions of records were compromised and companies' secure databases came under growing risk of being hacked. Although the monetary damage to these corporates are currently small in relation to their group revenues, it is the reputational damage suffered specifically for large(r) companies that is most impactful. We continue breaches to grow in scale and scope driven by factors such as big data, insiders, weak passwords and cybercrime among others.

Chart 7: Potential range of negative impacts on companies

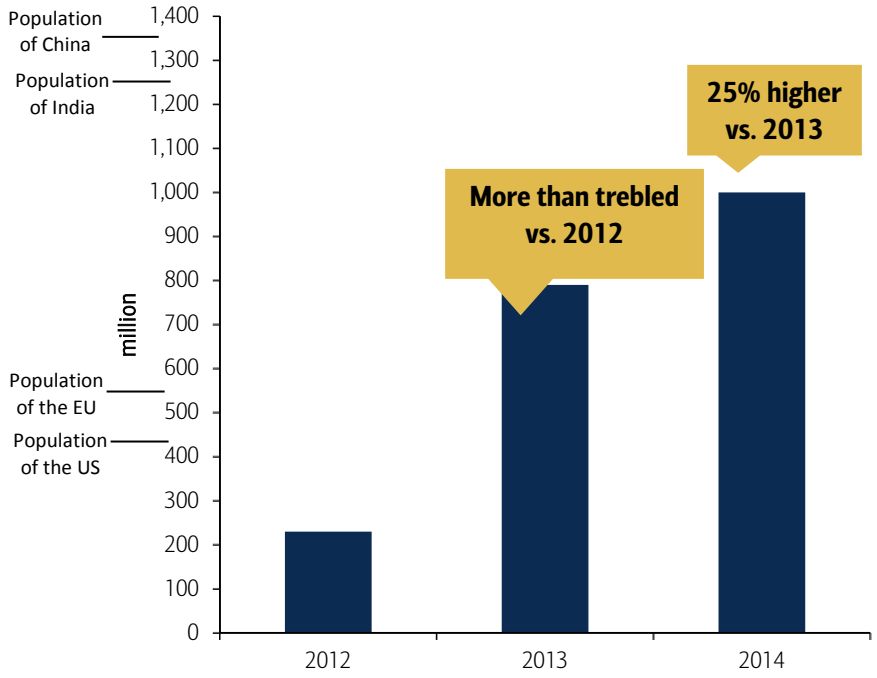


Source: HCSS based on Ponemon, Arbor

It's about the data: c.1bn records leaked in 2014

The rise of 'big data' means that data breaches – the intentional or unintentional release of secure information to untrusted environments – is exploding as data becomes a boon for criminals, hacktivists, and increasingly nation states. It is estimated that there were more than c.1bn leaked emails, credit card numbers, passwords and other types of personally identifiable information (PII) in 2014 – a 25% increase on 2013 (source: IBM).

Chart 8: Total records leaked by year

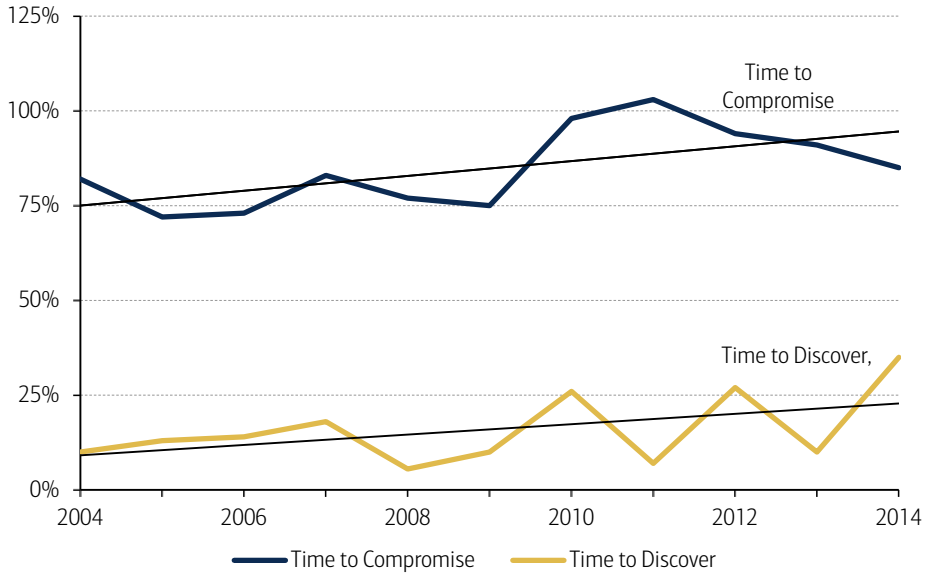


Source: IBM

Bad guys always ahead in breaches

In 60% of cases, cyber attackers were able to compromise an organization within minutes often remaining undetected for days (source: Verizon). During the past decade, the time between records being compromised initially has diverged from the time of discovery peaking in 2011 where there the so-called "defender-detection" gap was the greatest. Although this difference was closed in 2014, the general trend of the bad guys' breaches remaining undetected still holds true, and will continue to persist with advances in the threatscape, in our view.

Chart 9: "Defender-Detection" Gap

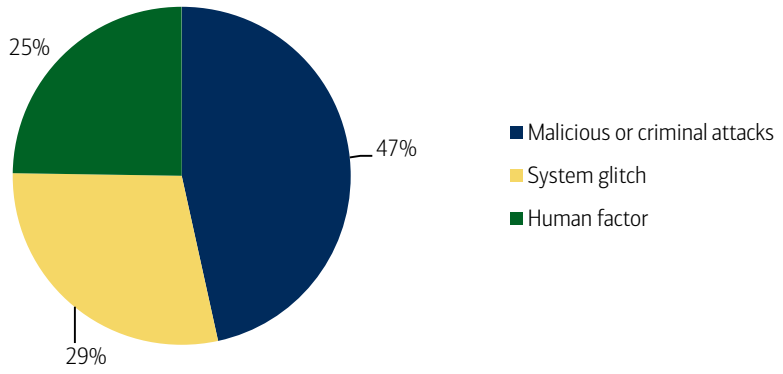


Source: Verizon

Malicious or criminal attacks are #1 cause of data breach

Malicious attacks are caused by hackers or criminal insiders (employees, contractors or other third parties). The most common types of malicious or criminal attacks include malware infections, criminal insiders, phishing/social engineering and SQL injection. Globally in 2015 47% of data breach incidents involved a malicious or criminal attack, 25% concerned a negligent employee or contractor (human factor), and 29% involved system glitches that include both IT and business process failures (Source: Ponemon Institute).

Chart 10: Root causes for data breaches globally



Source: Ponemon Institute, BofA Merrill Lynch Global Research

More worryingly, only a small number of organisations – only 31% - are discovering these intrusions on their own. 69% learned of the breach from an outside entity such as law enforcement - up from 67% in 2013 and 63% in 2012 (source: Mandiant).

Table 4: Frequency of data breaches by incident patterns and threat actor

	Crimeware	Cyber-espionage	Denial of service	Lost & Stolen Assets	Miscellaneous Errors	Payment cars skimmers	Point of sale	Privilege misuse	Web Applications
Activist	3%	5%	31%						61%
Organised crime	73%						6%		20%
State affiliated		97%							3%
Unaffiliated	41%	3%	5%	18%	2%	6%	1%	3%	22%

Source: Verizon

81% of organizations experience some data loss

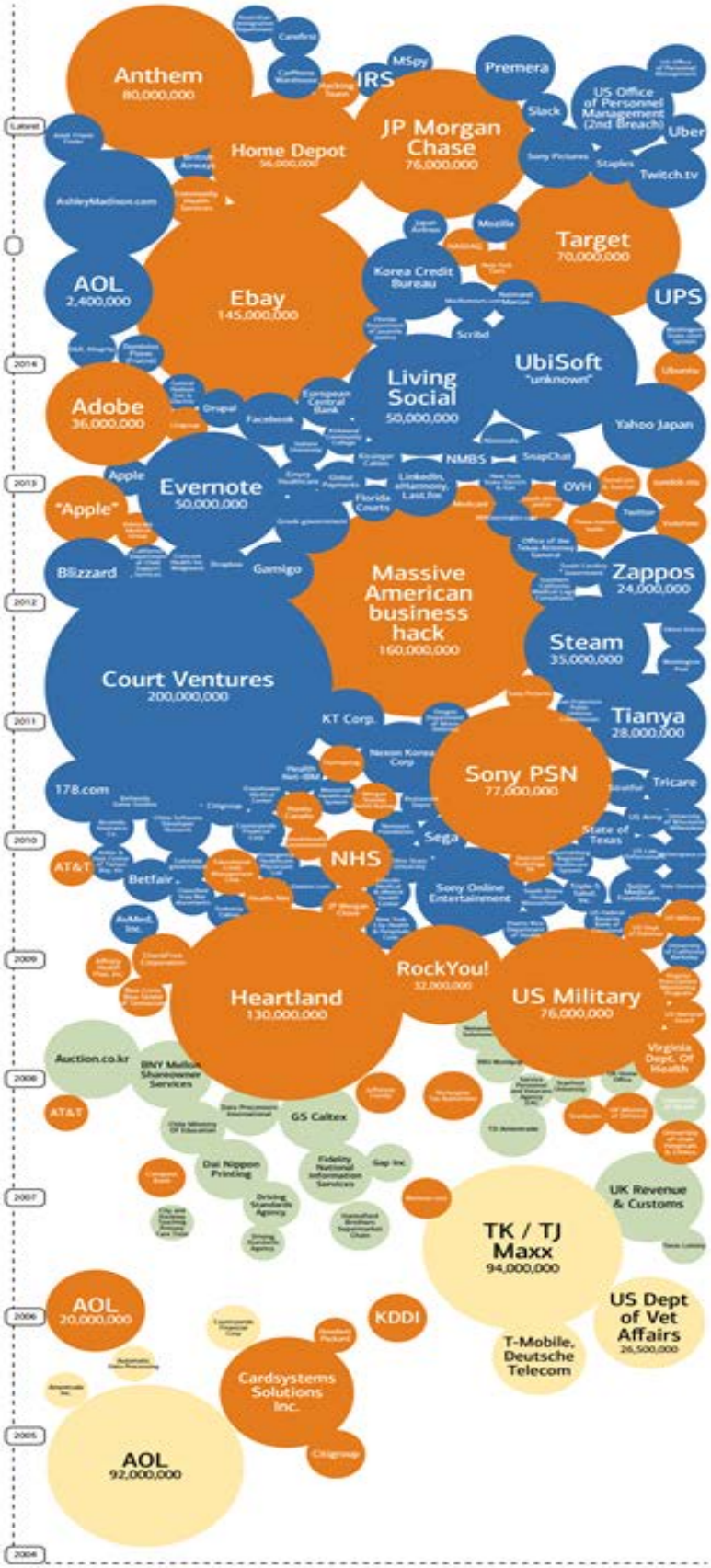
Data breaches often also have some form of internal vulnerability which attackers capitalise on. According to Check Point's study, the loss of proprietary information has increased 71% over the past 3 years, with organisations suffering data loss at a rate of 1.7 times per hour or 41 times per day in 2014. The most worrying fact from the study was that every 36 minutes sensitive data is sent outside an organization by employees either deliberately or negligently.

In a "candy drop" security test: USB drives and disks were dropped in parking lots:

- 60% of these were inserted into company or agency computers
- 90% were inserted if the USB drive or disk had an official logo

(source: US DHS)

Exhibit 5: Biggest data breaches timeline

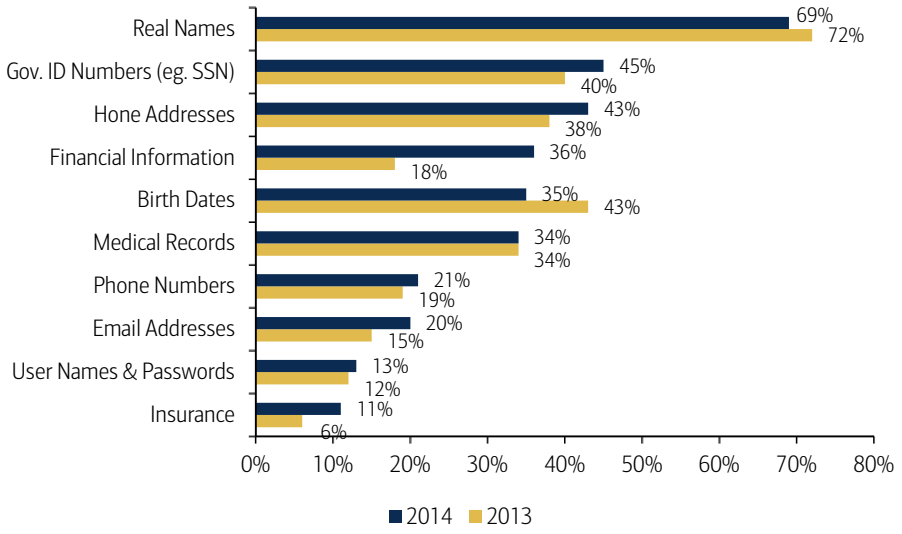


Source: InformationIsBeautiful.net

Identities are the #1 data stolen

Furthermore, nearly 70% of data breaches contained information pertaining to real names or identities in 2014 (source: Symantec). However the biggest category increase vis-à-vis information being exposed was financial information, which doubled from 18% in 2013, to 36% in 2014. This highlights that attackers are increasingly targeting information that can be leveraged for monetary gain, in our view.

Chart 11: Top 10 types of Information Exposed

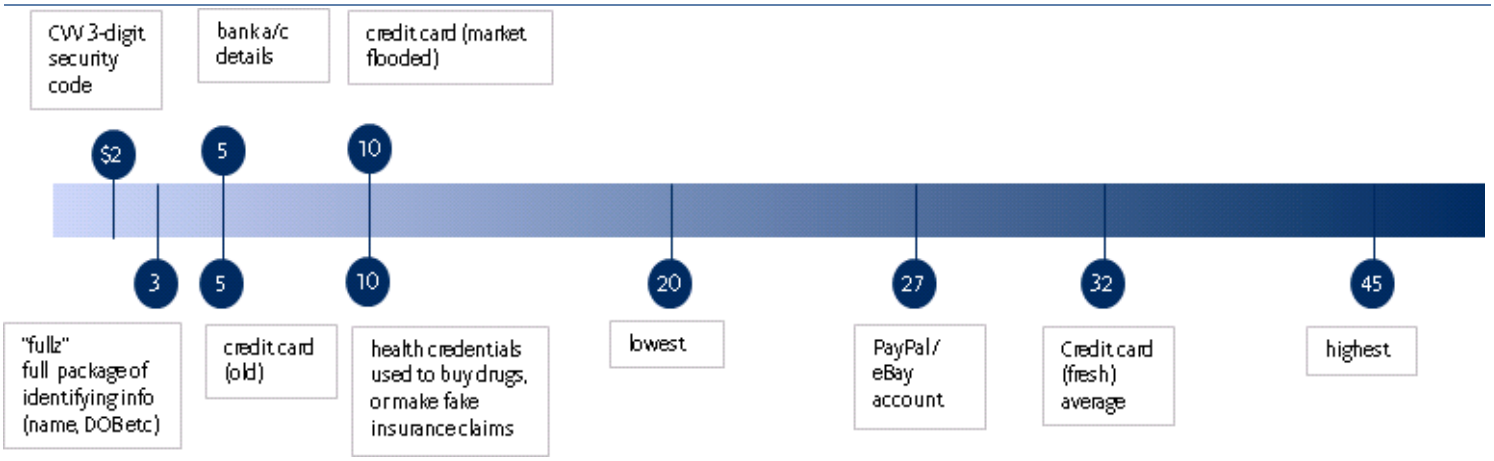


Source: Symantec

Criminal motivations: stolen data = $$$

Hence it shouldn't be surprising that a black market has developed for stolen identity details, especially for those in the financials and healthcare domain. The recent hacks at JPMorgan and Anthem are a harbinger for how cybercriminals will increasingly mine personal information from these sectors, in our view.

Exhibit 6: Value of stolen details



Source: InformationIsBeautful.net, BigDataBreaches, Holt & Smirnova (2014)

On the black market health credentials that could be used to buy drugs or make fake insurance claims could be bought for as little as $10 (source: informationisbeautiful). In addition credit card details used to make fraudulent purchases could fetch for up to $20 in 2014, according to Symantec. Perhaps the most interesting aspect of the underground cyber economy was that social network followers could be bought as well for $2-$12. In our view, this highlights that although identity theft remains at the core of cybercriminals' business model, novel ways to make money from cyber hacking are emerging.

Table 5: Timeline overview of recent major cyber data breaches at companies

Date	Company name	Incident	Overview
2015	Ashley Madison	37mn users' data were dumped online following cyber breach	The "Impact Team" claimed to have orchestrated the attack. Some were also reported to have been victims of ransomware via Bitcoin, as a company that offers infidelity services clandestinely this makes the hack all the more worrying for those affected.
2015	Dixons Carphone	2.4mn customer's personal details stolen from sophisticated attack	Carphone Warehouse division hit by a cyberattack, up to 90,000 encrypted credit card records may been accessed. The attack is thought to have been sophisticated and coordinated in nature
2015	Anthem	Theft of 80mn customers' social security numbers	First time personally identifiable information has been stolen e.g. medical IDs, birthdays , information was taken from a database that was not encrypted, estimated cost of US$100mn+
2014	Sony Pictures	Emails leaked, North Korean hacker threats led to cancellation of "The Interview" film premiere	Personal information of employees was stolen, communications between executives were posted online, details of unreleased films exposed, FBI investigation allege North Korea as source
2014	Apple	Photos from iCloud accounts of celebrities were hacked and leaked	Over 100 individual celebrities affected, with more than 500 personal photos stolen and circulated on the internet via a concerted effort targeting vulnerable passwords
2014	Home Depot	Server breach affecting 56mn debit cards in the US & Canada.	US$62mn paid out to recover from the hack, with insurance only covering US$27mn of the total cost
2014	JPMorgan	76mn household and 7mn small businesses compromised	Account holders' names, addresses, phone numbers and email addresses of the holders were hacked.
2014	eBay	128mn active users' accounts believed to have been compromised	Company advised all users to change passwords, Syrian Electronic Army (SEA) took responsibility for attack
2013	Target	Credit card data from 40mn accounts was stolen, 70mn accounts compromised	Customer names, credit or debit card numbers, expiration dates and CVVs were involved in the information theft. US$148mn in estimated damages.
2013	Adobe	38mn accounts breached.	The hackers stole parts of the source code to Photoshop along with usernames and passwords.
2013	Evernote	Usernames, email addresses, and passwords of users were accessed.	The popular note-taking software service had to reset the passwords of all of its 50mn users. Although the company did not find any indication that content or payment information was stolen.
2013	LivingSocial	Personal data of 50mn users stolen.	The company's computer systems were hacked, resulting in unauthorized access to personal data. The company updated its password encryption method after the breach.

Source: CSIS, company reports, press sources, BofA Merrill Lynch Global Research

Threat actors: insiders pose the no.1 threat

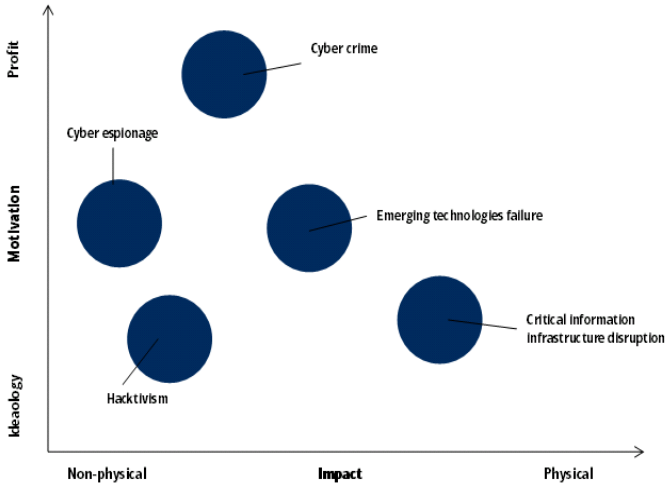
Cyber threats can come from numerous sources – hostile governments, terrorist groups, disgruntled employees, and malicious intruders and insiders, among others. Insiders actually account for the #1 threat. In 2014, 55% of attacks were carried out by 'insiders' – actors with internal access (physical or remote) to an organisation's systems (source: IBM).

> In over 95% of incidents, human error is a contributing factor – from poor password protection to using an unsecured internet connection (source: IBM)

Many different motivations

There are many different categories of cybersecurity threat, with varying motivations and impacts. While traditional cybercrime is driven mainly by criminals looking for profit, rising geopolitical tensions are leading to a rise in ideologically motivated attacks (source: ESADEgeo-Zurich Insurance).

Exhibit 7: Cyber risk landscape by motivation and impact



Source: ESADEgeo

Insiders account for 45% of attacks

In 2014, malicious insiders accounted for 31.5% and inadvertent actors 23.5% of insider attacks (source: IBM). Employees are not the only source of insider threats, however. The percentage of incidents attributed to current and former service providers, consultants, and contractors increased to 18% and 15%, respectively, in 2014 (source: PwC).

Table 6: Profiles of threat actors

Adversary	Motives	Targets	Impact
Nation State	Economic, political, and/or military advantage	Trade secrets Sensitive business information Emerging technologies Critical infrastructure	Loss of competitive advantage Disruption to critical infrastructure
Organized Crime	Immediate financial gain Collect information for future financial gains	Financial / Payment Systems Personally Identifiable Information Payment Card Information Protected Health Information	Costly regulatory inquiries and penalties Consumer and shareholder lawsuits Loss of consumer confidence
Hacktivists	Influence political and /or social change Pressure business to change their practices	Corporate secrets Sensitive business information Information related to key executives, employees, customers & business partners	Disruption of business activities Brand and reputation Loss of consumer confidence
Insiders	Personal advantage, monetary gain Professional revenge Patriotism	Sales, deals, market strategies Corporate secrets, IP, R&D Business operations Personnel information	Trade secret disclosure Operational disruption Brand and reputation National security impact

Source: PWC

Profiles of threat actors

- **Insiders pose the #1 threat** – As established, insiders pose the greatest cybersecurity risk encompassing: malicious insiders who deliberately steal information and data or cause damage (least frequent but highest impact – e.g. administrators with privileged identities); exploited insiders who are unwittingly taken advantage of by outsiders (i.e. to provide data or passwords); and careless insiders who make unintended mistakes.

- **State-affiliated actors threatening critical infrastructure & national security** – National cyber programmes cover the entire spectrum of threats to national interests (ie, propaganda, espionage, IP, technology, infrastructure disruption, loss of life). These actors commit the most targeted attacks as they know what they want (ie, to weaken, disrupt or destroy), have government commitment and resources, and are relentless in their efforts to obtain it.

These attacks, particularly from nations with highly sophisticated cyber programmes or disruptive intentions, pose the greatest threat to critical infrastructure and national security.

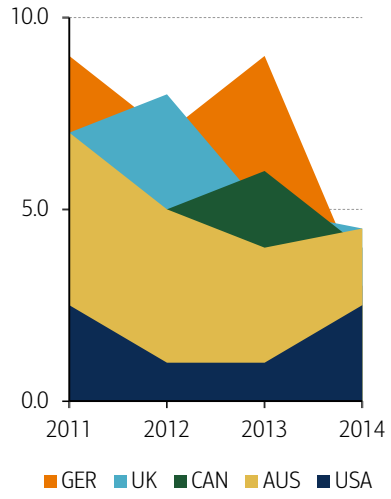
Cybersecurity is becoming a homeland security risk as nation-states are increasingly becoming actors in cyber warfare.

- **Organised crime becoming more sophisticated** – Cybercriminals are primarily motivated by profit (eg, monetary theft, industrial espionage, blackmail etc.) and cybersecurity including online fraud offers excellent ROI vs other types of crime. Criminals are well resourced, able to hire skilled people (cybercrime as a service), and are becoming more sophisticated (eg, using blended attacks: technical and social engineering, purchasing components to commit crime through online marketplaces).

In 2014, the FBI's Internet Crime Compliant Center (IC3) received 269,422 complaints with an adjusted dollar loss of US$800mn. The growth in fintech, mobile payments, and virtual currencies is also opening up new avenues of attack. And in recent years, the "cybercrime-as-a-service" (CaaS) market has grown with internet users now able to hire hackers for cUS$500 to perform cyberattacks on a specified target. The "Hacking Team" are perhaps the most well-known group within this space as they sell software that ranges from intruding a system to infecting a target's computer (source: Kaspersky). In our view, this reflects how cybercrime has evolved from just stealing credentials to sell for profit to becoming an active market of services.

The hacking software tools for sale market is an $11bn per year industry with a CAGR of 56% - Intel

Chart 12: Credit Card Prices in the Russian Cybercriminal Underground by Year (US$)



Source: Trend Micro

Table 7: Credit Card Prices in the Russian Cybercriminal Underground by Year (US$)

	2011	2012	2013	2014
USA	2.5	1.0	1.0	2.5
AUS	7.0	5.0	4.0	4.5
CAN	5.0	5.0	6.0	4.0
GER	9.0	7.0	9.0	3.0
UK	7.0	8.0	5.0	4.5

Source: Trend Micro

Table 8: Value of Information Sold on Black Market

Item	2014 Cost	Uses
1,000 Stolen Email Addresses	$0.50 to $10	Spam, phishing
Credit Card Details	$0.50 to $20	Fraudulent buys
Scans of Real Passports	$1 to $2	ID theft
Stolen Gaming Accounts	$10 to $15	Attaining valuable Virtual items
Custom Malware	$12 to $3500	Payment diversions, Bitcoin Stealing
1,000 Social Network Followers	$2 to $12	Generating viewer Interest
Stolen Cloud Accounts	$7 to $8	Hosting a C&C server
1mn verified email spam mail-outs	$70 to $150	Spam, phishing
Registered & activated Russian mobile SIMs	$100	Fraud

Source: Symantec

Nation-state actors and organised crime are increasingly converging their capabilities making the identification of threat actors increasingly difficult.

- **Hackers have a wide array of motivations -** Hackers look to exploit weaknesses in ICT systems and computer networks for reasons including profit, protest, challenge, enjoyment, through to aiding in the detection of weaknesses ('white hats'). The large majority of hackers are 'script kiddies, ie, young, tech-savvy individuals operating from their personal laptops, who do not have the requisite tradecraft to cause widespread disruption, but pose a high level of threat in terms of isolated and brief disruption.
- **Hacktivists are a small but committed group** – This is a small but committed group of active hackers (individuals and groups) looking to cause maximum disruption and embarrassment to their victims (individuals, corporates or governments) and/or to promote their cause. They have captured media attention with campaigns coordinated through social media.
- **Terrorists set to gain in prominence** – This group is currently less developed in its ICT capabilities and propensity to pursue cyberattacks, and still prefers bombs to bytes. Demographic changes and an influx of technologically savvy Millennials or 'script kiddies' into their ranks means that, unfortunately, cyberterror is set to gain in prominence.

"When you're in positions of privileged access, like a systems administrator
for these sort of intelligence agencies, you're exposed to a lot more information than the average employee." – Edward Snowden

- **Companies are targeting sensitive information -** The growing corporate espionage segment follows the trend seen in state-sponsored cyber-espionage of targeting sensitive information. Generally speaking, corporations can be involved in reconnaissance activities, intrusion and data breach. For instance, one corporation stealing proprietary IP or even causing damage to competitors within its domain.

Table 9: Cybersecurity threat landscape

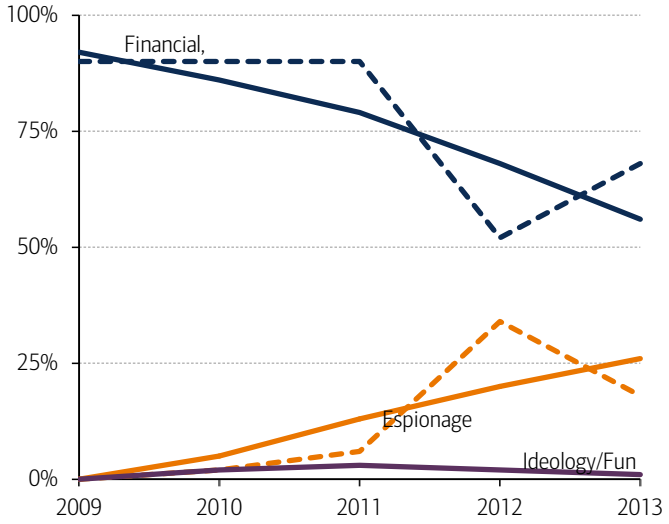
	Description	Examples	Main damage
Hacktivism	Use of networked platforms to pursue an ideological goal or obtain notoriety. No (or limited) physical effect.	DDoS attacks, website and server disruption, DNS hijacking, cybersquatting.	Data compromise or exposure, operational shut down or slow down, damage to organizational assets.
Cyber espionage	Unauthorized network penetration to access information. Risks related to IPR. Financial or ideological motivation. Generally non-physical effects.	Spyware, data theft, extortion, advanced persistent threat (APT).	Intellectual property infringement, theft or breach of confidential information, loss or corruption of data.
Cyber crime	Unauthorized network penetration to disrupt and damage systems, as well as stealing data, for financial gain. Mild physical effects.	Phishing, malware, APTs, viruses, worms, Trojans, spam, spoofing, ransomware, scareware, stolen devices, web-based attacks, adware, botnets, skimming, fast flux, spoofed apps.	Supply chain compromise, reputation damage, business interruption, online child sexual exploitation, identity theft, extortion, money laundering.
Emerging technologies failure	Risks related to the introduction of new technologies. Generally significant physical effects.	Internet of things, embedded medical devices, driverless cars, cloud systems.	Integrity, availability, performance and security of connected devices.
Critical information infrastructures disruption	Risks from disruptions to infrastructure. Attacks to SCADA systems. Strong physical effects.	Submarine cables, smart grid, electricity, financial systems.	Destruction, damage, or disruption of critical information infrastructures
Cyber warfare	Risks related to the use of networks by nation states or related groups to destroy or damage ICT systems. Targeting a nation's private sector may be a focus.	International conflicts.	Destruction, damage, or disruption of defence networked systems.

Source: ESADEgeo-Zurich Insurance

Small-scale cybercrime is #1, but that is changing

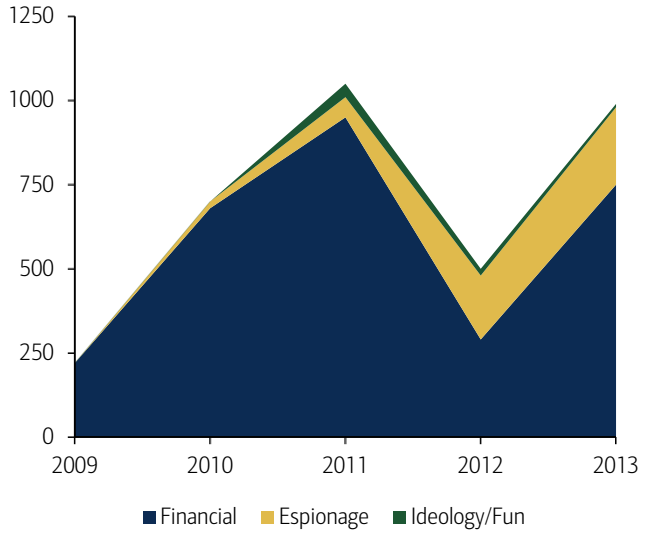
To date, relatively small-scale criminal attacks are the most common cyberattacks, with financial gain being the primary motivation.

Chart 13: Percent of breaches per threat actor motive over time



Source: Verizon

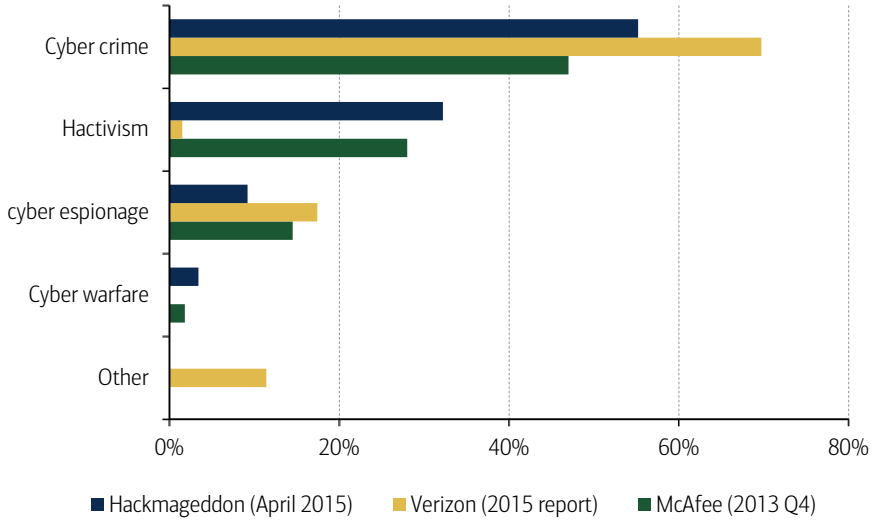
Chart 14: Number of breaches per threat actor motive over time



Source: Verizon

In contrast, sophisticated APTs that are conducted over a long time frame are rare, although we believe that they will see some of the fastest growth – particularly as hacktivism and cyber espionage and warfare pick up pace. .

Chart 15: Types of cyberattack by motivation

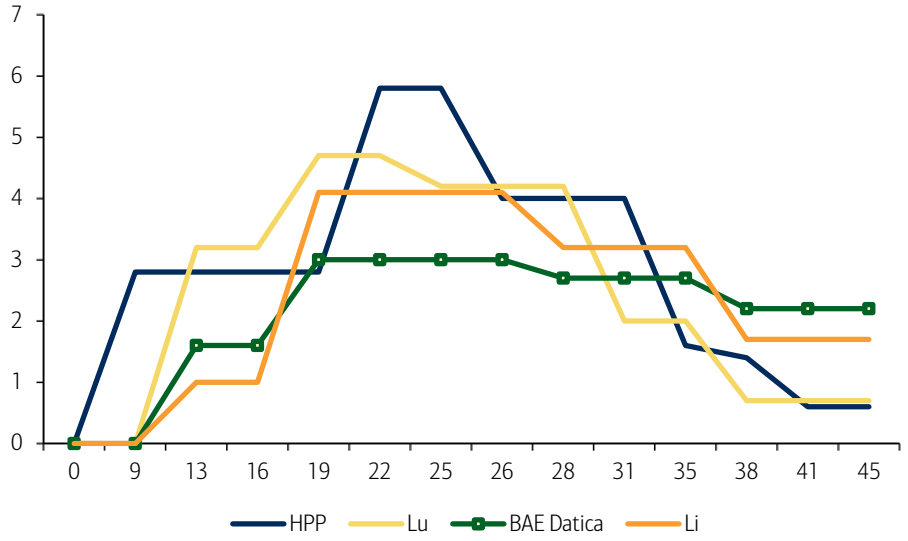


Source: Hackmageddon, Verizon, MacAfee

Demographics: Millennials hacking vs. elderly being targeted

As one might expect – the tech-savvy, digital generation – Millennials, the demographic cohort aged 18-34 – are the biggest perpetrators of cybercrime.

Chart 16: Age group of cybercrime perpetrators



Source: UNODC; HPP, Li, Lu, BAE Detica

In contrast, the elderly are one of the main targets of attackers with scammers targeting them via emails and websites for charitable donations, dating services, auctions, health care, and prescription medications – as well as for their pensions and savings.

No escaping: all industry sectors are being hit

All industry sectors with the exception of manufacturing saw a year-on-year increase in cybersecurity incidents in 2014 (source: IBM).

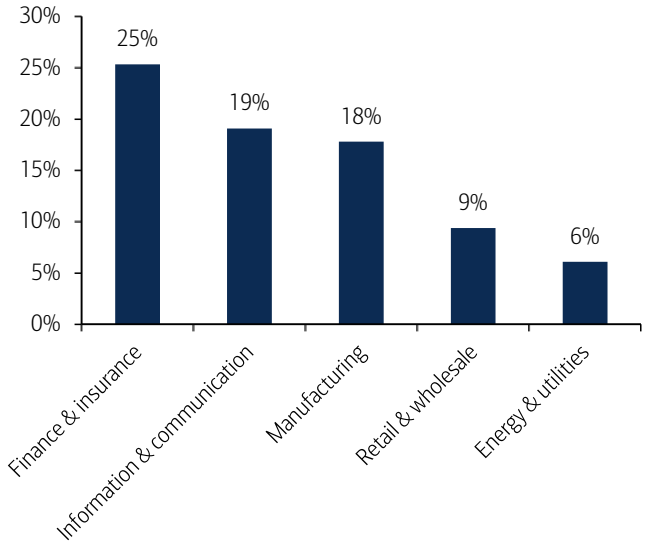
On an average day at an enterprise organisation:

- Every 24 seconds a host accesses a malicious website
- Every 34 seconds an unknown malware is downloaded
- Every 1 minute a bot communicates with its command & control centre
- Every five minutes a high-risk application is used
- Every six minutes known malware is downloaded
- Every 36 minutes sensitive data are sent outside the company (source: Check Point)

Financials, ICT and manufacturing: 62% of attacks

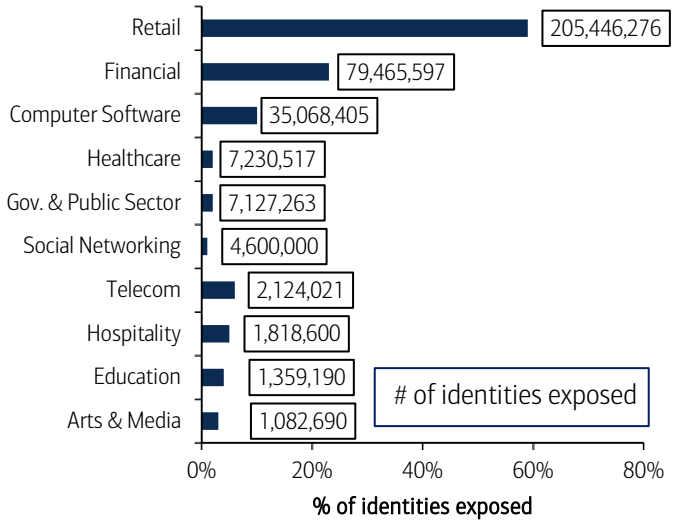
According to IBM Security Services, the finance and insurance industry has held the top spot for cybersecurity incidents for the past two years. ICT and manufacturing were no.2 and no.3, respectively. Together, the three sectors accounted for 62% of cybersecurity incidents in 2014 (source: IBM).

Chart 17: Cybersecurity incident rates across industries (2014)



Source: IBM

Chart 18: Top 10 sectors breached by number of identities exposed



Source: Symantec

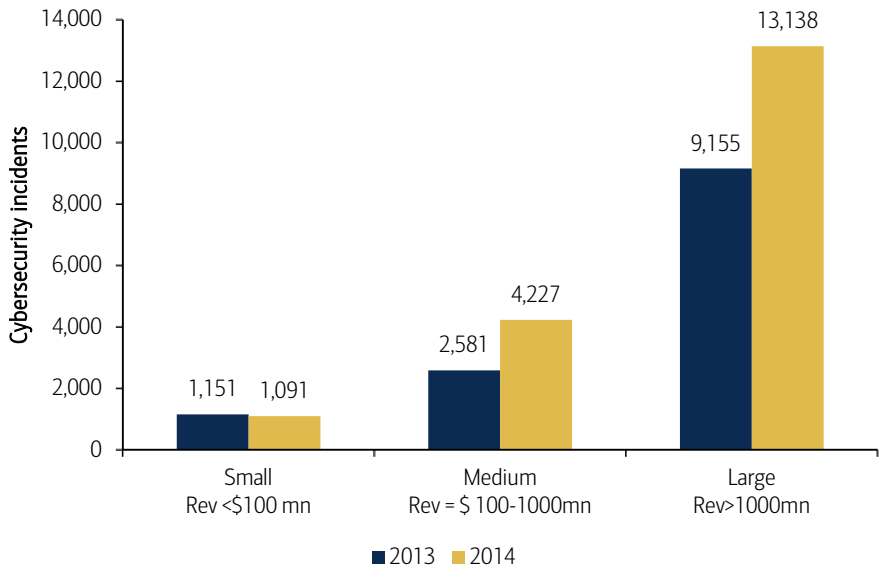
Retail seeing the fastest increase in attacks

Retail is the no. 4 most targeted sector according to IBM, but attacks grew by 3.2% YoY in 2014. There was also a huge increase in the incidence of data records being compromised in the industry in 2014, with retail accounting for close to 60% of identities exposed in the US alone (source: Symantec). The fast growth of point-of-sale (POS) systems explains this, in our view. POS is an attractive entry point for attackers and accounted for 40% of Trustwave's forensic investigations in 2014 vs 42% for e-commerce and 18% for corporate/internal networks (source: Trustwave).

Large organisations are #1 target

Threat actors tend to target large(r) corporations and organisations because the exploitation potential is greater, including trade strategy, IP, and volumes of consumer data that can be exploited, sold, or used for economic or military gain. On a positive note, large(r) organisations tend to have more mature cybersecurity processes and technologies in place, which allows them to uncover more incidents. According to PWC's survey, large organisations with revenues >US$1bn detected 13,138 incidents in 2014, +44% YoY.

Chart 19: Larger companies detect more cybersecurity incidents



Source: PWC

SMEs will increasingly become targets

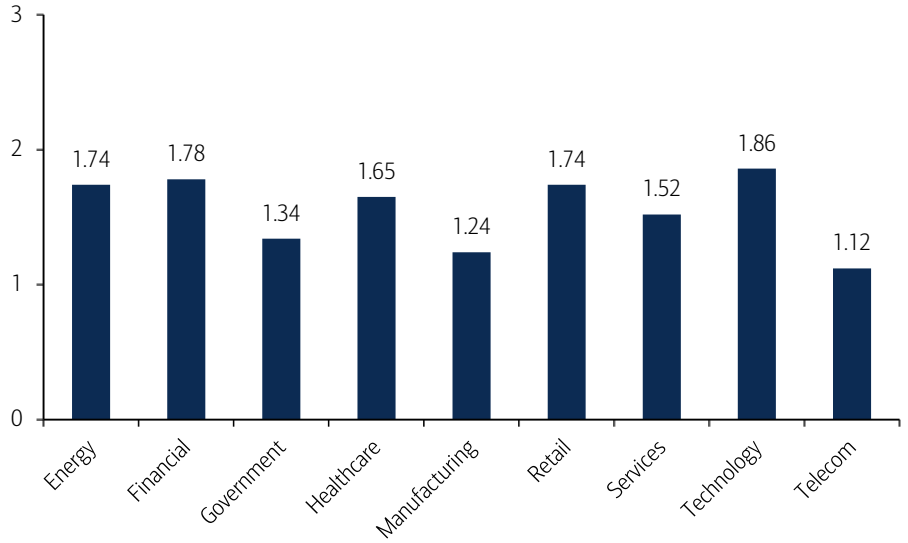
As larger organisations step up their cybersecurity efforts, threat actors are more likely to target SMEs. They are a key target for cybercrime because of their relatively limited awareness of this type of crime and misperception that they won't be targeted, in addition to budget, control and expertise constraints. Medium-sized enterprises with revenues of US$100mn-1bn saw a 64% jump in the number of incidents detected in 2014 (source: PWC). The impacts are also particularly profound with 20% of SMEs with fewer than 250 employees failing within six months of a cyberattack (source: Intel).

Companies are inadequately prepared

According to HP's 2015 State of Security Operations report, the most advanced enterprise security operations centres (SOCs) in the world typically achieve an overall score between 3 and 4 (out of 5) in their security operations capability. However, there are very few of these in existence with most organisations with a team focused on threat detection scoring between a 1 and 3:

- **One out of five SOCs are not minimally prepared to respond** to, much less detect, cyber threats affecting their organisation.
- **66% of SOCs and cyber defence organisations achieve only minimum ad hoc** threat detection and response capabilities.
- **87% of cyber defence organisations operate at sub-optimal maturity** and capability levels (source: HP).

Chart 20: Cybersecurity operations maturity by sector

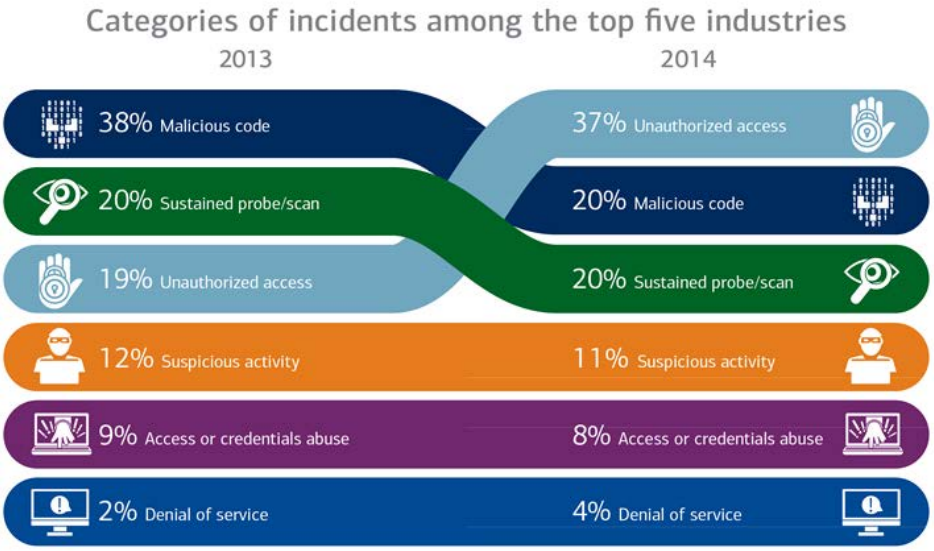


Source: HP

Security: unauthorised access and insiders the #1 threat

In 2014, unauthorised access topped the list of incident categories affecting the top five industries, accounting for 37% of incidents – nearly doubling from 2013. This category grew at the expense of malicious code, which fell to the no. 2 spot and sustained probes or scans, which fell to no. 3. The number of denial of service attacks doubled YoY (source: IBM).

Exhibit 8: Categories of cybersecurity incidents among top 5 targeted industries



Source: IBM

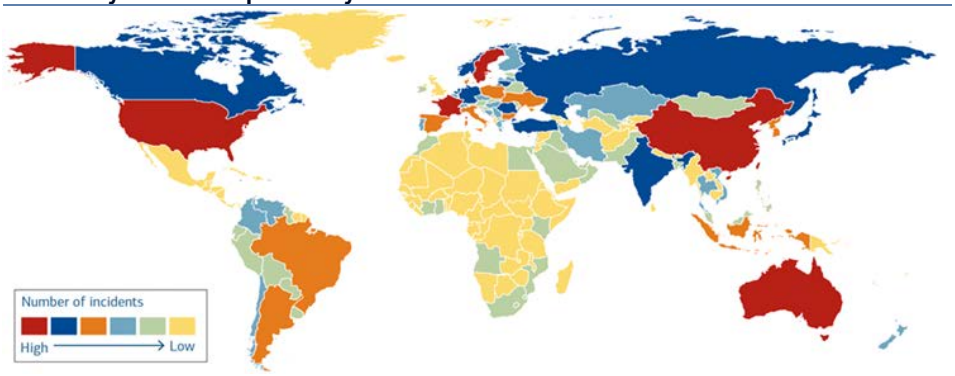
The bad guys: insiders are the #1 threat

In 2014, 55% of attacks were carried out by 'insiders' – actors with internal access (physical or remote) to an organisation's systems. While outsiders accounted for the remaining 45% of attacks – malicious insiders accounted for 31.5% and inadvertent actors 23.5% (source: IBM).

Where is it all happening: US is #1

The origin and target of cyberattacks are closely linked to the size of the country involved (including the size of its economy), internet penetration, and the availability of bandwidth.

Exhibit 9: Cyber incidents per country

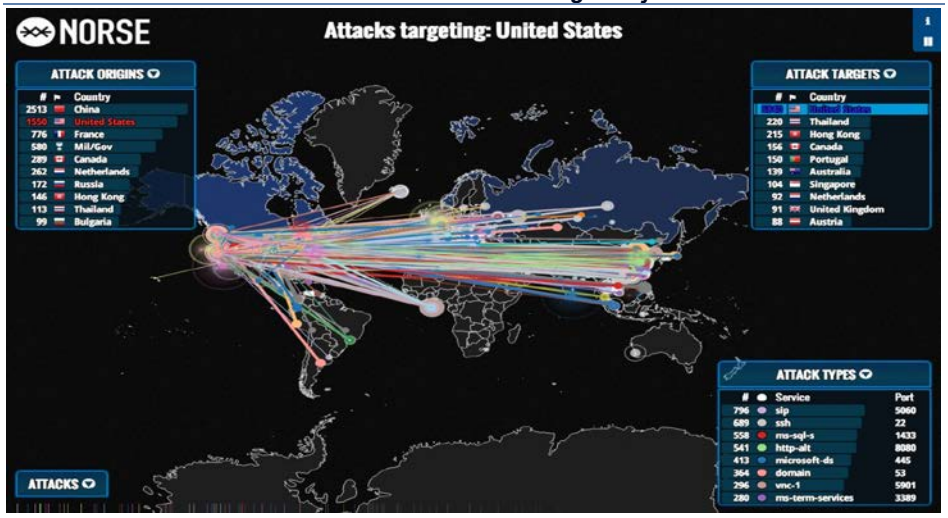


Source: NTT

Up to 50% of attacks originate in the US and 59% take place there

These factors go some way in explaining why 50% of attacks originated in the US and 59% took place there. China was a distant second in terms of where attacks originated (16%) and Japan in terms of where they took place (24%) (source: IBM).

Exhibit 10: Overview of live attacks via Norse's threat intelligence system

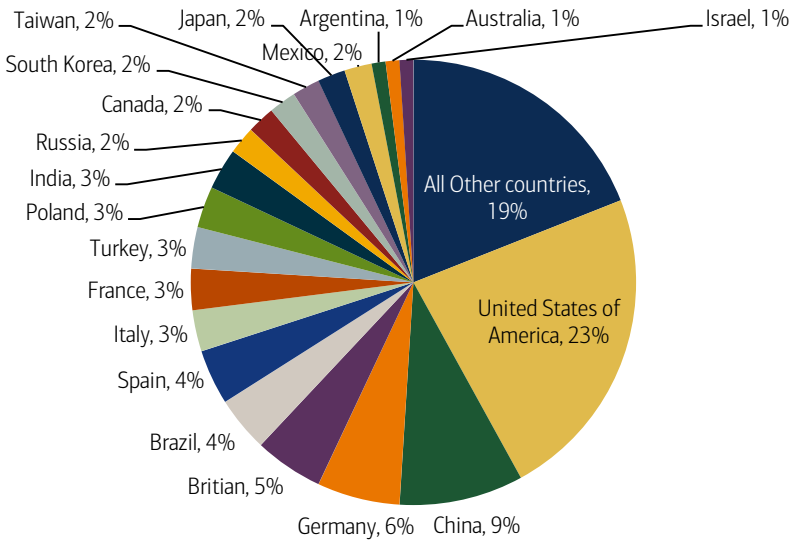


Source: Norse

US also #1 on cybercrime

Symantec has ranked the 20 countries that generate the most cybercrime. In compiling the list, Symantec looked at six factors: share of malicious computer activity, malicious code rank, spam zombies rank, phishing, bot rank, and attack origin. The US ranked #1, followed by China, Germany, the UK, and Brazil.

Chart 21: Top 20 countries with the highest rate of cybercrime

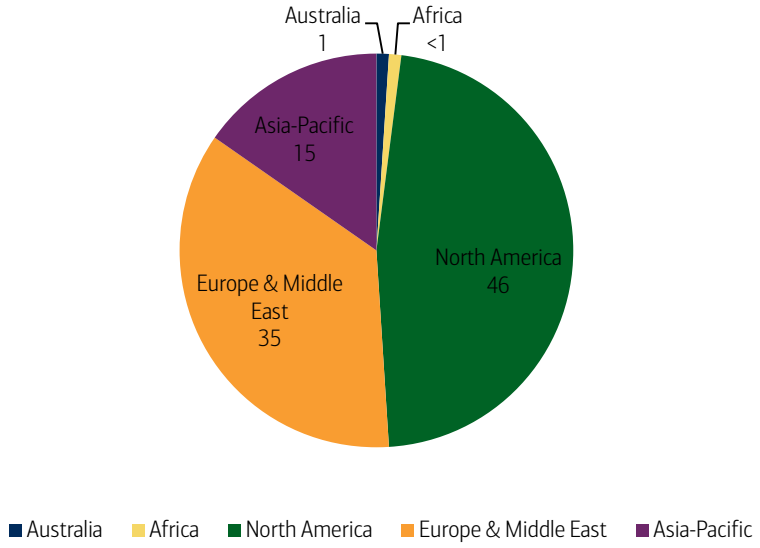


Source: Symantec

Who did it: challenge of attribution

However, it is important to stress that attempting to locate those behind the attack is fraught by challenges – ie, many attacks leave little in the way of traces. Hackers can generally mask their origin and re-route their attack to a different region. That said, nearly half of the world's servers which hosted 'suspicious' content appear to be located in North America, mainly the US, according to McAfee's analysis.

Chart 22: Location of servers hosting suspicious content (%) in 2015



Source: McAfee 2015

Be prepared: who is and who isn't

Assessing a country's cyber preparedness throws up a slight paradox in that the less connected a country is, the lower the risk of cyber threats. But the HCSS identified a number of indices assessing cybersecurity capabilities and commitments of countries with the US and UK ranking consistently highly ranked across the board – followed by Japan, Germany, Finland, Canada, Australia, South Korea and Sweden.

Table 10: Overview of surveys of cyber "preparedness"

	Country	Networked Readiness Index 2014	Cyber Readiness Index, 2013	ITU, Global Cybersecurity Index, 2014	Cyber Power Index, 2013	Cyber preparedness	Average
1	Argentina	1	1	1	2	n/a	1.25
2	Australia	3	4	4	3	2	3.2
3	Austria	3	3	3	n/a	2	2.75
4	Brazil	1	2	3	2	1	1.8
5	Canada	3	4	4	3	2	3.2
6	China	2	2	1	1	1	1.4
7	Denmark	3	1	2	n/a	3	2.25
8	Finland	4	3	2	n/a	4	3.25
9	France	2	3	2	4	3	2.8
10	Germany	3	3	3	4	3	3.2
11	India	1	1	3	2	1	1.6
12	Indonesia	1	1	1	1	n/a	1
13	Israel	3	2	3	n/a	4	3
14	Italy	2	1	2	3	1	1.8
15	Japan	3	4	3	4	2	3.2
16	Mexico	1	1	1	2	1	1.2
17	Netherlands	4	4	3	n/a	3	3.5
18	Russia	2	2	2	1	1	1.6
19	Saudi Arabia	2	1	1	1	n/a	1.25
20	South Africa	1	1	1	3	n/a	1.5
21	South Korea	4	2	3	3	n/a	3
22	Sweden	4	2	2	n/a	4	3
23	Turkey	2	1	2	1	n/a	1.5
24	United Kingdom	4	4	3	4	3	3.6
25	United States	4	4	4	4	3	3.8

Source: HCSS

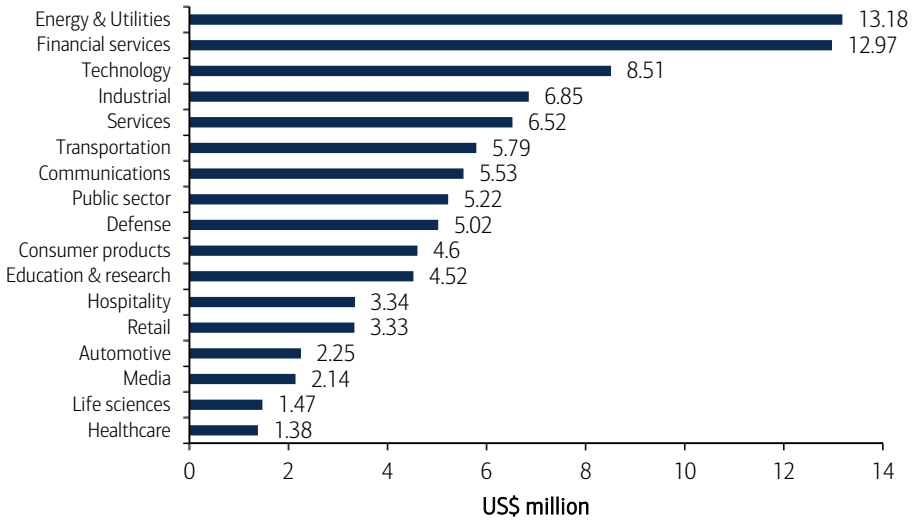
Costs: up to US$3tn at risk long-term

We explore the cost impacts of cybersecurity in greater detail in a dedicated section later in the report, but highlight that Ponemon puts the price of cybercrime for the average US company at a record US$12.7mn in 2014, while attacks cost the global economy up to US$575bn annually.

Highest cost for energy and utilities, financial services and technology in 2014

Cybersecurity has a cost implication for all industry sectors. Companies in energy and utilities, financial services and technology experienced the highest annualised cost in 2014. In contrast, peers in media, life sciences and healthcare incurred much lower costs on average.

Chart 23: Average annualized cost of cyberattacks by industry sector (US$mn)

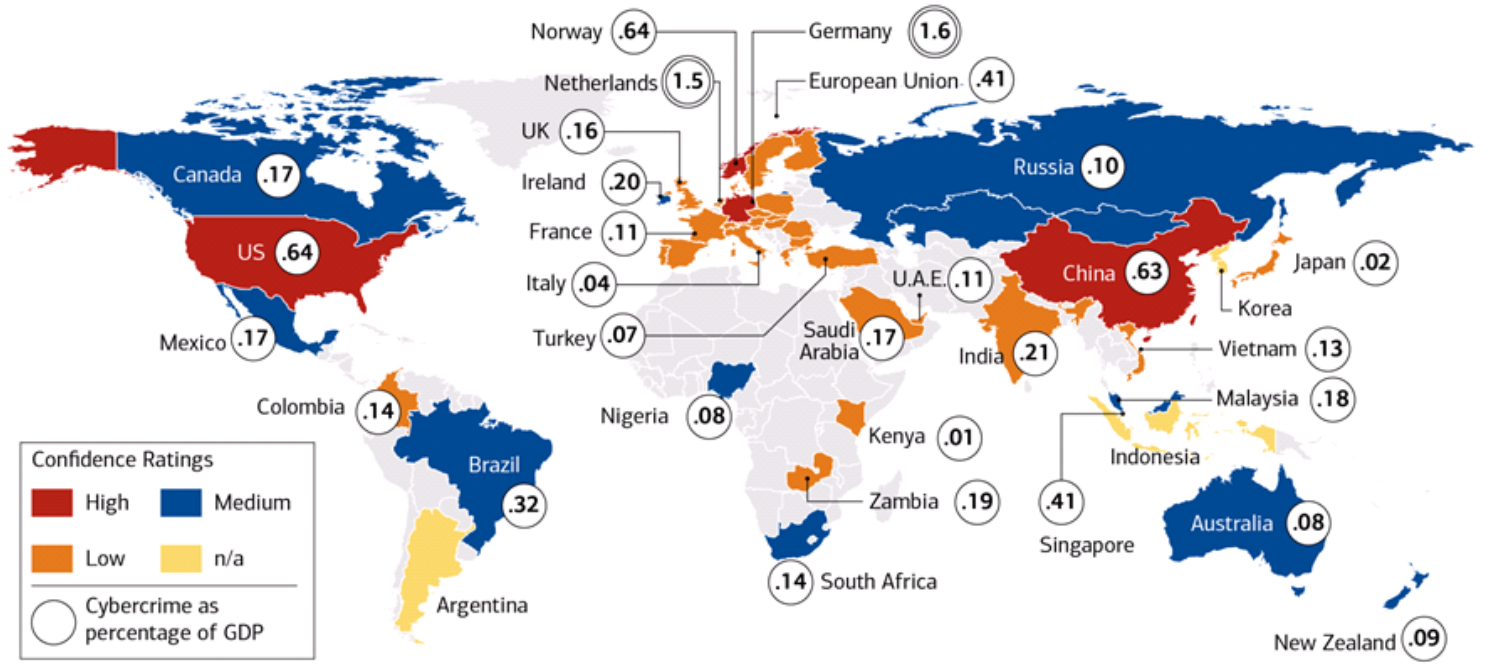


Source: Ponemon

Close to 1% of global GDP currently at risk

Global cybersecurity activity is adding up and is thought to account for 0.8% of global GDP annually with the impact largest in richer countries (source: McAfee).

Exhibit 11: Estimated costs of cybercrime as a percentage of GDP



Source: McAfee

Future does not look bright: US$3tn of economic value at risk

Projections of losses from cybersecurity are even more chilling. The WEF and McKinsey have estimated that if current cyber threat trends persist, there could be US$3tn in economic losses globally by 2020E vis-à-vis unrealised technological innovation gains. Others project that US$3tn of global economic value creation in the next five to seven could be at risk if organisations and governments are unable to adopt successful strategies to combat cyber threats (source: Bailey et al, McKinsey Quarterly, May 2014).

Table 11: A diverse array of cyber actors and impacts

	Financial theft/ fraud	Theft of IP or strategic plans	Business disruption	Destruction of critical infrastructure	Reputation damage	Threats to life/ safety	Regulatory
Organized criminals	Very High	Moderate	Low	Low	Very High	Low	Very High
Hacktivists	High	Moderate	Very High	High	Very High	Low	High
Nation-states	High	High	Very High	Very High	Very High	Low	Very High
Insiders	Very High	High	High	High	High	Moderate	High
Third parties	High	Moderate	Moderate	Moderate	Very High	Low	Very High
Skilled individual hackers	Very High	High	High	High	High	Low	High

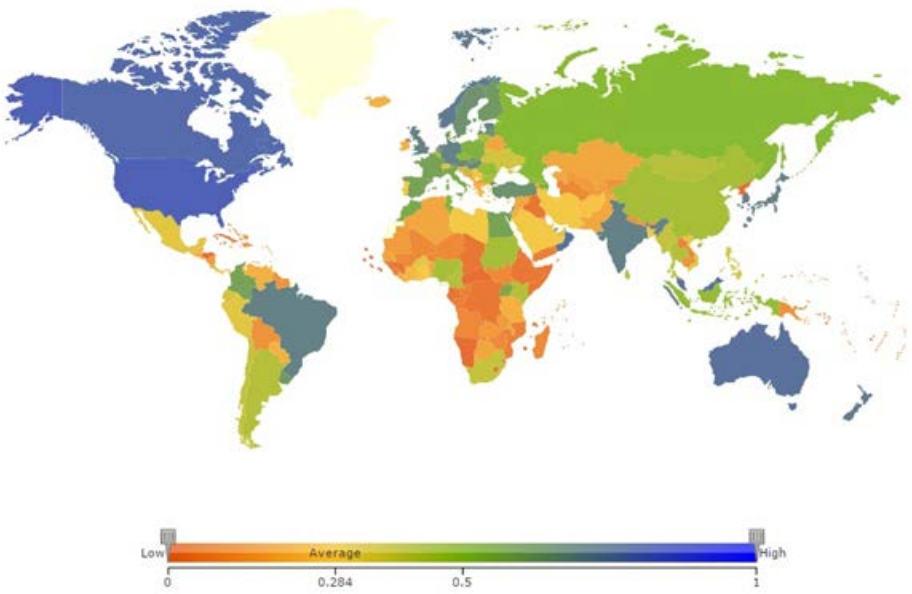
Source: Deloitte

Cyber meets homeland: critical infrastructure under attack

The US DoD has stated that it considers cyberspace another domain for warfare, and that cyberattacks are likely to eclipse terrorism as a domestic threat for western developed countries over the next decade. This threat increasingly encompasses critical infrastructure, including the energy, transport and water grids, as well as the finance sector and critical manufacturing.

In 2014 alone, there were 67,168 intrusions into federal systems in the U.S. – a 1,121% increase since 2006 (source: US GAO).

Exhibit 12: Global Cybersecurity Index (GCI) 2014: measure of each nation's level of cybersecurity development



Source: ITU-ABI Research

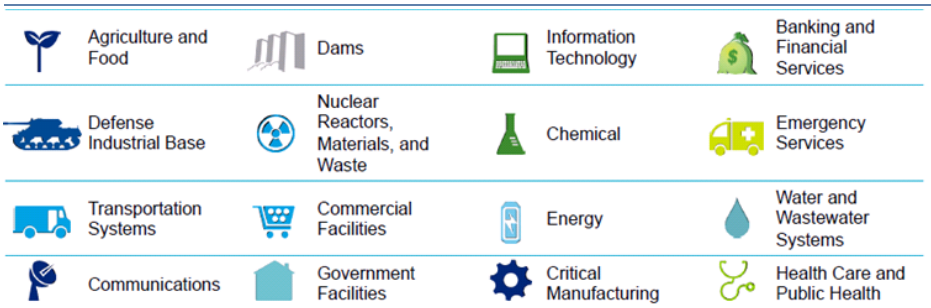
"We foresee an ongoing series of low-to-moderate level cyber attacks from a variety of sources over time, which will impose cumulative costs on US economic competitiveness and national security." -James R. Clapper Director of National Intelligence

Bank of America Merrill Lynch

16 critical infrastructure sectors at risk

The US DHS has identified a number of critical infrastructure sectors: chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food & agriculture; government facilities; healthcare & public health; IT; nuclear reactors, materials & waste; transportation systems; and water & wastewater systems

Exhibit 13: Critical Infrastructure sectors



Source: Deloitte

Critical infrastructure is perceived to be #1 risk

From a global perspective critical infrastructure is the joint #1 area, along with economic prosperity, that nations believe to be at risk from cyber threats, with national security in third place (source: Luiijf et al, 2013). Although this has been defined in countries' national cybersecurity strategy (NCSS), we believe more action needs to be taken to address this issue.

Table 12: Cyber threats posed to countries

Country	Critical Infrastructure	Defense Capabilities	Economic Prosperity	Globalization	National Security	Public Confidence In ICT	Social Life
AUS	●	●	●		●		●
CAN	●	●	●		●		●
CZE	●		●		●		○
DEU	●		●	●	○		
ESP	●		●		●	○	●
EST	●		●		○		
FRA	●	○	●		●		●
GBR	●		●		●	●	
IND	●		●	○			●
JPN	○		●	●	●		●
LTU	●		○		○	●	
LUX	●		●			○	
NLD	●	○	●		○	●	●
NZL	●		●		●	○	
ROU	●	●	○		●		
UGA	●		●			●	
USA	○		●		●	●	
ZAF	●		●		○	●	
Count	18	5	18	3	15	9	7

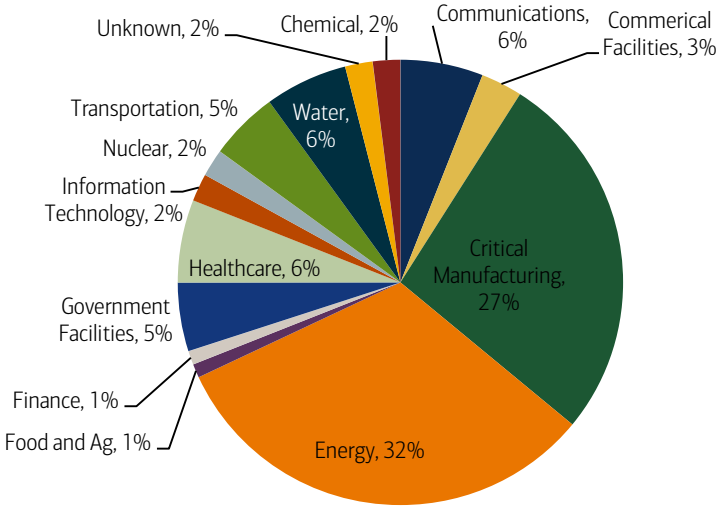
Source: HCSS based on Luiijf et al 2013

NOTE: ● – EXPLICITLY DEFINED; ○ – IMPLICITLY REFERENCED

Energy sector is the first line of attack

The US DHS's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) monitors and responds to cyber incidents across all critical infrastructure areas. In FY14, ICS-CERT received and responded to 245 incidents by asset owners and industry partners. It is important to note that many more incidents go unreported.

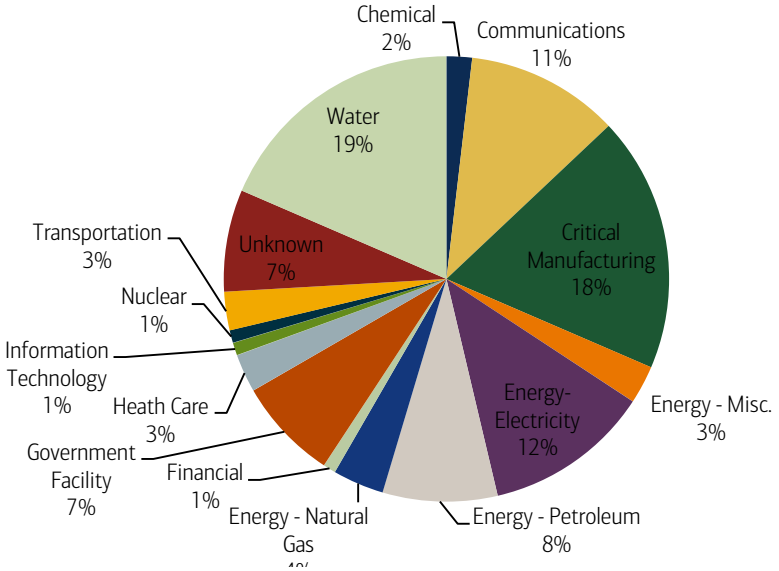
Chart 24: FY-14 mid-year critical infrastructure incidents by sector



Source: US Department of Homeland Security ICS-CERT Monitor

In the first half of FY15 (October 2014 to April 2015), ICS-CERT responded to 108 incidents. As in previous years, the energy sector leads all other areas with the most reported incidents. The water and critical manufacturing sectors also made up a notable proportion of incidents reported to ICS-CERT, at 19% and 18%, respectively.

Chart 25: FY-15 mid-year critical infrastructure incidents by sector



Source: US Department of Homeland Security ICS-CERT Monitor

Bank of America Merrill Lynch

Vast range of threats and methods to gain access

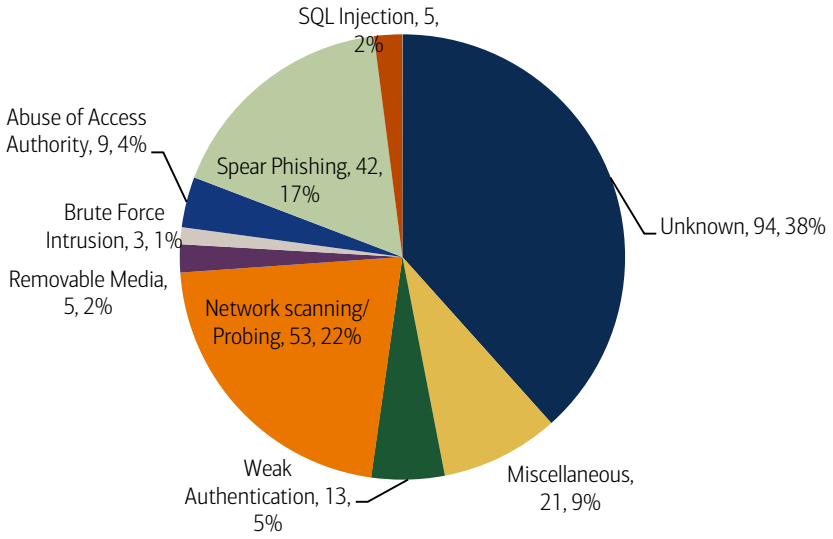
According to ICS-CERT, the incidents encompassed a vast range of threats and observed methods for attempting to gain access to both business and control systems infrastructure, including: unauthorised access and exploitation of internet-facing ICS/Supervisory Control and Data Acquisition (SCADA) devices; exploitation of zero-day vulnerabilities in control system devices and software; malware infections within air-gapped control system networks; SQL injection via exploitation of web application vulnerabilities; network scanning and probing; lateral movement between network zones; targeted spear-phishing campaigns; and strategic web site compromises (aka, watering hole attacks).

48% of electric utilities do not have integrated security systems with proper segmentation, monitoring and redundancies needed for cyber protection (source: Black & Veatch)

Origin of most incidents is 'unknown'

Worryingly, the majority of reported incidents were categorised as having an 'unknown' access vector (ie, the organisation was confirmed to be compromised, however, forensic evidence did not point to a method used for intrusion because of a lack of detection and monitoring capabilities within the compromised network (source: DHS ICS-CERT).

Chart 26: Incident by access vector



Source: US Department of Homeland Security ICS-CERT Monitor

There are over 1bn unique websites on the internet and 3.2bn Internet users today – while the number of devices connected to the Internet will grow to 50bn by 2020E

IoT ('internet of threats'): cyberattacks will skyrocket

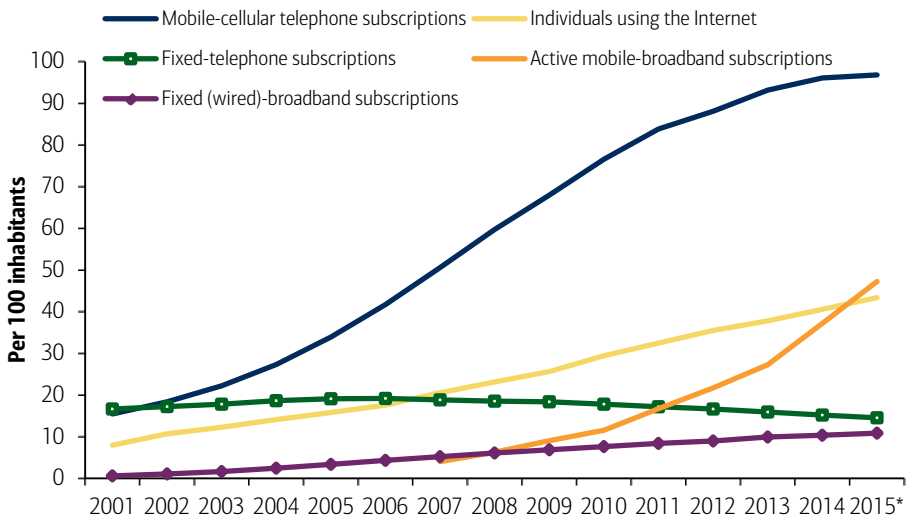
From a cybersecurity perspective, the proliferation in ICT – notably internet access and the IoT with an estimated 50bn devices that will be connected to the internet by 2020E – means a rise in valuable information and data via 50bn potential points of attack.

> US$14.4tn is at stake in connecting up what is now unconnected through the Internet of Everything (source: Cisco)

3.2bn internet users: 50% penetration by 2017E

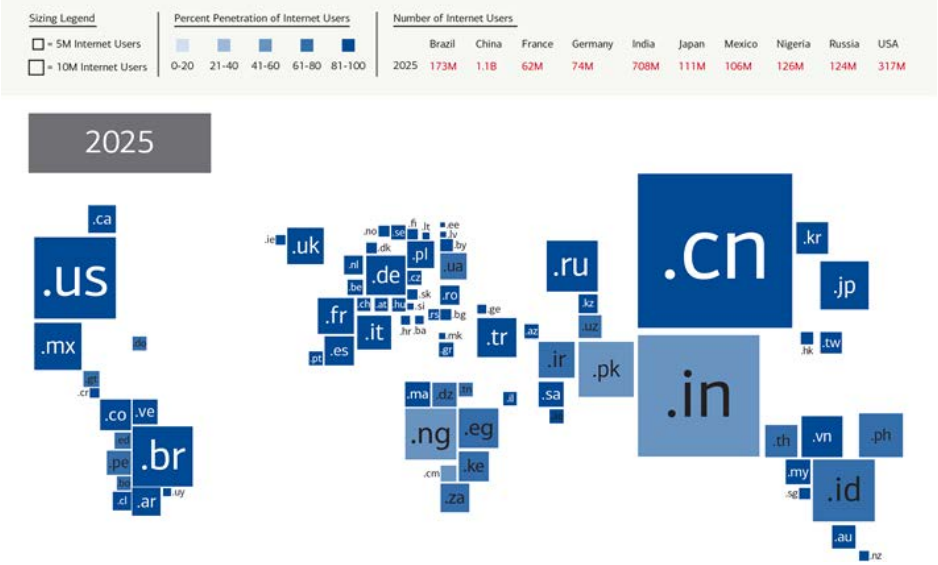
Global internet penetration rates grew 8x between 2000 and 2015 (6.5% to 43%), with 3.2bn internet users today and many developed countries experiencing penetration rates of >90%, according to ITU. The mobile broadband market has grown the fastest with the number of active connections increasing 12x from <4% in 2007 to 47% in 2015. There are now more than 7bn mobile cellular subscriptions, corresponding to a penetration rate of 97%, up from just 738mn in 2000 (source: ITU). The ITU estimates that there will be 25bn networked devices by 2020E.

Chart 27: Global ICT developments 2000 - 2015



Source: ITU, BofA Merrill Lynch Global Research

Exhibit 14: Global Internet adoption by 2025E*



Source: Microsoft. *The size of each country block (identified by its top-level domain name) conveys the number of Internet users in that country, while the color represents the proportion of Internet users relative to total population

An internet minute

In 2014, there were 3.0bn internet users, accounting for 40.4% of the global population. Every minute on the internet, there are 136mn emails sent +7% YoY); 4.2mn Google searches (+2%); c.672,000 in chart log-ins on Facebook (+30%); 433,000 tweets sent (+25%); 80,000 Amazon sales (+21%); 67,000 photos uploaded on Instagram (+76%); 50,200 Apple Apps downloaded (+36%); and 306 hours of content uploaded to YouTube (+196%) (source: TechSpartan).

Table 13: An internet minute, 2014

Facebook - Logins	672,222
Instagram - Photos uploaded	67,000
Twitter - tweets sent	433,000
Pintrest - pins added	3,400
Vine - vines uploaded	450
Google - searches	4,190,000
You tube - content uploaded	360
Apple - apps downloaded	50,200
Songs added	14
Amazon - sales	80,000
Emails sent	136,319,444

Source: TechSpartan, Squarespace

Cloud is increasing the threat surface by >4-10x

The rapid growth of the cloud (SaaS, IaaS et al) and the volume of accounts, apps, files, third-party data management and storage, and sensitive data are significantly increasing the threat surface for cybersecurity attacks. The growth in corporate cloud adoption has increased the attack surface by more than 4x through both external collaboration via public cloud apps and unique third-party cloud apps connected to corporate systems, and by over 10x for files stored in public cloud applications (source: CloudLock).

- **100,000 risky files per organisation are stored in cloud apps** that violate corporate data security policies.
- **4,000 files per organisation containing passwords** are stored in public cloud apps containing credentials to corporate systems.
- **One in four employees violates security policy** in public cloud apps (source: CloudLock).

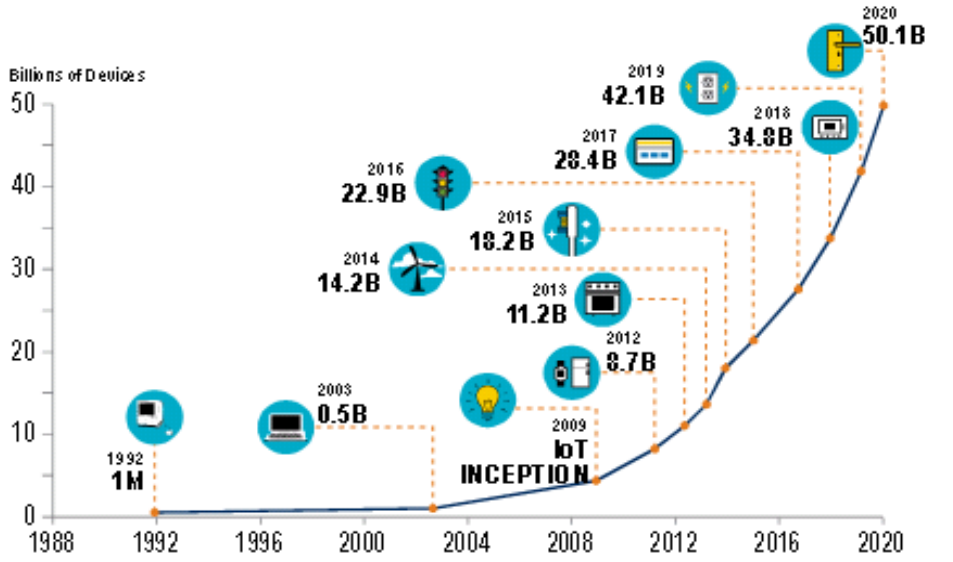
50bn connected devices by 2020E = 50bn points of attack

The Internet of Things (IoT) is fast becoming a reality with a growing number of people and things (from smartphones, alarms and cars to commercial and industrial equipment et al) linked to the cloud and networks, connected to the internet, and communicating with each other in real time, "resulting in volumes of data generated and processing of that data into useful actions that can 'command and control' things and make life much easier for human beings" (source: Freescale).

> The average household with two children will own c.50 internet-connected devices by 2020 (vs 10 today)

Cisco estimated that 8.7bn devices were connected in 2012 and predicts this will rise to around 50bn by 2020E including drones, additive manufacturing, smart appliances and driverless cars. The resulting potential to share data with everyone and everything will significantly ramp up cybersecurity risks.

Exhibit 15: Estimated device progression of IoT by 2020E



Source: NTCA, Cisco

'Cybergeddon': only one disruptive technology away

According to the WEF, a future in which cyber attackers (including hackers, organised crime and national militaries) "have an overwhelming, dominant and lasting advantage over defenders and could be just one disruptive technology away."

> Cybergeddon (from tech. cyber-, lit. "computer"; Hebrew: Megiddo, extracted from Har Megiddo ('mountain of final battle') refers to the cataclysm resulting from a large-scale sabotage of all computerised networks, systems and activities. It combines cyberterrorism, cyberwarfare, cybercrime, and hacktivism into scenarios of wide-scale internet disruption or economic collapse (source: the WEF)

Internet could cease to be a trusted medium

Such a 'Cybergeddon' scenario could result in large-scale internet-wide disruptions, the internet ceasing to be a trusted medium for communication or commerce, and individuals and business scared away from intensive reliance on the internet (source: WEF).

Table 14: Comparison of the five possible futures of cyber conflict and co-operation [I think the table is clearer with the extra rows to differentiate]

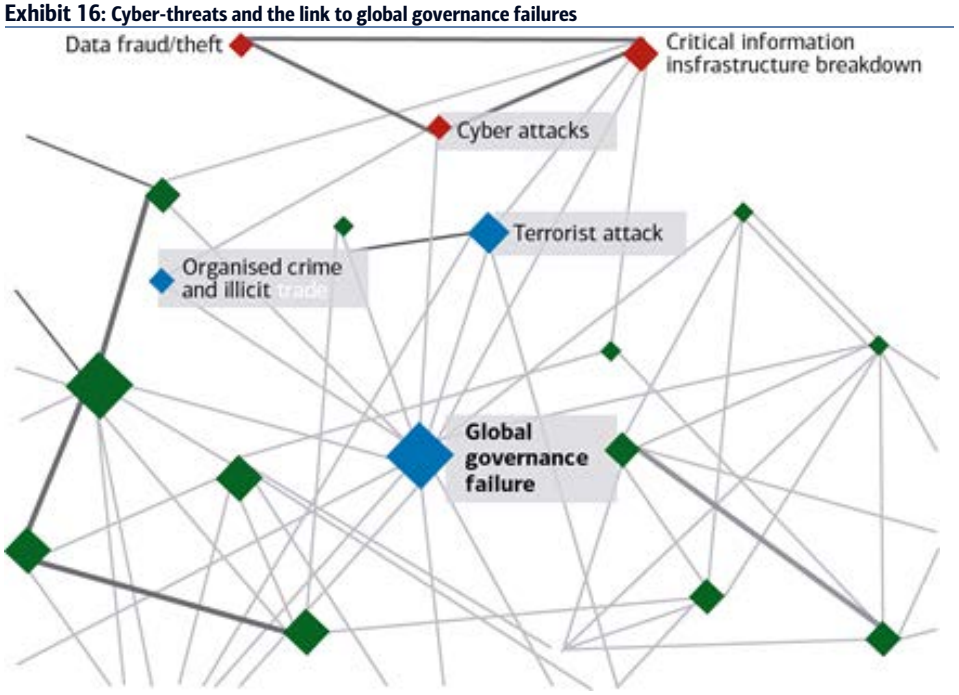
	Status Quo	Conflict Domain	Balkanization	Paradise	Cybergeddon
Description	Cyberspace conflict tomorrow looks like that of today; there are high levels of crime and espionage, but no massive cyber wars	Cyberspace has a range of human conflict, just like air, land, space and maritime domains	Cyberspace has broken into national fiefdoms; there is no single internet, just a collection of national internets	Cyberspace is an overwhelmingly secure place, as espionage, warfare and crime are extremely difficult	Cyberspace always un-ruled and unruly, has become a 'failed state' in a near-permanent state of disruption
Relationship between Offense and Defence	Offense > Defence	Offense > Defence	Unknown / Depends	Offense >>> Defence	Offense >>> Defence
Intensity and kind of conflict	Conflict is as it is today; but not catastrophic, with crime and spying	There is a full range of conflict: crime, spying, embargoes and full-blown international conflict	Nations are possibly blocking access to content, to and from each other, although there may be fewer outright attacks	All conflict is greatly reduced, although nations and other advanced actors retain some capability	Every kind of conflict is not just possible, but ongoing, all of the time
Intensity and kind of co-operation	There is healthy but limited sharing on response standards and cyber crime	To be stable, cyber co-operation requires norms and regimes, just as in other domains	Cyber co-operation requires international agreement to interconnect national internets	Co-operation is critical if stability depends on norms, or unnecessary if it depends on new technology	Co-operation is either useless, as attackers have the edge, or impossible, like trying to govern a failed state
Stability Why this is possible	Relatively stable Current trend line and massive attacks have not occurred yet, despite being expected for 15 years	Relatively stable Other domains have generally supported a range of human activity, from commerce to conflict	Unknown / depends Countries continue to build border firewalls, which UN control of the internet could exacerbate	Long-term stable New technologies or co-operation, long promised, could make security much easier	Long-term unstable Offense continues to outpace defence, as any new defensive technology or co-operation is quickly overcome

Source: Atlantic Council

Cybersecurity and global governance failures

As cybersecurity becomes the new frontier for controlling information and data, it is increasingly shaping the evolution of many other global risks, and exacerbating the overarching threat of global governance failures. We explore the weaknesses of global cyber governance later in the report.

Exhibit 16: Cyber-threats and the link to global governance failures



Source: WEF

Investors: looking to play US$75bn cyber solutions market

The cybersecurity theme is attracting growing numbers of investors. Key drivers are the size of the market and its growth rates, as well as the strong performance of companies with cybersecurity exposure.

US$75bn market today

The global cybersecurity solutions market is estimated at US$75-77bn in 2015 with growth of c.8.2% from 2014 (source: Gartner). The aerospace, defence and intelligence verticals are thought to be the largest contributors to cybersecurity solutions today (source: MarketsandMarkets). North America and Europe are the leading cybersecurity revenue contributors, while the APAC region is seeing rapid growth driven by China, India and Southeast Asia (source: TechSci Research).

Table 15: Cybersecurity Ventures' top 25 hottest and most innovative cybersecurity companies (at Q3-15)

#	Company	Cybersecurity Sector	Corporate HQ
1	FireEye	Advanced Threat Protection	Milpitas CA
2	Lancope	Network Visibility & Security Intelligence	Alpharetta GA
3	AlienVault	Threat Detection & Response	San Mateo CA
4	Norse	Live Attack Intelligence	San Mateo CA
5	Easy Solutions	Electronic Fraud Protection	Doral FL
6	AVG Technologies	Anti-Virus & Internet Security Software	Amsterdam, The Netherlands
7	RSA	Intelligence Driven Security	Bedford MA
8	IBM	Enterprise IT Security Solutions	Armonk NY
9	Veracode	Application Security Testing	Burlington MA
10	Lockheed Martin	Cybersecurity Solutions & Services	Bethesda MD
11	Clearwater Compliance	Risk Management and Compliance	Nashville TN
12	Palo Alto Networks	Threat Detection & Prevention	Santa Clara CA
13	Trend Micro	Server, Cloud, and Content Security	Tokyo, Japan
14	NuData Security	Online Fraud Detection	Vancouver, Canada
15	Code Dx	Software Assurance Analytics	Northport NY
16	Sera-Brynn	Cyber Risk Management	Suffolk VA
17	DFLabs	Automated Incident & Breach Response	Lombardy, Italy
18	Intel Security Group	Anti-Virus, Malware & Threat Protection	Santa Clara CA
19	BT	Security & Risk Management Solutions	London, UK
20	Cavirin	Automated IT & Cloud Security	Santa Clara CA
21	IT Security, Inc.	Application, Cloud, & Network Security	Pittsburgh PA
22	PwC	Cybersecurity Consulting & Advisory	London, UK
23	Herjavec Group	Information Security Services	Toronto, Canada
24	Nexusguard	Cloud Enabled DDoS Mitigation	San Francisco CA
25	SecuEra Technologies	Identity & Access Management Solutions	Washington DC

Source: Cybersecurity Ventures

US$170bn market by 2020E

It is estimated that the global cybersecurity solutions market will post a 9.8% CAGR from 2015 to 2020E to reach US$170bn (source: Markets and Markets). High growth segments include security analytics (SIEM) (10%); threat intelligence (10%+); mobile security (18%); and cloud security (50%) (source: IDC).

Exhibit 17: Network Sentry solutions

Source: Bradford Networks

Deal-making on the rise: 224 investments & 59 transactions in 2014-15

Major cybersecurity deals are on the rise – with cybersecurity start-ups having raised US$2.5bn across 224 investments in 2014 (vs <US$1bn from 108 deals in 2010) (source: CB Insights). The number of seven-figure deals increased by 40% YoY (source: FBR & Co.). There has also been a significant rise in cybersecurity M&A with 59 transactions in 2014-15 (vs 24 in 2012). Vista Equity's US$4bn acquisition of Tibco Software is the largest deal YTD in 2015 (source: Centaur Partners).

Table 16: Recent cybersecurity transitions (US$mn)

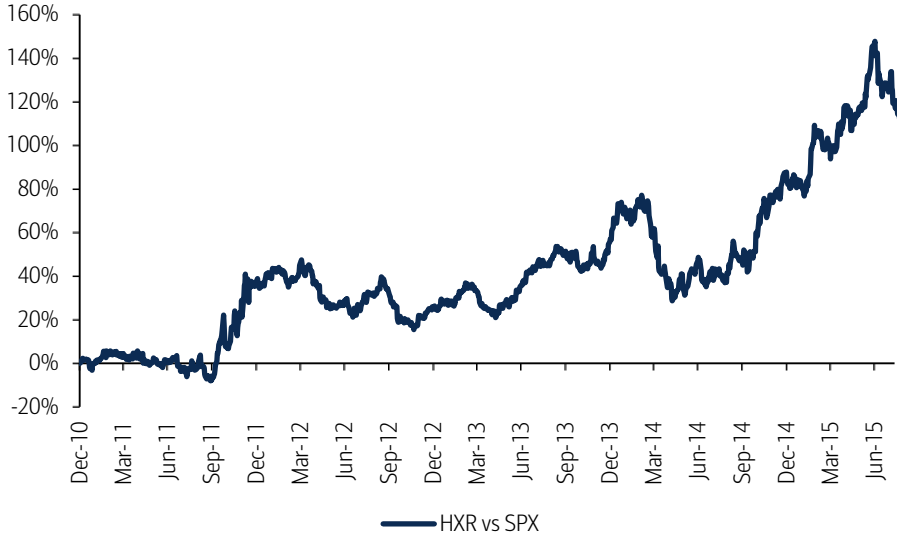
Announced	Acquirer	Target	Target Abstract	Val./Rev.	Total Deal Amt.	Target TTM Rev.
18/04/2015	Raytheon	Websense	Develops software to protect organizations from cyber attacks and data theft	3.7	3,958	1,076
29/09/2014	Vista Equity Partners	Tibco	Provides infrastructure and business intelligence software	3.7	3,958	1,076
02/03/2015	HP	Aruba	Provides enterprise mobility solutions worldwide	3.3	2,651	812
13/10/2014	Netscout	Arbor, Fluke, Tektronic	Providers of network security, testing and management solutions	NA	2,619	NA
02/07/2012	Dell	Quest Software	Enterprise Systems Management Software	2.8	2,382	857
23/07/2013	Cisco	Sourcefire	Provider of intelligent cybersecurity solutions	9.6	2,245	233
22/01/2014	Vmware	AW	AirWatch was a provider of enterprise mobile management and security solutions	NA	1,540	NA
13/03/2012	Dell	Sonicwall	Network security and data protection	4.8	1,250	260
12/12/2011	Thoma Bravo	Blue Coat	Business applications	2.4	1,105	467
28/10/2014	Engility	TASC	Provides wide range of IT security analysis	NA	1,100	NA
30/12/2013	FireEye	Mandiant	Information security company	NA	1,034	NA

Source: Centaur Partners

Cybersecurity becoming a major investment theme

Investors are increasingly looking to understand the investment potential of the cybersecurity theme. The past two years have seen the launch of thematic products such as Pure Funds ISE Cyber Security ETF (HACK), First Trust NASDAQ CEA Cybersecurity ETF, and the First Trust BofA Merrill Lynch Cybersecurity Portfolio (UIT).

Chart 28: ISE Cyber Security Index vs S&P 500 Index relative performance

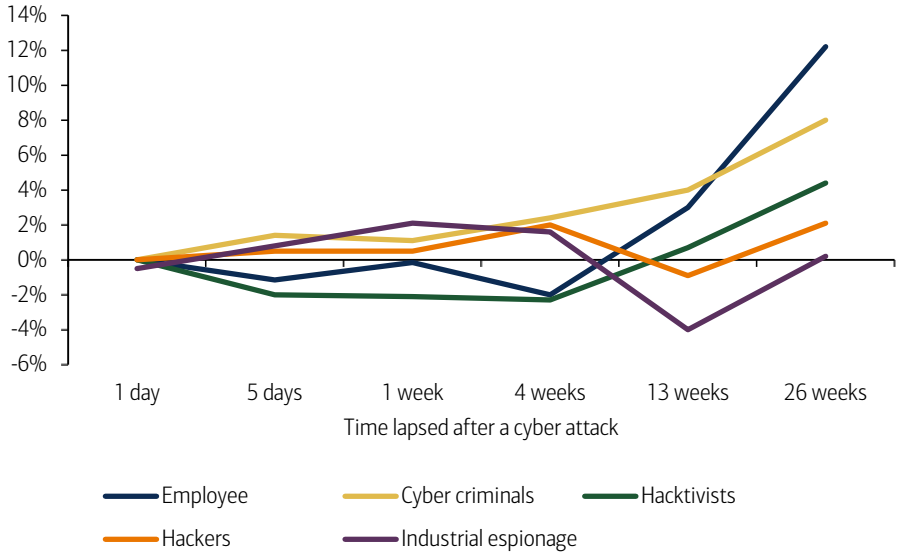


Source: Bloomberg
Rebased to 100 as on 31-Dec-2010

Growing shareholder scrutiny

In our view, the coming years will see growing efforts by shareholders for boardrooms to take cybersecurity more seriously. We are already seeing this with attacks by employees, cyber criminals, hacktivists/hackers, and industrial espionage having impacts on companies that have been attacked (source: Freshfields).

Chart 29: Which type of cyber attack spooks the markets most?



Source: Freshfields

We are already seeing signs in this regard including a prominent proxy advisor recommending the ousting of seven out of ten of Target Corp's board for "failure to provide sufficient risk oversight" on cybersecurity, a jump in cybersecurity resolutions at AGMs, and a rise in shareholder lawsuits against directors and officers.

Bank of America Merrill Lynch

Table 17: Share price declines of certain US and UK listed companies following cyber attacks

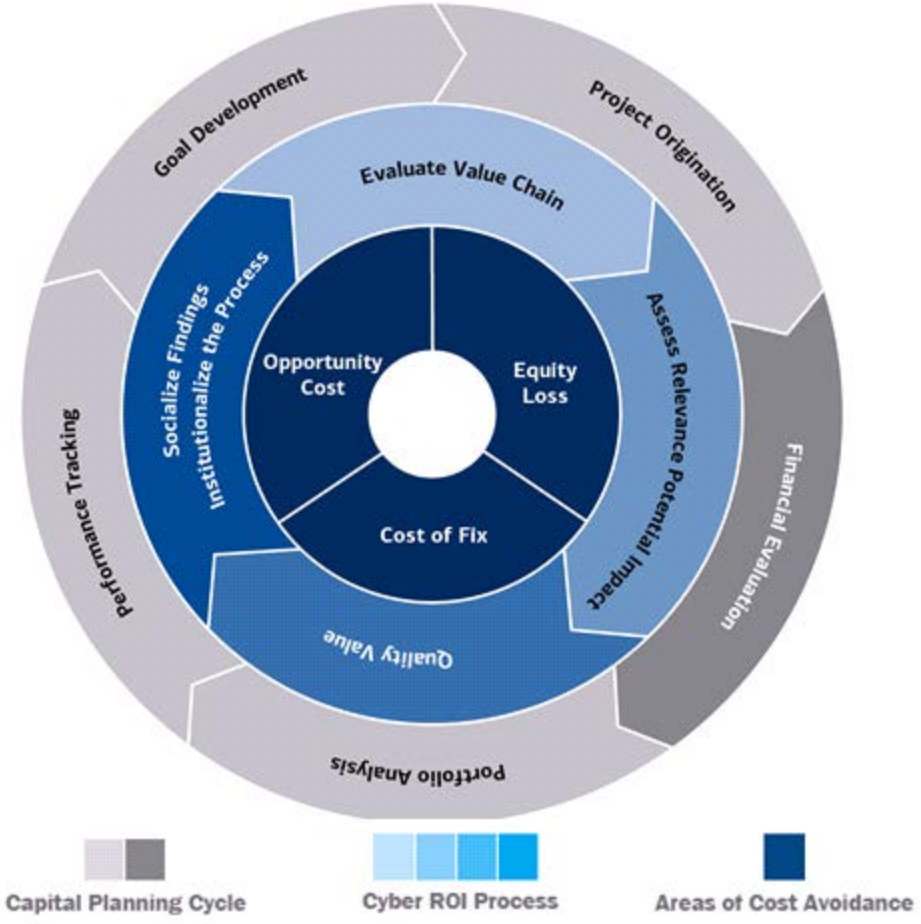
Company name	Date of announcement of cybersecurity breach	Negative drop in share price following breach (%)	
		Three days	One month
eBay	21-May-14	1.48%	7.35%
AOL	28-Apr-14	1.70%	23.56%
Target	19-Dec-13	2.41%	5.79%
Adobe	03-Oct-13	2.91%	4.04%
KT Corporation	29-Jul-13	1.30%	5.82%
Ubisoft	02-Jul-13	2.48%	2.48%
Betfair Group	30-Sep-11	13.67%	13.67%
Heartland Payment Systems	20-Jan-09	46.30%	49.54%
TK / TJ Maxx	17-Jan-07	1.82%	6.49%

Source: Slaughter & May

Cyber solutions ROI: huge financial benefits

Investments in cybersecurity make good business sense as the Pareto principle (80:20 rule) applies, with 80%+ of breaches avoidable through reasonable controls.

Exhibit 18: Cyber ROI planning cycle



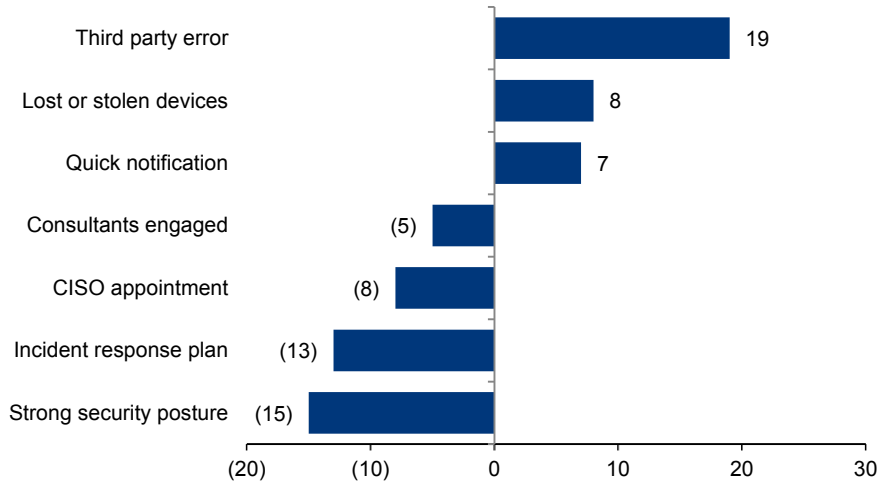
Source: Booz Allen Hamilton

The factors that impact the cost consequences

In the US – an incident response plan can reduce costs by up to $42 and strong security postures by $34

The Ponemon Institute has identified seven factors that the influence the cost consequences of a data breach – with third party errors, lost or stolen devices and quick notification increasing the per capita costs, and a strong security posture, incident response planning CISO appointments and consulting support decreasing the per capita cost.

Chart 30:Impact of seven factors on the per capita cost of data breach

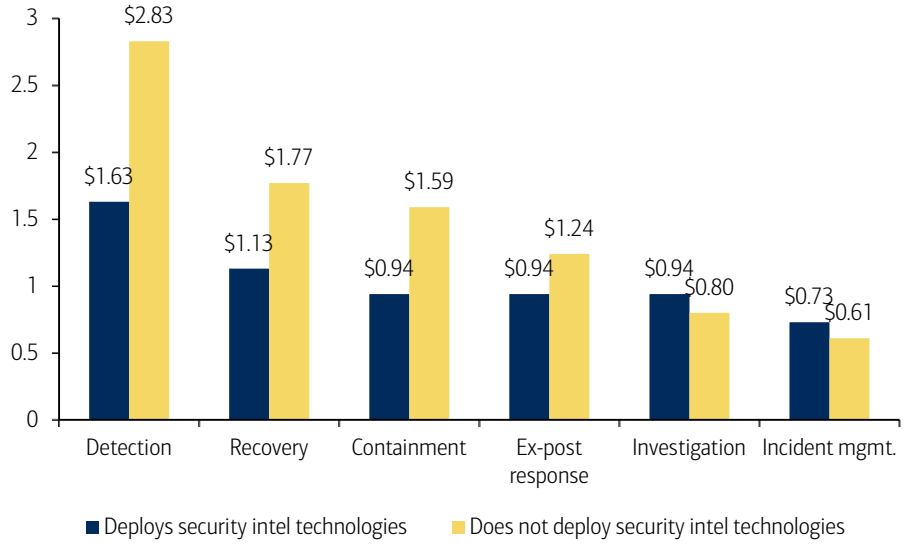


Source: Ponemon Institute, BofA Merrill Lynch Global Research

Stronger security measures = lower losses

Organisations deploying cybersecurity intelligence technologies realise a lower annualized cost of cybercrime. The largest cost differences pertain to detection, recovery and containment activities (Source: Ponemon Institute for HP Enterprise Security).

Chart 31: Activity cost comparison and the use of security intelligence technologies



Source: Ponemon Institute for HP Enterprise Security , BofA Merrill Lynch Global Research

Among the most seven commonly deployed security technologies - security intelligence systems and access governance tools facilitated the most substantial cost savings. In terms of the estimated ROI realised by companies, security intelligence systems ranked highest (21%), followed by extensive deployment of encryption technologies (18%) and advanced perimeter controls and firewall technology (14%).

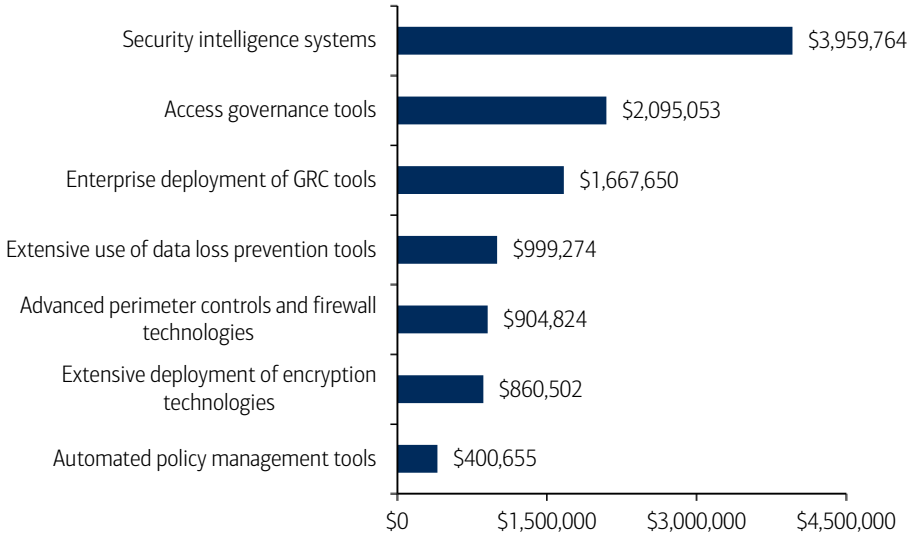
Bank of America Merrill Lynch

Table 18:Estimates ROI for seven categories of enabling security technologies

Security technologies	ROI
Security intelligence systems	21%
Extensive deployment of encryption technologies	18%
Advanced perimeter controls and firewall technologies	14%
Access governance tools	11%
Extensive use of data loss prevention tools	10%
Enterprise deployment of GRC tools	6%
Automated policy management tools	5%

Source: Ponemon Institute Research, BofA Merrill Lynch Global Research

Chart 32:Cost savings when deploying seven enabling security technologies



Source: Ponemon Institute Research, BofA Merrill Lynch Global Research

Companies need to adopt a lifecycle cost approach

There is a need for a proactive approach to cybersecurity from all stakeholders given the rising complexity and volume of threats. Organisations need to consider both the potential benefits and costs of their approach to Information Security with a holistic approach like the 'Total Lifecycle Cost of Information Security' model.

Table 19: Total lifecycle cost of Information security

Definition	Total Lifecycle Cost of Information Security	=	Lifecycle costs of deploying and operating security solutions	+	Reputational value	+	Intellectual Property value	+	Operational effectiveness	+	Financial impact of incidents
			Hardware/ software solutions Training Consultancy costs People costs		Brand volume Customer satisfaction/ confidence		R&D information Customer databases Competitive information		Productivity Ability to service customers Cost to serve customers		Direct financial loss from attack

Source: PwC, BofA Merrill Lynch Global Research

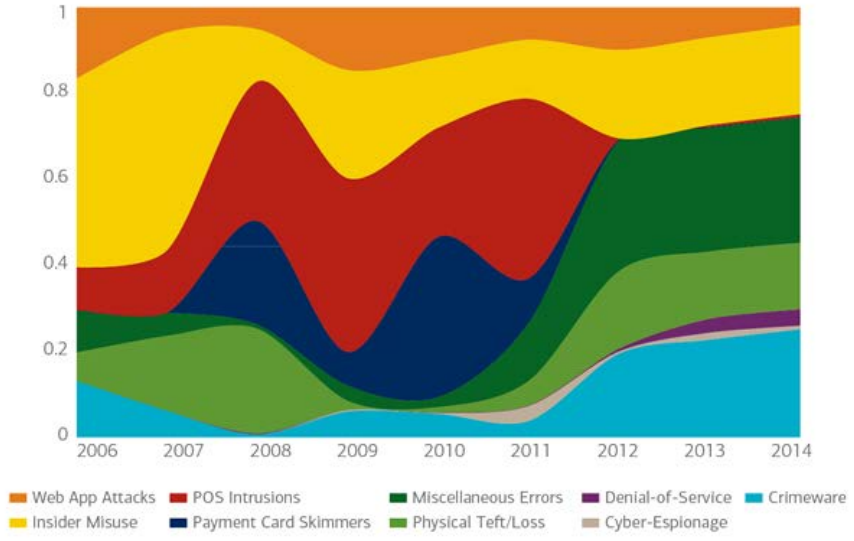
Threatscape: the "bad guy" is already on the inside

The cybersecurity "threatscape" encompasses the threat agents and attack vectors within the broad ICT domain. There have been 81-91mn+ cybersecurity incidents per year in recent years, or the equivalent of 222,856-251,415 incoming attacks per day. Worryingly, up to 71% of attacks are thought to be undetected, while only 31% of organisations are able to uncover intrusions internally. Advanced cyberattacks are also becoming increasingly sophisticated and challenging to detect – the bad guys are already on the inside – and are present on victims' networks for an average of 205 days before being picked up.

Cyber threats are coming from a growing number of actors including hostile governments, terrorist groups, disgruntled employees, and malicious intruders and insiders, among others. "Insiders" are the #1 threat accounting for 55% of incidents in 2014. In terms of external attackers, relatively small-scale criminal attacks have been the #1 threat with financial gain and ROI of up to 1,425% being the main motivation. We see significant growth in "homeland security" threats by and against nation-states and critical infrastructure, including espionage, cyberwarfare, hacktivism, and terrorism.

Cyber threats are set to continue to grow in sophistication. Malware, spam and phishing remain the most frequent threats, with the number of malware threats hitting 400mn in Q1-15. These irritating but controllable attacks are being superseded by a new wave of high-profile network attacks such as DDoS (distributed denial of service), which bring down websites and ICT systems and were the #1 network attack vector in 2014. Going forward, "nextgen" threats of increasing and unprecedented sophistication are likely to pose the greatest risk including zero-day attacks (for which there is no known patch or fix), advanced persistent threats (APTs), attacks against social media and networks, the IoT, cloud, and smart/connected devices, as well as cyber-espionage.

Exhibit 19: Rapidly changing cybersecurity threatscape, 2006-2014



Source: Verizon

Threatscape: events/incidents/attacks, agents and vectors

We provide a short summary of cybersecurity events/incidents/attacks, agents and vectors to give an understanding of the cyber threatscape.

Events, incidents and attacks: what are the threats

Distinctions can be made between cyber events, incidents and attacks, which IBM defines as follows:

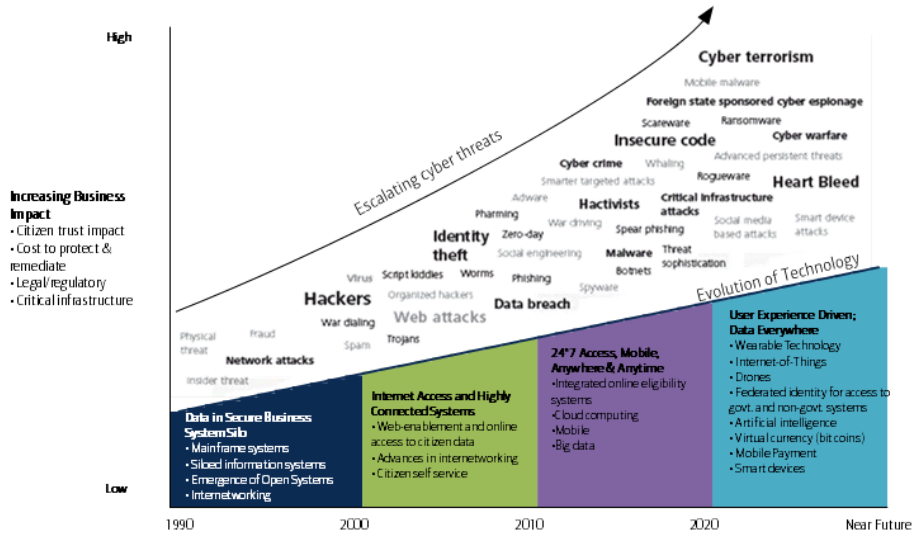
Bank of America Merrill Lynch

i) **Events**: occurrence on a system or network detected by a security device or application;

ii) **Incidents**: an event that has been reviewed and deemed worthy of deeper investigation; and

iii) **Attacks**: an event or incident that has been identified as malicious activity that is attempting to collect, disrupt, deny, degrade or destroy IT system resources.

Exhibit 20: Evolving technology and rapidly escalating cyber threats

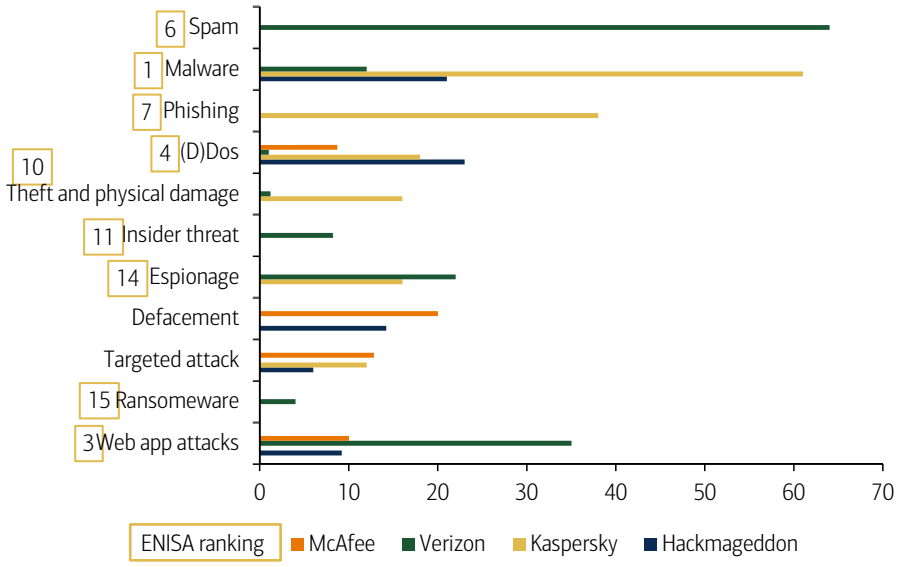


Source: Deloitte

From malware to DDoS to nextgen threats

Malware, spam and phishing, all of which are fairly common across the ICT domain, are the top 3 current cyber threats according to a collation of studies by the main players in the cybersecurity space (source: HCSS). However, after malware, distributed denial of service (DDoS) attacks are the most worrisome threat according to ENISA's ranking system, explained by their disruptive nature (eg, crashing websites, overloading servers). We are also seeing a new wave of nextgen threats, which we explore in greater detail below.

Chart 33: Comparison of top cyber attack tools & techniques by major bodies



Source: HCSS based on McAfee, Verizon, Kaspersky and Hackmageddon

2014 saw an escalation in almost all threats and against all platforms

On a more granular trend level, the #1 threat in 2014 was malicious code such as worms and trojans, which moved up from the #2 spot in 2013 (source: ENISA). The general trend in 2014 was an escalation in all threats across all platforms.

Table 20: Threatscape by trend in 2014

Rank	Threat	Current Trends	Cyber-Physical Systems and CIP	Mobile Computing	Cloud Computing	Trust Infrastr.	Big Data	Internet of Things	Netw. Virtuali-sation	Change in ranking vs 2013
1	Malicious code: Worms/Trojans	▲	▲	▲	▲	▲		▲	▲	↑
2	Web-based attacks	▲	▲	▲	▲	▶		▲		↓
3	Web application attacks /Injection attacks	▲	▲	▲	▲	▲		▲	▲	→
4	Botnets	▼		▲	▲					↑
5	Denial of service	▲	▲		▶	▶		▲	▲	↑
6	Spam	▼	▲							↑
7	Phishing	▲		▲		▲	▲	▲	▲	↑
8	Exploit kits	▼		▲		▲		▲		↓
9	Data breaches	▲			▲		▲		▲	↑
10	Physical damage/theft /loss	▲	▲	▲		▲	▲	▲	▲	↓
11	Insider threat	▶	▲		▲		▲	▲	▲	NA New Threat
12	Information leakage	▲	▲	▲	▲	▲	▲	▲	▲	↑
13	Identity theft/fraud	▲	▲	▲	▲	▲	▲	▲	▲	↓
14	Cyber espionage	▲	▲		▲	▲	▲		▲	→
15	Ransomware/ Rogueware/ Scareware	▼		▲						↓

Legend: ▼ =Declining ▲ =Increasing ▶ =Stable

Source: ENISA 2014

Agents: who's doing the attacking

As we highlighted earlier in the report, the range of agents and actors behind cyberattacks is expanding, driven by the ever-growing usage of technology by organisations. Threat agents encompass a range of insiders (careless and exploited employees and malicious insiders) and external actors (nation-state affiliated, organised crime, hackers, hacktivists, terrorists and companies.

Insiders are the #1 source of attacks

Insiders are the #1 threat. In 2014, 55% of attacks were carried out by insiders – actors with insider access (physical or remote) to an organisation's systems. Malicious insiders accounted for 31.5% and inadvertent actors 23.5% (source: IBM).

Criminals perceived as #1 threat to nation-states, foreign nations/war/terror #2

Criminals and organised crime groups are perceived as the #1 universal threat actor for nation-states which have outlined a national cybersecurity strategy (source: Luiijf et al 2013). However, the joint #2 threat actor is foreign nations/cyberwarfare and terrorists. Consequently, many countries view the future of cyber threat actors as global and see it as a homeland issue, which we analyse further in this report.

Table 21:Coutnries' perception of cyber threats from:

Country	Activism/ Extremists	Criminals/ Organized crime	Espionage	Foreign Nations/ Cyber War	Terrorists	Large scale attacks	Mismatch of Technology and Security
AUS		●	●		●		
CAN		●	●	●	●	○	
CZE		●		●	●		
DEU		●	●	●	●	●	●
ESP	○	●	●	●	●	○	
EST		●		●	●		
FRA		●	●	●	●		
GBR	●	●	●	●	●	●	
IND		●		●		○	
JPN		○	○	●		●	●
LTU		●				●	
LUX		●					
NLD	●	●	●	●	●		
NZL	●	●	●		●		
ROU	●	●	●	●	●		
UGA		●		●	●	○	
USA		○	●	●	●	○	
ZAF		●					
Count	5	18	11	13	13	9	2

Source: HCSS based on Luiijf et al 2013
NOTE: ● – EXPLICITLY DEFINED; ○ – IMPLICITLY REFERENCED

Agents are using all threat vectors

Agents use all the main cyber threat vectors to attack victims, as illustrated in the table below. The one exception is "ransomware", which is mainly used by cyber criminals for small-scale financial gain (source: ENISA).

Table 22: Involvement of threat agents in the top threats

	Threat Agents								
	Corporations	Nation States	Hacktivists	Cyber Terrorists	Cyber Criminals	Cyber Fighters	Script Kiddies	Online Social Hackers	Employees
Malicious code: Worms/Trojans	✓	✓	✓	✓	✓	✓			✓
Web-based attacks	✓	✓	✓	✓	✓	✓		✓	
Web application attacks /Injection attacks	✓	✓	✓	✓	✓	✓	✓		
Botnets			✓		✓				
Denial of service	✓	✓	✓	✓	✓	✓			
Spam				✓	✓	✓	✓	✓	
Phishing	✓	✓	✓	✓	✓	✓	✓	✓	✓
Exploit kits		✓	✓	✓	✓	✓	✓		✓
Data breaches	✓	✓	✓	✓	✓	✓	✓		✓
Physical damage/theft /loss	✓	✓	✓	✓	✓	✓			✓
Insider threat	✓	✓	✓	✓	✓	✓			✓
Information leakage	✓	✓	✓	✓	✓	✓	✓	✓	✓
Identity theft/fraud	✓	✓	✓	✓	✓	✓	✓	✓	✓
Cyber espionage	✓	✓							✓
Ransomware/ Rogueware/ Scareware					✓				

Source: ENISA

Vectors: how they are attacking

Cyberattack vectors are the paths or methods by which an attacker implements an attack or the "how" in the cybersecurity risk process. As the threatscape has evolved, so have the vectors, which now come from multiple angles and increasingly target an organisation's most valuable assets (eg, intellectual property, national security details).

Table 23: Multiple vectors combine to target an organization's valuable assets

Spear Phishing	⇨	CFO	⇨	Financial Information
Web-Based Attach	⇨	Director of Engineering	⇨	Intellectual Property
File-Based Attach	⇨	Government Employee	⇨	National Security Info

Source: RSA, FireEye

Four main attack vectors: more unknown, sophisticated and persistent threats

The concept of attack vectors can differ according to the stakeholder attacked and there is no one catch-all definition. That said, there are four main attack vector categories, which are the most frequent and documented cases, as outlined below. Overall, the main change in the cyber vector landscape is the move from known threats to those which are unknown, sophisticated and persistent in nature.

- **Targeted attacks** are based on some specific knowledge about the victim/target. They normally entail the perpetrator "baiting" the victim via specifically coded messages that are tailored. The main threat form of this vector is via spear-phishing, which uses trending real-life relatable events to lure the victim.

- **Drive-by attacks** entail the victim visiting a manipulated, but legitimate, website/page/application whereby he or she is then redirected or "injected" with malware, often unknowingly. The main threat form comes from HTML links and applications/add-ons which often exploit weaknesses in the system, such as outdated software patches.

- **Watering hole attacks** are a combination of targeted and drive-by, in that they target a certain group of users unknowingly when they visit websites – the embedded malware then installs automatically onto the host machine. In addition, watering hole attacks are known as "strategic web compromise" (SWC) in that the main difference from a drive-by attack is that SWC starts with reconnaissance of a target group of users. Hence, one motivation for these attacks can be espionage.

- **Advanced persistent threats (APTs)** refer to narrowly targeted campaigns performed by threat agents with high capabilities often over a long period. As the most complex vector, the threat types of these attacks are often unknown and tend to evade the cybersecurity perimeter altogether. The main motivations behind APTs are espionage and sabotage, often conducted by those with high cyber capabilities. The huge amount of resources and planning required means state-affiliated agents are the main actors in this space. We outline the full risks associated with APTs in much greater detail later in this report (source: ENISA).

"Kill-chain" framework: different threats operate across different spectrums

Another way of understanding the more advanced cyber threats is via the "kill chain", a term coined by Lockheed Martin, which describes seven categorised flow stages of a cyberattack via the information used by hackers. As illustrated in the table below, different cyber threats operate across different spectrums of the chain, with some being broader than others. However it is important to stress that the framework is not universally accepted as a one-size-fits-all method to model cyber threats.

Table 24: "Kill-chain" framework to describe stages of cyber attacks

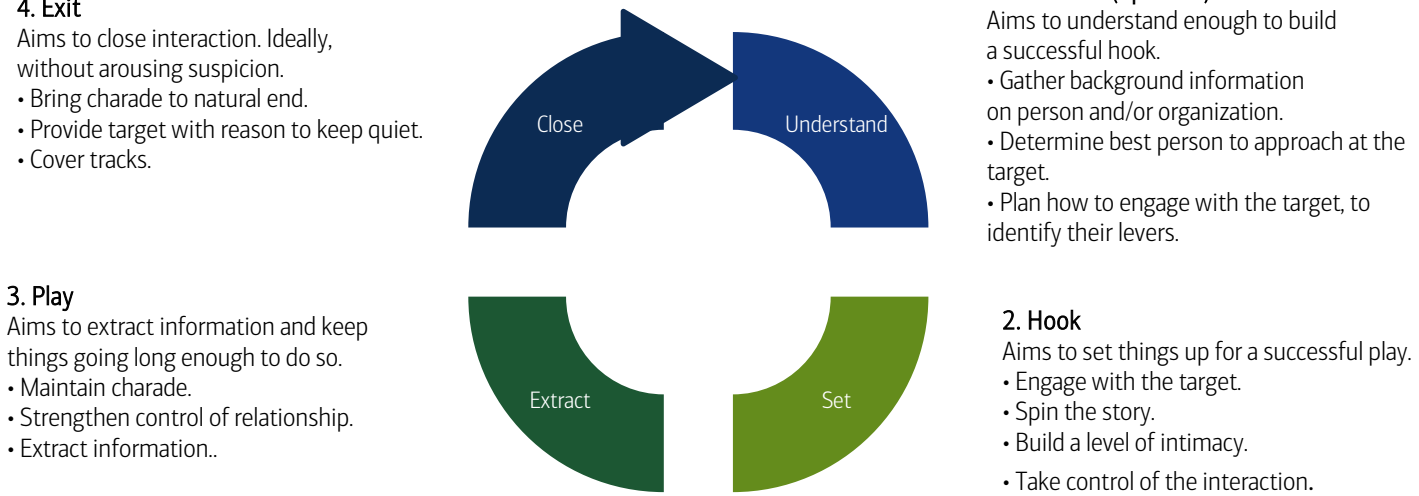
	Reconnaissance	Weaponization	Delivery	Exploitation	Installation	Command and Control	Actions on Objectives
Malicious Code: Worms/Trojans					✓	✓	✓
Web based attacks		✓	✓	✓			
Web application/Code injection	✓			✓	✓		
Botnets						✓	
Denial of Service	✓	✓				✓	✓
Spam		✓	✓	✓	✓		
Phishing	✓	✓	✓				
Exploit Kits		✓	✓	✓	✓		
Data Breaches	✓	✓	✓	✓	✓	✓	✓
Physical damage/theft & loss				✓			✓
Insider threat	✓	✓	✓	✓	✓	✓	✓
Information Leakage	✓	✓	✓	✓			✓
Identity theft/fraud	✓	✓	✓				✓
Cyber espionage (Targeted attacks, APT)	✓	✓	✓	✓	✓	✓	✓
Ransomware/Rogueware/ Scareware			✓	✓	✓		✓

Source: ENISA

Social engineering emerging as common theme among attack vectors

Social engineering is defined as the manipulation of individuals in order to induce them to carry out specific actions or to divulge information that can be of use to a cyber attacker. The increasing use of social engineering is a key driver of the threatscape as hackers exploit human trust to access systems (especially vis-à-vis insiders). Attackers do not necessarily need advanced tools as they can simply "hack the human operating system" according to McAfee.

Chart 34: The four phases of social engineering

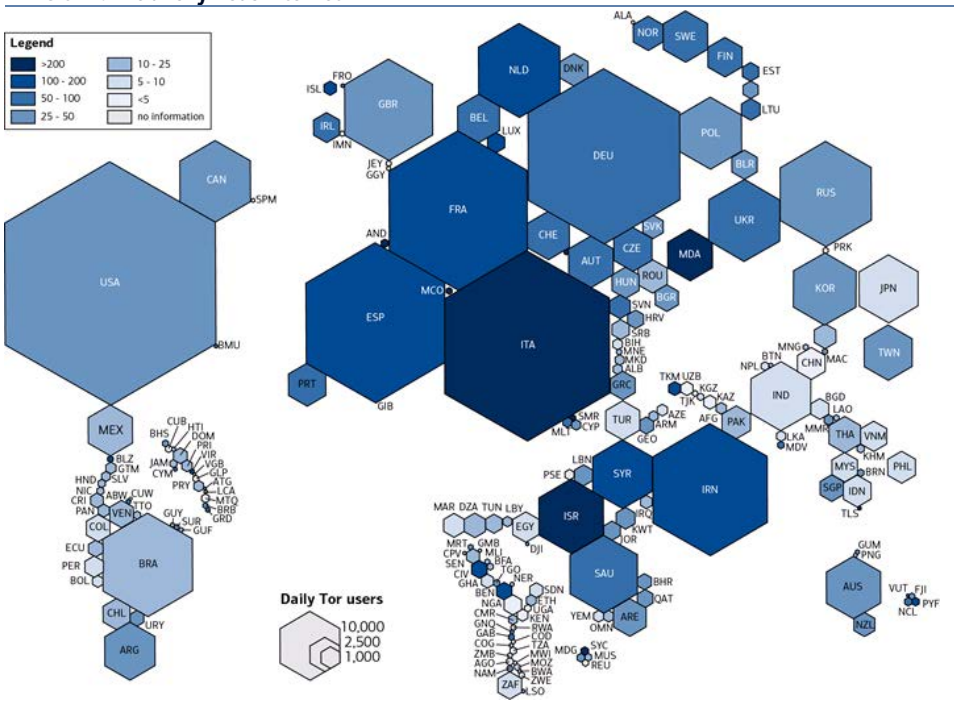


Source: McAfee

Dark side of cyberspace is the breeding ground

One key platform for hackers is the "darknet", which is the space in network domain where users operate anonymously, often conducting illegal activities, and which is not easily accessible to your everyday Internet user. The "darknet" is also referred to the as the "dark web" or "Tor" (The Onion Router), the latter being the most popular software program to access this domain. Tor is used globally by over 750,000 Internet users every day, with over half of being located in Europe - or an average of 80 per 100,000 European Internet users (source: Oxford Internet Institute).

Exhibit 21: The anonymous Internet



Source: Oxford Internet Institute,

Unsurprisingly, the United States has the highest average number of users per day, with over 126,000 people accessing the Internet through Tor. However, relative to its Internet population, Italy has one of the highest daily Tor users a day at 76,000 - one fifth of the entire European daily user base. Tor is also particularly popular in Israel, which accounts for more Tor users than India, while having less than 4% of its Internet users. It is also popular in Iran, which accounts for the largest number of Tor users outside Europe and the United States (source: Oxford Internet Institute).

Traditional threats, a pesky but controllable breed

Malware, spam and phishing, all of which are fairly common across the ICT domain, are the top 3 current cyber threats (source: HCSS). These are often seen as the traditional cyber threats, often seen as a nuisance rather than truly serious as to cause alarm. Although they can usually be detected by basic software such as firewalls, anti-virus software, one should not underestimate their potential to cause damage especially given that new variants crop up every so often.

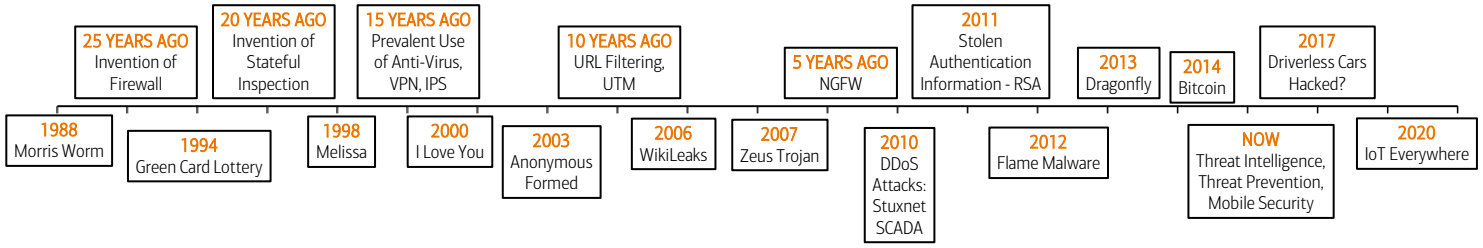
> Malware threats hit the 400mn mark in 1Q15 vs. 200mn (1Q14) and 100mn (1Q13) - McAfee

Malware: 400mn threats at Q1-15 and #1 most common threat

Malware, or malicious code, is perhaps the most common "basic" cyber threat and is a catch-all term that encompasses different attack vectors from botnets to viruses. It is software used or created to disrupt computer operation, gather sensitive information, or gain access to private computer systems.

Bank of America Merrill Lynch

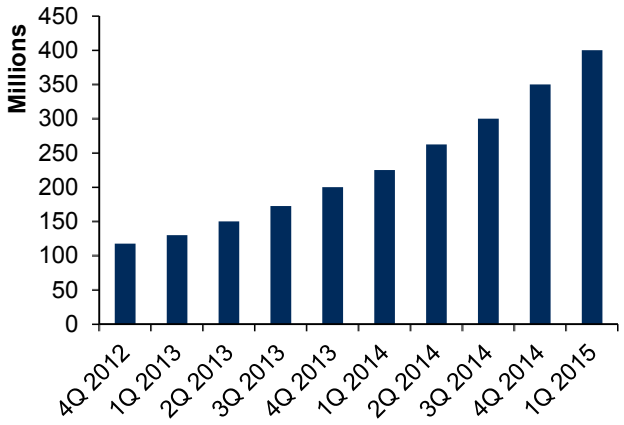
Chart 35: The Evolution of Malware



Source: Check Point, BofA Merrill Lynch Global Research

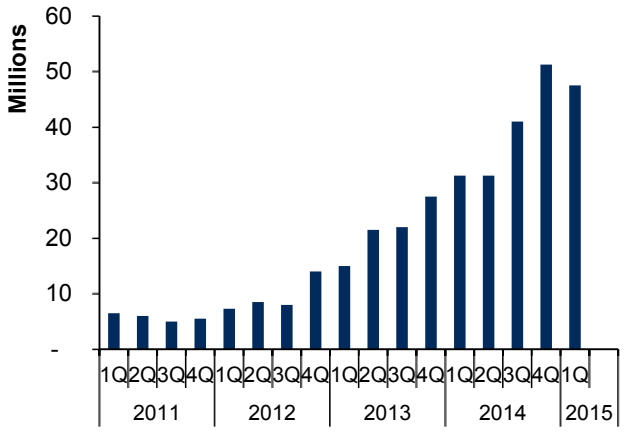
IT users are likely to have come across malware in some form or another due to its pervasiveness. Malware threats hit the 400mn mark in Q1-15 (vs 200mn in Q1-14 and 100mn in Q1-13) (source: McAfee).

Chart 36: Total malware samples in the McAfee labs database



Source: McAfee Labs Database, BofA Merrill Lynch Global Research

Chart 37: New malware database



Source: McAfee Labs Database, BofA Merrill Lynch Global Research

Malware universe

The following are examples of the most common types of threats within the malware universe:

- **Adware** or advertising-supported software automatically delivers advertisements to host machines. Common examples include pop-up ads on websites and advertisements with software attached.
- **Spyware** involves monitoring and harvesting data in a host machine and feeding this information back to the hacker. Common applications include stealing login details and passwords.
- **Trojan** is a type of malware that disguises itself as a normal file or program to trick users into downloading and installing malware. Once installed, its malicious features are fairly similar to a "rootkit" (see section below)
- **Viruses** replicate themselves and spread to other computers from the infected machine. Common transmission methods are email attachments and URL links.
- **Worms** are similar to viruses in many ways but differ in that they can spread without any human action, by taking advantage of system networks (source: Veracode).

Table 25: Top five biggest virus of all time

Year	Virus Name	Description	How it worked	Spread	Spreading time	Damages ($bn)	PCs Infected
2004	Mydoom	A worm that spread through email as what appeared to be a bounced message.	When the unsuspecting victim opened the email, the malicious code downloaded itself and then pilfered the new victim's Outlook address book.	From there, it spread to the victim's friends, family and colleagues. It spread faster than any worm seen prior.	10 minutes	$38	2,000,000
2003	Sobig.f	A worm that replicates itself, but also is a Trojan, as it disguises itself as something other than malware.	Once the user opened the email, it triggered the worm, which then went hunting for addresses.	The flood of messages it then sent were capable of succumbing other users' inboxes or computer systems by the sheer volume of emails. It briefly brought down freight and computer traffic in Washington, D.C. to a halt, grounded Air Canada and slowed down computer systems at many major companies.	2 Hours	$37.1	2,000,000
2001	Code red	A worm that exploited an operating system vulnerability in machines running Windows 2000 and Windows NT.	This allowed it to deface and take down some websites, most memorably the whitehouse.gov website and forced other government agencies to temporarily take down their own public websites as well.	The worm spread by randomly selecting 100 IP addresses at a time, scanning the computers for the Microsoft system and then spreading only to those computers	14 Hours	$2.6	1,000,000
2000	I love you	An innocent looking email attachment labeled "I Love You".	When opened, it unleashed a malicious program that overwrote the users' image files. It was designed to steal Internet access passwords.	The virus emailed itself to the first 50 contacts in the user's Windows address book.	9 Hours	$15	500,000
2003	Slammer	An Internet worm (also called Sapphire) that caused a denial of service on some Internet hosts and dramatically slowed down general Internet traffic.	It worked by releasing a deluge of network packets, units of data transmitted over the Internet, bringing the net on many servers to a near screeching halt.	As it began spreading throughout the Internet, it doubled in size every 8.5 seconds. It selected IP addresses at random to infect, eventually finding all susceptible hosts. Among its list of victims was Bank of America's ATMs, a 911 emergency response system in Washington State, Continental Airlines and a nuclear plant in Ohio.	96 Hours	$1.2	200,000

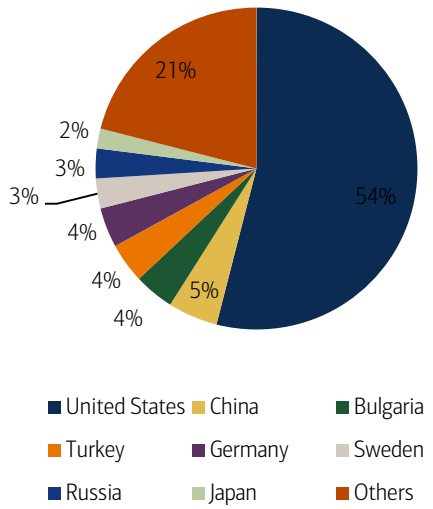
Source: Symantec Norton

Spam: 28bn/day & #1 nuisance threat

Spam is normally more of a nuisance for victims such as in the form of junk mail, but it can be more malicious if it contains malware or is used for phishing purposes. The estimated global spam volume per day was 28bn in 2014, which is down from 30bn in 2012 (source: Symantec). The overall spam rate dropped to 49.7% in June 2015, the first time it has fallen below 50% of total email volume in over a decade, according to Symantec's database. Overall, despite the generally declining volume of spam in recent years, it remains one of the most common cyber threats with scope to inflict damage on victims who are not vigilant on cybersecurity.

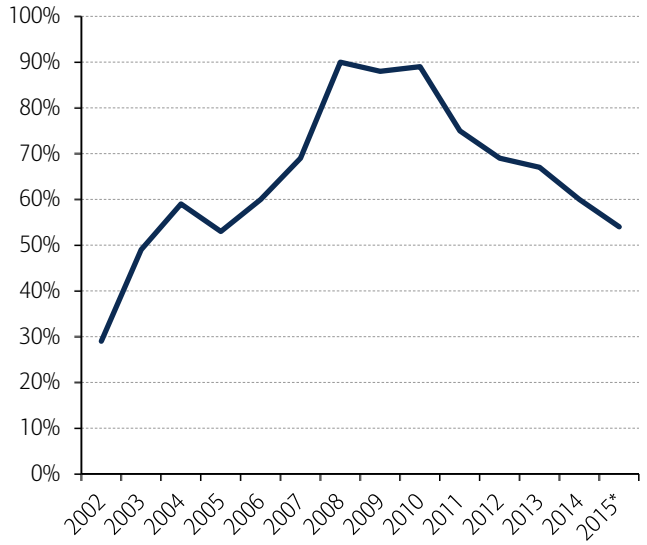
> The estimated global spam volume per day was 28 billion in 2014, vs. 30 billion in 2012 (source: Symantec).

Chart 38: Top countries hosting spam domains



Source: McAfee

Chart 39: Average email spam rates by year



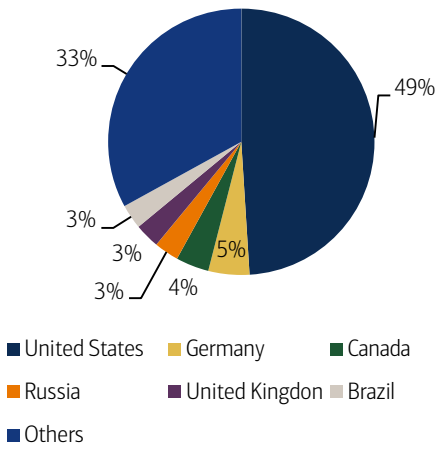
Source: Symantec

Phishing: declining but emergence of higher-risk spear phishing

Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details, often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication such as email. Phishing essentially expands on the threat capabilities of spam mail, with the main intention to steal confidential details rather than be a nuisance. For instance, a common phishing practice is to trick victims into a false payment via their PayPal account to cybercriminals. However, like spam, phishing volume trends are declining as actors increase their sophistication in other areas of the cyber threatscape.

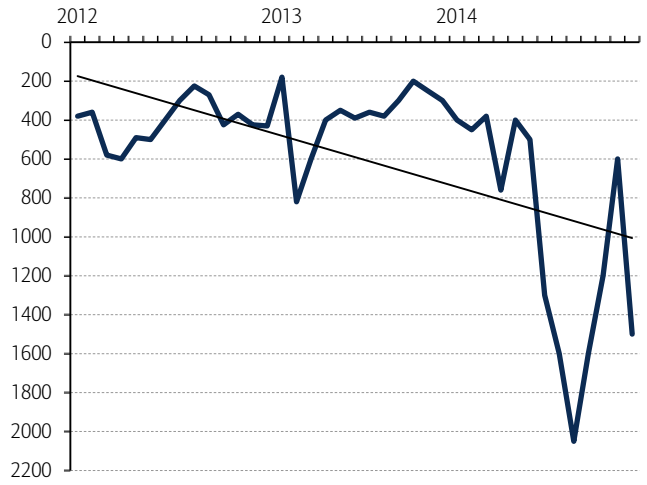
> The phishing rate decreased from 1 in 392 (2013) to 1 in 954 emails (2014) - Symantec

Chart 40: Top countries hosting Phishing domains



Source: McAfee

Chart 41: Phishing Rate, 2012-2014



Source: Symantec Smaller number = Greater Risk

Emergence of spear phishing: poses a great risk

However, the emergence of "spear phishing" highlights how this type of threat can grow in complexity. It is more targeted than traditional phishing campaigns because it combines more relatable information that pertains to the victim. This form of phishing poses a greater threat because it employs social engineering techniques to entice users and takes a traditional threat to a higher risk level.

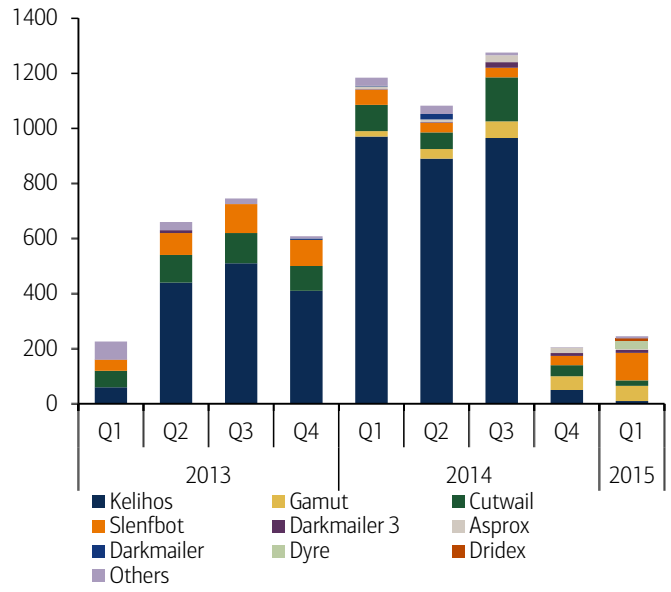
Exhibit 22: Spear-phishing email word cloud: most commonly used words in attacks

Source: Symantec

Botnets: leading the way on attack count but subject to crackdown

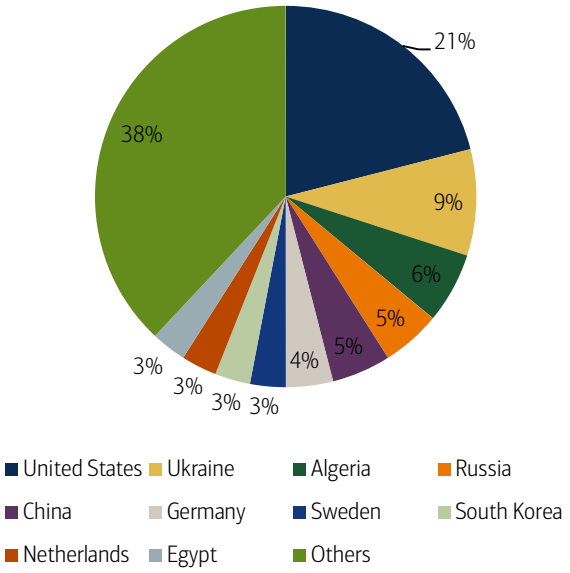
Botnets are software programs that can automatically perform specific malicious actions. Many bots can be combined to create "botnets", which is a collection of zombie computers that is controlled by a third party "command & control" centre to launch a concerted attack. Common examples of botnets in operation are coordinated spam email attacks, used to launch DDoS attacks. Bots can inflict substantial damage ranging from stealing bank credentials to opening the backdoor to further attacks, which was the main threat activity in 2014.

Chart 42: Spam Emails from top 10 Botnets



Source: McAfee

Chart 43: Top locations of Botnet Control Servers



Source: McAfee

83% of organisations hit by 1+ botnet

83% of organisations had at least one bot infection in 2014. 47% of those were active for more than four weeks – communicating with its command and control (C&C) centre every minute, according to Check Point's database. More worrying is that the speed and frequency of this progress represents a 95% jump from 2012 (source: Check Point). According to Check Point, the "Zeus" botnet and its variants had the highest attack count in 2014, primarily targeting the financial details of individuals.

> Bots communicate with their third party command and control centre every 1 minute – Check Point

Table 26: Top 10 Botnets in 2014

Family	Attack count	Damage
Zeus	51,848,194	Steals banking credentials
Graftor	21,673,764	Downloads malicious files
Ramnit	12,978,788	Steals banking credentials
Conficker	12,357,794	Disables system security services, gains attacker remote access
Sality	11,791,594	Steals sensitive information
Smokeloader	9,417,333	Installs malware
Ramdo	5,771,478	Performs click-fraud
Gamarue	3,329,930	Opens a backdoor for attacks
Torpig	3,290,148	Steals sensitive information

Source: Check Point

Law enforcement agencies cracking down

However, recent trends show botnet activity has declined, driven by international law enforcement agencies such as the FBI and Europol working with IT firms to disrupt and shut down the network. The most notable example in 2014 was the shutting down of the "Gameover Zeus" botnet (peer-to-peer variant), which was responsible for millions of infections worldwide since its arrival in 2011 (source: Symantec).

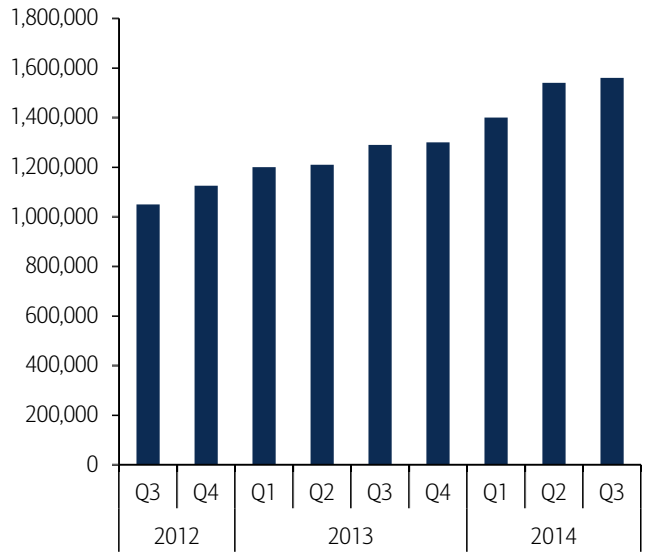
Toolkits: on the rise but increasing fragmentation of actors

Toolkits comprise software designed to remotely access or control a computer without being detected by users or security programs. When installed, third parties can steal sensitive information without the authorization of the user. Exploit kits and rootkits typically target software vulnerabilities associated with commonly used computer plugins such as Oracle Java, Adobe Reader & Flash and Microsoft Silverlight.

Arrest of Blackhole creator has fragmented the market

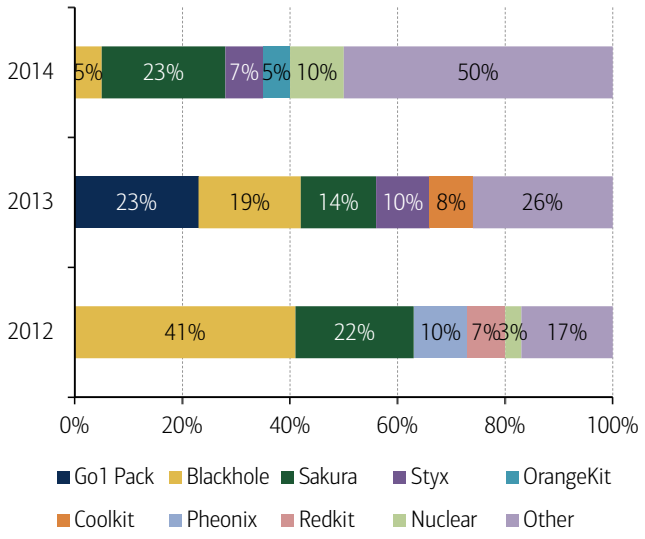
The total number of rootkits has risen steadily from just under 1.2mn to in 1Q13 to nearly 1.6mn by 1Q15 (source: McAfee). However, the most important development in this space is the change in the key vectors that make up this space. In 2012, the "Blackhole" exploit kit accounted for nearly 50% of all toolkit attacks and was widely considered to be the most prevalent threat on the web (source: Symantec). However, by 2014, its percentage share of the toolkit threatscape had tumbled to just 5%. This was partly driven by the arrest of the alleged creator of "Paunch" in late 2013, thus opening up the toolkit space for fragmentation of players.

Chart 44: Total Rootkit Malware



Source: McAfee

Chart 45: Top 5 web attack toolkits, 2012-2014

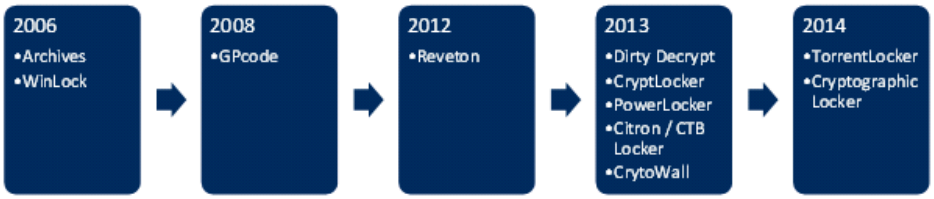


Source: Symantec

Ransomware: one of the most damaging tools used by attackers

Ransomware is a type of malware that enables criminals to lock your computer from a remote location and then claim that you will not be able to access your data until you pay them. The best defence against this attack is to keep a separate backup of files offline to restore from. The market is estimated to be worth US$150mn every year, according to the FBI. Although ransomware has been around the threatscape for some time, it has recently resurged as one of the most damaging tools used by attackers.

Exhibit 23: Timeline history of ransomware



Source: Trustwave

Bank of America Merrill Lynch

Attacks doubled in 2014 and are becoming more sophisticated and malicious

Ransomware attacks more than doubled from 4.1 million in 2013 to 8.8 million in 2014, representing a 113% increase (source: Symantec). This has been driven by so-called "crypto-ransomware", which is more sophisticated and malicious because rather than locking your desktop behind a traditional ransom wall, it encrypts your personal files and holds the private keys to their decryption for ransom at a remote site.

> "Crypto-ransomware" threats grew 45x from 8,274 in 2013 to 373,342 incidences in 2014 – Symantec

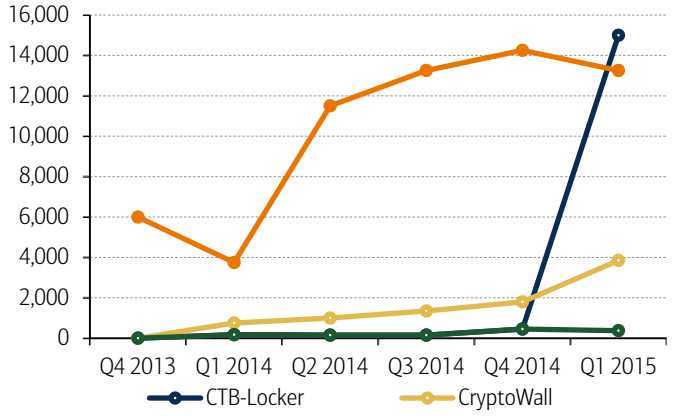
Worrisome rise in crypto-ransomware

One trending example of crypto-ransomware is the "CTB-Locker" virus, from which hackers claim to be making $15,000-$18,000 per month, with a net profit of $8,000-$10,000, and with 7% of all victims paying the requested ransom (source: McAfee). Uniquely, this threat forces users to pay the ransom to unblock the encryption in Bitcoin to avoid being traced or detected by the authorities.

Exhibit 24: Sample window of "CTB –Locker" ransomware window

Source: McAfee

Chart 46: New samples of prominent ransomware families



Source: McAfee

ROI of 1400%+

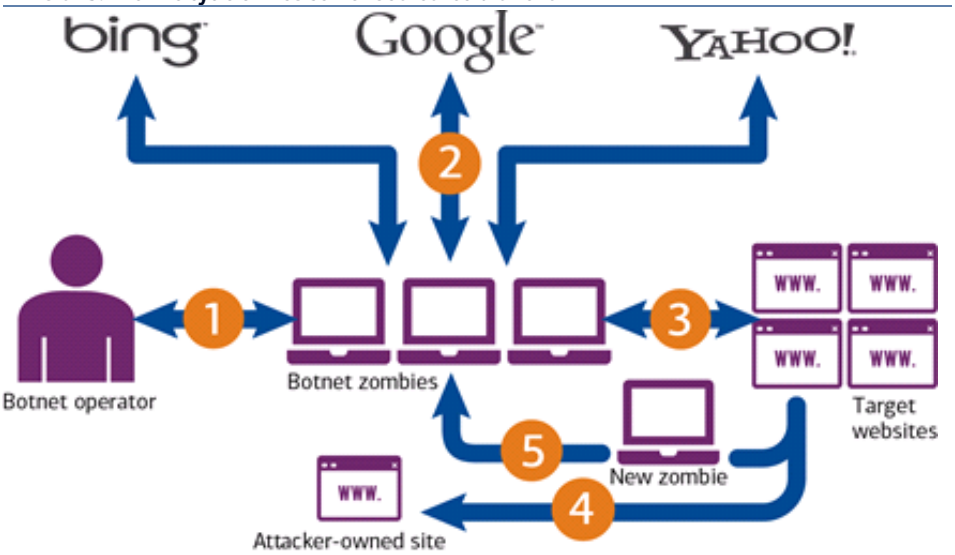
In addition, cyber criminals can generate up to a 1,425% return on investment (Source: Trustwave). From purchasing a ransomware toolkit at an average cost of $5,900, cybercriminals could potentially gain up to $90,000 in return in just one month, according to Trustwave's scenario analysis.

> "Cybercrime can potentially be a lucrative business, with up to 1500% return on investment from ransomware kit" - Trustwave

Network, web & hacking threats

Unlike many of the traditional threats such as malware, network, web and hacking attacks are more targeted and specific in nature as they seek to overwhelm host machines or servers with a sheer volume of traffic overload.

Exhibit 25: The Life cycle of web server botnet recruitment

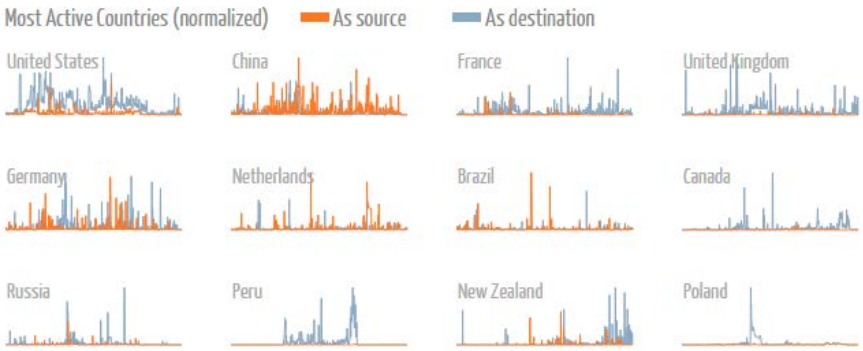


Source: Trustwave

Most big profile attacks are network attacks

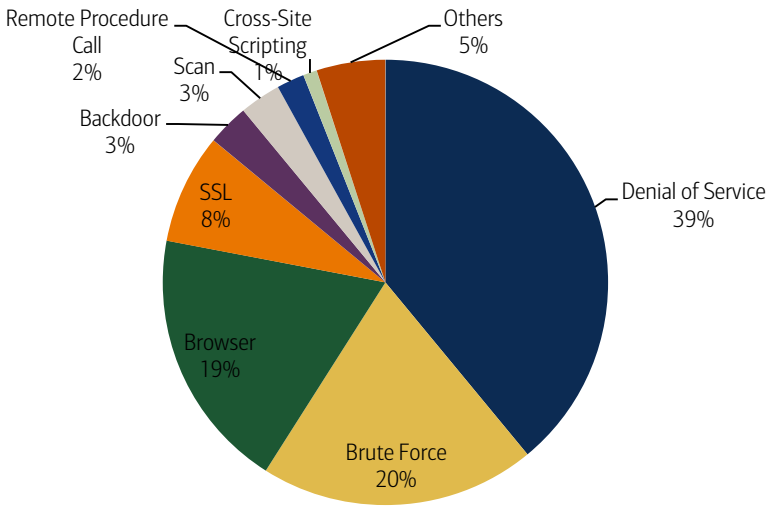
The majority of high profile cyber incidents where websites have crashed or been hijacked in recent years have come under this umbrella term of so-called "network attacks" e.g. JPMorgan and BofA in 2014. The most common network attacks are distributed denial of service (DDoS) attacks followed by brute force (exhaustively trying to break down a system's encryption) and browser attacks (source: McAfee). In terms of the source of these attacks, the lion's share comes from China with the United States the main victim, according to Arbor Networks' database. We outline how each networks attack works below:

Exhibit 26: Most active countries by network traffic attacks



Source: Digital Attack Map via Arbor Networks

Chart 47: Top Network Attacks

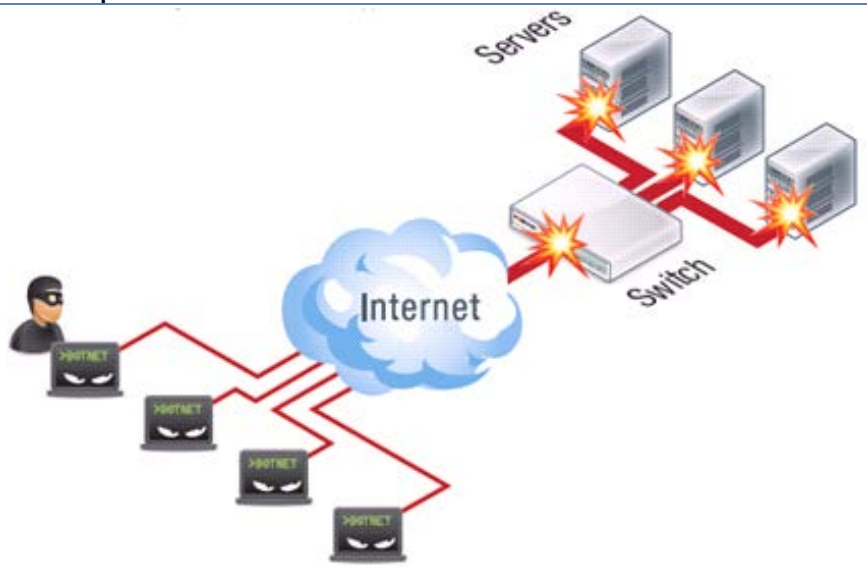


Source: McAfee

Distributed denial of service (DDoS) attacks: 39% of network attacks

Distributed Denial of Service (DDoS) attacks are an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources. They target a wide variety of important resources, from banks to news websites, and present a major challenge to making sure people can publish and access important information. This involves incoming traffic that comes from often thousands of unique IPs to crash the victim's machine via brute force. In 2014, DDoS attacks were the #1 network attack vector accounting for 39% of all attacks, according to McAfee database.

Exhibit 27: Example of DDoS attack on a network switch and servers



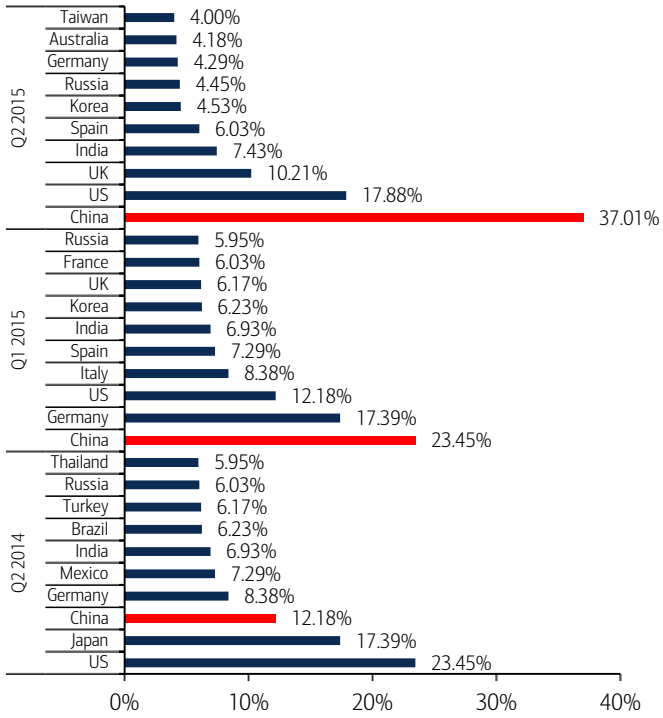
Source: Fortinet

48 DDoS attacks occurred every day in 2014 – Check Point

Driven by increasing bandwidth and hacktivists

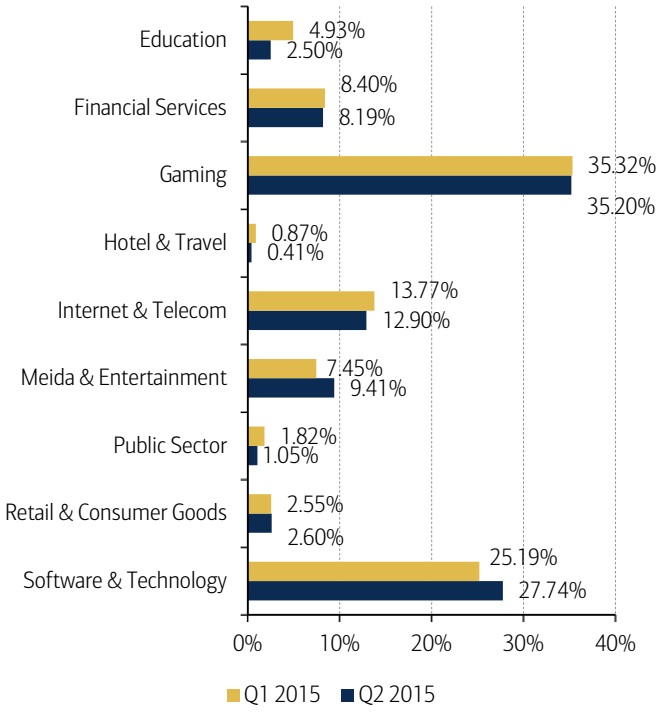
DDoS attacks are common among "script-kiddies" (please see Glossary for definition) and have recently been used by "hacktivists" to overwhelm the target's network. One example was when "Lizard Squad" brought down the PlayStation Network for gamers in mid-2014. We expect DDoS attacks to continue to grow driven by the increasing bandwidth of internet traffic usage. Gaming networks are the #1 sector hit by DDoS attacks, with China now the leading nation-state initiating this cyber threat – increasing from around one-tenth to one-third of the global share (source: Akamai).

Chart 48: Top 10 Source Countries for DDoS Attack by Quarter



Source: Akamai

Chart 49: DDoS Attack Frequency by Industry



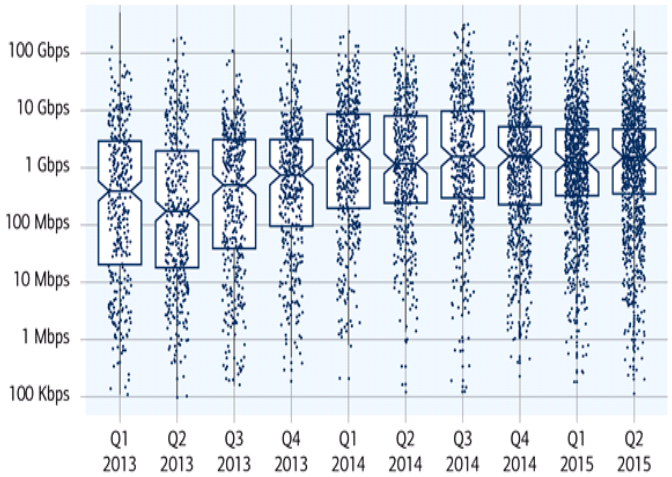
Source: Akamai

> "More than 2000 daily DDoS attacks alone are observed around the world"
> – Arbor Networks

Largest DDoS attack ever in 2014

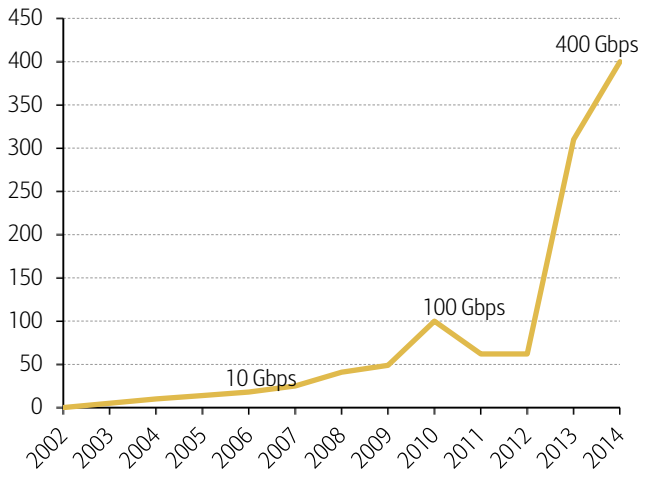
The traffic volume of network attack size has skyrocketed in the past two years. In 2012 the surveyed peak attack size was only just above 50 Gbps, but by 2014 this had ballooned to 400 Gbps – the largest DDoS attack ever by volume (source: Arbor Networks). The number of +100 Gbps "mega attacks" increased from just six in 2Q14 to 12 by 2Q15 (source: Akamai). Just like data breaches, the magnitude of DDoS attacks appears to be spiralling each year – an extremely worrying trend for defenders, in our view.

Exhibit 28: DDoS Size as a Function of Time



Source: Akamai

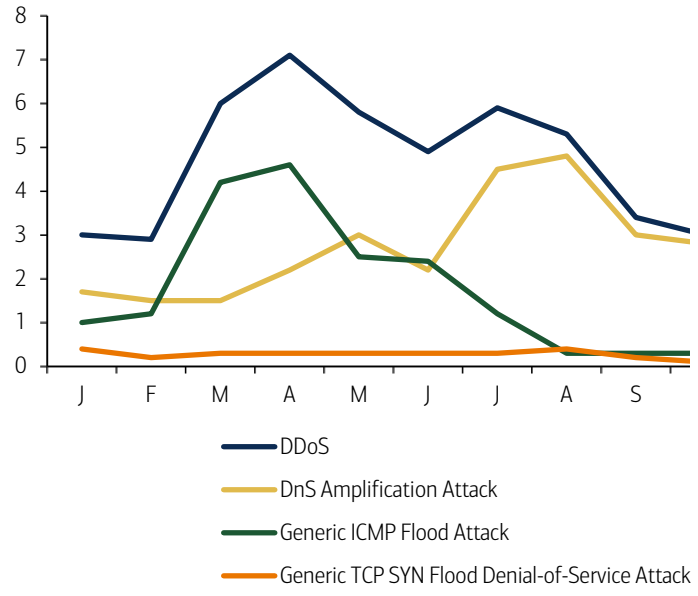
Chart 50: Survey peak attack size year over year



Source: Arbor Networks

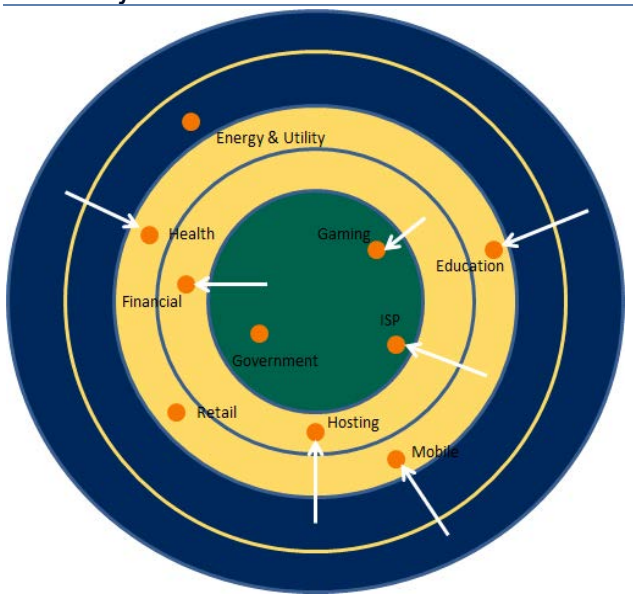
"1/3 of all network downtime incidents are attributed to DDoS attacks" - VeriSign

Chart 51: DDoS Attack Traffic seen by Symantec in 2014



Source: Symantec

Exhibit 29: Likelihood of industry being hit by DDoS attack in "ring of fire" of analysis



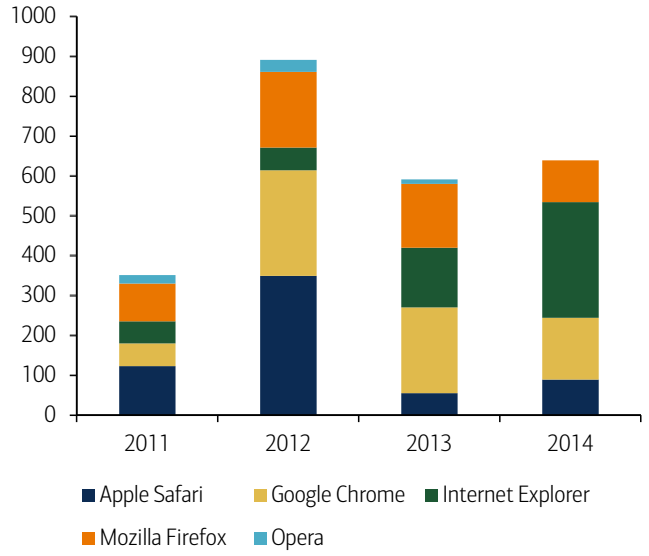
Source: Radware

→ Change from 2013

Browser vulnerabilities: Microsoft IE #1

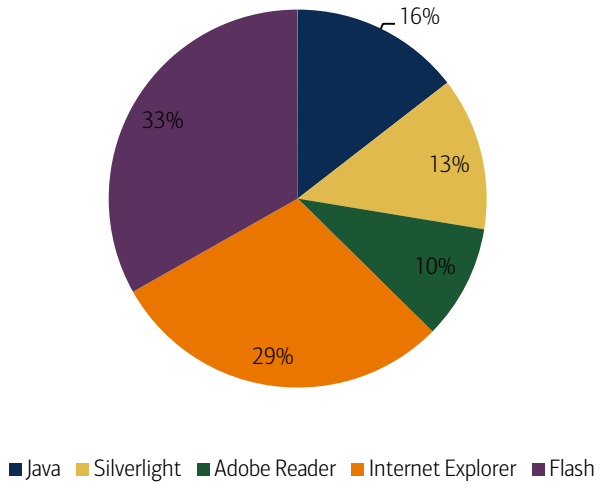
Microsoft's Internet Explorer was the web browser with the largest number of vulnerabilities in 2014, accounting for over half of reported incidences, according to Symantec's database. In contrast, Apple Safari has shrunk its percentage of vulnerabilities relative to the other five major browsers. In addition, the most exploited plug-in application that attackers use as a vector is Adobe Flash, which accounted for a third of total online vulnerabilities in 2014 (source: Trustwave).

Chart 52: Browser Vulnerabilities, 2011-2014



Source: Symantec

Chart 53: Most exploited plug-in applications



Source: Trustwave

Attacks also centre around websites' encryption certificates, such as OpenSSL, where discovery of the "Heartbleed" bug in 2014 exposed the vulnerability of a supposedly secure cybersecurity solution. It was estimated that Heartbleed affected 17% of SSL web servers, which use certificates issued by trusted authorities (source: Symantec). This was also a "zero-day" threat (unknown until detection), which we describe further in this report.

Table 27: Top 3 web vulnerabilities in 2014

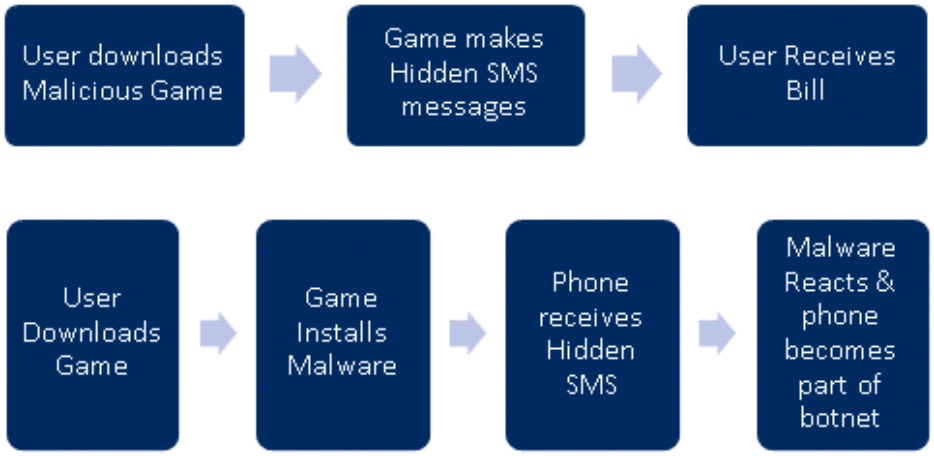
	Heartbleed	Shellshock	Poodle
Discovered	Apr-14	Sep-14	Oct-14
Type	SSL Bug	UNIX Shell Bug	SSL Bug
Affected systems	Any system using open SSL	UNIX, LINUX, OS X, clients and servers	Any clients or server using SSL v3
# of systems affected	Majority of the internet	Most of the internet and internal systems	Small % of the internet
Risk	Theft of SSL, encryption keys and data protected by those keys	Complete system takeover	DATA protected by SSL encryption
Severity	4/5	5/5	2/5
Ease of exploit	1/5	2/5	4/5
Fix/Difficult	Patch/Easy	Patch/Easy	Suspend use / Hand change code

Source: Imperva

Mobile & apps: apps & BYOD driving risks

The past few years have seen a huge explosion in mobile devices, smartphones and tablets globally – with an ensuing boom in attacks against them via rootkits, botnets, and other malware. Attackers have moved on from simple destructive malware to spyware and mobile malware that makes them money. We've seen attackers exploit vulnerabilities to bypass system protections and gain greater control over mobile devices. In 2014 the rate of growth of new mobile malware surpassed that of new malware targeting PCs (source: McAfee).

Exhibit 30: Two common mobile malware scenarios

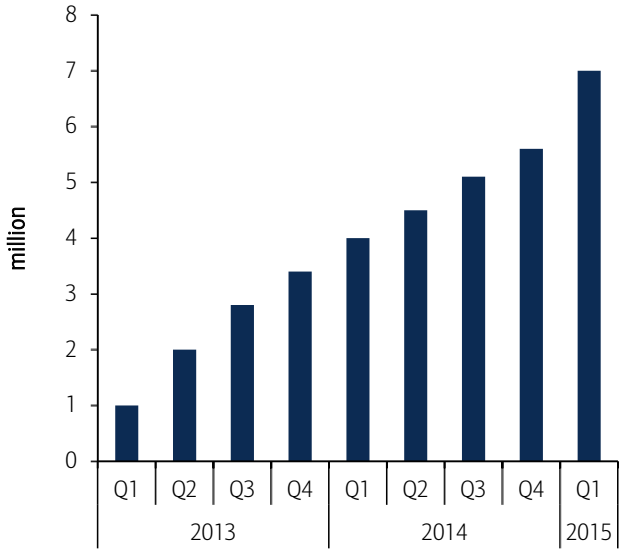


Source: Trustwave

Apps & BYOD devices will widen the threatscape

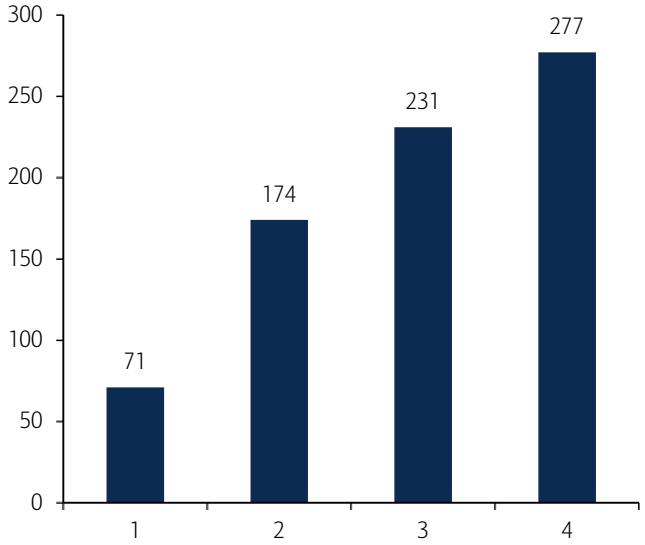
The adoption of personal and business communication apps will widen the platform for breaches, as will the use of personal devices in the workplace, with Bring Your Own Devices (BYOD) policies putting additional strain on enterprise infrastructure (source: McAfee, Sophos). The great majority of mobile attacks, and their malware, stem from and attack third-party markets, particularly in China and Russia. In addition, Kaspersky note that hackers are increasingly exploiting the growth of mobile banking apps, by installing trojans to steal financial assets and details.

Chart 54: Total mobile malware



Source: McAfee

Chart 55: Cumulative Android Mobile Malware Families, 2011-2014

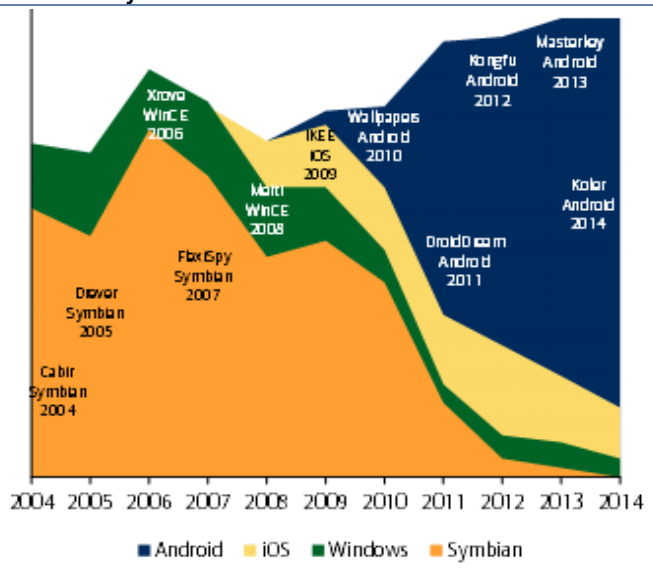


Source: Symantec

Android, #1 targeted mobile OS

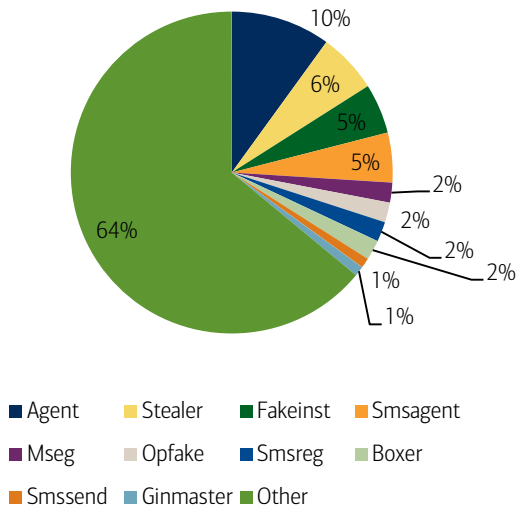
Malware on platforms running Android in particular has skyrocketed relative to other platforms such as iOS, Windows in recent years (source: HP). This is not surprising given that Android is the most commonly used mobile operating system globally on smartphones. However, more worrying is that less than 40% of Android devices had some kind of anti-malware solution installed vs more than 90% of Windows-operated mobile devices, according to HP. On the other hand, Symbian, which used to be the most exposed to mobile malware, has declined over the past decade, driven by fewer users on the platform who have migrated to other brands.

Exhibit 31: Ten years of mobile malware



Source: HP

Chart 56: Top Android malware families in 2014



Source: HP

iOS, attack surface is increasing

Since Google's Android forms the lion share of the mobile operating system on smartphones, Apple's iOS has relatively fewer cyber incidents and because of the stricter review process on their App Store, which isn't fully opened to developers unlike the Google Play Store. That said, Apple mobile devices are increasingly gaining traction as evidenced by the 2014 "Celebgate" iCloud incident, emergence of "cyberflashing" and the "biggest ever hack" of iPhone devices in late-2015 where 225,000 Apple account details on jailbroken devices were stolen (source: Palo Alto Networks). The top 6 cybersecurity threats, according to Check Point, going forwards for iOS devices are:

1. **Mobile remote access trojans (mRATs)** - these attacks jailbreak a device removing all the built-in iOS security mechanisms, and install surveillance and mRAT software that gives the attacker the ability to remotely gain access For example, in February 2013, a jailbreaking technique, nicknamed Evasi0n, garnered 7M hacked devices in just four days

2. **Fake developer certificates** - these attacks use distribution certificates to 'side-load' an application (with malware), which means it does not have to go through Apple's app store validation process and can be downloaded straight onto the device. For instance, in mid-2013, a rogue Chinese site used an enterprise certificate to distribute pirated iOS-based apps.

3. **Malicious profiles** - these attacks leverage the permissions of a profile to circumvent typical security mechanisms to do almost anything ultimately. A profile is an extremely sensitive optional configuration file that can re-define different system functionality parameters, such as mobile carrier, MDM and network settings

Bank of America Merrill Lynch

4. **WiFi man-in-the-middle (MitM)** – these occur when the device connects to a rogue WiFi hotspot. Since all communications are passed through the attacker-controlled network device, they can eavesdrop and even alter the network's communication. MitM attacks have always been a concern for wireless devices, however, the prevalence of smartphones in an individual's personal and business life has made mobile devices much more attractive targets for this attack.

5. **Web kit vulnerabilities -** enable web browsers to render web pages correctly for a user. Attackers will exploit vulnerabilities in a Webkit to execute scripts of their own. Attackers commonly use them as a springboard for remote device infection. An example of a WebKit was the popular iOS4 jailbreaking technique, named JailbreakMe.

6. **Zero-Day Attacks -** represent exploits of vulnerabilities that have been uncovered – but not yet released. Once on the device, they may enable the attacker to steal passwords, corporate data and emails, as well as capture all keyboard activity (key logging) and screen information (screen scraping).

Social media & networks: breeding ground for cyberattacks

Social media and social networking sites are breeding grounds for spam, scams, scareware, and a host of other attacks. These sites can be very real and serious threats to organisations. There are many Trojans, worms, phishing and other attacks targeted specifically at the users of these sites. One big problem is the inherent trust component these sites carry, much like email did many years ago. Furthermore, people that use these sites for entertainment purposes, such as online games, are rewarded for accepting friend requests even from people they don't know, which makes the platform a very fertile ground for identity thieves.

> 160,000 Facebook accounts are hacked everyday – Marc Goodman, founder of "Future Crimes"

Most common social media and network threats

The following are the most common social network threats currently, by definition and frequency, according to Symantec's database:

- **Manual sharing** – These rely on victims doing the work of sharing the scam by presenting them with intriguing videos, fake offers or messages that they share with their friends.

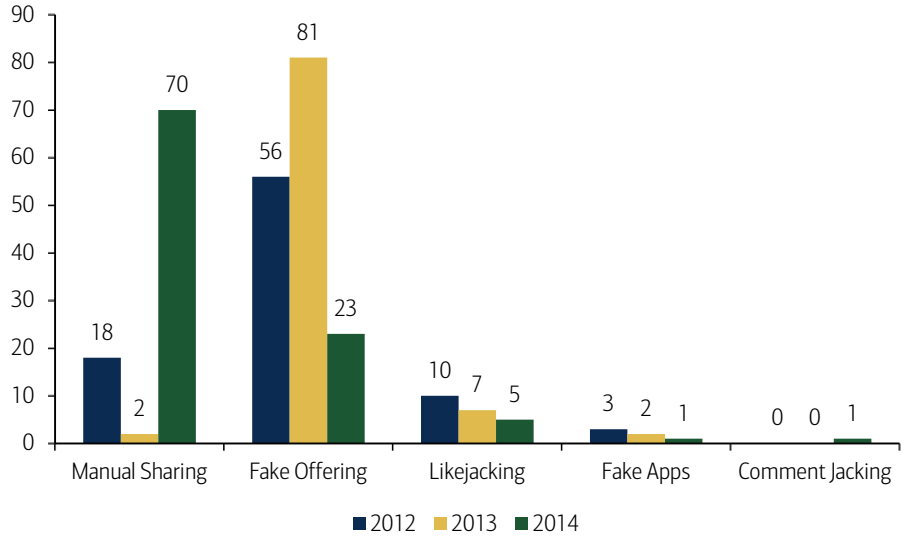
- **Fake offering** – These scams invite social network users to join a fake event or group with incentives such as free gift cards. Joining often requires the user to share credentials with the attacker or send a text to a premium rate number.

- **Likejacking** – Using fake "Like" buttons, attackers trick users into clicking website buttons that install malware and may post updates on a user's newsfeed, spreading the attack.

- **Fake apps** – Users are invited to subscribe to an application that appears to be integrated for use with a social network, but is not as described and may be used to steal credentials or harvest other personal data.

- **Comment jacking** – This attack is similar to the "Like" jacking where the attacker tricks the user into submitting a comment about a link or site, which is then posted to his/her wall.

Chart 57: Most common social network threats



Source: Symantec

Hijacking the power of "social proof": the rise of manual sharing scams

Criminals are increasingly hijacking the power of "social proof" – the idea that we attribute more value to something if it is shared or approved by others. Criminals are exploiting this by hacking real accounts on instant messaging, dating and photo-sharing platforms. The big trend shift in social media scams has been the uptick in manual sharing scams. This is where people voluntarily and unwittingly share videos, stories, pictures, and offers or endorsements that actually include links to malicious or affiliate sites.

> 70% of social media scams were *manually* shared in 2014, where cybercriminals tricked people into scamming their own friends online - Symantec

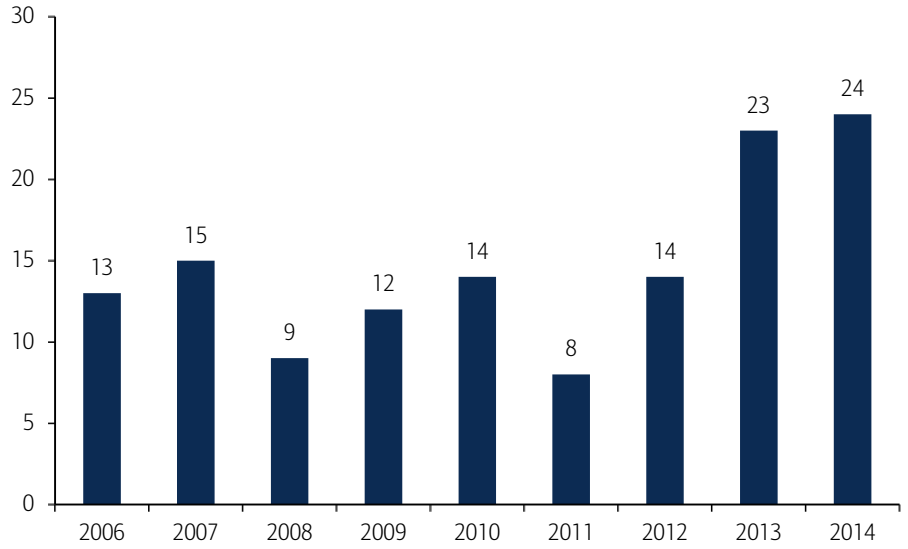
Next-gen threats: unprecedented sophistication

In the past few years, there has been an increase in cyberattacks of unprecedented sophistication. These demonstrate that malicious actors have the ability to compromise and control millions of computers that belong to governments, corporates and ordinary citizens. We expect next-gen threats to become increasingly sophisticated – remaining undetected in victims' systems for prolonged periods and exhibiting zero-day qualities (ie, no known patch or fix). This situation – of the perpetrator or "bad guy" having the advantage over the victims – is only set to get worse in the coming years, in our view.

Zero-day attacks: driving threatscape expansion

Zero-day attacks are when an attacker can compromise a system based on a known vulnerability but for which no patch or fix exists and the hacker manages to avoid detection entirely. A few years ago, zero-day exploits were pretty rare but they are fast becoming a serious threat to IT systems around the world.

Chart 58: Zero-day vulnerabilities total, 2006-2014



Source: Symantec

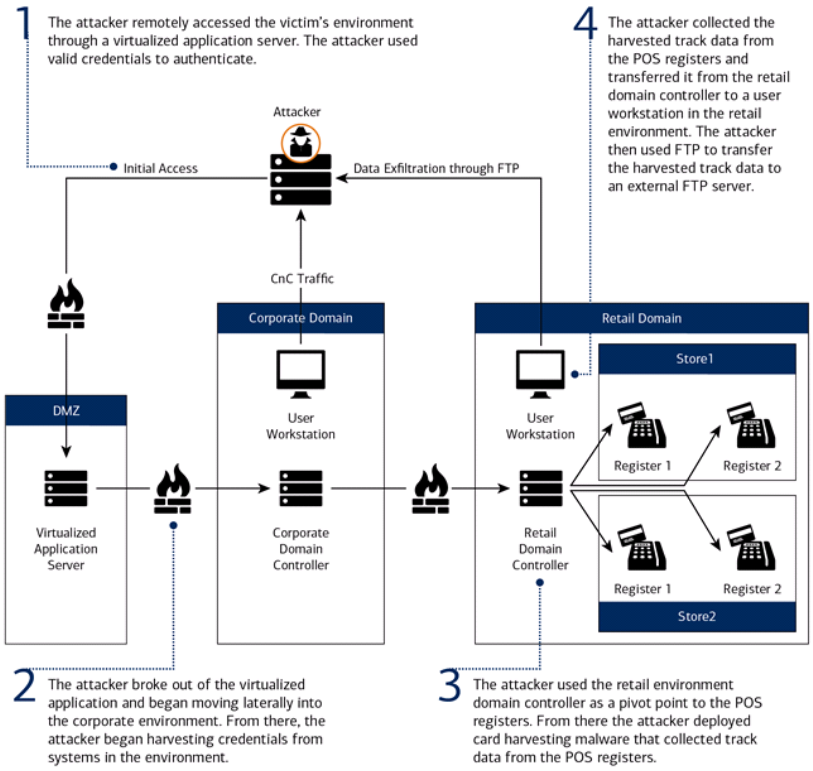
> In total, the top 5 zero-days attacks actively exploited by attackers before patches were available increased from 19 days (2013) to 295 days (2014) - Symantec

A potential hotbed for potential zero-day attacks is Windows XP because Microsoft has now stopped providing updates for this operating system. This is significant because it leaves those organisations still using XP vulnerable to the latest cyber threats without the user knowing.

APTs: skyrocketing and traditional defences are ineffective

An emerging form of zero-day attacks is "advanced persistent threats" or APTs – cyber threats that are more sophisticated, human-controlled and occur over a longer period of time. They pose a greater risk to users because not only do they remain undetected, but they actively operate within the victim's system as a "mole", collecting valuable information throughout the process before inflicting damage. They also have the ability to escalate their privileges with the system because, unlike simple malware such as a bot, these threats are controlled by a human source allowing them to interact and trick users (source: Mandiant).

Exhibit 32: Summary of APT attack

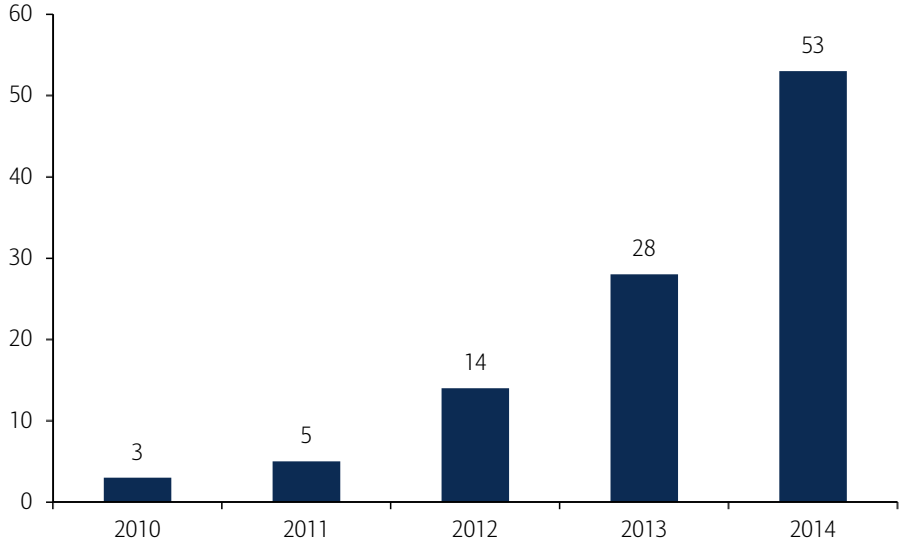


Source: Mandiant

18x increase in 5Y

In 2010 there were only 3 APTs analysed, but by 2014 this number had grown to 53, representing an 18x increase in just five years (source: ESET). In our view, this figure still underestimates the number of potential APTs lurking in systems because of the likelihood of several more having exploited zero-day vulnerabilities.

Chart 59: Growth in the amount of analyzed APTs



Source: ESET

Bank of America Merrill Lynch

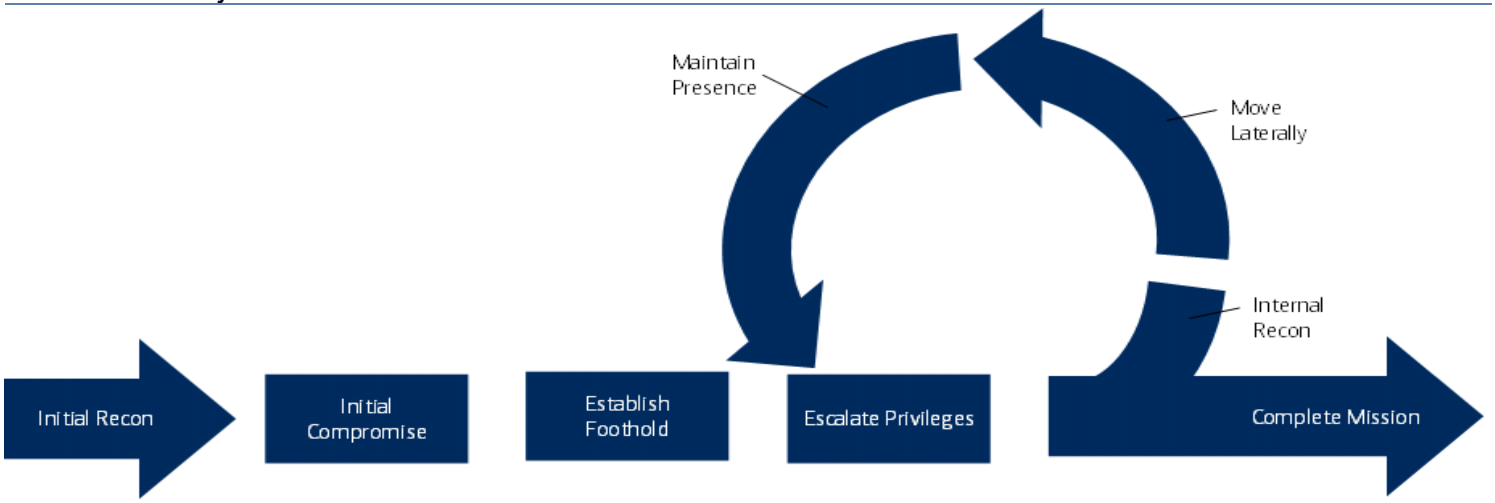
Traditional defences ineffective against APTs

Firewalls or perimeter security defences, which are the dominant security architecture for organisations today, are largely ineffective at protecting against APTs. This is because the attackers are likely to have already breached the system via multi-layered attacks on specific individuals or access vulnerabilities with the organisation.

> 90% of organizations are being breached - on average a breach goes undetected for 205 days - Mandiant

Once attackers are inside the perimeter walls, they typically have free reign over the network because it is not security-aware. Using stolen credentials, they then move laterally, spreading across the network, conducting forensics to see what information they can gain access to. Along the way, they upgrade their credentials until they can gain access to the privileged accounts that house sensitive information or control network systems.

Exhibit 33: Attack lifecycle model



Source: Mandiant

Hacking privileged accounts is a common APT theme

The common factor in many of the major cyber breaches reported in the press recently is breaches in privileged credentials, eg, login details, passwords etc. FireEye's incident response arm (Mandiant) found that 100% of the breaches it resolved were caused by compromised credentials to privileged accounts. We outline below how the following cyber incidents stemmed from these privileged credentials being compromised in the first place:

- **Anthem** (February 2015) – External attackers obtained the credentials to an administrator of a database hosting 80 million customer medical records
- **Sony Entertainment** (December 2014) – Hackers disrupted the network, compromised and exposed the personal data of 47,000 employees and released several major upcoming films on the internet.
- **NSA** (June 2013) – Edward Snowden is known for being the most disruptive inside attacker in history, where he used his privileged account credentials to compromise over 1 million confidential NSA files.
- **Target** (December 2013) – Credentials of a third-party contractor were compromised using a "pass the hash" attack. The credentials were copied and used

to access Target's systems and compromise 40 million credit cards.

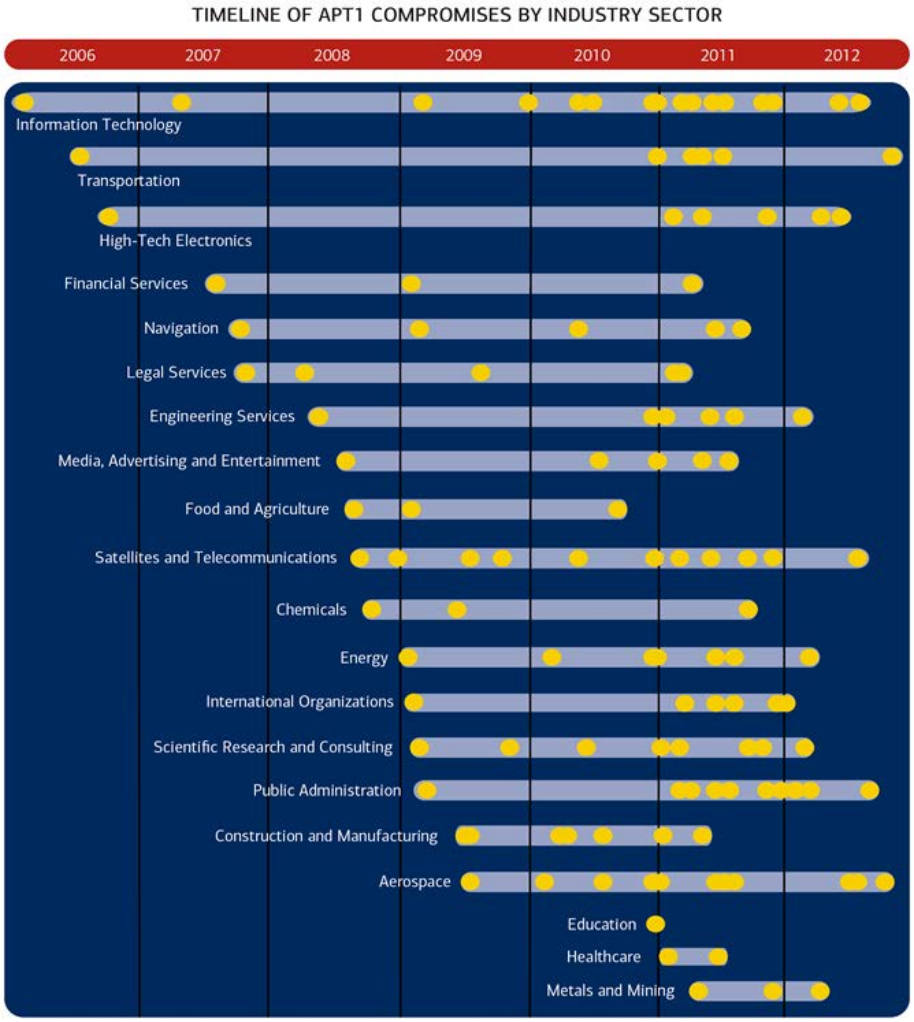
- **Stuxnet** (June 2010) – Attackers compromised the industrial control system of the Iranian nuclear proliferation system and destroyed its ability to operate.

Perhaps more worrying is that many organisations do not know how many privileged accounts they have, according to CyberArk's proprietary analysis. Companies can have 2-4x more privileged accounts than employees, with many Fortune 100 organisations having hundreds of thousands, and even millions, of privileged accounts to manage. Furthermore, 68% of large enterprises either do not know, or have grossly underestimated, the magnitude of their privileged account security problem and one-third of employees, when surveyed, did not know where to find these higher-level credentials in their organisations (source: CyberArk).

Persistent (unknown) attacks across all sectors

The ICT and Transportation sectors were hit by APTs as early as 2006 according to Mandiant, compared to Healthcare and Metals & Mining where attacks occurred more recently. The indiscriminate and pervasive nature of APTs across all sectors is the most worrying aspect of this emerging threat, in our view. In particular, there was a high concentration of these attacks during 2011, according to Mandiant's database.

Exhibit 34: Timeline of APT1 compromises by Industry sector



Source: Mandiant

An increasing source of international cyber-disputes

In addition, APTs are increasingly gaining press coverage as a source of international cyber disputes e.g. supposed OPM hack by China in mid-2015. In particular, recent media coverage of cyberattacks on critical government infrastructure, perpetrated by and against China and the US, has highlighted how damaging they can be to international relations.

Exhibit 35: Observed global APT1 activity

Source: Mandiant

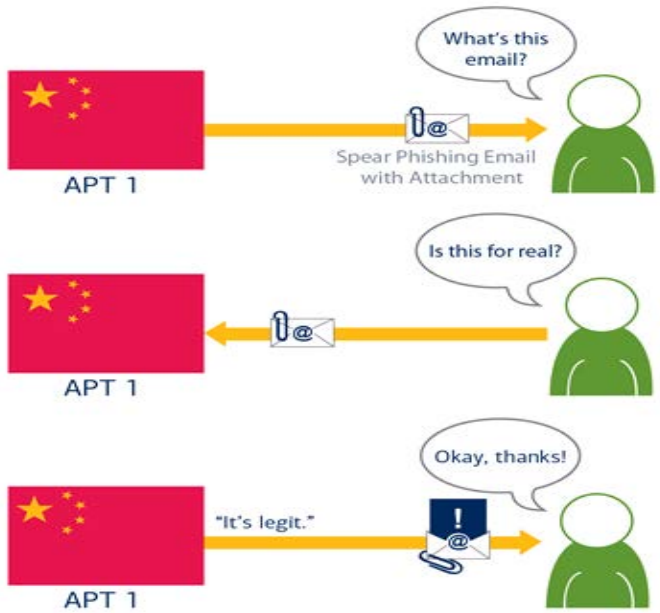
Chinese APTs: state-sponsored cyberespionage

China, in recent years, has been accused of being the main perpetrator of APT attacks, from spying on foreign governments to stealing corporate secrets, with the US thought to be the main victim. One of the most topical studies in this space was the "APT1" (name of Chinese military hacking group) report published by Mandiant, accusing the nation of sponsoring hacking on an unprecedented scale.

> "Chinese hackers have access to a compromised system for 356 days, on average. However, the longest period on record was 4 years and 10 days (1470 days)" - Mandiant

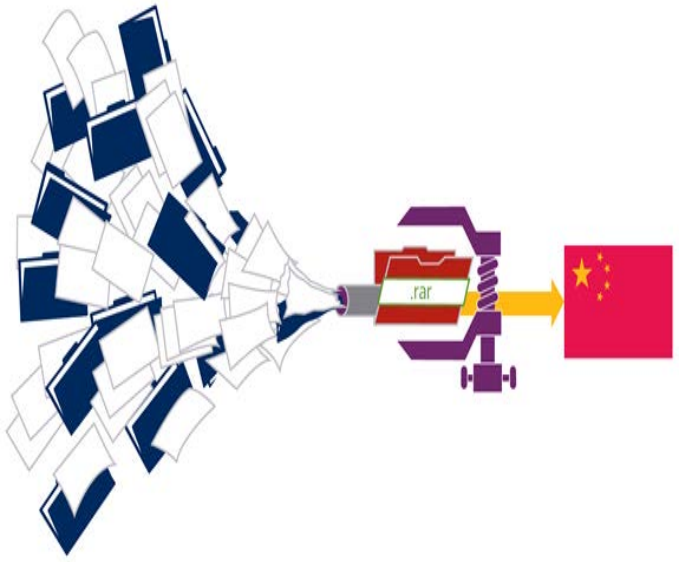
The illustration below demonstrates how an APT can actively adapt to its surroundings. For instance, in one case a person replied, "I'm not sure if this is legit, so I didn't open it" in reply to a spear phishing message. Within 20 minutes, someone in APT1 responded with an email back: "It's legit". Furthermore, attackers send stolen files back to their servers in the form of zipped RAR files that reduces suspicion of any breach. In our view, this case study underlies the serious risks associated with APTs which have evolved from basic malware.

Exhibit 36: Example of APT1 interaction



Source: Mandiant

Exhibit 37: APT1 method of extracting stolen files to avoiding detection



Source: Mandiant

IoT, cloud & smart / connected devices: 50bn points of attack

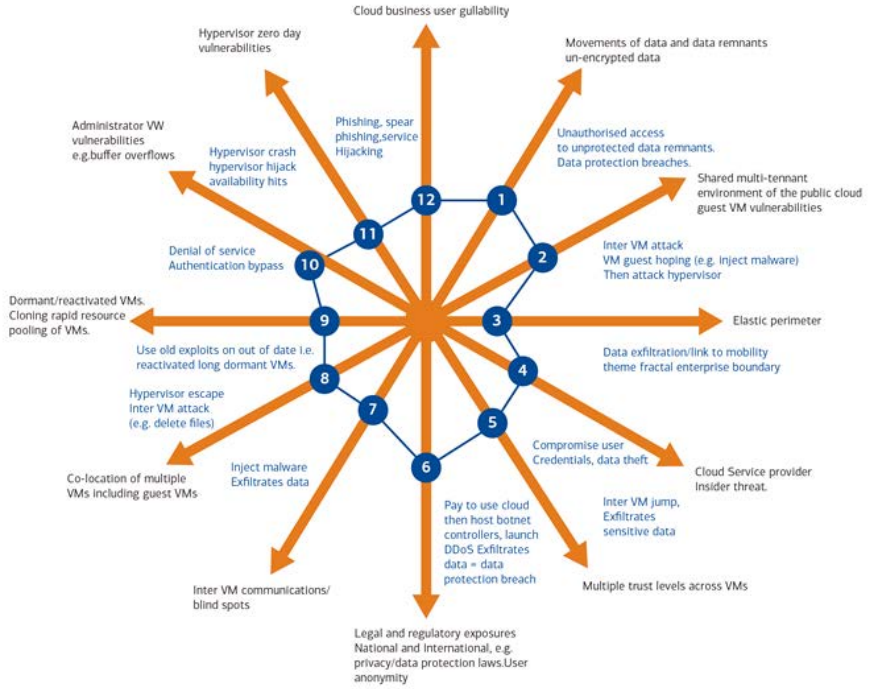
From a cybersecurity perspective, the proliferation in ICT – notably internet access, the cloud, and the IoT, with an estimated 50bn devices that will be connected to the internet by 2020E – means a proliferation of valuable information and data, via 50bn potential points of attack. The growth of big data is also a driver here where to put this into perspective, IDC forecast that the digital universe will multiply 10x between 2013 and 2020E – from 4.4 trillion gigabytes to 44 trillion gigabytes - or enough data to fill 318 iPhones (32GB) per household on average globally by 2020E.

> US$14.4tn is at stake in connecting up what is now unconnected through the Internet of Everything – Cisco

Cloud is increasing the threat surface by >4-10x

The rapid growth of the cloud (SaaS, IaaS et al) – and the volume of accounts, apps, files, third-party data management and storage, sensitive data – is significantly increasing the threat surface for cybersecurity attacks. The growth in corporate cloud adoption has increased the attack surface by over 4x via both external collaboration through public cloud apps and unique third-party cloud apps connected to corporate systems – and over 10x for files stored in public cloud applications (source: CloudLock).

Exhibit 38: Cloud & cyber threats



Source: BT

Greater security needed to boost cloud governance

Companies will need to collaborate on addressing security issues to boost confidence in cloud computing, where data and software are stored on servers and accessed via the internet, especially in the corporate space where the potential market size is much larger than the retail space. A top risk is a loss of governance as the user cedes control to the cloud provider. This leads to the possibility of unauthorized access to sensitive data as well as concerns over business continuity which go beyond the control of the user (source: ENISA, IDC).

> "1 in 4 employees violate a company's data security policy by storing sensitive info in the public cloud" – CloudLock

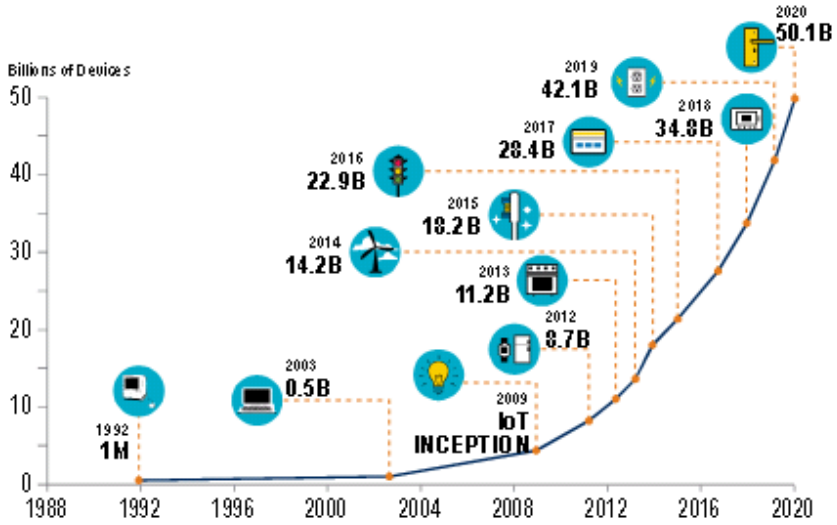
IoT: 50bn connected devices by 2020E = 50bn points of attack

The Internet of Things (IoT) is fast becoming a reality with a growing number of people and things (from smartphones to alarms to cars to commercial and industrial equipment, etc) linked to the cloud and networks, connected to the internet, and communicating with each other in real time, "resulting in volumes of data generated and processing of that data into useful actions that can 'command and control' things and make life much easier for human beings" (Source: Freescale).

> The average household with two children will own c.50 internet-connected devices by 2020 (vs 10 today) - Cisco

Cisco estimated that 8.7bn devices were connected in 2012 and predicts some 50bn devices will be connected by 2020E including drones, additive manufacturing, smart appliances and driverless cars. The resulting potential to share data with everyone and everything will significantly ramp up cybersecurity risks.

Exhibit 39: Estimated device progression of IoT by 2020E



Source: NTCA, Cisco

Smart and connected devices: new tech = new threats

Perhaps the most worrying prospect for the growth in IoT is that all the newly connected / smart devices in the coming decades that could be hacked. Certain areas are of more concern than others. For instance, connected planes, trains and automobiles are more at risk because of the prospect of cyber-attacks inflicting physical losses (eg, crashing a plane full of people), compared with the non-physical losses associated with a smartphone being hacked.

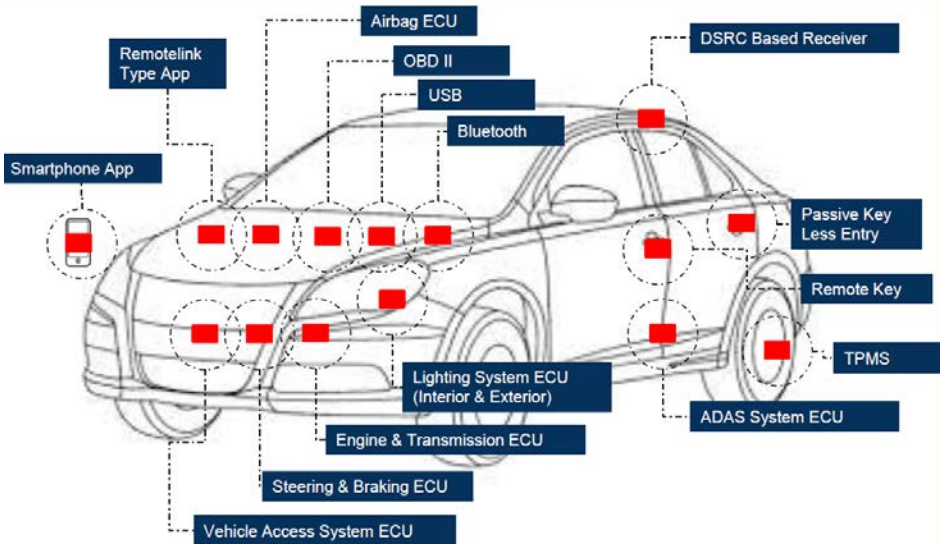
In addition, the threatscape can extend to people's homes where a recent report by Proofpoint found that between 2013/14 nearly 100,000 connected devices sent more than 750,000 malicious emails. More worryingly 25% of these emanated from everyday household appliances such as few smart TVs and refrigerators. Although attacks launched by smart TVs and fridges do not at this point threaten people's lives, they do compromise people's privacy which can be unsettling for the victims involved.

> 70% of the most commonly used IoT devices contain vulnerabilities – HP

Autonomous or self-driving cars

Cyber threats are likely to drive additional auto safety concerns as we have seen with hacks against Chrysler, Tesla, VW and Fiat Chrysler vehicles in recent press sources. The recall of 1.4 million Jeep Cherokee for the latter highlights the increasingly vulnerability of automobiles to cyber attacks, in our view. The increasing reliance on technology installed in a car's components and systems exposes these respective parts to cyber attackers with almost 16 clear attack points already existing in the connected car today via a smartphone (source: Frost & Sullivan).

Exhibit 40: Cyberattack points in the connected car via smartphone



Source: Frost & Sullivan

Table 28: List of potential threats to the connected car

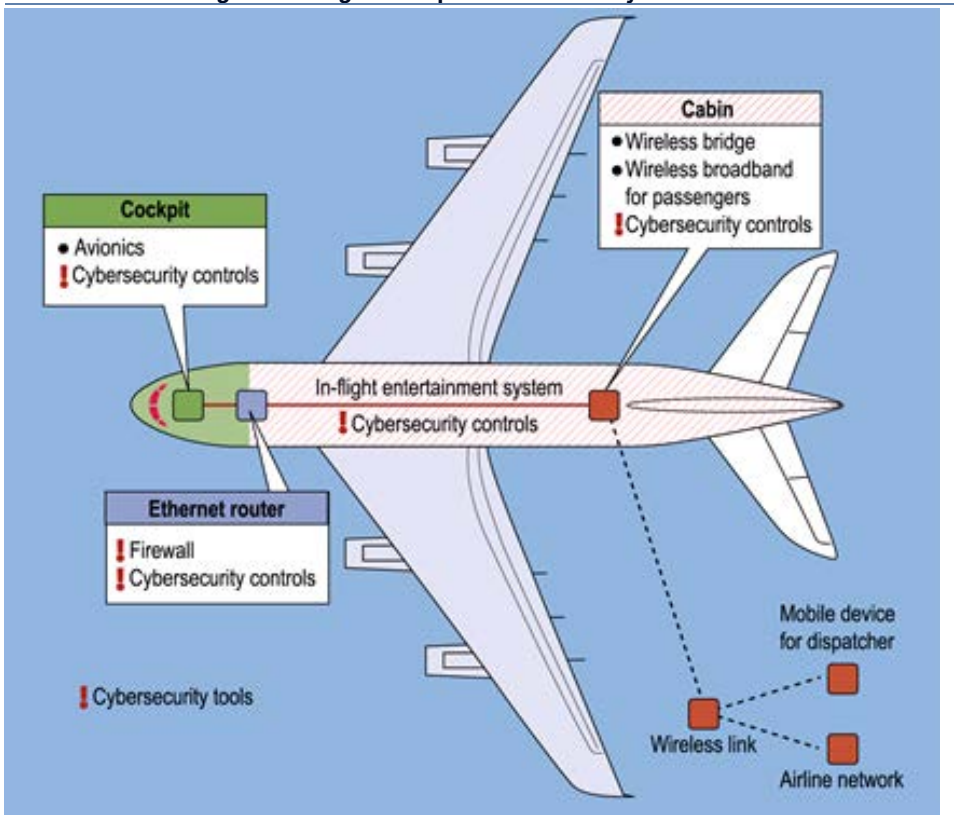
Threat	Description
Falsification of speedometer reading of the vehicle	An attacker may alter the speedometer reading seen by the driver, which may cause the driver to make wrong driving decisions.
Disruption of the braking system of the vehicle	An attacker may disable the braking system while the car is in motion, or apply brakes when the driver doesn't expect it.
Disruption of the emergency response system of the vehicle (eg, OnStar)	Some modern vehicles are equipped with emergency response systems, where the driver and passengers can contact some party to request assistance in emergency situations. An attacker may completely disable this system or falsify any information provided by the system.
Generating false check lights on the vehicle dashboard	Drivers depend on information displayed on the dashboard for warnings such as low tire pressure and low fuel level. An attacker may alter this information to trick the driver into driving the car until it runs out of fuel or making him/her pull over due to a false tire pressure warning.
Locking the gearstick in a fixed position	An attacker can use such an attack to render the vehicle immobile.
Sending deceptive messages to the infotainment system	Such an attack will be able to send information about a required detour to the driver and direct the driver into a trap.
Remotely updating the firmware of an ECU	Attacker may update an ECU of the vehicle with malicious firmware forcing the vehicle to misbehave.

Source: Othmane et al

Commercial flights

Planes are coming under increasing cyber risk. According to a 2015 US Government Accountability Office (GAO) report which says that hackers have devised methods from hijacking the plane via its Wi-Fi network and using USB entertainment ports. 2015 has seen two alleged cyber hacks of passenger planes, with one hacker claiming to have "moved the plane sideways" by connecting into the aircraft's controls via its entertainment system. Despite the existence of firewalls that prevent any "easy" cyberattacks, there remains the possibility of more complex, malicious approaches, according to the GAO report. At some stage, governments may have to step in if the issue escalates in the context of augmented national aviation security.

Exhibit 41: Aircraft diagram showing internet protocol connectivity

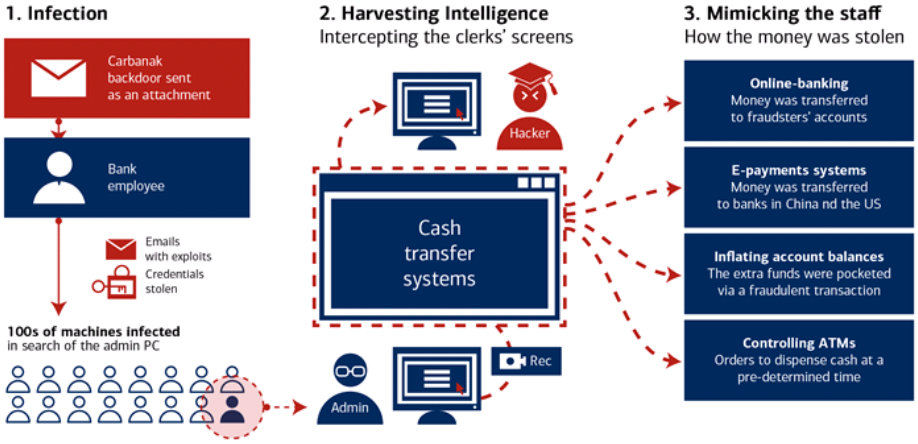


Source: GAO

Point of sales (PoS) attacks: mPayments = growing risk

Although point-of-sale (PoS) attacks date back to 2005, the last few years have seen an upsurge in attacks aimed at obtaining payment card data, including the high-profile data breaches at Target (40mn cards) and Home Depot (56mn cards).

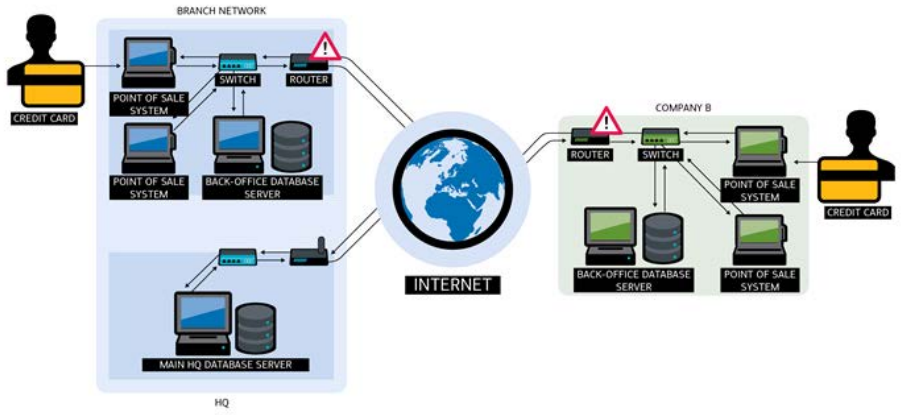
Exhibit 42: Threat to financial institutions



Source: Kaspersky

This has been driven by so-called "RAM scrapers" – malware fixed to payment terminals that search for confidential data such as credit card numbers (source: Symantec). Such attacks are likely to increase significantly driven by the IoT and the move away from the use of cash towards mobile or e-payments (eg, debit and credit cards, NFC payments, etc).

Exhibit 43: : PoS cyberattack works move "laterally" through a victim's network

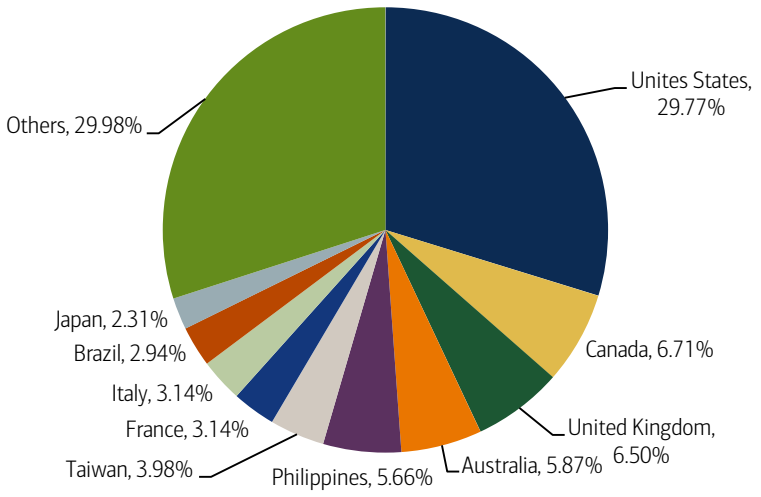


Source: Trend Micro

US is #1 victim of PoS attacks: no 2-step/chip & pin for debit and credit cards

PoS systems are vulnerable because of a widespread lack of security, including poor or non-existent encryption of data, software vulnerabilities, reliance on out-of-date software such as Windows XP (which Microsoft stopped supporting in 2014), and the slow adoption of EMV (i.e. two-factor/chip & pin authentication) by countries, most notably in the US. Hence it should be no surprise that it is also the #1 country to be hit by PoS malware, accounting for nearly 30% of all attacks globally (source: Trend Micro). That said, the growth in mobile wallet technology such as Apple Pay or Samsung Pay is a potential solution to this threat. This is because it encrypts the details of the user during the payment system before sending it over the network to the company's main server.

Chart 60: Country distribution of systems where PoS malware were found in 2014

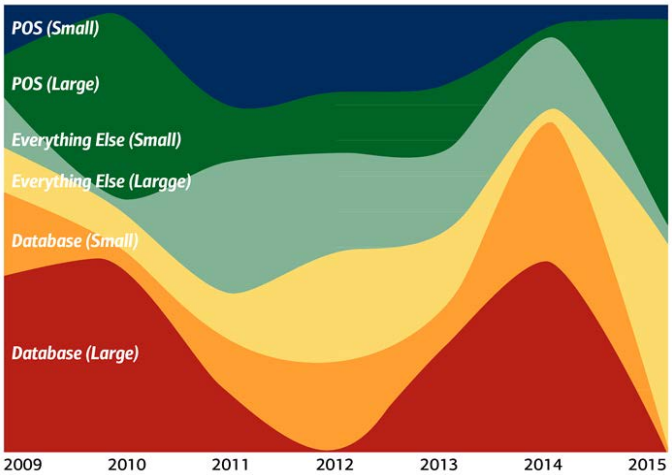


Source: Trend Micro

PoS attacks are becoming "gateway threats" for larger attacks

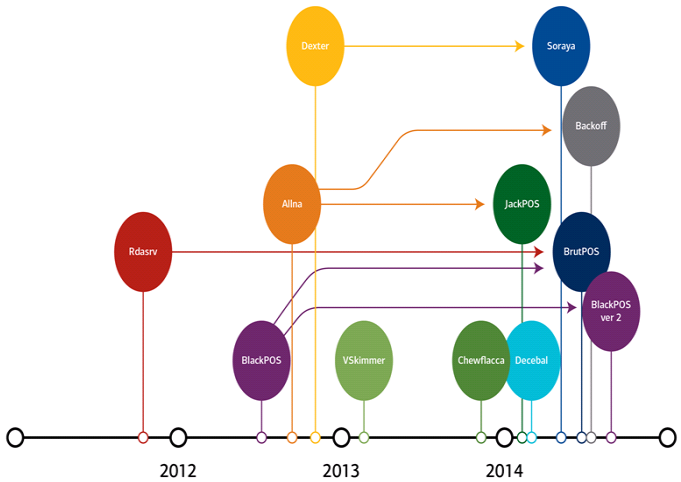
PoS attacks are increasingly targeting large(r) organisations as a "gateway" threat to enter into their system before initiating a second cyberattack. The threatscape is evolving from traditional "card skimmers", who are motivated by small-scale cybercrime, to more sophisticated attacks. Large-scale PoS attacks as a percentage of compromised payment card records grew throughout 2014 to its largest figure by the start of 2015 (source: Verizon). In addition, the growth in new variants of PoS "RAM scraper" vectors grew to five in 2014 compared with just two in 2013 (source: Trend Micro).

Exhibit 44: Compromised payment card records from assets by organisational size



Source: Verizon

Exhibit 45: PoS RAM scraper family tree



Source: Trend Micro

Cyberespionage: #1 threat vs critical infrastructure and national security

There has been an escalation in reported "cyberespionage" threat activity, particularly since the revelations of Wikileaks and Edward Snowden. Cyberespionage is a growing risk for stakeholders because it uses a blend of all the cyber threats mentioned so far, making the attacks ever more sophisticated. These attacks, particularly from nations with highly sophisticated cyber programmes or disruptive intentions, pose the greatest threat to critical infrastructure and national security.

Whole range of national objectives at risk

National cyber programmes pose a threat along the entire spectrum of objectives that could harm national interests (i.e. propaganda, espionage, IP, technology, infrastructure disruption, loss of life). These actors commit the most targeted attacks as they know what they want (ie, to weaken, disrupt or destroy), have government commitment and resources, and are relentless in their efforts to obtain or attack it.

Significant escalation in activity

2014 saw an escalation in cyberespionage activity. For instance, "Regin" was discovered in 2014 and took nearly eight months to be dissected, where the generally accepted conclusion was that only a nation-state with vast resources could have developed this complex threat over many years (source: Symantec). The recent emergence of the "Equation Group", dubbed the most advanced cyberespionage group in the world, further underlies this trend, in our view.

Table 29: Recent engineered cyberespionage toolkits

	Stuxnet	Duqu	Flame	Gauss
Discovered	Jun-10	Sep-11	May-12	Jun-12
Created in	2008-2009	2007-2011	2006-2011	2011-2012
Target	Iranian Nuclear Plants	Iran + Sudan	Middle East	Middle East
Affected	Siemens PLCs	Windows PCs	Windows PCs	Windows PCs
Victims	+150k	~50	~10,000	~2,500
Investment	US$ 10-50 mn	US$ 1-10 mn	-	-

Source: Kaspersky

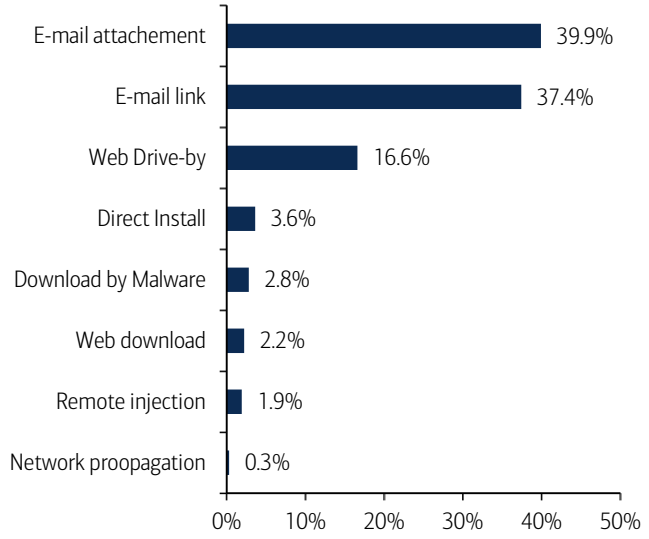
Attribution is difficult but high cyber capability actors are likely behind it

Although attribution is difficult, security companies such as Kaspersky have highlighted that the rise of cyberespionage toolkits is likely to have been created by nation-states with high cyber capabilities, such as the US and Israel. The premises of this theory are:

Bank of America Merrill Lynch

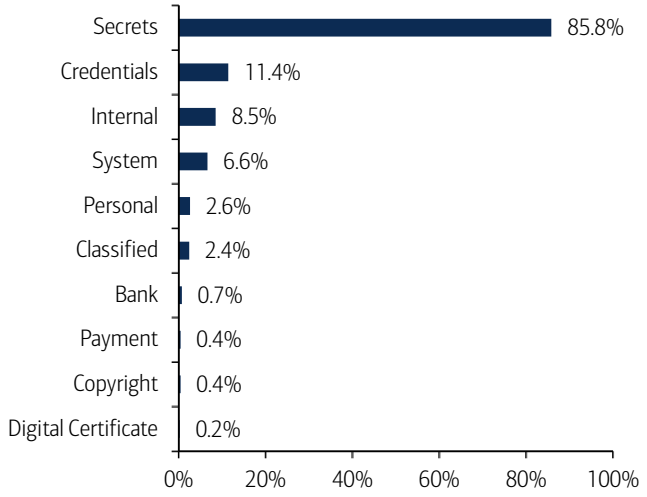
amount invested in their development, target region and critical infrastructure (Stuxnet attacked and disrupted uranium enrichment in Iran) and likelihood of origination.

Chart 61: Top vectors used in cyberespionage



Source: Verizon

Chart 62: Main data compromised by cyberespionage



Source: Verizon

Extension into the corporate and warfare domains

This threat is not restricted to the nation-state domain and extends into the corporate space. One definition of this threat is: use of computer networks to gain illicit access to confidential information, typically that held by a government or organisation. Hence the next stage of this threat would be "cyberwarfare", where the intention is to damage rather than spy. We outline further cyber threats in our Homeland section later in this report.

Costs: US$575bn today; US$3tn at risk

We expect cybersecurity to have a growing impact on companies' bottom lines, driven by business disruption, time and money spent responding to incidents, direct financial losses (eg, loss of assets, fines), indirect financial losses (ie, theft of IP), damage to customer value (turnover) as well as reputational damage, among others. We are already seeing the short-term impact of cybersecurity on share prices, with one-month post-attack declines of up to 50% for major recent breaches (source: Slaughter & May).

The cost of cybercrime for the average US company reached a record US$12.7mn in 2014 (vs US$6.5mn in 2010). Costs averaged US$8.1mn for German companies, US$6.9mn in Japan, US$6.4mn in France and US$4.0mn in Australia. Globally, virtually every industry is affected by cybercrime, with the highest average annualised cost of US$13mn experienced by energy & utilities and financial services companies in 2014 (source: Ponemon Institute). The average cost of data breaches reached a record US$6.5mn for US companies in 2014 – with the healthcare, education, pharma, financials and communications sectors hardest hit (source: Ponemon Institute).

Malicious cyber activity is estimated to cost the global economy between US$375bn and US$575bn, encompassing damage to company performance, trade, competitiveness, innovation, and national and global economic growth (source: Intel/McAfee). The rise in disruptive technologies means that we are facing a potential Cybergeddon scenario where the 'bad guy' has the permanent advantage. US$3tn of global economic value could be at risk if companies and governments are not able to combat cyber threats (source: WEF).

Globally up to US$575bn in economic costs

Malicious cyber activity for corporates encompasses the loss of IP and sensitive business information, and can lead to opportunity costs, the additional cost of securing networks, insurance and recovery from cyberattacks, and reputational damage to the hacked company.

Estimating a global loss figure: US$375-575bn

Intel's McAfee attempted in 2014 to estimate the global cost of cybercrime and cyberespionage in light of the reality of poor reporting and data collection. It came up with three estimates:

- **US$575bn:** using the loss in high-income countries to extrapolate a global figure.
- **US$445bn:** aggregating costs as a share of regional incomes to get a global total.
- **US$375bn:** taking the total amount for all countries where it could find open source data and using it to extrapolate global costs.

c.1% of global GDP: on par with narcotics and counterfeiting/piracy

Cybercrime and cyberespionage cost 0.8% of global GDP, which is roughly on a par with narcotics (0.9%) and counterfeiting/piracy (0.89%). The cost impact is thought to be highest for developed economies including Germany (1.6%), the Netherlands (1.5%), the US (0.64%), Norway (0.64%) and the EU (0.4%) – as well as China (0.63%) (source: Intel's McAfee).

What cybercrime means for the world

According to Intel's McAfee, the most important cost of cybercrime lies in its damage to company performance and to national economies. Cybercrime harms trade, competitiveness, innovation, and global economic growth:

- **The cost of cybercrime will continue to increase** as more business functions move online, and more companies and consumers around the world connect to the internet.
- **Losses from the theft of intellectual property will also increase** as acquiring countries improve their ability to use it to manufacture competing goods.
- **Cybercrime is a tax on global innovation and slows its pace** by reducing the rate of return to innovators and investors (source: Intel's McAfee).

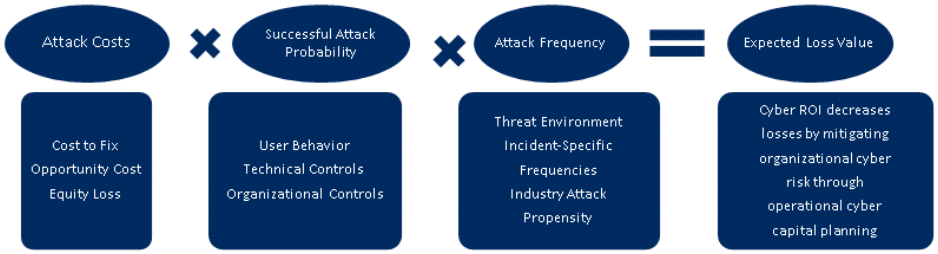
Significant impact on employment: 200k US and 150k EU jobs

For developed countries, cybercrime also has serious implications for employment, leading to a potential shift away from jobs that are driven by intellectual property, which create the most value in an economy. In the US alone, studies suggest that the losses incurred by cybercrime could cost as many as 200,000 jobs. Meanwhile, it is thought that Europe could lose as many as 150,000 jobs (source: Intel's McAfee).

Corporates: average attack costs up to US$12.7mn

The estimated average cost of cybercrime across a group of companies around the world ranged between US$3.33mn in Russia and US$12.7mn in the US (source: Ponemon Institute).

Exhibit 46: Expected loss from cybersecurity incidents

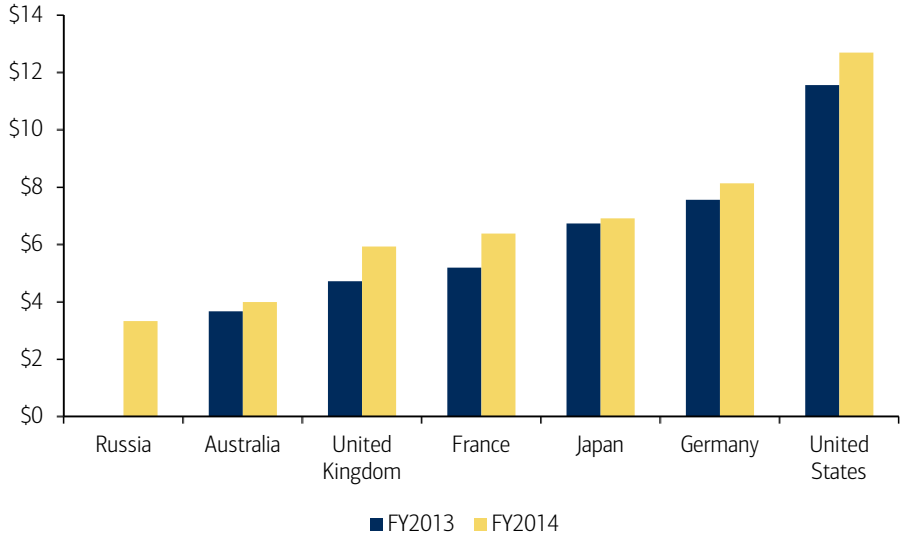


Source: Booz Allen Hamilton

US experiences the highest costs

The average cost of a cyberattack for US companies reached US$12.7mn in 2014 (up from US$6.5mn in 2010), with a range of US$1.6mn to US$61mn per company. The estimated average cost of cybercrime was US$5.93mn in the UK, US$8.13mn in Germany, US$6.38mn in France, US$3.33mn in Russia, US$3.99mn in Australia and US$6.91mn in Japan (source: Ponemon Institute).

Chart 63: Average cost of cybercrime in seven countries (US$mn)

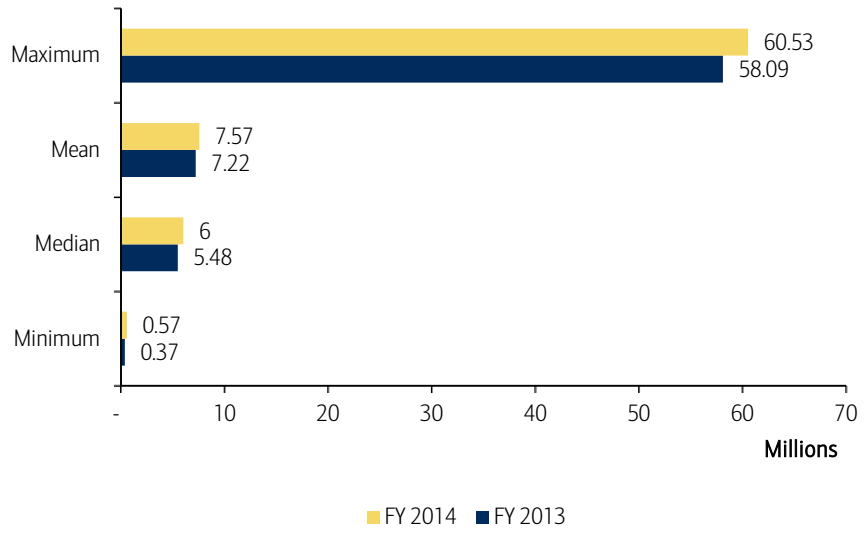


Source: Ponemon Institute Research, BofA Merrill Lynch Global Research

More denial-of-service attacks in the US

Possible reasons for the higher cost impact for US companies include the type and frequency of attacks (eg, denial of services, malicious code, web-based incidents), as well as the importance that companies place on the theft of information assets versus other consequences of the incident (source: Ponemon Institute).

Chart 64: Global cost of cybercrime (US$)



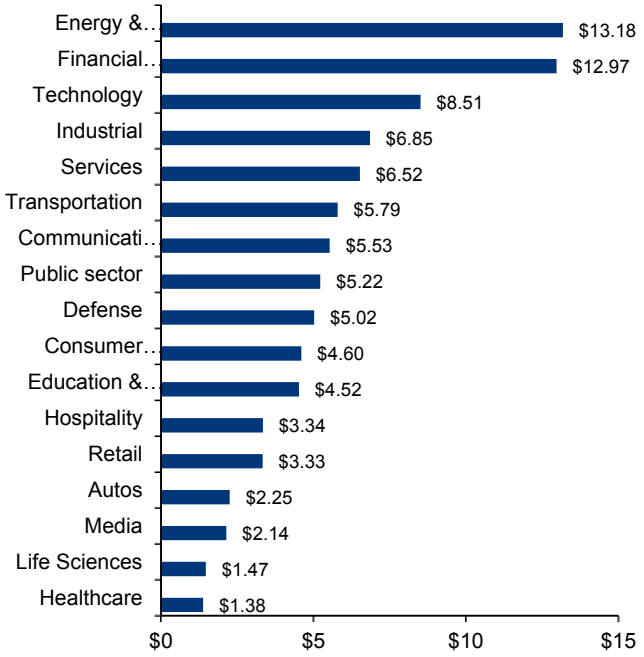
Source: Ponemon Institute , BofA Merrill Lynch Global Research

> "Annualised cost of cybercrimes for Energy & Utilities is 2x the cost in Services and 4x that of Retail" – Ponemon

All industries affected: utilities and financials worse hit

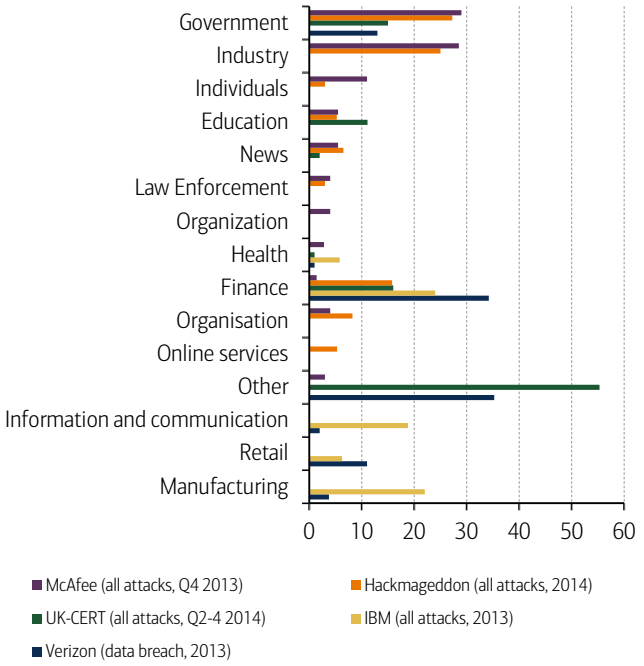
Globally, virtually every industry is affected by cybercrime, ranging from healthcare (lowest average cost) to energy and utilities (highest average cost). The average annualised cost of cyberattacks was US$13.18mn for energy and utilities companies around the world in 2014 (source: Ponemon Institute). This is 2x the cost in the services sector and 4x the cost in retail. In our view, this underlines how cyberattacks are increasingly targeting key infrastructure such as energy and utilities, often with devastating results.

Chart 65: Average annualised cybercrime cost by global industry sector (US$mn)



Source: Ponemon Institute, BofA Merrill Lynch Global Research

Chart 66: Comparison of sector with most cyber attacks



Source: HCSS et al

Companies' share prices decline post cyber attacks

Cyber breaches also have an impact on the stock price for companies affected. The general trend is that share prices tend to drop more over the one-month period after the breach is announced compared to the immediate three days this reaches investors. The most dramatic example of this was the cyber breach at Heartland Payment Systems in early 2009, where the company's stock value dropped by nearly 50% in a month (source: Slaughter & May). It is also important to flag the reputational damage associated with such hacks. Although the economic costs are often the yardstick to measure the impact of a breach, the fallout vis-à-vis customer distrust should not be discounted, in our view.

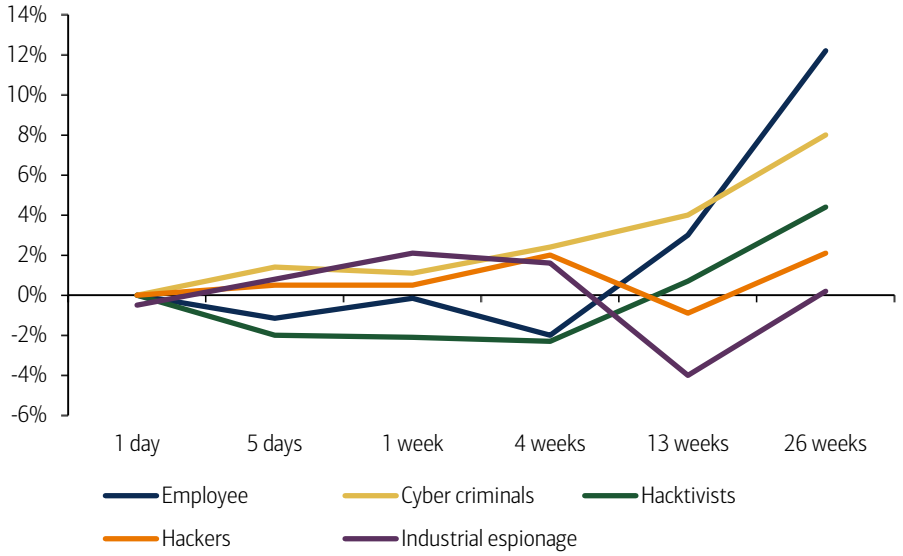
Table 30: Share price declines of certain US and UK listed companies following cyber attacks

		Negative drop in share price following breach (%)	
Company name	**Date of announcement of cybersecurity breach**	**Three days**	**One month**
eBay	21-May-14	1.48%	7.35%
AOL	28-Apr-14	1.70%	23.56%
Target	19-Dec-13	2.41%	5.79%
Adobe	03-Oct-13	2.91%	4.04%
KT Corporation	29-Jul-13	1.30%	5.82%
Ubisoft	02-Jul-13	2.48%	2.48%
Betfair Group	30-Sep-11	13.67%	13.67%
Heartland Payment Systems	20-Jan-09	46.30%	49.54%
TK / TJ Maxx	17-Jan-07	1.82%	6.49%

Source: Slaughter & May

In a separate study, Freshfields flagged hacktivists attacks as causing the greatest immediate downside to a company's stock price. However, in most instances after one month the stock price normally recovers after a 4 week period. Although these findings appear contrary to Slaughter & May study, it is important to stress the following which Freshfields cite as the counter-intuitively drivers: (1) the study found only a small sample of companies publicly reporting a breach which suggests an unwillingness to admit being hacked in the first place (2) share price rebound suggests investors seem unfazed and even complacent on the true risks and costs associated with cyber attacks.

Chart 67: Which type of cyber attack spooks the markets most?



Source: Freshfields

Data breaches cost up to US$6.5mn

The global average cost of a data breach was US$3.8mn in the latest 2015 survey conducted by the Ponemon Institute & IBM. However, US companies face the costliest data breaches with an average of US$6.5mn rising form US$5.9mn in 2014.

> The average cost of a data breach to a US company was approximately US$6.5mn in 2015

Chart 68: The average total cost of data breach for an US organisation (US$mn)

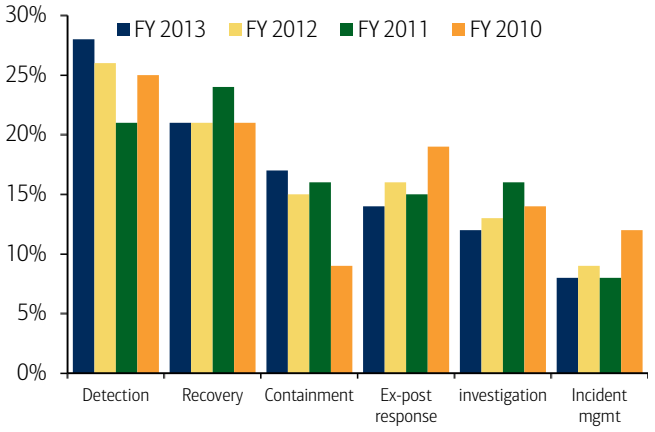
Source: Ponemon Institute, Symantec Research, BofA Merrill Lynch Global Research

Extensive cost impacts

The cost implications are significant and encompass business disruption, time and money spent responding to incidents, direct financial losses (eg, loss of assets, fines), indirect financial losses (ie, theft of IP), damage to customer value (turnover, diminished acquisition), as well as reputational damage, among others.

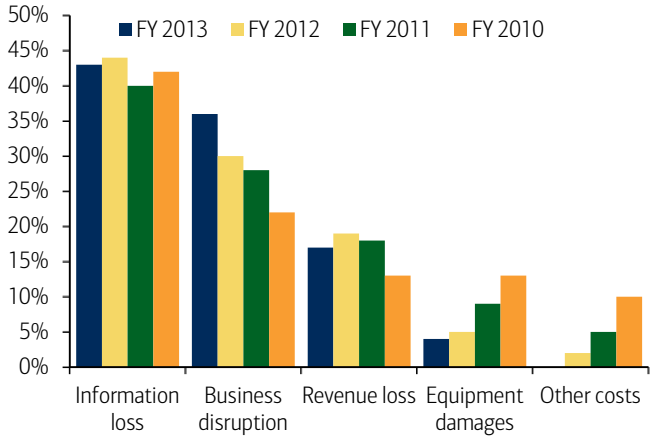
Bank of America Merrill Lynch

Chart 69: Percentage cost by internal activity centre



Source: Ponemon Institute for HP Enterprise Security, BofA Merrill Lynch Global Research

Chart 70: Percentage cost for external consequences



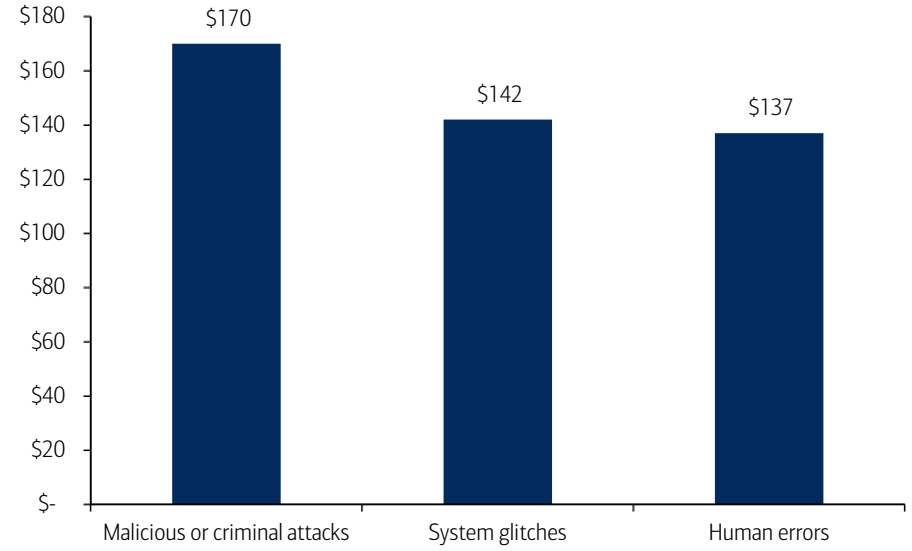
Source: Ponemon Institute for HP Enterprise Security, BofA Merrill Lynch Global Research

Malicious attacks are the costliest data breaches

> Data breaches due to malicious or criminal causes cost an average of US$170 per capita - Ponemon

Globally, data breaches due to malicious or criminal attacks cost companies US$170 per capita, which is higher than the US$142 per capita stemming from system glitches or US$137 from human error (source: Ponemon Institute).

Chart 71: Per capita cost of root causes for data breaches globally

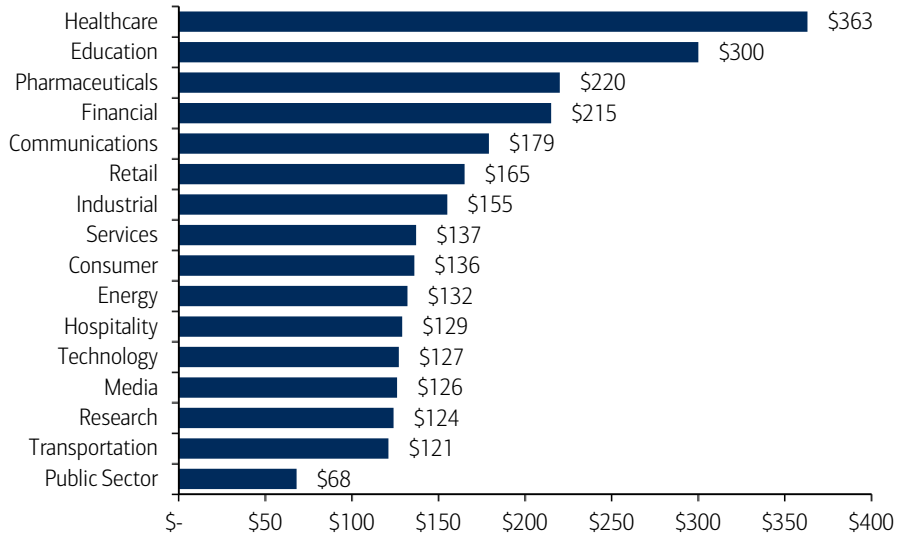


Source: Ponemon Institute, BofA Merrill Lynch Global Research

Sectors affected: healthcare, education and pharma hit hardest

In terms of the sectors that were hit hardest by high per capita cybersecurity costs – healthcare was no.1, followed by education, pharma, financials and communications (source: Ponemon Institute).

Chart 72: Per capita cost by industry classification (US$)



Source: Ponemon Institute, BofA Merrill Lynch Global Research

Homeland security & cyber war: governments & infrastructure under attack

Cybersecurity has become a homeland security threat as growing, concentrated cyber-attacks are threatening nations' ability to defend themselves, their economies and national wealth. Cyber attacks have progressed from initial curiosity probes and progressed into well-funded and well-organised operations for political, military, economic and technical espionage. The US DoD now considers cyberspace another domain for warfare – and Gen. Keith Alexander, former head of the NSA and U.S. Cyber Command described the theft of national IP in cyberspace as the 'greatest transfer of wealth in history.

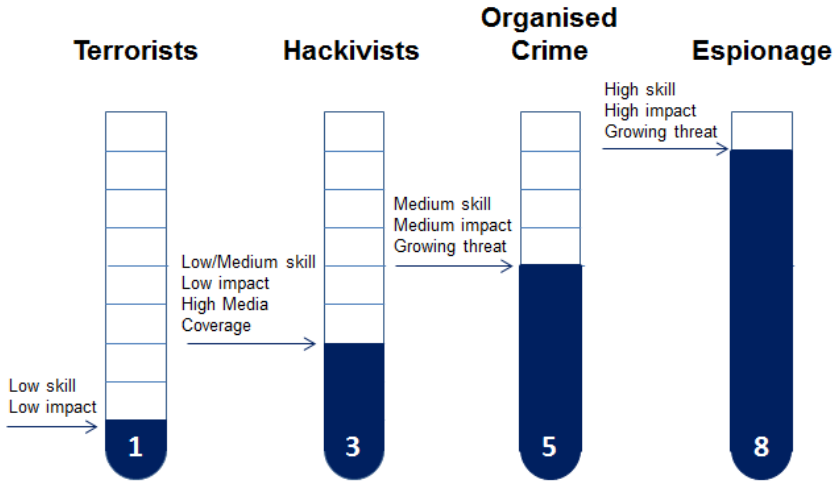
The origin and target of cyberattacks are closely linked to the size of the country involved (including the size of its economy), internet penetration, and the availability of bandwidth. The U.S. is by far and away the number one victim of cyberattacks (23% of total attacks), followed by China, Germany, and the UK (Source: Europol, Symantec). We are seeing growing attacks against government IT systems – with a 1,121% increase in intrusions into federal systems in the U.S. since 2006 (source: US GAO). Critical infrastructure is perceived as the #1 threat posed against nation-states (source: HCSS, Luijif), with the energy sector seeing being the first line of attack followed by critical manufacturing, according to the US DHS' Industrial Controls Systems Cyber Emergency Response Team (ICS-CERT).

In a worst case scenario, cyber-attacks have the ability to trigger a financial crisis by hitting banks, cause national emergencies by infiltrating the IT systems of hospitals or water treatment plants, and bring countries to a standstill by taking out power plants. Assessing a country's cyber preparedness is thus key for investors. In terms of cyber preparedness, the US and UK rank consistently highly ranked across the board – followed by Japan, Germany, Finland, Canada, Australia, South Korea and Sweden (source: HCSS et. al.).

Our Aerospace & Defence team expects demand for advanced technologies in cyber warfare to increase as nation-states and non-state actors vie for dominance in this dimension. Despite their forecast that overall defense spending will decrease in the future, they expect spending in the cyberspace arena will increase as cyberspace garners more attention from the Obama administration, Congress and the media. This could make cyberspace an area of potential growth for defense electronics.

We also need to be cognisant of the growing stakeholder focus on the role of national security organisations in the cyberspace, as evidenced by the Snowden disclosures to the media about the NSA's electronic surveillance and data collection programmes. Such affairs raises concerns about: whether anything in the cyber world can be trusted, Internet governance, the risk of the fragmentation or "Balkinisation" of the internet, and people's trust in government (source: Cisco, WEF).

Chart 73: Cyber security & cyber-espionage threatscape



Source: Frost & Sullivan, BofA Merrill Lynch Global Research

Governments & critical infrastructure under attack

Much of the cybersecurity focus going forward is likely to be on the growing threats of cybersecurity and cyberespionage including government-focused efforts and industrial espionage. The cyber-homeland nexus has been likened to spreading like contagion, or a "global epidemic" according to Adrian Jones, Symantec's executive vice president of global sales.

NAm, infrastructure cybersecurity is #1 perceived risk

Cyber-attacks and the failure of critical infrastructure are the leading risks that North America respondents perceive they are least prepared for, according to the WEF. Nowhere else in the world do these two risks come in the survey's top 3 risks by region. Instead other types of risks such as societal (#1 in LatAM) and geopolitical (#1 in East Asia) are at the forefront of respondents' minds.

Exhibit 47: Cyber attacks are the #1 risk concern in North America

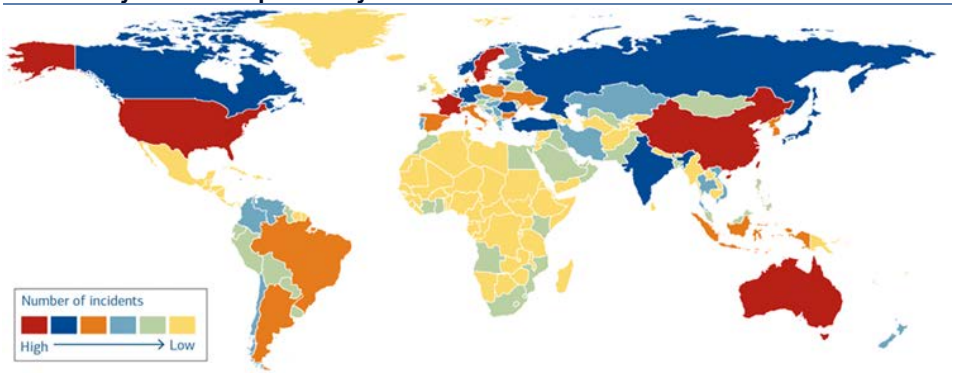
Source: World Economic Forum

Bank of America Merrill Lynch

Where are the cyber incidents happening: US is #1

The origin and target of cyberattacks are closely linked to the size of the country involved (including the size of its economy), internet penetration, and the availability of bandwidth. The United States is by far and away the number one victim of cyberattacks (23% of total attacks), followed by China, Germany, and the UK (Source: Europol).

Exhibit 48: Cyber incidents per country

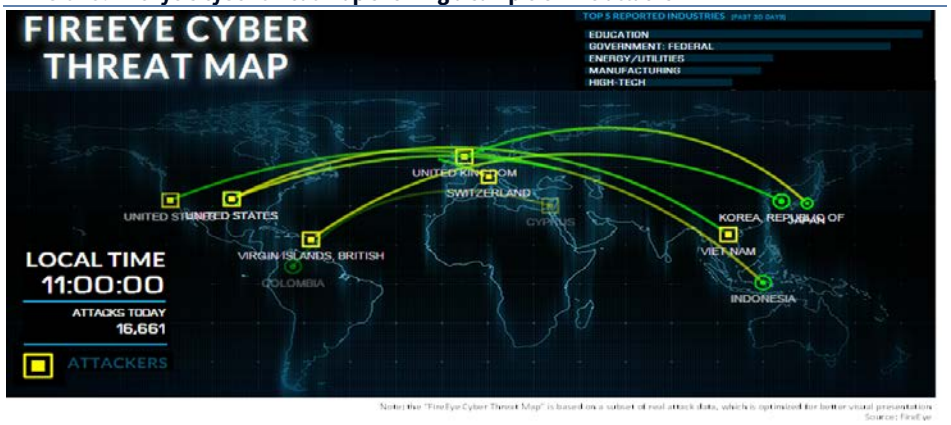


Source: NTT

Up to 50% of attacks originate in the US and 59% take place there

These factors go some way in explaining why 50% of attacks originated in the US and 59% took place there. China was a distant second in terms of where attacks originated (16%) and Japan in terms of where they took place (24%) (source: IBM).

Exhibit 49: FireEye's cyber threat map showing a sample of live attacks

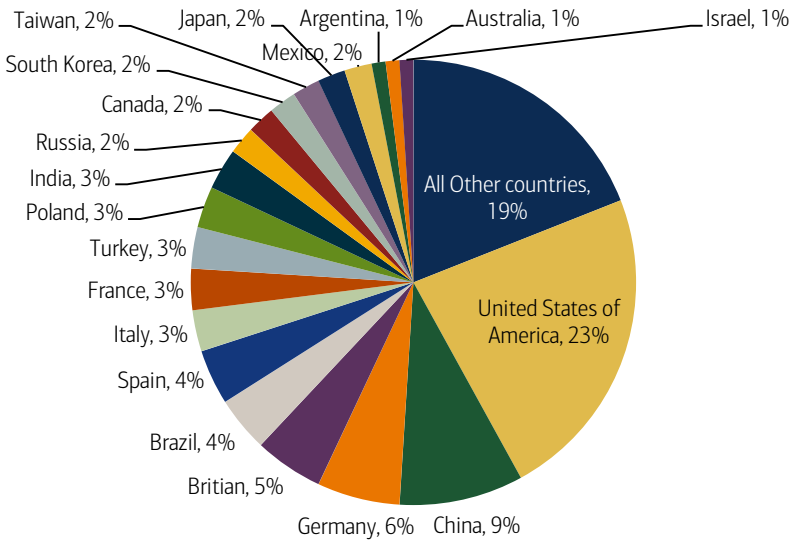


Source: FireEye

US also #1 on cybercrime

Symantec has ranked the 20 countries that generate the most cybercrime. In compiling the list, Symantec looked at six factors: share of malicious computer activity, malicious code rank, spam Zombies rank, phishing, bot rank, and attack origin. The US ranked #1, followed by China, Germany, the UK, and Brazil.

Chart 74: Top 20 countries with the highest rate of cybercrime



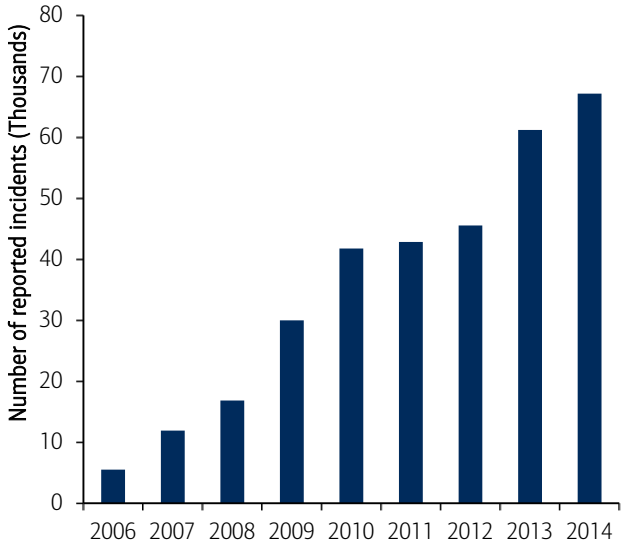
Source: Symantec

In 2014 alone, there were 67,168 intrusions into federal systems in the U.S. – a 1,121% increase since 2006 (source: US GAO).

Increasing attacks against government institutions & agencies

In addition the number of suspicious IT "incidents" at US federal agencies have grown 1,100% since 2006 increasing from c5,000 to c.65,000 in 2014 alone (source: GAO).

Chart 75: Number of reported cybersecurity incidents at US federal agencies



Source: GAO

The US Office of Personnel Management (OPM) was allegedly breached by Chinese hackers in throughout the early part of 2015 whereby over 21mn records were stolen (source: OPM). This made the incident the largest cyber breach for a US government department to date.

Bank of America Merrill Lynch

Table 31:Major cyber attacks on governments

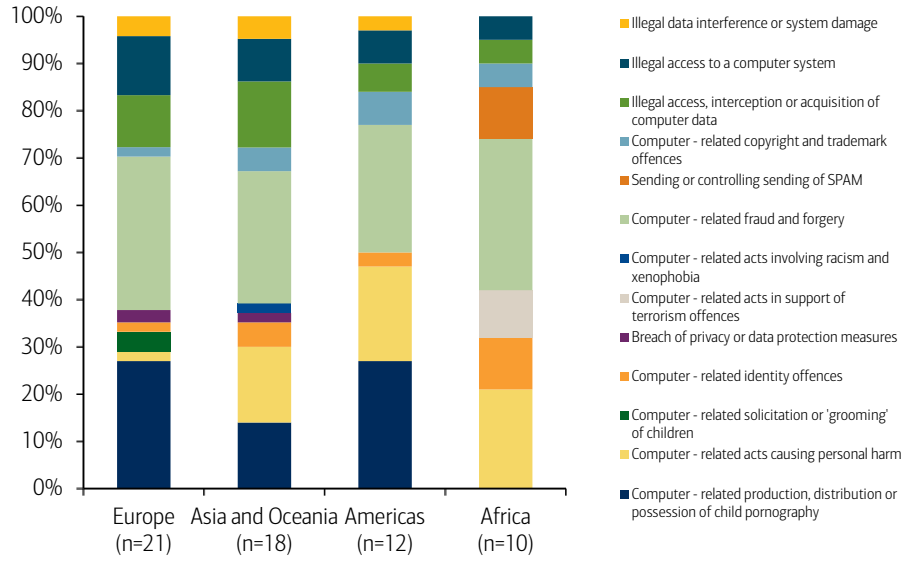
Year	Affected Country	Description
2015	US Office of Personnel Mgmt (OPM).	- US government allege Chinese hackers stole sensitive personal information e.g. social security numbers from over 21 million people including government job applicants, federal contractors, related partners among others
2015	Germany	- Hackers stole data from Bundestag computers, attackers used malicious programs to infect many of the 20,000 machines used
2014	Austria & Switzerland	- Using fraudulently obtained certificate, cyber criminals obtain access to 300 government and company websites in a multiyear operation.
2013	US Federal Reserve	- Hacking collective Anonymous breached internal websites, accessing the personal data of 4,000 bank executives. Mailing addresses, phone numbers and business emails were accessed and published by the hackers online.
2011	Multiple countries	-Operation Shady RAT is an ongoing series of cyber attacks that began in mid-2006 and have been targeted at national governments, military contractors and organisations such as the United Nations.
2010	India	-Pakistan Cyber Army allegedly hacked into the website of India's Central Bureau of Investigation.
2010	Pakistan	-Indian Cyber Army allegedly accessed websites operated by the Pakistan Army and several government ministries, including the foreign affairs, education and finance ministries.
2010	United States	-United States Department of Defence admits its internet traffic was rerouted through China for a period of 18 minutes in April. China denied the claim.
2010	United Kingdom	-Head of Britain's Government Communications Headquarters, warns that the UK faces a "real and credible" threat of cyber attacks from hostile states and criminals and that government systems are targeted 1,000 times every month.
2010	Iran	-Iran's Natanz nuclear facility is targeted by the Stuxnet worm, described as the most advanced piece of malware ever devised.
2009	United States & South Korea	-Coordinated denial-of-service attacks against government, media and financial web sites in the US and South Korea

Source: CSIS, press sources, BofA Merrill Lynch Global Research

It's a global rather than a US phenomenon

Although the cyber-homeland nexus is often centred on cybersecurity attacks in against the U.S., it is important to stress that this theme is a global phenomenon. It has recently been

Chart 76: Most common cybercrime acts encountered by national police



Source: UNODC

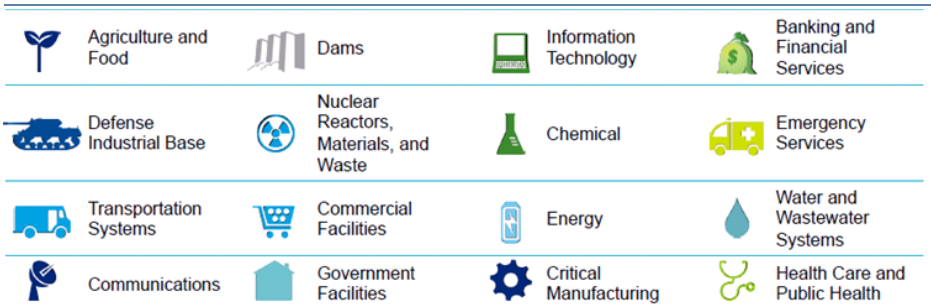
Critical infrastructure, increasingly under attack

One reason why cybersecurity has increasingly become a homeland matter is because of the increase in attacks on critical infrastructure including the energy, transport and water grids as well as the finance sector and critical manufacturing.

16 critical infrastructure sectors at risk

The US DHS has identified a number of critical infrastructure sectors: chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food & agriculture; government facilities; healthcare & public health; IT; nuclear reactors, materials & waste; transportation systems; and water & wastewater systems

Exhibit 50: Critical Infrastructure sectors



Source: Deloitte

Critical infrastructure is perceived to be #1 risk

From a global perspective critical infrastructure is the joint #1 area, along with economic prosperity, that nations believe to be at risk from cyber threats, with national security in third place (source: Luiijf et al, 2013). Although this has been defined in countries' national cybersecurity strategy (NCSS), we believe more action needs to be taken to address this issue.

Table 32: Cyber threats posed to countries

Country	Critical Infrastructure	Defense Capabilities	Economic Prosperity	Globalization	National Security	Public Confidence In ICT	Social Life
AUS	●	●	●		●		●
CAN	●	●	●		●		●
CZE	●		●		●		○
DEU	●		●	●	○		
ESP	●		●		●	○	●
EST	●		●		○		
FRA	●	○	●		●		●
GBR	●		●		●	●	
IND	●		●	○			●
JPN	○		●	●	●		●
LTU	●		○		○	●	
LUX	●		●			○	
NLD	●	○	●		○	●	●
NZL	●		●		●	○	
ROU	●	●	○		●		
UGA	●		●			●	
USA	○		●		●	●	
ZAF	●		●		○	●	
Count	18	5	18	3	15	9	7

Source: HCSS based on Luiijf et al 2013
NOTE: ● – EXPLICITLY DEFINED; ○ – IMPLICITLY REFERENCED

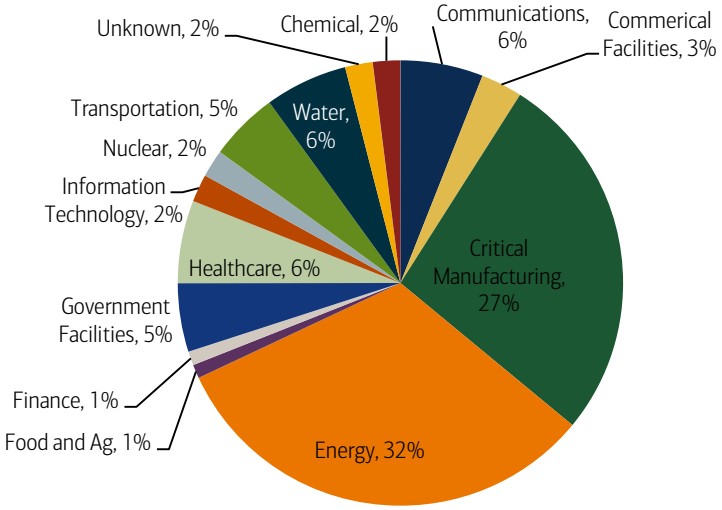
Energy sector is the first line of attack

The US DHS's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) monitors and responds to cyber incidents across all critical infrastructure areas.

By the end of 2015, the potential security risks to the smart grid will reach 440mn new hackable points (source: North American Energy Standards Board)

In FY14, ICS-CERT received and responded to 245 incidents by asset owners and industry partners. It is important to note that many more incidents go unreported.

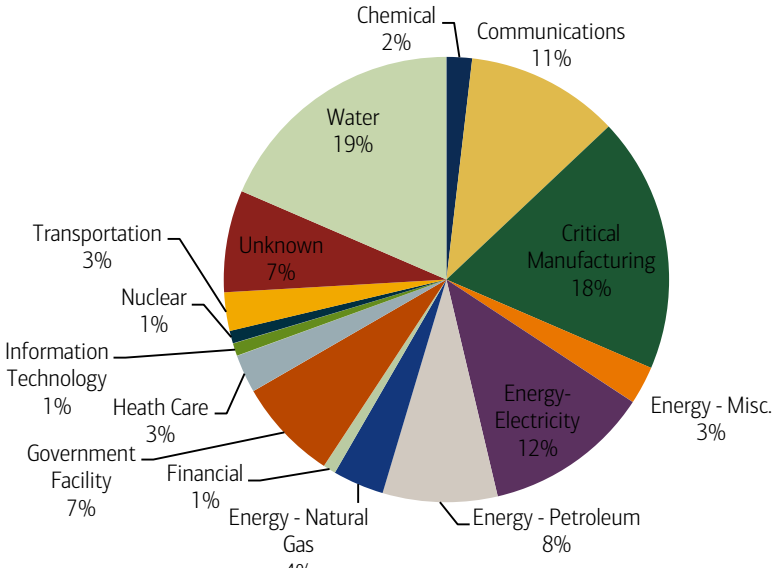
Chart 77: FY-14 mid-year critical infrastructure incidents by sector



Source: US Department of Homeland Security ICS-CERT Monitor

In the first half of FY15 (October 2014 to April 2015), ICS-CERT responded to 108 incidents. As in previous years, the energy sector leads all other areas with the most reported incidents. The water and critical manufacturing sectors also made up a notable proportion of incidents reported to ICS-CERT, at 19% and 18%, respectively.

Chart 78: FY-15 mid-year critical infrastructure incidents by sector



Source: US Department of Homeland Security ICS-CERT Monitor

US power grid attack could cost up to $1tn in losses

The failure of the electricity grid in the US could cost the economy between US$243bn – US$1tn in loss output according to a cyber-scenario analysis (source: Lloyd's, University of Cambridge, Centre for Risks Studies). The scenario involves a trojan threat (similar to "Stuxnet" attack on Iran's nuclear program) that would take up to 100 power plants offline and hence bring a mass blackout across the US. As a result the US insurance industry would likely have to pay out between US$21.4bn - US$71.1bn. Although it is important to stress that the $1tn in loss is a "worst-case" scenario, we still believe this highlights the extensive damages and fallout a cyber attack can cause.

"Smart Grid", $14bn invested by 2018E

Cumulative investments in shoring up cybersecurity in "smart grids" are projected to total US$14 billion between 2011 – 2018E, of which 63% will be focused on utility control system segments (Source: Pike Research). In the US utilities industry alone, this figure is projected to hit US$7.5bn between 2013 – 2020 (source: Zpryme).These investments are significant in that it highlights the growing importance of preventing future cyber attacks both from a stakeholder point of view, but also vis-à-vis these companies being part of a nation's "critical" infrastructure.

Banks & finance: from crime to infrastructure-based attacks

Cyber risks threatening financial services has evolved from reactively small, organized cybercriminals motivated by monetary gain to increasingly larger, well-organized skilled hackers, such as hacktivist groups and nation-states, who are driven by political, social agendas designed to cause chaos in the markets infrastructure.

> "[Cybersecurity] is one of the risks that I would place very near the top of the things that the financial sector needs to work on…it's something that a lot of resources should be into" – Ben Bernanke, Former Fed Chairman

This is illustrated in Deloitte's table analysis below where hacktivists are seen as actors with a very high risk of causing business disruption, and nation states having a similar the impact capability in destroying critical infrastructure in a bank.

Table 33: A diverse array of cyber actors and impacts

	Financial theft/ fraud	Theft of intellectual property on strategic plans	Business disruption	Destruction of critical infrastructure	Reputation damage	Threats to life/ safety	Regulatory
Organized criminals	Very High	Moderate	Low	Low	Very High	Low	Very High
Hacktivists	High	Moderate	Very High	High	Very High	Low	High
Nation-states	High	High	Very High	Very High	Very High	Low	Very High
Insiders	Very High	High	High	High	High	Moderate	High
Third parties	High	Moderate	Moderate	Moderate	Very High	Low	Very High
Skilled individual hackers	Very High	High	High	High	High	Low	High

Source: Deloitte

> 88% of attacks initiated against financial services companies are successful in less than a day, only 21% of these are discovered within the same period – Verizon / Deloitte

Maintenance of legacy infrastructure preserves vulnerabilities

The outdated IT systems that major banks continue to use also leave them highly vulnerable to cyberattacks, in our view. Globally, nearly three quarters of IT spending at

banks is directed towards maintenance on average, with European banks in particular having the highest percentage dedicated to this segment (cf. new investments). In our view, this highlights the continued burden of legacy systems at banks, which leaves employees and customers more vulnerable to the ever-evolving threat of cyberattacks – from installing malware internally to online banking hacks (source: GAO)

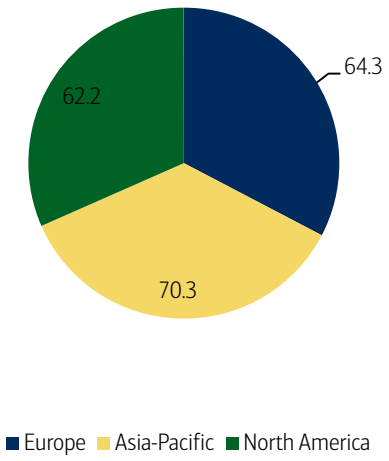
Exhibit 51: Steps involved in financial account takeovers

Target victims	Install malware	Online Banking	Collect and transmit data	Initiate funds transfer(s)
• Criminals target victims by way of phishing, or other social engineering techniques	• The victims unknowingly install malware on their computers, often including key logging and screenshot capabilities	• The Victims visit their online banking website and log on as usual	• The malware collects and transmits data to the criminals through a back-door connection	• The criminals user the victim's online banking credentials to transfer funds from the victim's account

Source: GAO

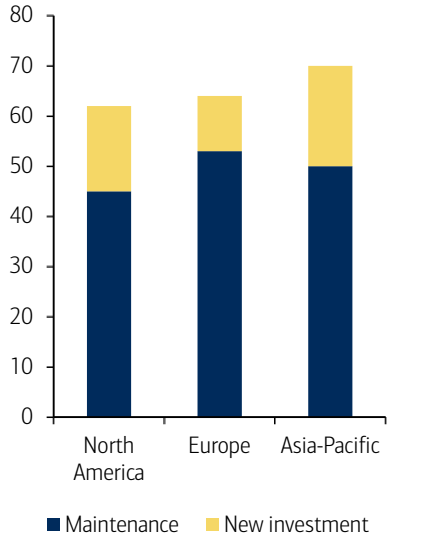
Globally, banks are forecasted to spend nearly $200bn on IT by 2015 year-end, and this figure is projected to grow c.5% per year henceforth (source: Celent). APAC is likely to be the leading region by spend followed by Europe and North America. It is also the region expected to drive new investment spend, almost double the amount expected in Europe.

Chart 79: Estimated bank spend on IT



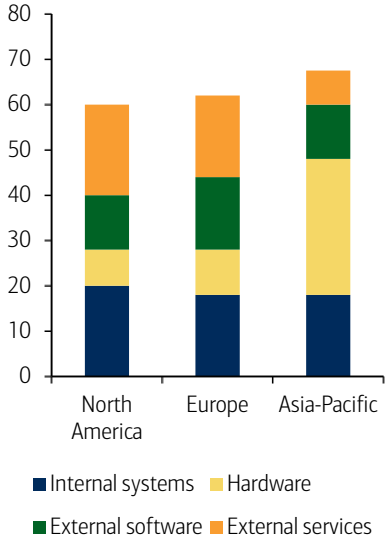
Source: Celent

Chart 80: Maintenance vs new investment spend on IT by banks



Source: Celent

Chart 81: IT equipment spend by banks



Source: Celent

Vast range of infrastructure threats and methods to gain access

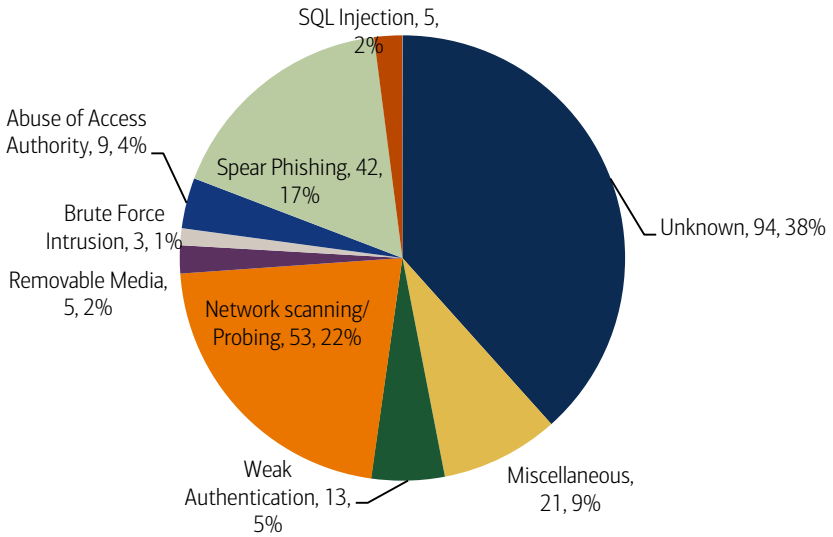
According to ICS-CERT, the incidents encompassed a vast range of threats and observed methods for attempting to gain access to both business and control systems infrastructure, including: unauthorised access and exploitation of internet-facing ICS/Supervisory Control and Data Acquisition (SCADA) devices; exploitation of zero-day vulnerabilities in control system devices and software; malware infections within air-gapped control system networks; SQL injection via exploitation of web application vulnerabilities; network scanning and probing; lateral movement between network zones; targeted spear-phishing campaigns; and strategic web site compromises (aka, watering hole attacks).

48% of electric utilities do not have integrated security systems with proper segmentation, monitoring and redundancies needed for cyber protection (source: Black & Veatch)

Origin of most incidents is 'unknown'

Worryingly, the majority of reported incidents were categorised as having an 'unknown' access vector (ie, the organisation was confirmed to be compromised, however, forensic evidence did not point to a method used for intrusion because of a lack of detection and monitoring capabilities within the compromised network (source: DHS ICS-CERT).

Chart 82: Incident by access vector



Source: US Department of Homeland Security ICS-CERT Monitor

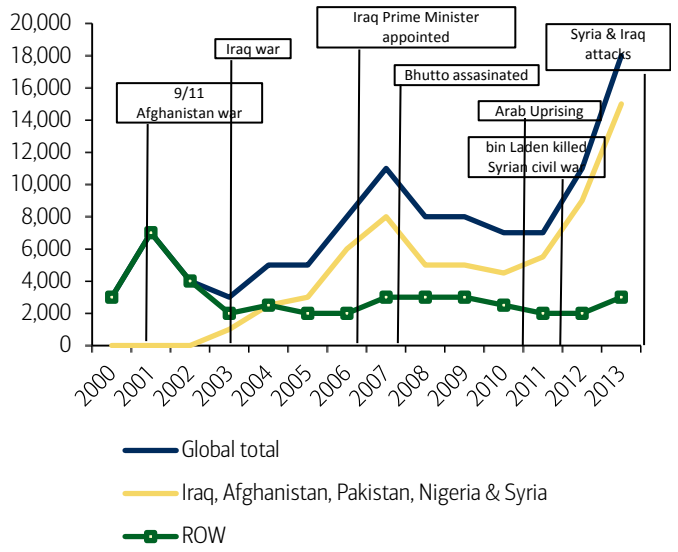
US$109bn in cyber spend on critical infrastructure by 2019E

Global cybersecurity spending in critical infrastructure – encompassing defence, energy, financial services, health care, ICT, public security, transportation and water and waste management – is projected to hit US$109 billion by 2020E, according to ABI Research. The bulk of the spending is in Europe and North America – with the government-funded defence industry the biggest spender, followed by the energy and financial sectors. Cyber critical infrastructure spending in APAC is forecasted to reach US$22bn by 2020E with China, Japan and South Korea as the main drivers (Source: ABI Research).

Terrorism: cyberspace being used to spread the message

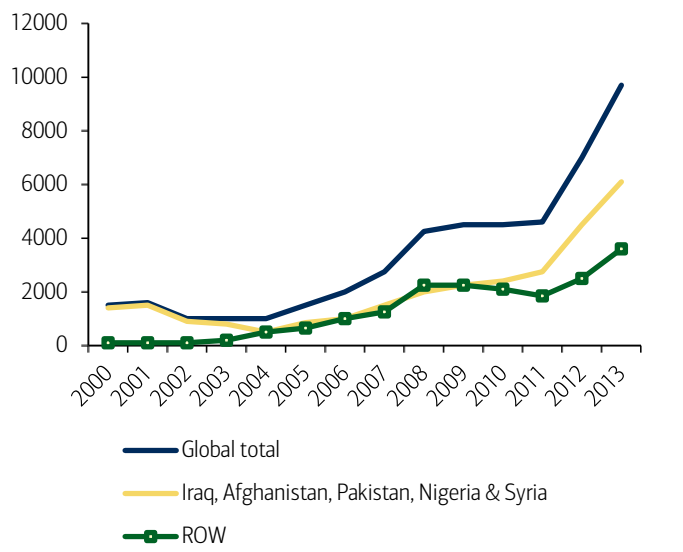
Terrorists are currently not well developed in their ICT capabilities and propensity to pursue cyberattacks, and still prefers bombs to bytes. However, demographic changes and an influx of technologically savvy Millennials or 'script kiddies' into their ranks means that, unfortunately, cyber terror is set to gain in prominence. We are already seeing this with the trend of using cyberspace to spread messages pertaining to terrorism. For instance, ISIS uses social media platforms such as Twitter to spread their mission statement and US military Twitter accounts have been hacked by those claiming to be affiliated to ISIS. The account of the US Central Command experienced a cyber-breach in January 2015 whereby individuals hijacked the online account and tweeted messages with hashtags "#CyberCaliphate" and "#CyberJihad" attached to them (source: US CENTCOM)

Chart 83: Deaths from terrorism 2000-2013



Source: Global Terrorism Index

Chart 84: Terrorist Incidents, 2000-2013

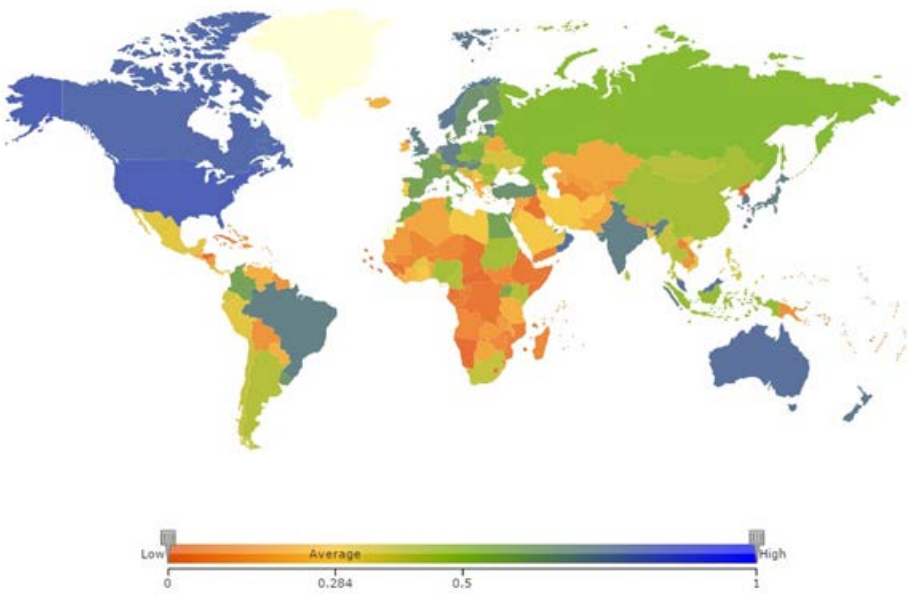


Source: Global Terrorism Index

Be prepared: who is and who isn't

In a worst case scenario, cyber-attacks have the ability to trigger a financial crisis by hitting banks, cause national emergencies by infiltrating the IT systems of hospitals or water treatment plants, and bring countries to a standstill by taking out power plants. As a result, we are seeing a growing talk by governments on mitigating the risks associated with cyber attacks, but their efforts are still far from par with the growing nature of the threats.

Exhibit 52: Global Cybersecurity Index (GCI) 2014: measure of each nation's level of cybersecurity development



Source: ITU-ABI Research

Assessing country's cyber-preparedness

Assessing a country's cyber preparedness throws up a slight paradox in that the less connected a country is, the lower the risk of cyber threats. But the HCSS identified a number of indices assessing cybersecurity capabilities and commitments of countries

with the US and UK ranking consistently highly ranked across the board – followed by Japan, Germany, Finland, Canada, Australia, South Korea and Sweden.

Table 34: Overview of surveys of cyber "preparedness"

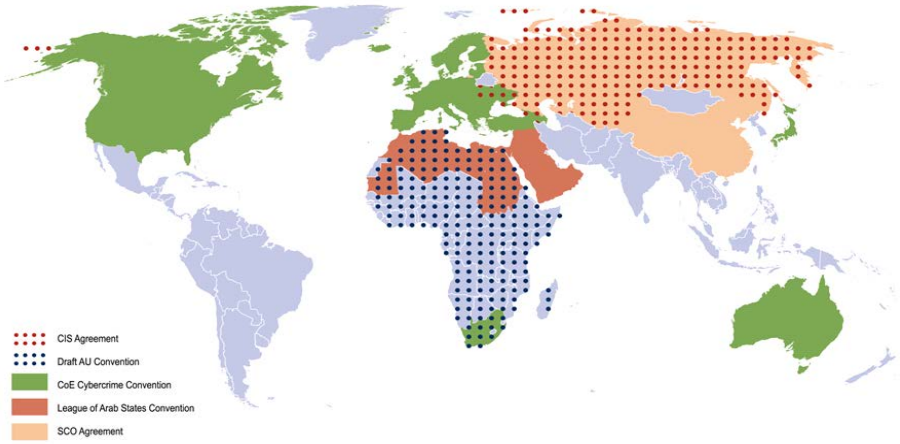
Country	Networked Readiness Index 2014	Cyber Readiness Index, 2013	ITU, Global Cybersecurity Index, 2014	Cyber Power Index, 2013	Cyber preparedness	Average
1 Argentina	1	1	1	2	n/a	1.25
2 Australia	3	4	4	3	2	3.2
3 Austria	3	3	3	n/a	2	2.75
4 Brazil	1	2	3	2	1	1.8
5 Canada	3	4	4	3	2	3.2
6 China	2	2	1	1	1	1.4
7 Denmark	3	1	2	n/a	3	2.25
8 Finland	4	3	2	n/a	4	3.25
9 France	2	3	2	4	3	2.8
10 Germany	3	3	3	4	3	3.2
11 India	1	1	3	2	1	1.6
12 Indonesia	1	1	1	1	n/a	1
13 Israel	3	2	3	n/a	4	3
14 Italy	2	1	2	3	1	1.8
15 Japan	3	4	3	4	2	3.2
16 Mexico	1	1	1	2	1	1.2
17 Netherlands	4	4	3	n/a	3	3.5
18 Russia	2	2	2	1	1	1.6
19 Saudi Arabia	2	1	1	1	n/a	1.25
20 South Africa	1	1	1	3	n/a	1.5
21 South Korea	4	2	3	3	n/a	3
22 Sweden	4	2	2	n/a	4	3
23 Turkey	2	1	2	1	n/a	1.5
24 United Kingdom	4	4	3	4	3	3.6
25 United States	4	4	4	4	3	3.8

Source: HCSS

Lack of global governance

If we look at cyber governance geographically around the world, a non-standardised picture emerges. On the one hand most developed, Western countries are part of the CoE Cybercrime Convention (US, Europe). On the other hand China and Russia adhere to cyberspace rules in the Shanghai Cooperation Organisation (SCO) agreement (Source: UNODC, Zurich). Hence it is important to stress that no legal convention or agreement has been signed by the so-called "big three" (US, China, Russia) affected by cyber issues.

Exhibit 53: International & regional instruments



Source: UNODC

Bank of America Merrill Lynch

In addition, there is an absence of one universal international organization or supranational that governs risks pertaining to the cyber "threatscape". Although INTERPOL cover areas such as hacktivism and cybercrime, they do not cover key areas like international cyber warfare which is a growing risk. Whereas bodies like the UN can prevent an escalation in real-world war conflicts, they don't currently have a remit to tackle warfare pertaining to cyber. This represents a significant global geopolitical risk, in our view, due to the potential with which cyber warfare can theoretically escalate without a supranational check.

Table 35: Cyber warfare not governed by international organisations

	Description	Examples	Main damage	International organizations (IOs)
Hacktivism	Use of networked platforms to pursue an ideological goal or obtain notoriety. No (or limited) physical effect.	DDoS attacks, website and server disruption, DNS hijacking, cybersquatting.	Data compromise or exposure, operational shut down or slow down, damage to organizational assets.	INTERPOL, EC3, CEC (BC), ISF
Cyber espionage	Unauthorized network penetration to access information. Risks related to IPR. Financial or ideological motivation. Generally non-physical effects.	Spyware, data theft, extortion, advanced persistent threat (APT).	Intellectual property infringement, theft or breach of confidential information, loss or corruption of data.	INTERPOL, EC3, CEC (BC)
Cyber crime	Unauthorized network penetration to disrupt and damage systems, as well as stealing data, for financial gain. Mild physical effects.	Phishing, malware, APTs, viruses, worms, Trojans, spam, spoofing, ransomware, scareware, stolen devices, web-based attacks, adware, botnets, skimming, fast flux, spoofed apps.	Supply chain compromise, reputation damage, business interruption, online child sexual exploitation, identity theft, extortion, money laundering.	INTERPOL, EC3, FIRST, CEC (BC), ISF, NRO
Emerging technologies failure	Risks related to the introduction of new technologies. Generally significant physical effects.	Internet of things, embedded medical devices, driverless cars, cloud systems.	Integrity, availability, performance and security of connected devices.	ICANN, IETF, ISOC, IEEE, ENISA, W3C, IEC, ISO
Critical information infrastructures disruption	Risks from disruptions to infrastructure. Attacks to SCADA systems. Strong physical effects.	Submarine cables, smart grid, electricity, financial systems.	Destruction, damage, or disruption of critical information infrastructures.	ENISA, ITU, UN-GGE
Cyber warfare	Risks related to the use of networks by nation states or related groups to destroy or damage ICT systems. Targeting a nation's private sector may be a focus.	International conflicts.	Destruction, damage, or disruption of defense networked systems.	

Source: Zurich, ESADEgeo

Homeland security: the cyber warfare reality & opportunity

Defense Update: Deciphering defense, an industry primer 04 May 2015

The United States Army, Navy, and Air Force have the capabilities to fight in four dimensions of warfare: land, sea, air, and space. Rapid technological advances in the past few decades gave birth to the fifth dimension in warfare: cyberspace.

As the world becomes more digitalized, new military threats surface. Most recent headlines have highlighted the real threat in cyberspace. Considering that modern life is so reliant upon technology, from key infrastructure like water systems and transportation to banking services and power grids, the scope of cyberspace is vast, extending beyond any physical or geographic barriers.

As such, the US faces hard decisions on how to conduct cyber warfare, when conventional warfare weapons like $3bn DDG-1000 destroyers, $2bn B-2 bombers, $136mn F-22 fighters can be countered by a botnet kit bought online or a sophisticated DDoS attack purchased on the darknet.

What is war in the cyberspace like?

Cyber warfare is a form of warfare that uses computers and the Internet to conduct attacks by hacking into computer systems and networks. Cyber attacks can range from vandalism of websites or programs, Distributed Denial of Service attacks to cripple servers, compromising software and hardware with malicious software, hacking into networks to damage critical infrastructure to conducting cyber espionage. Nation-states and non-state actors like terrorist groups, criminal organizations, and hackers are the major players in the domain.

Products offered

Defense firms currently work hand in hand with commercial information security companies to protect existing government information systems. The government buys commercial-off-the-shelf products (COTS) from hardware firms like Cisco and Juniper and software products from companies like Check Point Software Technologies, McAfee, Symantec, and Websense. Defense companies with cyberspace capabilities then integrate the various systems the government uses to build a comprehensive information security system. To integrate the information security systems, defense companies can provide three main products/services:

- Vulnerability assessment – to identify existing system weaknesses and test security systems
- System development – to plug holes in COTS and fix identified vulnerabilities
- Customized products – to provide proprietary hardware or software that commercial companies do not offer (products like insider monitoring, forensic analysis, reverse engineering, tracing and attribution, etc.)

Who are the players?

Since cyberspace can involve national security, information from the government is mostly classified. Similarly, since the sector is still in the growth stage, defense companies do not fully disclose their strategies in order to protect their competitive advantage. So at this point, many companies do not disclose their full capabilities in the domain and specific information about strategies are not available. In a few years, Boeing, Lockheed Martin, Northrop Grumman and Raytheon have initiated separate cyber-security focused units to increase their presence in the domain. There are few pure-play cyber companies and only one that is publicly traded. Keyw Holding Corp went public in September 2010.

Cyberspace trends

We expect demand for advanced technologies in cyber warfare to increase as nation-states and non-state actors vie for dominance in this dimension. Despite our forecast that overall defense spending will decrease in the future, we expect spending in the cyberspace arena will increase as cyberspace garners more attention from the Obama administration, Congress and the media. This could make cyberspace an area of potential growth for defense electronics.

The US government is still in the process of determining who will have jurisdiction in cyberspace. As the Department of Defense and Department of Homeland Security, and their subordinate organizations like the US Air Force, Army, Navy, Defense Agencies, and Commands battle for jurisdiction and funding, the result is a fragmented system muddled with political agenda, which hinders the development of a more secure system. Despite disagreements over jurisdiction, all parties agree that cyberspace will garner more attention in the future.

Increasing awareness of cybersecurity

The 2014 high profile cyber-attack on Sony Pictures highlights the growing capability of nation-state aggressors. Cyber attacks have shifted from theft and detection to destruction. Destruction of national assets by cyber attacks is considered an act of war by the US There will likely be increased public/private partnerships as the US government and US companies address the threats. Additionally, the US government will likely procure more commercial off the shelf solutions as commercial technology has surpassed the capability of purposefully built military solutions in many cases.

Theft of national intellectual property: 1-3% of GDP

The IP impacts are profound and include the pirating of products, diversion of research and development information, impacts to innovation, stolen product designs or prototypes, theft of business and manufacturing processes, as well as loss of sensitive information such as M&A plans and corporate strategy (source: PWC).

The estimated impact of trade-secret theft ranges from 1% to 3% of a nation's annual GDP (source: Center for Responsible Enterprise And Trade). Using the World Bank's annual global GDP estimate of $74.9tn in 2013, loss of trade secrets may range from US$749bn to as high as US$2.2 trillion annually.

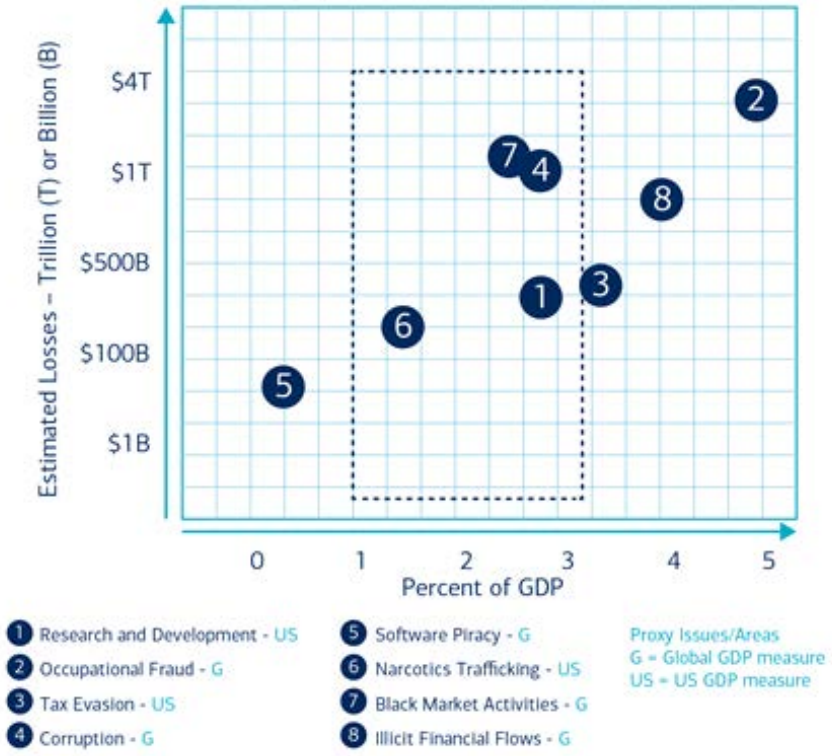
Effects of IP theft

According to The Report of the Commission on the Theft of American Intellectual Property, the effects of IP theft are two-fold:

- **Loss of revenue and reward** for those who made the inventions or who have purchased licenses to provide goods and services based on them, as well as of the jobs associated with those losses.

- **Undermining both the means and the incentive for entrepreneurs to innovate**, which will slow the development of new inventions and industries that can further expand the world economy and continue to raise the prosperity and quality of life for everyone

Exhibit 54: Proxies for Estimate of Trade secret theft

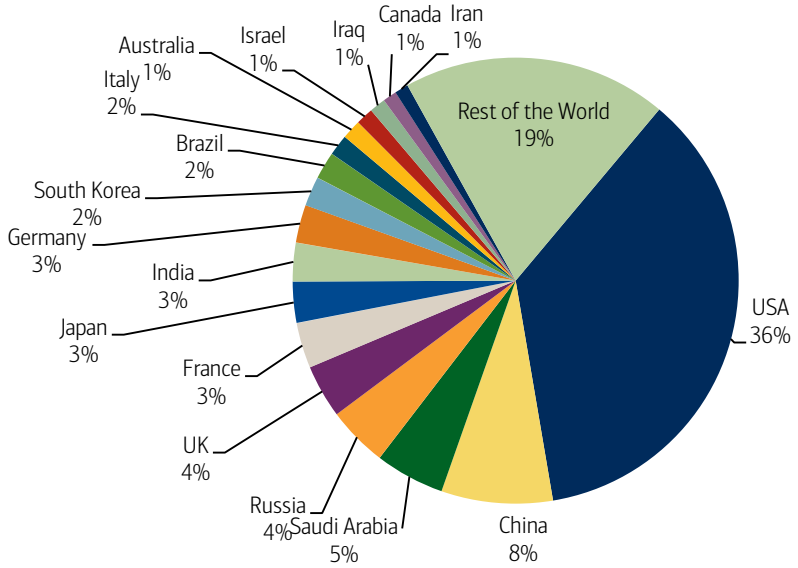


Source: Center for Responsible Enterprise And Trade

Defence spending, US still #1

Global defence spending is still essentially a story of Emerging Markets (EM) growth with a bleak outlook and budget squeezes in Western Europe and the US. That said, the US remains the largest defence spender with 36% of the global budget in 2014 (Source: Military Balance, BofA Merrill Lynch Global Research) and global defence spending totals are higher than in any year between the end of World War II and 2010.

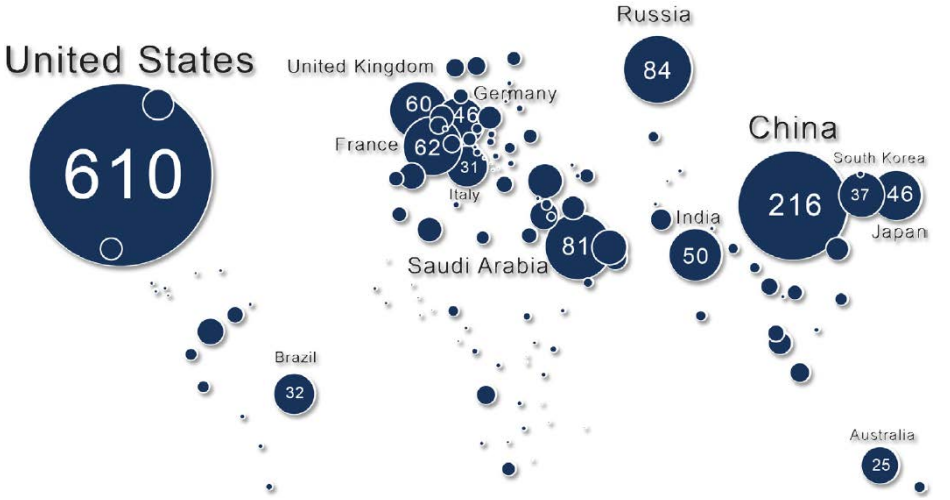
Chart 85: Geographical breakdown of military defence spending in 2014



Source: BofA Merrill Lynch Global Research, The Military Balance 2015

"US spends more on its defense budget than the next 15 countries combined"
"US Pentagon spends more than is spent on health, education, welfare, and safety by all 50 US states combined."
"US has 5% of the world's population, but almost 50% of the world's total military expenditure"

Exhibit 55: The world's largest defence budgets ($bn)

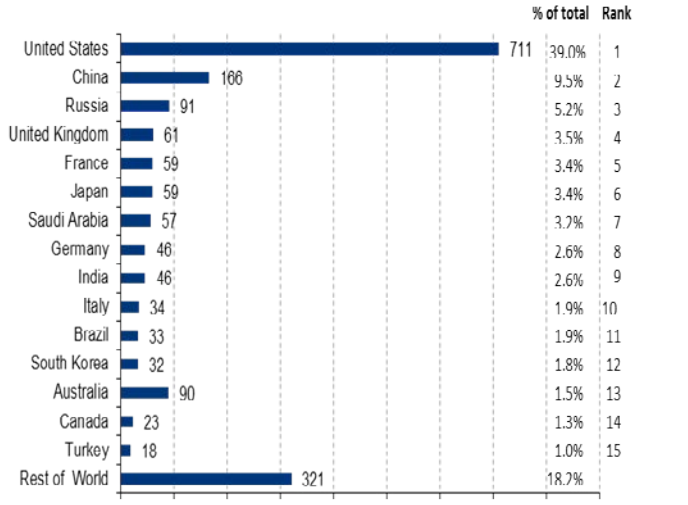


Source: Mapping Worlds, SIPRI, BofA Merrill Lynch Global Research

EMs catching up

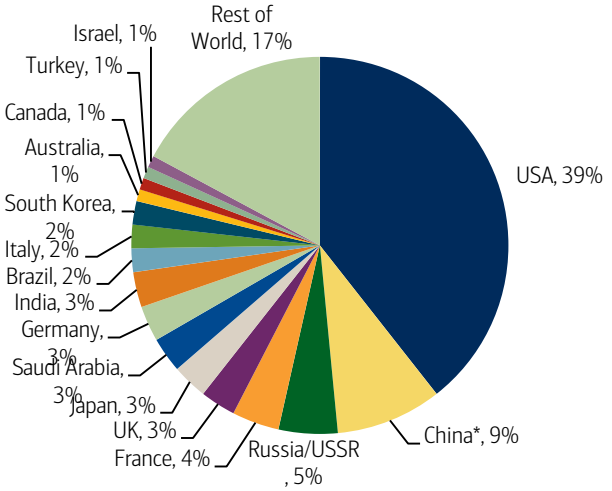
Several countries like China, India Saudi Arabia Indonesia and Turkey driven by internal and external security challenges, are forecasted to double their national security spending over the 2008-2018 period. Most other countries' national security spending growth rate will be linked to their GDP growth (Source: HSRC, SIPRI).

Chart 56: Military spending in 2012 ($bn, and % of total)



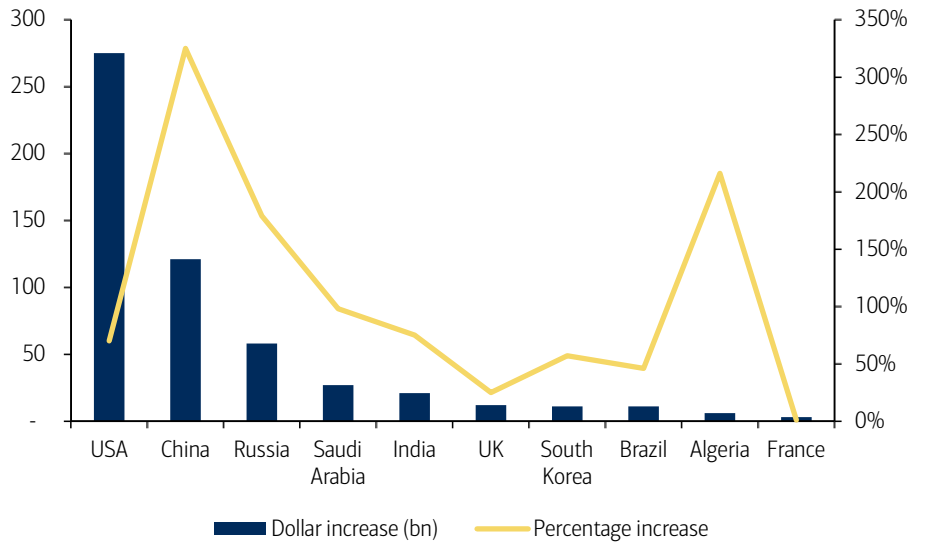
Source: Stockholm International Peace Research Institute www.sipri.org; *= SIPRI estimates

Chart 57:Geographical breakdown of military defense spending in 2010 (constant US$)



Source: Stockholm International Peace Research Institute www.sipri.org; *= SIPRI estimates

Chart 86:Military Expenditure increase 2000-2012



Source: SIPRI

Bank of America Merrill Lynch

Cybersecurity opportunities: US$75bn market today to US$170bn by 2020E

The global cybersecurity solutions market continues to grow and is estimated at US$75-77bn in 2015, with YoY growth of more than 8% from 2014 (source: Gartner). It is estimated that the market will expand at a CAGR close to 10% to reach US$170bn by 2020E (source: Markets and Markets). We anticipate fast growth for the likes of analytics, APTs, cloud security, critical infrastructure & homeland security, e-commerce & payments, encryption, mobile security, network security, and threat intelligence.

A key driver for growth is the increase in corporate spending on cybersecurity, which is now averaging 6% of IT budgets vs. 2% in 2010. The telecoms, financial services, technology and manufacturing sectors are leading the way in spending. US cyberspend budgets have grown at almost double the rate of IT budgets over the past two years, with close to 40% of retail and consumer companies – which have been targets of high-profile attacks – increasing their spending by 20%+ (source: PwC). Such investments make clear business sense in our view, given the growing financial impacts of attacks and that up to 80% of breaches are avoidable through reasonable controls.

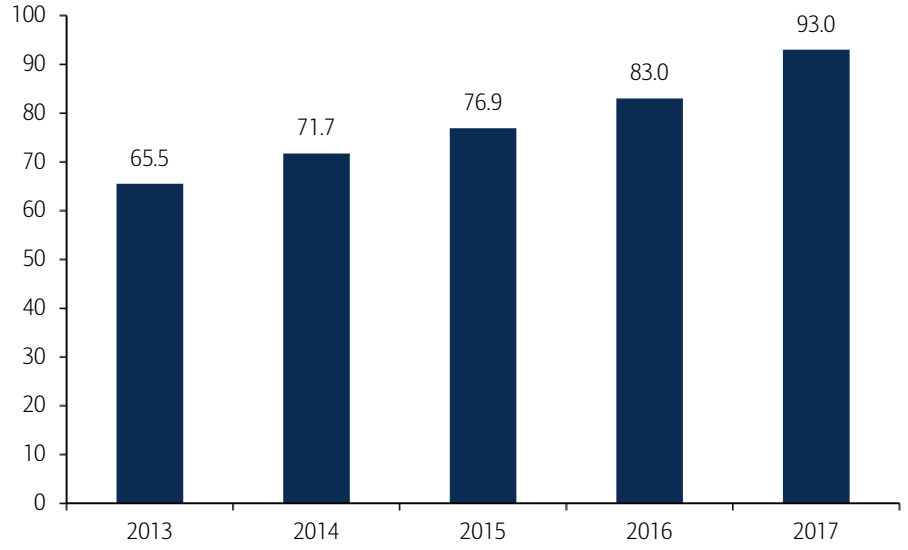
Cybersecurity is increasingly emerging as a dedicated investment theme. Beyond the size of the market itself – cybersecurity start-ups raised US$2.5bn across 224 investments in 2014, while there have been 59 cybersecurity M&A transactions in 2014-15 (source: CB Insights, Centaur Partners). We are also seeing the launch of cybersecurity ETFs and UITs – driven by their relatively strong performance vs. the benchmark.

Cyber market to more than double by 2020E

The global cybersecurity solutions market is estimated at US$75-77bn in 2015 with YoY growth of c.8.2% from 2014 (source: Gartner).

- **The aerospace, defence and intelligence vertical continues to be the largest contributor** to cybersecurity solutions today (source: MarketsandMarkets).
- **North America and Europe are the leading cybersecurity revenue contributors**, while APAC is growing rapidly driven by China, India and Southeast Asia (source: TechSci Research).

Chart 87: Global cybersecurity spending (US$bn)



Source: Gartner

Largest cybersecurity vendors

Gartner recently listed the top-five cybersecurity software vendors by revenue in 2014. From a market growth perspective, low growth in endpoint protection platforms and a decline in consumer security software — markets that together account for 39% of the market — offset the strong performance of high-growth areas, such as security information and event management (SIEM), secure Web gateway (SWG), identity governance and administration (IGA) and enterprise content-aware data loss prevention (DLP).

Symantec was the largest security software vendor by revenue ($3.7bn) and market share (17%). However IBM led the pack in terms of the growth rate 17% - more than three times its nearest competitor Intel, driven by strong SIEM solutions uptake. Overall the global security software market was valued at $21.5bn in 2014 (source: Gartner)

Table 36: Top Security Software Vendors, Worldwide, 2013-2014 (Millions of Dollars)

Company	2014 Revenue	2014 Market Share (%)	2013 Revenue	2013-2014 Growth (%)
Symantec	3,690	17.2	3,738	-1.3
Intel	1,825	8.5	1,745	4.6
IBM	1,486	6.9	1,270	17
Trend Micro	1,052	4.9	1,110	-5.2
EMC	798	3.7	760	5
Others	12,571	58.8	12,995	-3.2
Total	21,422	100	20,348	5.3

Source: Gartner

However it is the smaller players in the cybersecurity market that are making the most noise so far in 2015. According to "Cybersecurity Ventures Top 500 Companies" list, it is players like FireEye (advanced threat protection) and Norse (live attack intelligence) that are ranked as the most innovative. IBM was the highest ranked large-cap company at number 9.

Table 37: Cybersecurity Ventures' top 25 hottest and most innovative cybersecurity companies (at Q3-15)

#	Company	Cybersecurity Sector	Corporate HQ
1	FireEye	Advanced Threat Protection	Milpitas CA
2	Lancope	Network Visibility & Security Intelligence	Alpharetta GA
3	AlienVault	Threat Detection & Response	San Mateo CA
4	Norse	Live Attack Intelligence	San Mateo CA
5	Easy Solutions	Electronic Fraud Protection	Doral FL
6	AVG Technologies	Anti-Virus & Internet Security Software	Amsterdam, The Netherlands
7	RSA	Intelligence Driven Security	Bedford MA
8	IBM	Enterprise IT Security Solutions	Armonk NY
9	Veracode	Application Security Testing	Burlington MA
10	Lockheed Martin	Cybersecurity Solutions & Services	Bethesda MD
11	Clearwater Compliance	Risk Management and Compliance	Nashville TN
12	Palo Alto Networks	Threat Detection & Prevention	Santa Clara CA
13	Trend Micro	Server, Cloud, and Content Security	Tokyo, Japan
14	NuData Security	Online Fraud Detection	Vancouver, Canada
15	Code Dx	Software Assurance Analytics	Northport NY
16	Sera-Brynn	Cyber Risk Management	Suffolk VA
17	DFLabs	Automated Incident & Breach Response	Lombardy, Italy
18	Intel Security Group	Anti-Virus, Malware & Threat Protection	Santa Clara CA
19	BT	Security & Risk Management Solutions	London, UK
20	Cavirin	Automated IT & Cloud Security	Santa Clara CA
21	IT Security, Inc.	Application, Cloud, & Network Security	Pittsburgh PA
22	PwC	Cybersecurity Consulting & Advisory	London, UK
23	Herjavec Group	Information Security Services	Toronto, Canada
24	Nexusguard	Cloud Enabled DDoS Mitigation	San Francisco CA
25	SecuEra Technologies	Identity & Access Management Solutions	Washington DC

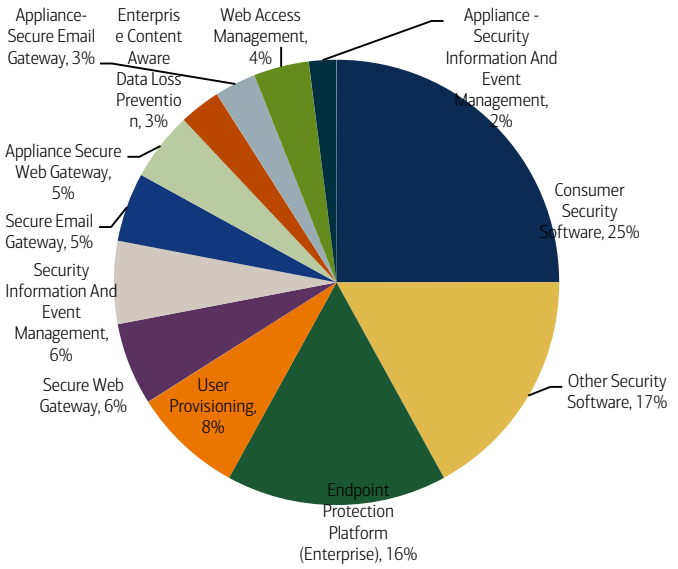
Source: Cybersecurity Ventures

Security software: $26.6bn market by 2019E

Software: Software Primer: BofA Merrill Lynch handbook for navigating Software Part V 18 May 2015

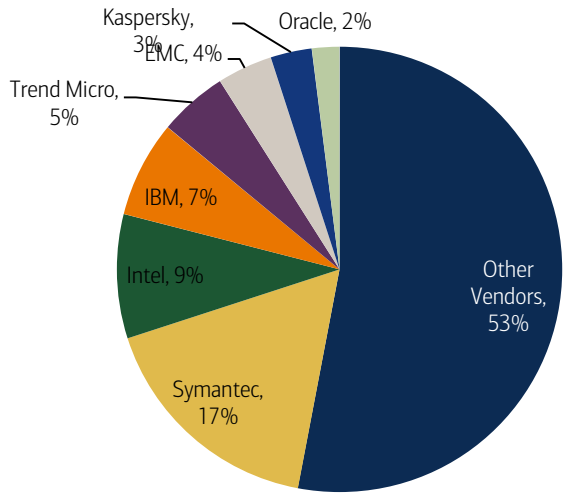
Cybersecurity software continues to be among the most resilient areas of IT spend as the sheer amount of cyber threats continues to rise. In addition, with the increase in digital commerce, consumers have the need of protecting their identity and computing devices from getting hacked. The cybersecurity software market is highly diverse with products that address a variety of security needs. Consumer and Enterprise endpoint security comprise the largest pieces. Symantec and McAfee (Intel) are the major security software providers for both enterprise and consumer markets with 17% and 9% share respectively (source: Gartner).

Chart 88: Security software vendor



Source: Gartner

Chart 89: Company market shares

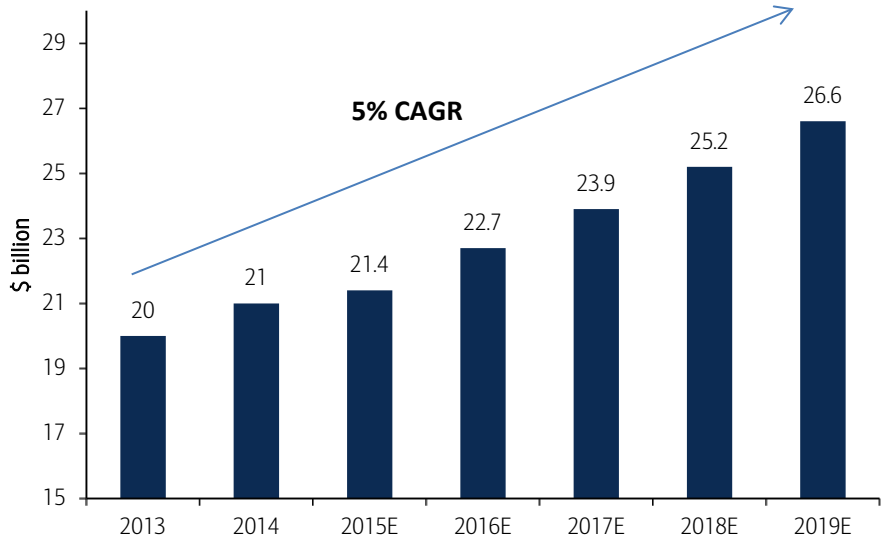


Source: Gartner

5% CAGR to 2019E

The security software market is expected to grow at a 5% CAGR from US$21.4bn in 2015 to $26.6bn by 2019E (source: Gartner). The main drivers of the market are expected to be: new freemium model, increasing adoption of security appliances and security for cloud operators & mobile/tablet devices. In addition managed security software and access management are expected to be the biggest contributors to security software growth as well

Chart 90: Security software market growth



Source: Gartner

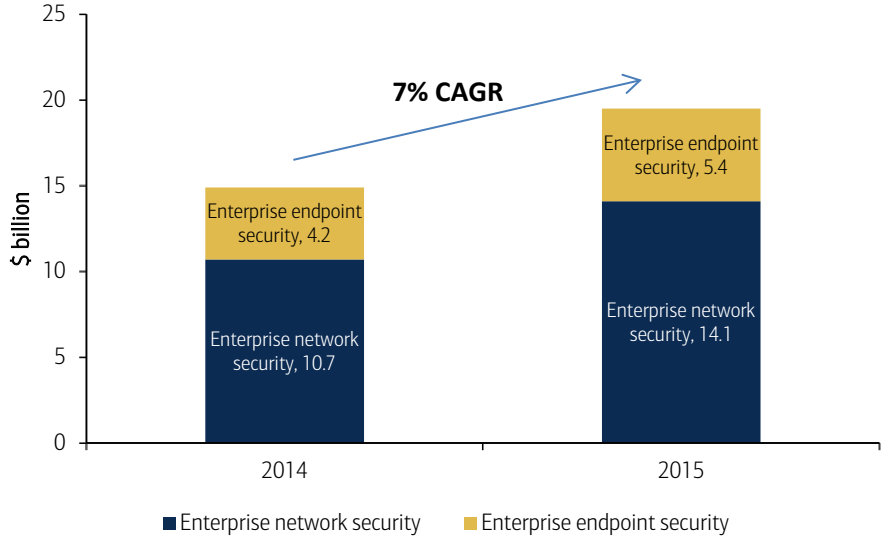
$14.53bn endpoint security market by 2019E

The global endpoint security market including: anti-virus/malware, firewall, IDS/IPS, BYOD Security, Mobile Security, MDM, MAM among others, is estimated to grow from $10.03 billion in 2014 to $14.53 billion by 2019E with a CAGR of 7.7% (source: MarketsandMarket).

$19.5bn enterprise market by 2018E

The enterprise market, comprising of both endpoint and network segments, is forecasted to growth from just under $14.9 billion in 2014 to $19.5 billion by 2018E (source: Palo Alto Networks, IDC). The market players can roughly be defined as those serving customers within the small corporates to large organisations domain, rather than consumers or end-users per se.

Chart 91: Enterprise security market



Source: Palo Alto Networks, IDC

Bank of America Merrill Lynch

$4.5bn SIEM market by 2019E

Security information and event management (SIEM) is defined as applying security analytics to real time events for the detection of targeted attacks and data breaches, and hence logging these for reference to prevent future attacks in an enterprise environment. It is considered a mixture of both software and serviced based cybersecurity solution. The total SIEM market is expected to grow from $2.57 billion in 2014 to $4.54 billion by 2019E at a CAGR of 12.0% (source: MarketsandMarkets). However the main weakness of SIEM is that it is only able to detect known threats, with unknown entities often being able to bypass the system. Hence emerging areas such as big data analytics, which we outline later, are crucial in driving the SIEM space to be able to deal with the latest threats.

Exhibit 58: Magic Quadrant for security information and event management

Source: Gartner

$170bn cybersecurity market by 2020E

It is estimated that the global cybersecurity solutions market will deliver a CAGR of 9.8% to reach US$$170bn from 2015 to 2020E (source: Markets and Markets). High-growth areas include security analytics (SIEM) (10%), threat intelligence (10%+), mobile security (18%) and cloud security (50%) (source: IDC).

Company spending is finally on the rise

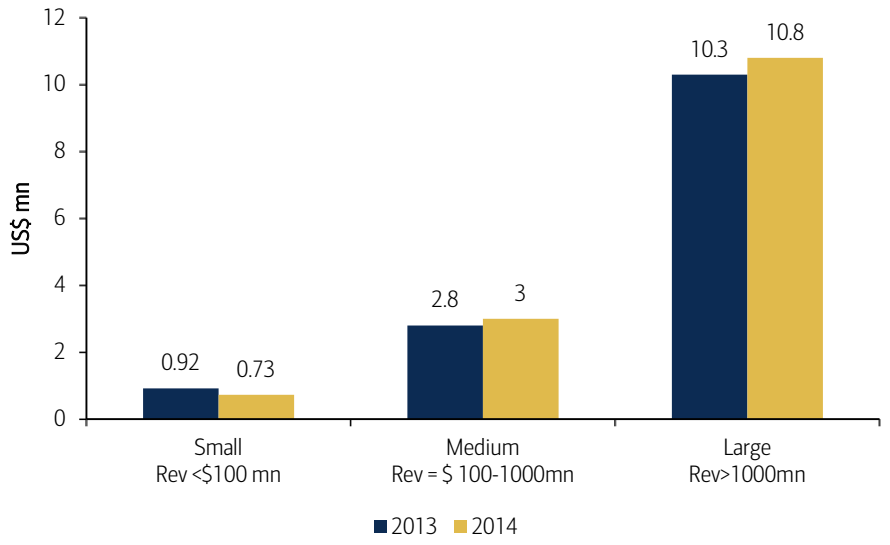
In response to the increasing number of threats and incidents, and sophistication, corporates are finally looking to increase their cybersecurity budgets. This has been a traditional challenge with one in eight companies thought to have been spending less than 1% of their IT budget on cybersecurity in recent years. Positively, cybersecurity spending is now averaging as much as 6% of IT budgets across sectors and growing at close to double the rate of IT budgets (source: PwC).

> US cybersecurity budgets have grown at almost double the rate of IT budgets over the last two years (source: PWC)

Cybersecurity budgets for large caps: +5% in 2014

Cybersecurity budgets for large-cap companies with revenues of US$1bn+ increased by 4.96% YoY in 2014 to reach US$10.8mn. Spending for medium-sized companies rose by 7.1% over the same period, while small cap companies registered a 20.6% decline. Large caps are also more likely to substantially increase cybersecurity spending – with 20% of companies with >10,000 employees raising investment by 20%+ in 2014 (source: PWC).

Chart 92: Cybersecurity budget by company size (US$, 2013-2014)



Source: PWC

Cyber spend by sector: 6% of IT budget on average

As most companies do not disclose cybersecurity spending, estimates of actual spend vary widely. PwC's latest surveys show that cyber represents an average of 6% of total IT spend across sectors (vs. c.2% in 2010). The telecoms, financial services, technology and manufacturing sectors spend the most at >8% of the IT budget, while travel, leisure and entertainment, retail & distribution, and property & construction spend below the 6% average (source: PwC).

Table 38: Sector spend most on security

Average rate of increase (net # of companies reporting increase)	Average current security spend (as % of IT spend)		
	Below average (<6%)	Aver. (6-8%)	Above aver. (>8%)
High (more than +50%)	Travel, leisure and entertainment		Telecommunications
Average (between +30% and +50%)	Retail and distribution	Utilities, energy and mining	Financial services, Technology, Manufacturing
Low (less than +30%	Property and construction	Government, health or education	

Source: PWC, BofA Merrill Lynch Global Research

> The appropriate level of cybersecurity investment varies by sector, threat environment, current levels of spending, and the maturity of cyber defences

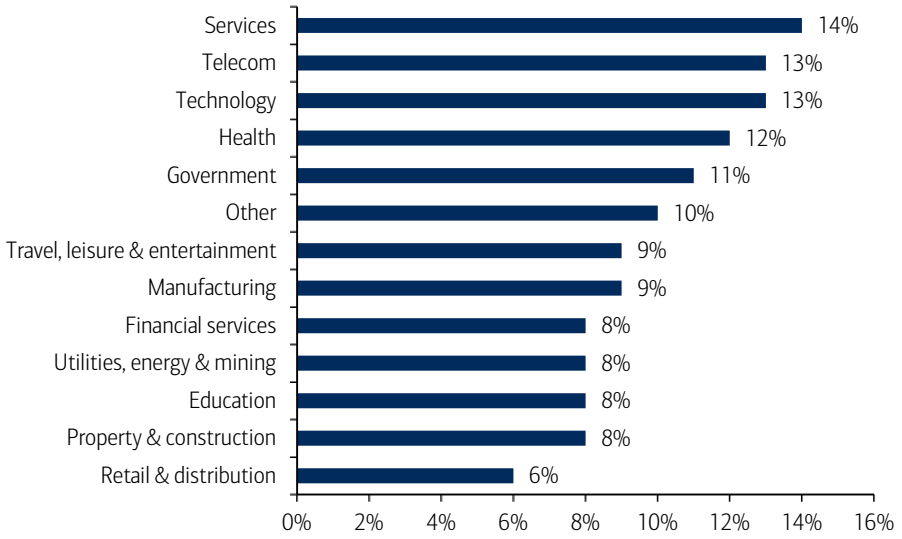
UK cyberspend estimates: 6-14% of IT spend

According to one recent survey, the leading UK sector in terms of allocating the largest proportion of its IT budget to cybersecurity is services (14%) followed by telecoms

Bank of America Merrill Lynch

(13%) and technology (13%) in joint second (source: BIS, PwC). What is surprising is the relatively low IT spend on cyber in the financial services industry where other industries such as travel, leisure and entertainment rank above it. In our view, this underlies the potential risk of underinvestment in an industry where monetary losses from cyber breaches are likely to be much higher than in other sectors.

Chart 93: % of the IT budget being spent on cybersecurity



Source: BIS, PwC

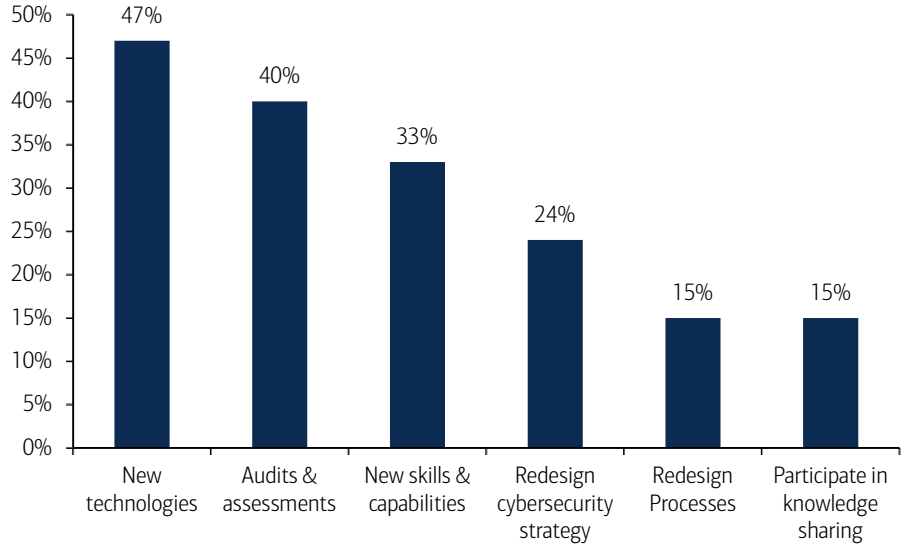
Retail & consumer sectors increasing budgets most significantly

US cybersecurity budgets have grown at almost double the rate of IT spending over the past two years. At a sector level, 38% of retail and consumer companies, which are frequent targets of attack, increased their security spending by 20%+ in the past year, higher than in any other industry. In contrast, only 17% of banking and finance and 15% of healthcare respondents reported 20% increases in security budgets (source: PwC).

Spending priorities: new technologies, audits & assessments

New technologies rank as the #1 priority for increased cybersecurity budgets followed by audits and assessments, according to a 2015 PwC collaborative survey with CSO, the U.S. Secret Service, and the Software Engineering Institute CERT Division at Carnegie Mellon University. Technology is a clear focus with 69% of respondents to PwC's 2015 Digital IQ survey saying they are investing in cyber tech more than any other spending category. Somewhat worryingly, only 33% of surveyed executives prioritised spending on adding new skills and capabilities.

Chart 94: Cybersecurity spending priorities



Source: PwC

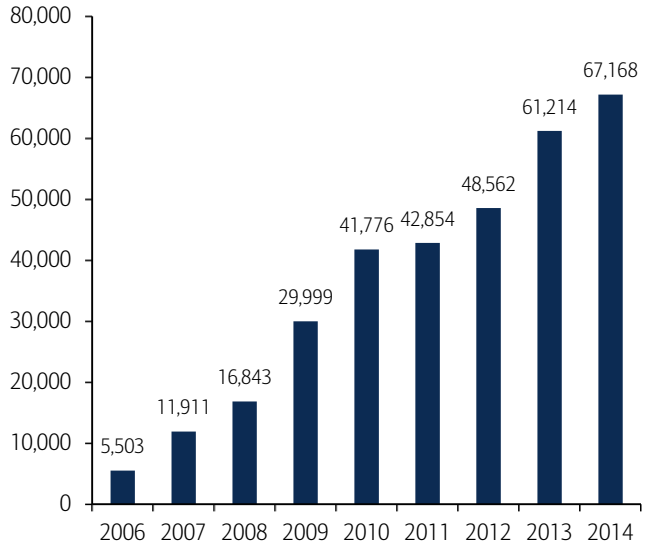
Government spend also accelerating

Just like corporates, governments are also increasing their cybersecurity spend as part of their national budgets. Unsurprisingly the US government are the leaders in this space given cyber is increasingly also becoming a homeland problem and with the growing number of attacks each day. However other countries are also recognising cyber as a national risk and picking up their efforts in response.

US, $78.8bn cumulative cyber spend between 2006 – 2013…

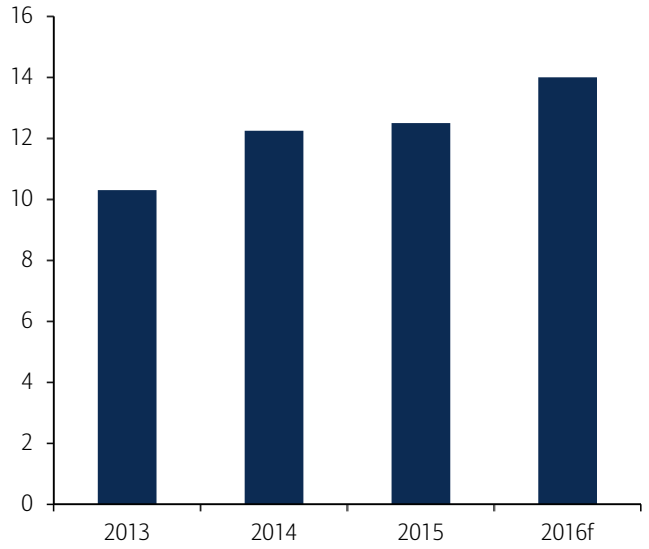
The number of information security incidents affecting systems supporting the federal government increased each year between 2006 - 2014. This figure rose from just 5,503 in 2006 to 67,168 by 2014 representing an increase of over 12x (source: GAO). In response the US Federal Government spent US$78.8bn in total on cybersecurity between 2006 – 2013, and this is expected to reach US$14bn in 2016E alone (source: Business Sweden et al). Despite cuts to IT budget by the US government since 2011, cybersecurity spend has by in large still grown steadily.

Chart 95: Incidents reported by Federal agencies



Source: GAO

Chart 96: Cyber spending by US Federal Govt (US$bn)

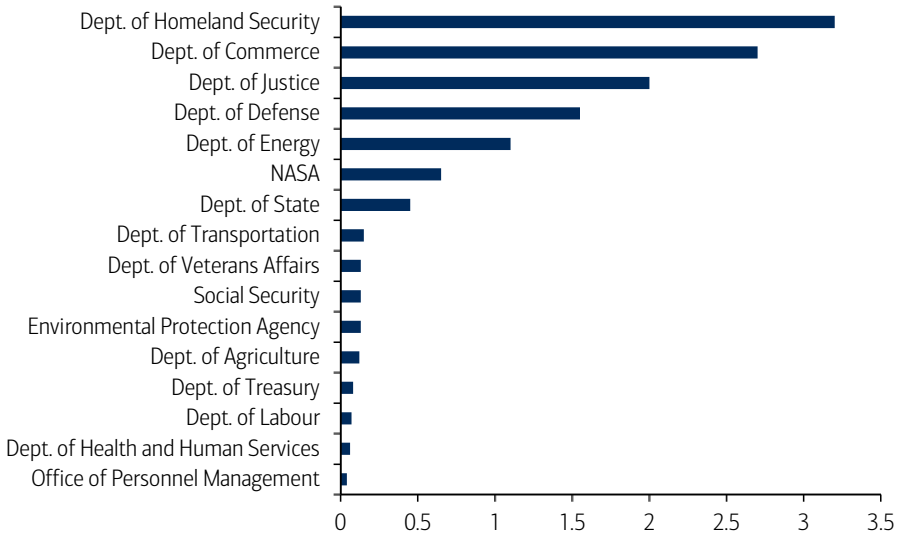


Source: Business Sweden et al

...but cyber still less than 4% of US dept. budgets

However US departments are still not spending enough on cybersecurity, in our view. Despite seemingly facing an increasing wave of attacks, spend on cybersecurity as a percentage of total department budget is still low. In fact, only the Department of Homeland Security spends more that 3% of its 2014 budget on cybersecurity (source: US office of Management & Budget) The Office of Personnel Management spent the lowest percentage on cybersecurity out of all the departments, which is significant since it suffered the biggest US agency breach to date.

Chart 97: % of 2014 big budget spend on cybersecurity



Source: OMB

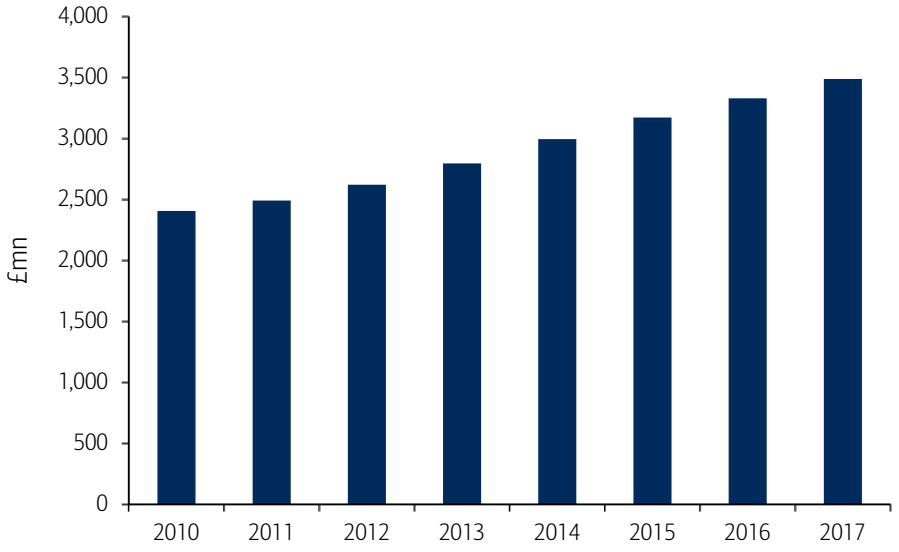
UK, £3.5 billion market by 2017E

The UK has the fifth largest, and arguably the second most mature, market for IT products and services in the world, with particular pockets of need like financial services in the City of London; thus there is a proportionately high demand by organisations for cyber solutions to meet their particular need. A considerable British cyber security skill-base within the UK operations of foreign-owned companies, such as IBM, HP, Capgemini, Lockheed Martin etc., and thus addressing many of the different market sub-segments.

> "Britain's military systems, which together make up the single-largest computer network in Europe, log more than 1 million suspicious incidents every 24 hours. The MoD has to fend off hundreds if not thousands of cyber-attacks everyday" – Brigadier Alan Hill, Head of MoD's ISS

The cybersecurity market in the UK is forecasted to grow from £2.8 billion in 2013 to £3.5 billion in 2017E, with a CAGR of 5.7% (Source: Pierre Audoin Consultants). By comparison, the total IT market in the UK is set to only grow by 2.1% CAGR during the same period. This underlines our view that we expect cyber to continue to be a high growth market even developed markets.

Chart 98: UK Cyber security market size



Source: Pierre Audoin Consultants

Israel, $6bn+ cyber products exported

Israel stands out as a leader in small specialists; due to its political position and history, it has a very focused agenda to produce leading-edge solutions for the military/intelligence community (although like the UK, there is a long history of its best startups being acquired by larger overseas players mainly in the US).

Israel is considered an international leader in cybersecurity with its "Unit 8200" which is the largest military unit of the Israel Defence Forces (IDF). For instance, in 2014, Israel exported more than $6 billion in cybersecurity products which was double the total in 2013 (Source: 5th Annual International Cybersecurity Conference, 2015).

Bank of America Merrill Lynch

Cyber deal-making is on the rise

Major cybersecurity deals are on the rise – with cybersecurity start-ups having raised US$2.5bn across 224 investments in 2014 (vs. <US$1bn from 108 deals in 2010) (source: CB Insights). The number of seven-figure deals increased by 40% YoY (source: FBR & Co.).

- **The most active investors from 2010 to 2Q15** were Intel Capital. Kleiner Perkins Caufield & Byers, Andreessen Horowitz, and Accel Partners. Together, the six actors each invested in 10 or more cybersecurity companies during the period. Andreessen Horowitz was the most active early-stage investor, while Google Ventures and Accel Partners shared second (source: CB Insights).

- **The biggest funding recipients over the same period** were Good Technology which raised more than US$500bn, Lookout with close to US$300mn and OpenPeak with over US$200mn (source: CB Insights).

Significant increase in M&A activity

There has also been a significant increase in cybersecurity M&A with 59 transactions for 2014-15 (vs. 24 in 2012). Vista Equity's US$4bn acquisition of Tibco Software is the largest transaction YTD in 2015 (source: Centaur Partners)

Table 39: Recent cybersecurity transitions (US$mn)

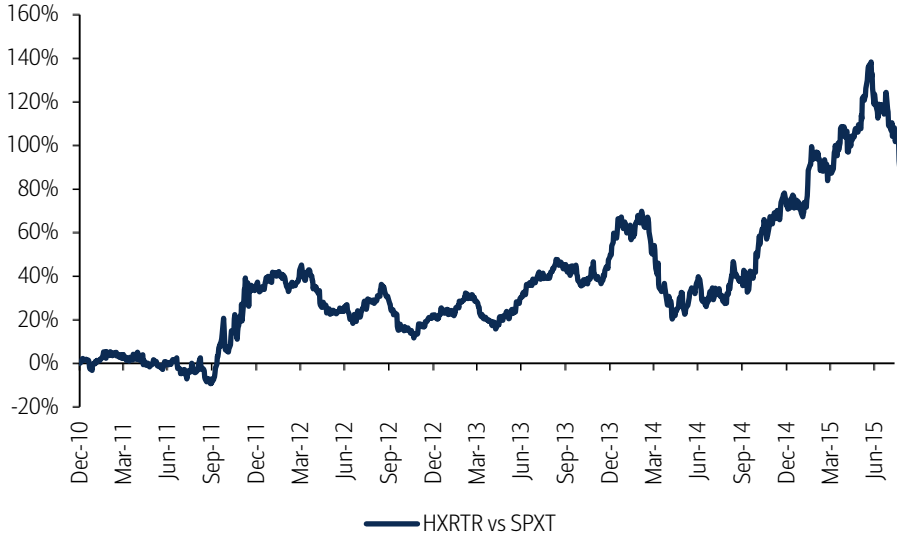
Announced	Acquirer	Target	Target Abstract	Val./Rev.	Total deal amt.	Target TTM rev.
18/04/2015	Raytheon	Websense	Develops software to protect organisations from cyberattacks and data theft	3.7	3,958	1,076
29/09/2014	Vista Equity Partners	Tibco	Provides infrastructure and business intelligence software	3.7	3,958	1,076
02/03/2015	HP	Aruba	Provides enterprise mobility solutions worldwide	3.3	2,651	812
13/10/2014	Netscout	Arbor, Fluke, Tektronic	Providers of network security, testing and management solutions	NA	2,619	NA
02/07/2012	Dell	Quest Software	Enterprise Systems Management Software	2.8	2,382	857
23/07/2013	Cisco	Sourcefire	Provider of intelligent cybersecurity solutions	9.6	2,245	233
22/01/2014	Vmware	AW	AirWatch was a provider of enterprise mobile management and security solutions	NA	1,540	NA
13/03/2012	Dell	Sonicwall	Network security and data protection	4.8	1,250	260
12/12/2011	Thoma Bravo	Blue Coat	Business applications	2.4	1,105	467
28/10/2014	Engility	TASC	Provides wide range of IT security analysis	NA	1,100	NA
30/12/2013	FireEye	Mandiant	Information security company	NA	1,034	NA

Source: Centaur Partners

Cybersecurity is becoming a major investment theme

Investors are increasingly looking to understand the investment potential of the cybersecurity theme. Ove the past two years, we have seen the launch of thematic products such as Pure Funds ISE Cyber Security ETF (HACK), First Trust NASDAQ CEA Cybersecurity ETF, and the First Trust BofA Merrill Lynch Cybersecurity Portfolio (UIT).

Chart 99: ISE Cyber Security Index vs S&P 500 Index relative performance

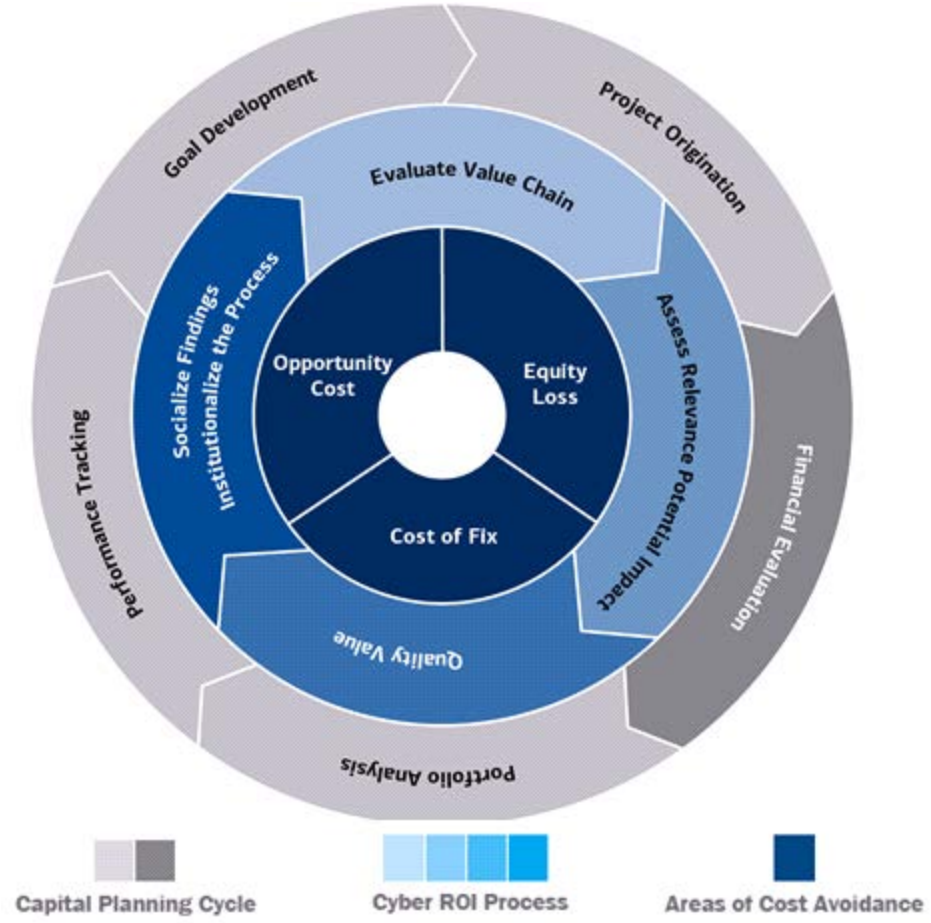


Source: Bloomberg
Rebased to 100 as on 31-Dec-2010

Cyber solutions ROI: huge financial benefits

We anticipate that the financial impacts of cybersecurity will increasingly hit companies' bottom lines. While disclosure is relatively sparse on the impacts, North Korea's hack on Sony resulted in a major hit to total sales for FY14 of less than 2% (source: Company reports). The corollary is that investments in cybersecurity make good business sense as the Pareto principle (80-20 rule) applies, with 80%+ of breaches avoidable through reasonable controls.

Exhibit 59: Cyber ROI planning cycle



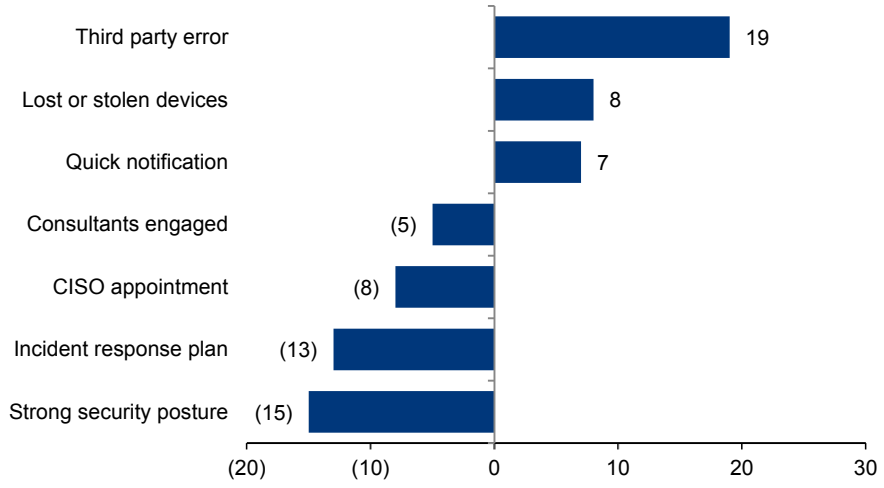
Source: Booz Allen Hamilton

The factors that impact the cost consequences

> In the US, an incident response plan can reduce costs by up to US$42 and strong security postures by US$34

The Ponemon Institute has identified seven factors that the influence the cost consequences of a data breach: third-party errors, lost or stolen devices, quick notification, a strong security posture, incident response planning, CISO appointments and consulting support.

Chart 100: Impact of seven factors on the per capita cost of data breach

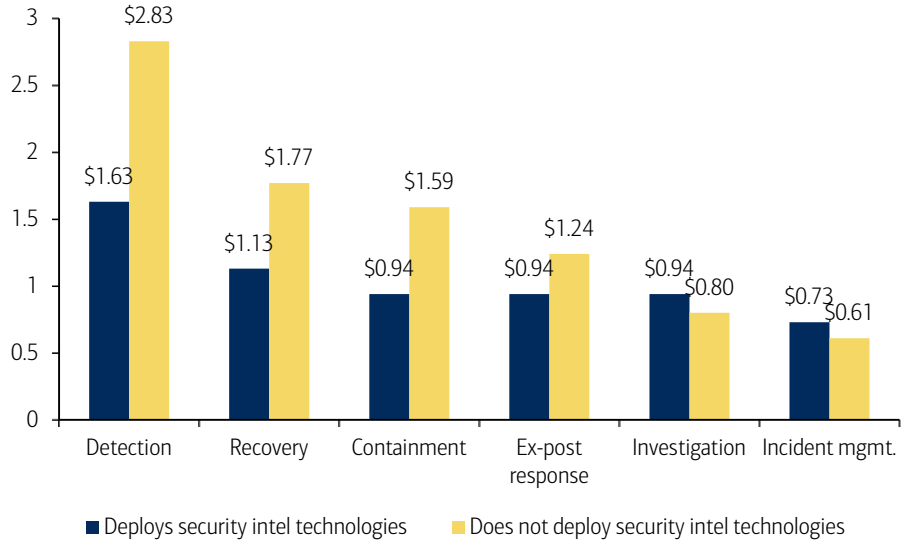


Source: Ponemon Institute, BofA Merrill Lynch Global Research

Stronger security measures = lower losses

Organisations deploying cybersecurity intelligence technologies realise a lower annualised cost of cybercrime. The largest cost differences pertain to detection, recovery and containment activities (Source: Ponemon Institute for HP Enterprise Security).

Chart 101: Activity cost comparison and the use of security intelligence technologies



Source: Ponemon Institute for HP Enterprise Security , BofA Merrill Lynch Global Research

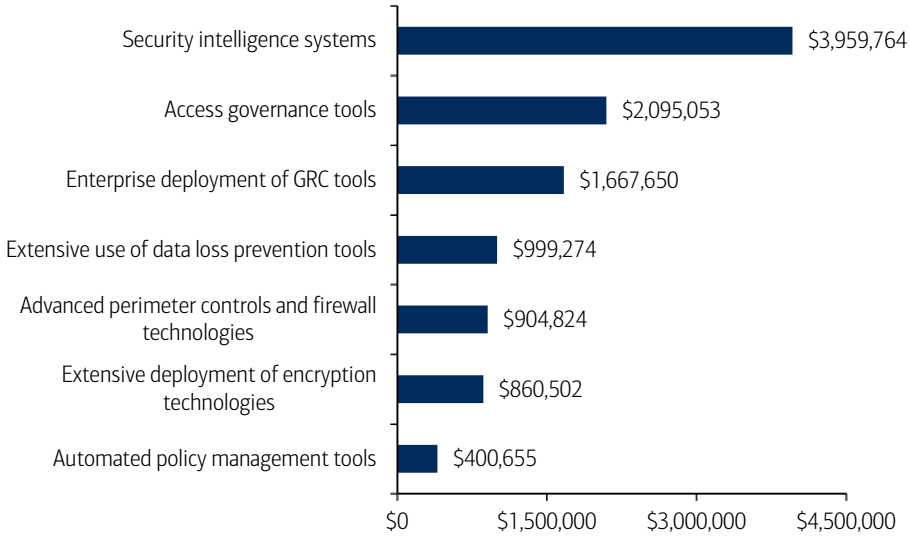
Among the most seven commonly deployed security technologies, security intelligence systems and access governance tools facilitated the most substantial cost savings. In terms of the estimated ROI realised by companies, security intelligence systems ranked highest (21%), followed by extensive deployment of encryption technologies (18%) and advanced perimeter controls and firewall technology (14%).

Table 40: Estimates ROI for seven categories of enabling security technologies

Security technologies	ROI
Security intelligence systems	21%
Extensive deployment of encryption technologies	18%
Advanced perimeter controls and firewall technologies	14%
Access governance tools	11%
Extensive use of data loss prevention tools	10%
Enterprise deployment of GRC tools	6%
Automated policy management tools	5%

Source: Ponemon Institute Research, BofA Merrill Lynch Global Research

Chart 102: Cost savings when deploying seven enabling security technologies



Source: Ponemon Institute Research, BofA Merrill Lynch Global Research

Companies need to adopt a lifecycle cost approach

There is a need for a proactive approach to cybersecurity from all stakeholders given the rising complexity and volume of threats. Organisations need to consider both the potential benefits and costs of their approach to Information Security with a holistic approach like the 'Total Lifecycle Cost of Information Security' model.

Table 41: Total lifecycle cost of Information security

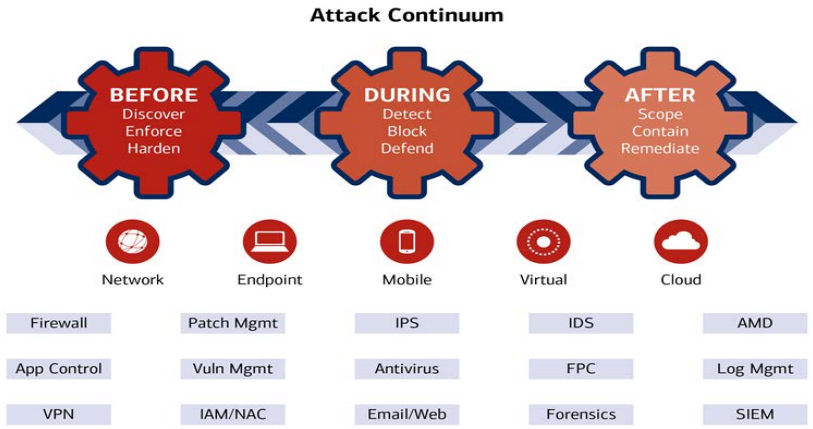
Definition	Total Lifecycle Cost of Information Security	= Lifecycle costs of deploying and operating security solutions	+ Reputational value	+ Intellectual Property value	+ Operational effectiveness	+ Financial impact of incidents
		Hardware/software solutions Training Consultancy costs People costs	Brand volume Customer satisfaction/ confidence	R&D information Customer databases Competitive information	Productivity Ability to service customers Cost to serve customers	Direct financial loss from attack

Source: PwC, BofA Merrill Lynch Global Research

Solutions: next-gen technologies & the road to resilience

Totally eliminating cybersecurity risk is impossible, in our view. Instead, organisations must look to develop better cyber resilience – the ability to resist, react to and recover from potentially catastrophic cybersecurity threats, and reshape their environments for increasingly secure, sustainable cyber operations. This will require both traditional and nextgen technology solutions and processes, as well as more resilient leadership cultures and networks, and change readiness (source: Ernst & Young).

Exhibit 60: The Threat-Centric Security Model



Source: Cisco

Given that threats are coming from multiple vectors and becoming increasingly sophisticated with advanced attacks going undetected for a median of 205 days (source: Mandiant), traditional perimeter-oriented defences and standalone solutions are becoming out-dated. A one-size-fits-all approach is no longer a solution; instead, organisations need to adopt multiple tools that are tailored to the different layers of their specific threatscape (eg, across applications, BYOD, data, IoT, networks, endpoints, mobiles, virtual, the cloud etc.) – as well as before, during and after attacks.

We anticipate fast growth for the next generation of cybersecurity solutions, which can help defenders to become more resilient and keep up with the 'bad guys' including: analytics, advanced persistent threats (APTs), automated incident response, biometrics, cloud security, cognitive security, consulting services, critical infrastructure & homeland security,
e-commerce & payments, endpoint security for IoT, encryption, hardware-enhanced security, mobile security, nextgen firewalls, network security, privileged account management (PAM), and threat intelligence.

Table 42: Cybersecurity threat defenses used by organisations in 2014

	Security threat defences used		Defenses administered via cloud-based services	
	SecOps	CISO	SecOps	CISO
Network security, firewalls/intrusion prevention	57%	64%	30%	39%
Web security	56%	62%	33%	41%
Email/messaging security	53%	58%	33%	41%
Data loss prevention	55%	55%	-	-
Encryption/privacy/data protection	52%	55%	-	-
Access control/authorization	55%	52%	24%	24%
Authentication	54%	51%	24%	22%
Mobility security	48%	54%	24%	32%
Secured wireless	47%	52%	22%	30%
Endpoint protection/anti-malware	45%	52%	24%	27%
Vulnerability scanning	44%	51%	24%	26%
VPN	49%	46%	25%	27%
Identity administration/user provisioning	43%	47%	16%	23%
Security Information and Event Management (SIEM)	39%	46%	-	-
Network forensics	41%	43%	-	-
Patching and configuration	38%	40%	-	-
Penetration testing	39%	37%	20%	19%
DDoS defense	35%	37%	-	-
Endpoint forensics	29%	33%	-	-

Source: Cisco

Traditional software: first line of defence

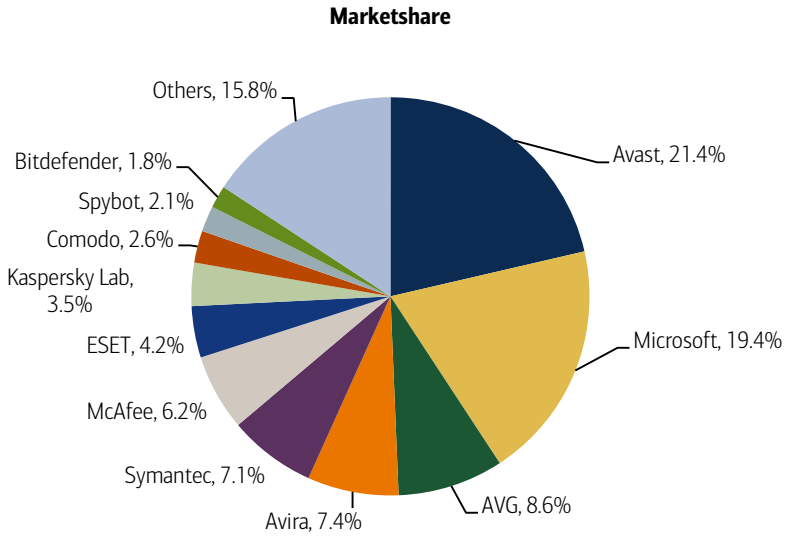
Traditional consumer and enterprise cybersecurity software safeguards against viruses, phishing, and other Internet threats; blocks dangerous websites and identifies unsafe links in websites, social networks, email, and instant messages; and protects against identity theft by detecting phishing emails and providing password management features (source: Trend Micro). Such solutions are becoming increasingly ineffective given the rapidly expanding threatscape, but are still necessary as a first line of defence to attackers.

Antivirus software

Antivirus software protects programmable devices from attack by detecting and eliminating viruses. It was mainly shareware in the early years of the internet, but there are now several free security applications on the internet to choose from for all platforms. Security suites were first offered for sale in the early 2000s and contain a suite of firewalls, anti-virus, anti-spyware and more.

Such software relies purely on signatures, which makes it fundamentally incapable of detecting advanced persistent threats that exploit vulnerabilities inside commercial software. It could take months for AV software to develop a signature for a threat, and practitioners therefore note a low detection rate of about 50%. Today's advanced threats are able to run directly inside the OS kernel, have full access to the endpoint's resources, therefore making them impossible to detect by anti-virus.

Chart 103: Antivirus market share by vendor, 2015



Source: OPSWAT, Avast

Firewalls

Firewalls provide protection against outside attackers by shielding computers or networks from malicious or unnecessary network traffic and preventing malicious software from accessing the network. These generally consist of gateways and filters which vary from one firewall to another (eg, packet filters, stateful firewalls and application-level firewalls). Firewalls also screen network traffic and are able to block traffic that is dangerous

Firewalls are not designed to inspect the data payload of network packets, making them blind to malicious content inside network traffic. Firewalls are also unable to detect and block weaponised links within emails since they do not interact with SMTP. Lastly, firewalls are unable to block threats that have bypassed the perimeter and spread onto internal file shares or that have attempted to enter through a different vector of attack, such as through the email gateway.

Email and web filters

Anti-filters protect users from everyday threats such as phishing, spam and malicious content that is delivered via email or web portals. Email filters check the origin or content of a mail against a set of rules and automatically puts this in a junk folder if it detects abnormality. Similarly, web filters block out pages from websites that are likely to include spyware, viruses, drive-by-downloads, and pornographic content among others. In most instances, filters are offered for free as part of the basic package for programs like Microsoft Outlook (email) and Google Chrome (browsers). Although these filters block common and known signature-based threats, they are unlikely to be able to detect more sophisticated threats.

Passwords

A password is a string of characters used to authenticated a user and hence grant him or her access to a system. Although not software per se, passwords are still an important part of the traditional cybersecurity architecture as they are used universally in many IT devices, from computers to ATMs. Password security has undergone a series of changes since the very first were use, which includes improving the complexity of the character sequence, two-factor authentication and one-time-password tokens. However, passwords by themselves are still not enough to counteract modern-day cyber threats because of the possibility of human error such as disclosing it unknowingly via a phishing scam.

Intrusion detection/prevention (IDS/IPS)

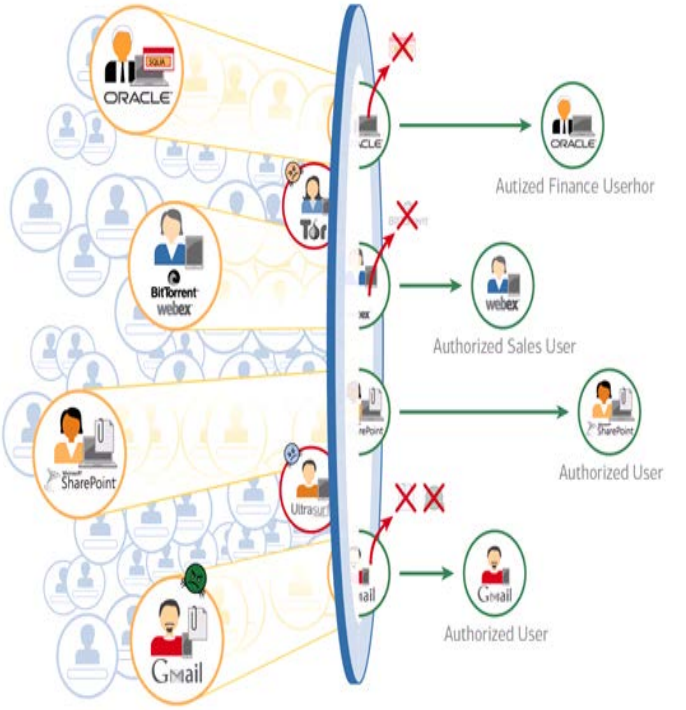
IDS/IPS products are sold as standalone solutions. They are connected to a switch or a network node, and actively monitor and/or analyse network traffic to detect and/or stop attacks. IPS/IDS were developed to address firewalls' visibility and granularity limitations. One key limitation of these solutions is embedded in their underlying detection mechanism. Similar to antivirus solutions, IPS/IDS products compare the incoming traffic to a database of known threat signatures, making them reactive and unable to spot unknown vulnerabilities. IPS technology was built originally to detect and analyse network service-based attacks, rather than the client-side application attacks that have become the more popular target for hackers, which include browsers, PDF readers and flash plug-ins.

UTM: single-security system performing multiple functions

United threat management (UTM) essentially seeks to perform multiple cybersecurity functions through one single system – providing a 'silver bullet' solution for stakeholders – by integrating security features: traditional firewalls, intrusion detection systems, anti-malware, and web filtering among others (source: IDC).

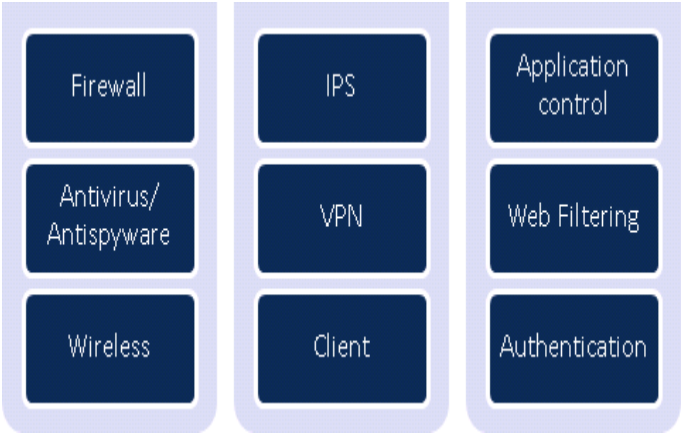
UTM is also described as next generation firewalls (NGFW), as a mark-up from the traditional firewall protection methods, ie, move away from identifying threat signatures to monitoring behaviour patterns. For instance, it can read the content of incoming traffic, not only its IP address, and make decisions based on the type of application and a set of access policies. Overall, UTM reflects a general trend over the past decade for incumbents and new entrants alike to provide a solution that deals with the ever evolving threatscape.

Exhibit 61: Palo Alto's illustration of its next generation firewalls



Source: Palo Alto Networks

Exhibit 62: Overview of what security products are included in a UTM platform



Source: Fortinet

US$4.5bn market by 2019E: Check Point and Palo Alto are the leaders

The UTM market is expected to increase from US$2.6bn in 2014 to US$4.5bn by 2019E at a CAGR of 11.5% (source: MarketsandMarkets). Many market providers of UTM are still deemed 'niche players' who lag the capabilities of cyber attackers with very few 'leaders', according to Gartner's 'Magic Quadrant' matrix. As of mid-2015, Check Point

and Palo Alto Networks are seen as the true leaders in this space followed by Fortinet and Cisco as the 'challengers'.

Exhibit 63: Magic Quadrant for enterprise network firewalls

Source: Gartner

Next-gen software: protection against unknown APTs

With threat agents increasingly being found within a system, stakeholders need to move away from traditional 'static' perimeter defences, in our view. Instead, organisations must explore new threat protection models in which their defence architecture incorporates a 'behavioural-based' layer that goes beyond signature identification to address today's new breed of cyberattacks. Overall, next-gen cyber solutions are intended to augment, not replace, existing security systems by adding a layer to the threat-protection fabric that defends against more sophisticated cyberattacks, which often have already breached the traditional first line of security defence.

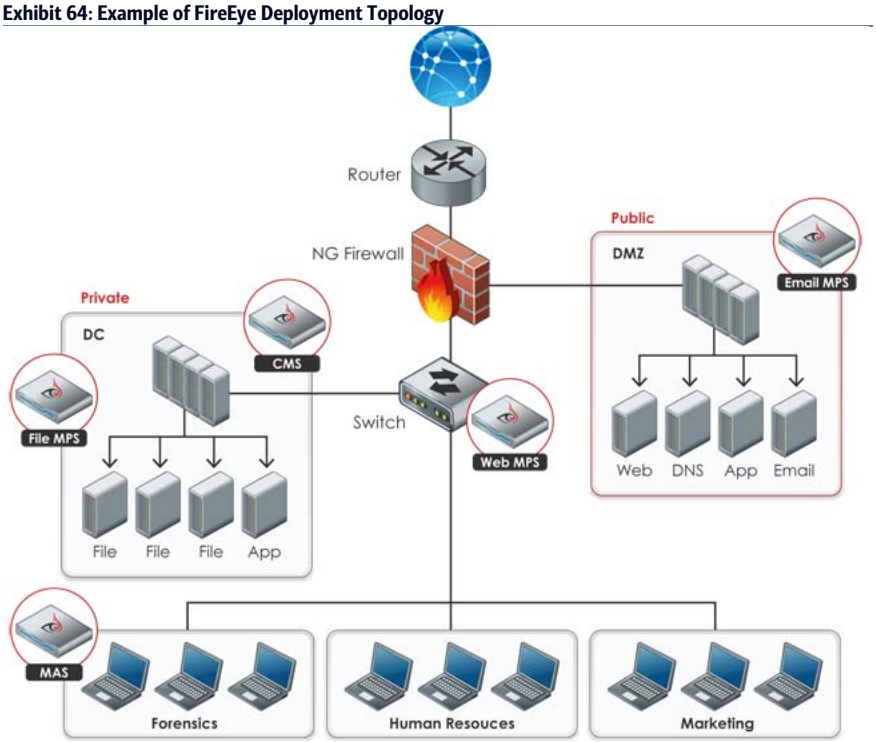
APTs: spotting abnormal behaviour in the 'sandbox'

FireEye Inc.: Redefining network security; initiating with a Buy 15 October 2013

Instead of being limited to a list of known threats, advanced threat protection (ATP) solutions focus on the behaviour of traffic (ie, abnormal activity by the 'bad guy') rather than signature. Players in this space emulate the desktop environment of the target recipient in an isolated location, tricking the incoming traffic into thinking that it has reached its final destination. It then simply watches its behaviour for abnormalities (opening files, sending emails, etc.) – a method dubbed 'sandboxing'. It also employs procedures that aim to detect steps typically taken by threats. For example, it 'listens' to the return path, trying to detect if the threat is reporting to its base ('phoning home') about a successful penetration.

Bank of America Merrill Lynch

Exhibit 64: Example of FireEye Deployment Topology



Source: Company reports

How companies like FireEye operate

Appliances (MPS) typically are installed at internet egress points in corporate networks and next to email and file servers. These appliances sit either directly on the traffic's path (in-line) or outside it (out of band). The inbound traffic is inspected across multiple types for exploits (incl. HTTP, SMTP, JavaScript, images, flash and PDF), while outbound traffic is analysed for unauthorised call back to criminal servers (Command and Control Centre, or CnC), indicating an infected PC is within the corporate network.

When network traffic enters the appliance, it is captured through the kernel, which then begins various kinds of analyses to determine if the traffic is suspicious. The analysis tends to vary based on the type of infection, malware, OS and web, and can run slightly differently between the various FireEye products. Traffic is examined for statistical and heuristic anomalies, which may be indicative of exploits. Typical analysis includes:

- Statistical analysis, which looks for abnormal traffic that could indicate propagating malware.
- Signature analysis, which examines network traffic payloads for callback activity.
- Virtual machine (VM) analysis, which basically replays suspicious traffic within a virtual machine environment.
- Heuristics analysis, which looks for malicious data such as hidden text, header data, rarely used functions, and suspicious user interface elements within application-based traffic (HTML, PDF, and JavaScript).

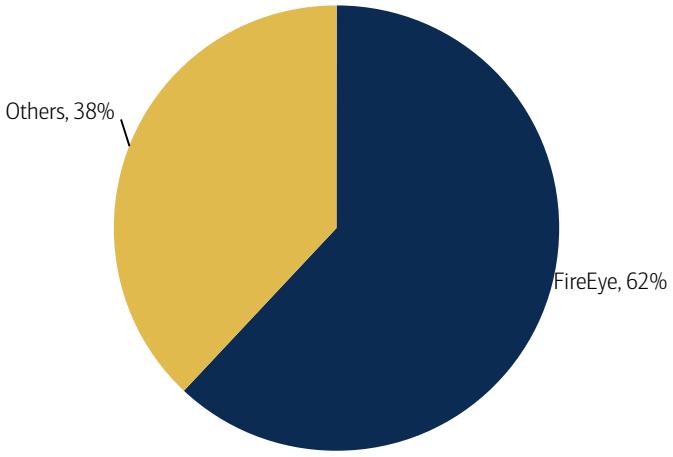
Traffic determined to be suspicious is put through signature-matching components, which then run analysis-based signatures and historical patterns to determine whether traffic is suspicious or coming from a known botnet. If the traffic matches a signature or a pattern of a known threat, an alarm is sent to the administrator. Suspicious traffic that does not match a known signature or pattern is sent to the analysis environment, which uses a virtual machine to run and monitor the traffic and determine if malicious

behaviour is detected. This analysis essentially emulates the environment of a vulnerable client to ensure that the malware executes within the VM.

US$3.5bn market by 2019E

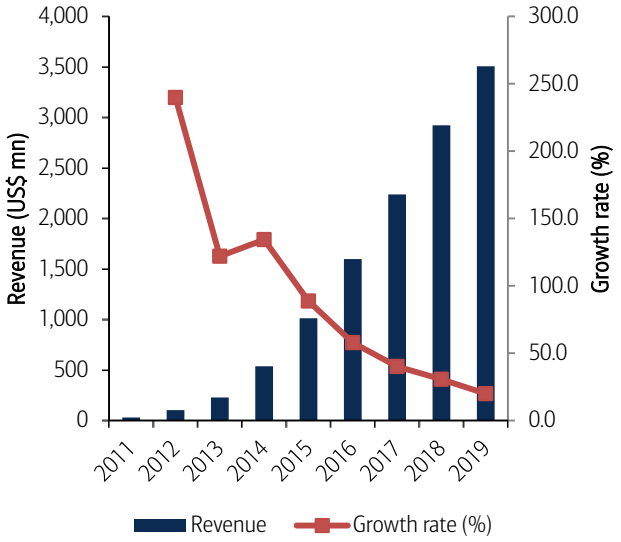
The network security sandbox market is expected to grow from over US$536.8mn in 2014 to US$3.5bn by 2019E at a CAGR of 45.6% (source: Frost & Sullivan). As of 2014, FireEye had a 62% market share as it continues to capitalise on its first mover advantage, with 90% of the market being concentrated within the top three players in this space.

Chart 104: Total Network security sandbox market, 2014



Source: Frost & Sullivan

Chart 105: Total Network security sandbox market (2011-2019)

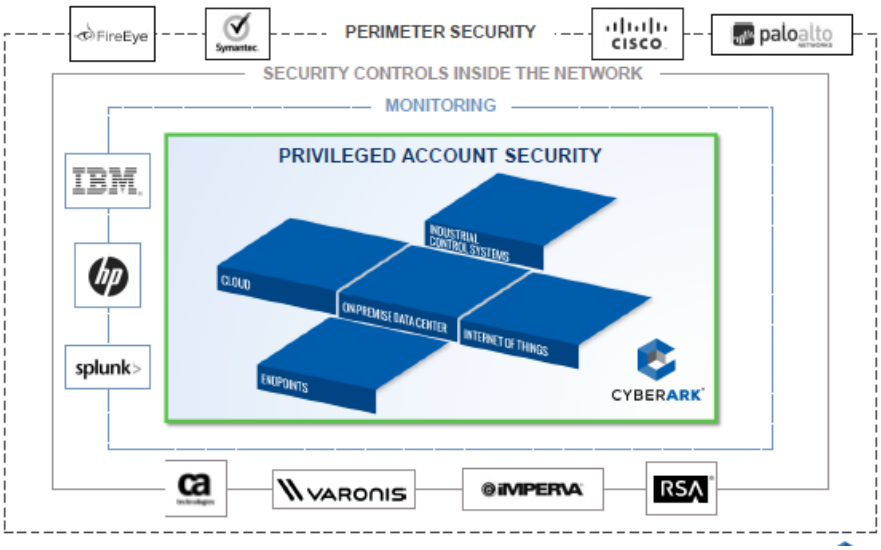


Source: Frost & Sullivan

Privileged account management (PAM)

Privileged account management (PAM) seek to secure the 'privileged accounts' of a system, which often hold the keys to the domain, such as login authentication credentials to assets that store sensitive intellectual property, customer account information, credit card data, medical records, among other sensitive information.

Exhibit 65: Privilege account security vs. other cybersecurity solutions

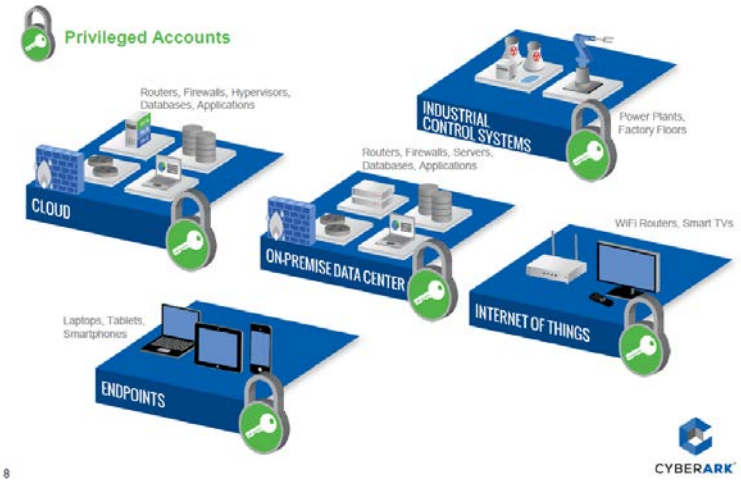


Source: CyberArk

CyberArk: Initiating with Buy; Unique approach to network security 23 March 2015

Once the credentials to PAs are obtained, attackers can take control of and disrupt an organisation's IT and industrial control infrastructures, and steal confidential information. Many organisations have difficulties keeping track of and managing access to these privileged accounts given the average company has 2-4x more accounts than employees. PA credentials are used by system administrators, third-party contractors, cloud service providers, and application and business users, and they exist across connected devices, databases, servers, industrial control systems, hypervisors, etc.

Exhibit 66: Examples of privileged accounts



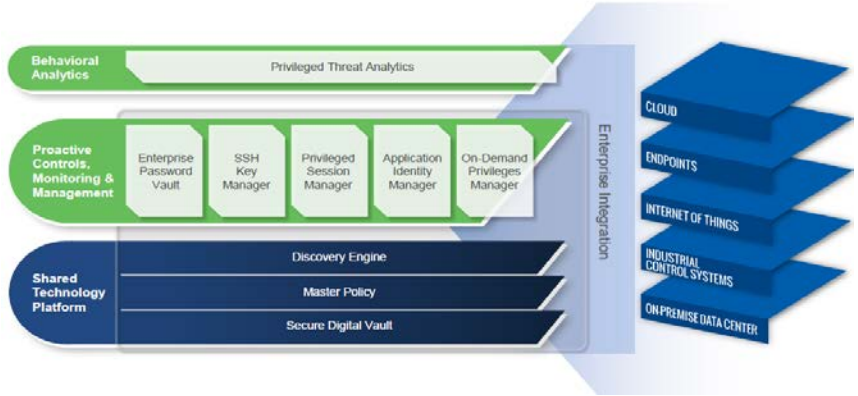
8

Source: CyberArk

Securely centralises, segregates, and enables policy control functions

Many organisations do not centrally and securely store privileged account credentials. Instead, they store passwords on an unsecure hard drive, piece of paper, or even in a folder labelled passwords, making it easy for insiders and external threat actors to obtain and misuse these credentials. Organisations grant independent contractors/third parties access to privileged accounts as a part of conducting everyday business, creating a security risk if the contractor goes rogue (like Edward Snowden) or if the third party has a weak security posture (Target breach).

Exhibit 67: Privileged account software solutions

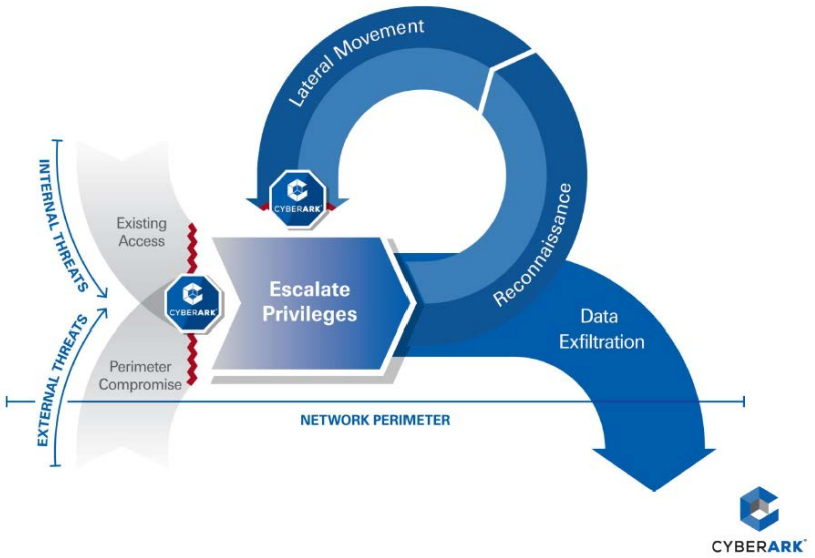


Source: CyberArk

Privileged threat analytics, proactive threat protection

Privileged threat analytics is one of the newer solutions within this space that incorporates big data, providing real time threat detection/protection of privileged accounts. Threat analytics applies behavioural intelligence using proprietary algorithms to detect abnormal activity and misuse of privileged accounts. Threat analytics build a profile for each privileged account holder by learning their behaviours such as usage patterns (account access location, time, etc) and then compares it with the current session to detect abnormal activity. It then provides a risk rating based on the level of deviation from the normal user profile. For example, an alert might be created if an administrator accesses the firewall from a country different from the one he/she works in, or if the administrator of a server downloads 3x more data than the historical average. Lastly, the proprietary analytics are continuously evolving to update for changes in user habits, becoming smarter and smarter over time.

Exhibit 68: CyberArks solutions protect privileged accounts from external/internal threats



Source: CyberArk

Emerging fields: analytics & intelligence, cloud & mobile solutions

Although the growth in IoT represents an increase in the attack surface that threat actors can use, it should also be seen as an opportunity to develop more robust cybersecurity solutions: specifically in big data, cloud and mobile. Indeed, in a survey conducted by the Ponemon Institute on behalf of Raytheon, big data analytics and cybersecurity intelligence were within the top three technologies that organisations believe would gain the most in importance over the next three years in the fight against cyber threats.

Exhibit 69: Cyber Security Roadmap

Source: Frost & Sullivan

Big data analytics: improves cybersecurity in 9/10 cases

Big data analytics seek to harness the increasingly abundant information that organisations possess, and utilise this to analyse and potentially predict unknown threats as they materialise in real-time. This essentially builds on traditional SIEM

platforms, which often only log known threats as a data point and are not able to act immediately to counteract these. However, as the industry moves towards second generation SIEM platforms, which marry information with intelligence, big data analytics should allow organisations to deal with threats more dynamically. Indeed, 86% of IT professionals believe big data analytics would significantly improve their organisation's cybersecurity (source: Splunk).

> The percentage of global firms adopting big data analytics for at least one security and fraud detection case is expected to increase from just 8% in 2014 to more than 25% by 2016 (source: Gartner)

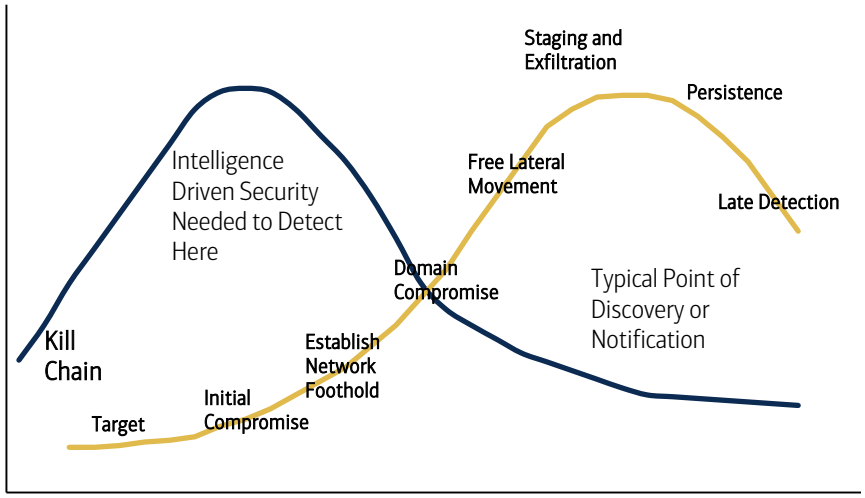
At the core of big data analytics is the closer tie-up of information and situational awareness in its context setting. For example, it can be employed to analyse financial transactions, log files, and network traffic to identify anomalies and suspicious activities, and henceforth correlate all this information into a coherent bigger picture. Splunk outlines five ways in which big data can augment the current cybersecurity solution landscape:

7. Perform research on adversarial threats posed to systems, operations and missions.
8. Analyse collected data to derive facts, inferences and projections concerning attacks.
9. Use context to more accurately determine false-positives and false-negatives.
10. Identify attacks by piecing together snippets of abnormal behaviour spread over time and across systems.
11. Contribute to profiling adversarial behaviour by making data more meaningful to users.

Threat intelligence, US$5bn market by 2020E

An emerging hotbed in the use of big data analytics vis-à-vis cybersecurity is threat intelligence. By using big data effectively, defenders are able to predict attacks in real-time by analysing indicators such as events, patterns and live feeds among others. EY defines cyber threat intelligence (CTI) as: "an advanced process that enables an organization to gather valuable insights based on the analysis of contextual and situational data and can be tailored and adapted to the organization's specific threatscape".

Chart 106: Intelligence Driven Security stops cyber attacks before damage is done



Source: EMC

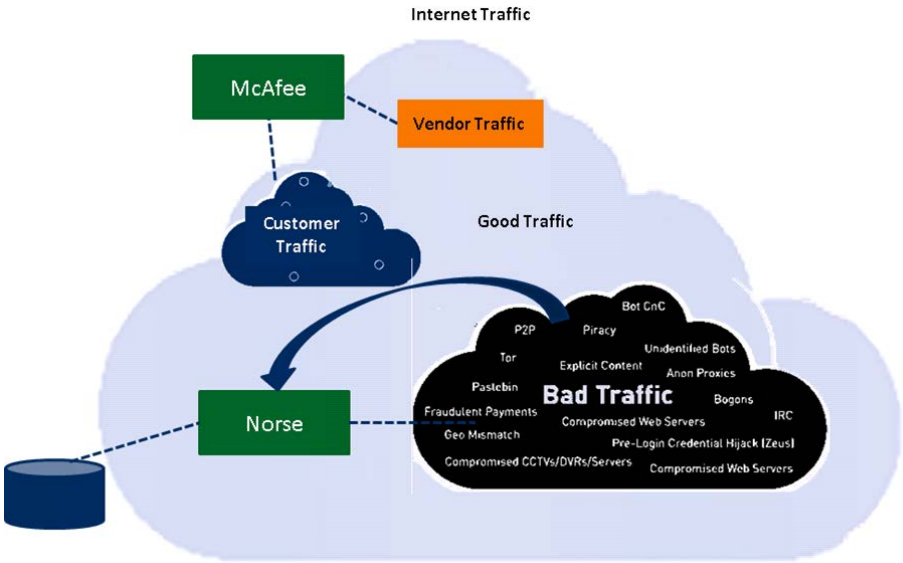
CTI is about likelihood & understanding what's happening in the broader world

However, it is important to stress that CTI does not predict the future, nor is it a panacea for cyber security programs. CTI is all about likelihood – utilising incident history, understanding the internal environment and pinpointing probable targets for threat actors – and keeping an eye on what is going on in the outside world to enable the organisation to develop a better defence framework in an evolving threatscape environment. Threat intelligence is a hot development with the cybersecurity solution space because it not only allows organisations to prevent the 'bad guys' from breaching systems, but also takes the fight back to attackers, which many other solutions are unable to do.

Cognitive security: AI meets cyber

Cognitive security is the field of applying artificial intelligence and machine learning techniques to detect advanced cyber threats, and in many ways overlaps with the areas observed in the threat intelligence field. An example of this space is the McAfee and Norse joint cybersecurity solution that searches the darkest segments of the internet where the bad guys operate and monitors their IP addresses. From here, the programme identifies anomalies such as those IP addresses where malware resides, while the malware is in development or before it is launched, to provide visibility into the darknet and defend against these attacks.

Exhibit 70: Protection against host of threats



Source: McAfee, Norse

The global threat intelligence security market is expected to grow from US$3bn in 2015 to US$5.9bn by 2020E at a CAGR of 14.3%, with North America expected to be the largest segment on the basis of spending and adoption of the technology (source: MarketsandMarkets). IBM, Symantec, McAfee, Trend Micro and Dell SecureWorks are expected to be the largest players in the threat security market.

Identity access management (IAM)

LifeLock, Inc.: Secure identity with LifeLock; 31 October 2012

LifeLock is utilising big data to reduce cybercrime within the growing identity access management (IAM) space. The company does this by continuously monitoring credit and identity related events for its more than 2.25mn members to alert them if it detects a fraud. LifeLock also offers risk assessment and fraud protection services to enterprises through its ID Analytics subsidiary. The combined subsidiary group has a vast data network that monitors +220mn transactions annually, analysing over 750bn data elements and covering nearly 100% of the US adult population. LifeLock's patented analytics analyse data to recognise risks and provide members with real-time, actionable alerts.

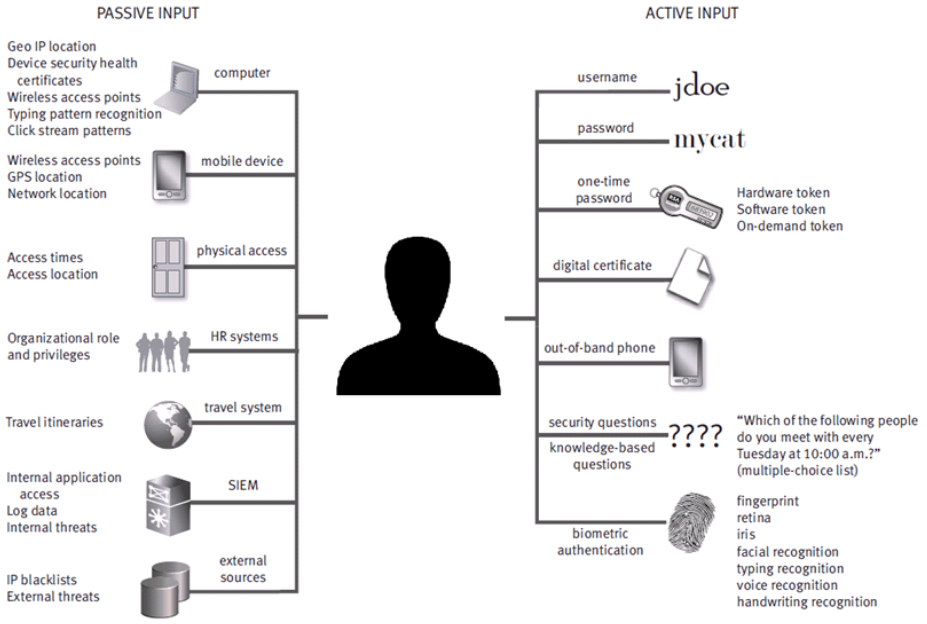
Exhibit 71: LifeLock (with ID Analytics) provides comprehensive ID theft protection for consumers and risk assessment for enterprises

Source: Company data, BofA Merrill Lynch Global Research

LifeLock's products are based on an extensive network of data built from members, enterprise customers, and third-party partners. This data repository includes personally identifiable information, transaction data, and fraud instances collected though years of experience and continuously updated with new data from customers and monitored transactions. Data is gathered from a combination of consumer customers, enterprise customers, and paid third parties such as EWS and CSID. Enterprise customers provide on average 45mn new data points per day. This allows LifeLock to monitor not only changes in credit score, as many competitors do, but the entirety of the customer's identity, including bank, credit card, cell phone, pay day loans, court records, changes of address, and more.

LifeLock applies patented proprietary analytics to its data repositories to generate intelligence that allows a proactive response to identity theft. The most important pieces of this data repository are provided by IDA, which includes nearly 100% coverage of the US adult population through its partnerships with enterprise customers. This data allows LifeLock to create a picture of connections between almost all consumers, and allow alerts to be sent out when high-risk scenarios are identified. For example, suspicious transaction activity is identified in real time. Credit card applications, wireless accounts, mortgage applications, and much more are tracked and analysed for potential threats. Also, personal information is analysed, and anything suspicious such as phone numbers, SSNs, or addresses shared between multiple people is flagged and further analysed. These processes are perpetually improved as the data repository grows and patterns regarding transaction risk are recognised and investigated.

Exhibit 72: Big data enhances identity verification

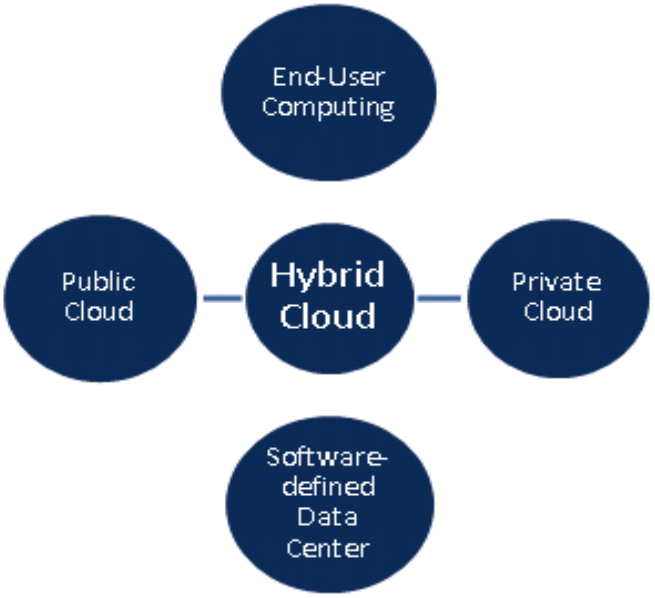


Source: RSA

Cloud: data migration requires new security

At the crux of cloud security is securitising the private domain and preventing information being leaked into the public space. Hence, cloud computing used by organisations generally falls into three categories: public, private or hybrid. Furthermore, the service can be divided into three broad types: (1) software-as-a-service (SaaS) eg, Salesforce; (2) platform as-a-service (PaaS), eg, Windows Azure; and (3) infrastructure-as-a-service (IaaS) eg Amazon Web Services (source: ICS).

Exhibit 73: Hybrid Cloud



Source: VMWare

Given that cloud infrastructures are growing in popularity with organisations, the transfer and storage of data must be managed effectively from a risk standpoint. This includes ensuring that data is encrypted when migrating it from the drive to maintaining authorised access throughout the process. Furthermore, traditional cybersecurity

solutions already described such as firewalls and antiviruses are applied to the cloud architecture setting to maintain security.

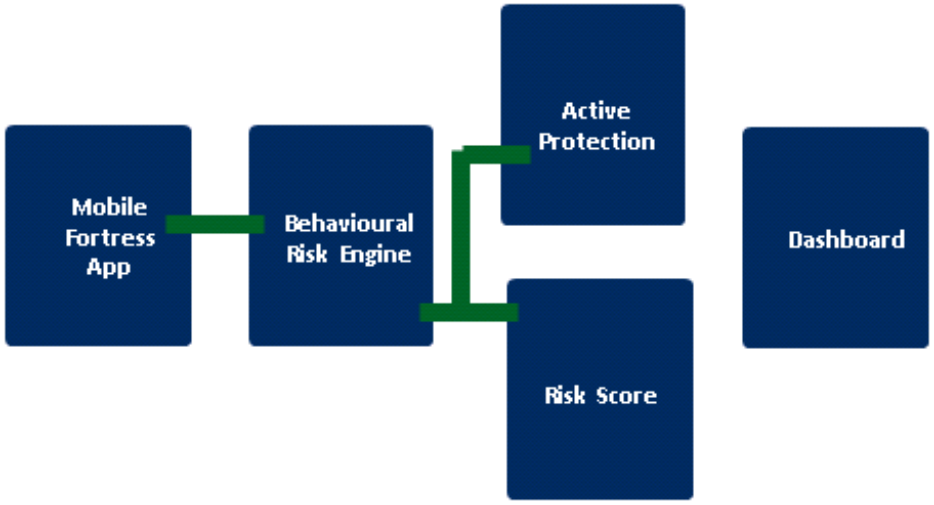
US$11.84bn market by 2022E

The global cloud security market is forecast to grow from US$4.50bn in 2014 to US$11.84bn by 2022E, at a CAGR of 12.8% (source: Transparency Research). The main players in this market are expected to be: CA Technologies, IBM, Symantec, Symplified, Fortinet, McAfee, Sophos, Trend Micro, Zscaler, and Panda Security.

Mobile: apps and BYOD driving growth

One can divide the mobile security market into two segments: consumer and enterprise. While increasing smartphone penetration, personal use and growth of apps is driving the consumer side, the growth of 'BYOD' is also driving uptake for mobile security vis-à-vis the enterprise workplace. Hence, at the core of cybersecurity on mobile devices is ensuring users are adequately educated on risks and equipped with the latest technology software to protect against cyber threats

Exhibit 74: Example of using behaviour monitoring to allow enterprises to monitor BYOD



Source: Check Point

US$34.8bn market by 2020E

The global mobile security market is expected to reach US$34.8bn by 2020E, registering a CAGR of 40.8% between 2014 and 2020, according to Allied Market Research. This will be driven primarily by BYOD adoption as enterprises allow employees more flexibility in using their own devices. According to IDC, iOS, BlackBerry, Android and Windows Mobile are the leading OS platforms where mobile security is provided for by the world's leading vendors.

Table 10: Global mobile security software vendors by OS

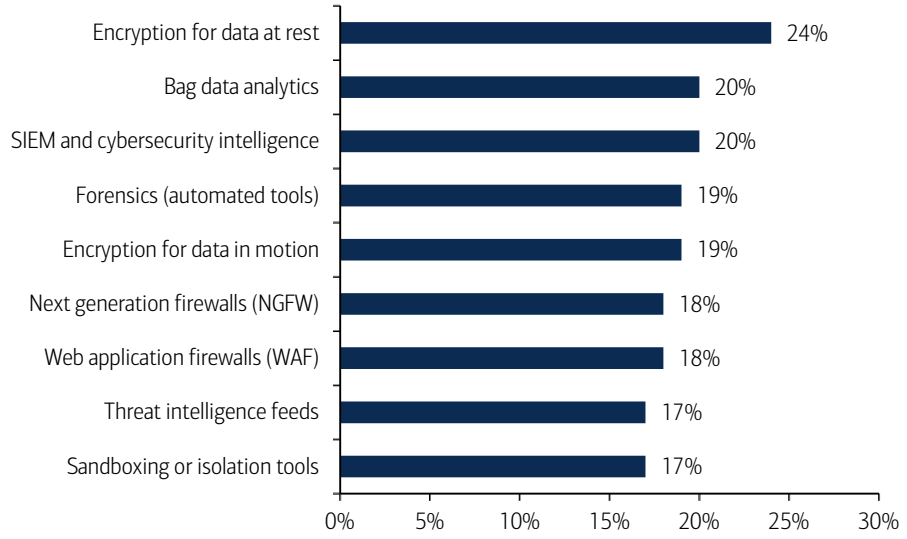
	iPhone	BlackBerry	Android	Windows Mobile	Palm	Symbian
BullGuard		○	○			○
Check Point				○	○	○
CREDANT		○		○	○	○
ESET				○		○
Gemalto	○	○				
Kaspersky		○	○	○		○
McAfee	○		○	○		○
Mobile Iron	○	○	○	○		○
Quest Software	○	○	○	○	○	
RIM		○				
RSA	○	○	○	○		○
Sophos	○		○	○		
Sybase	○		○			
Symantec	○	○	○			○
Trend Micro	○	○	○	○		○
Zenprise	○	○	○	○	○	

Source: Trend Micro, IDC, BofA Merrill Lynch Global Research

Encryption alternative: c.US$5bn software market by 2019E

A possible alternative solution to increasing cybersecurity is 'strong encryption', which refers to the act of scrambling data in such a way that it cannot be understood by anyone without the correct password. Encryption software can be broadly broken into 'at rest' for storage or 'point-to-point' during transit, both of which makes data cryptographically more secure. A recent Ponemon Institute survey conducted on behalf of Raytheon ranked encryption for data at rest as the #1 technology for enabling security, and encryption for data in motion as #5.

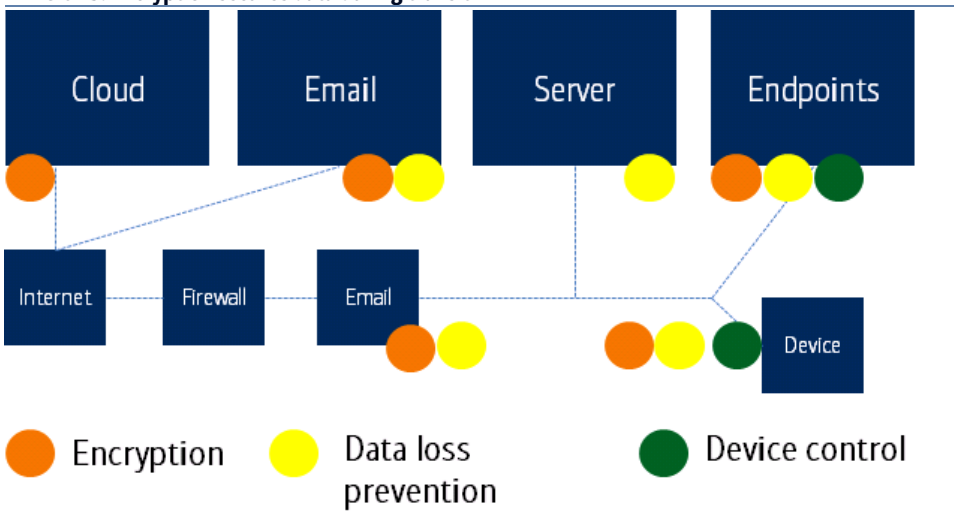
Chart 107: Change in importance of enabling security technologies (%)



Source: Ponemon Institute, Raytheon

Even law enforcement agencies such as the FBI or NSA cannot read this data because the owner is the only individual with the access key. The global encryption software market is forecast to grow from US$1.85bn in 2014 to US$4.82bn by 2019E (source: MarketsandMarkets).

Exhibit 75: Encryption secures data during transit

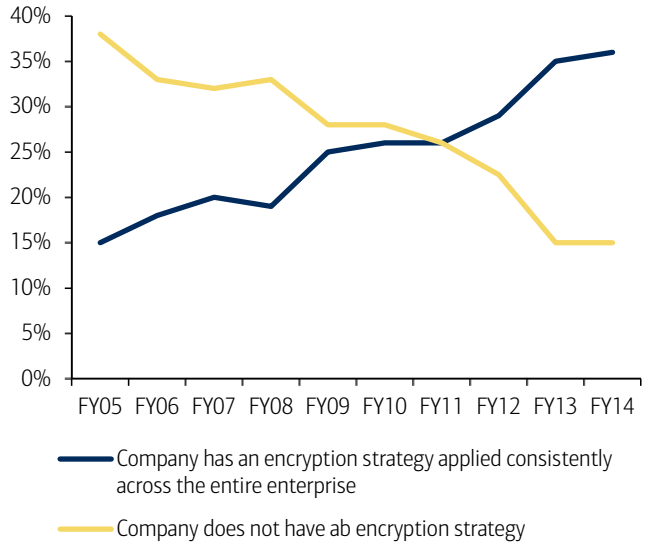


Source: Trend Micro

36% of companies applying encryption strategies

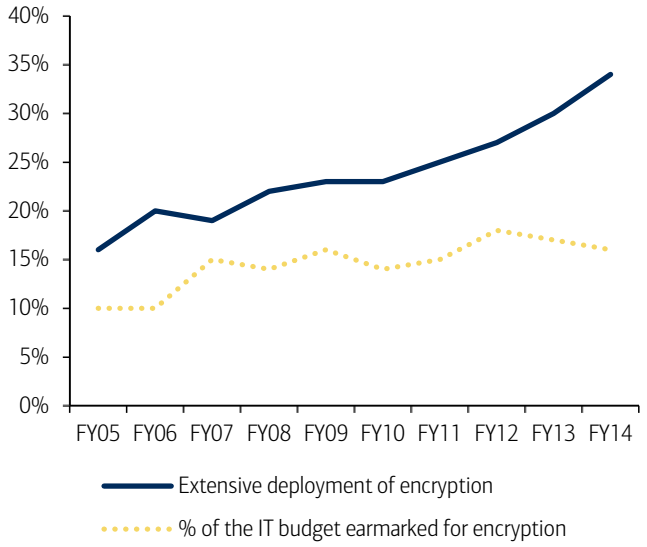
The general trend is that more companies are adopting some sort of encryption strategy, and that those who don't encrypt are on the decline. According to a study conducted by the Ponemon Institute for Thales, the percentage of companies which consistently applied an encryption strategy across their enterprise platform increased from 15% in 2005 to 36% by 2014. In addition, it is important to stress that the use of encryption technologies has increased even though the % of the IT budget allocated to it has remained relatively stagnant at c.15% over the same period (source: Ponemon Institute, Thales). We view this as a harbinger going forwards as companies increasing adopt the technology to protect their proprietary data.

Chart 108: Trends in encryption strategy



Source: Ponemon Institute, Thales

Chart 109: Trend on the extensive use of encryption technologies



Source: Ponemon Institute, Thales

Bank of America Merrill Lynch

Wide usage: Apple, WhatsApp, Facebook etc.

Strong encryption is already widely used in some of the most popular tech products in the world, eg, Apple (including iPhone,) WhatsApp and Facebook. It is a key reason why government agencies often have to ask these organisations for their data rather than 'tapping' into it with their own surveillance tools. However, the majority of data is still either only basically encrypted or not at all, leaving scope for strong encryption opportunities, in our view.

Exhibit 76: Transactions in the clear and encrypted transactions

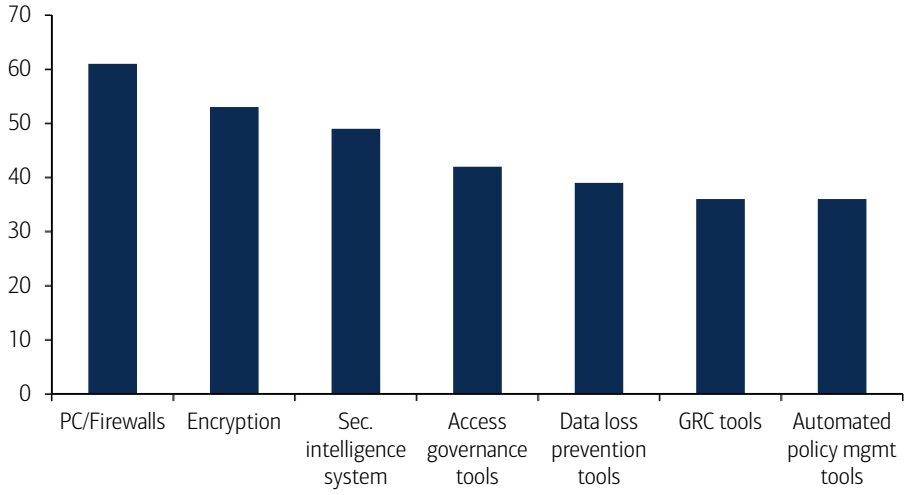
Source: Visa

In addition, stakeholders within the retail space accepting payment via card stand to benefit. As we flagged earlier with PoS attacks, many transactions are at risk because hackers can steal personal data at the point of purchase on the payment terminal or when this is transmitted back to the mainframe.

Increasing part of cybersecurity budgets: up to 39% of spend

Encryption accounted for just 17% of US companies' cybersecurity budgets, but by 2014 this figure had increased to 39%, according to Business Sweden interviews with sample stakeholders. Furthermore, as a cybersecurity solution technology used by companies, it was only second to firewalls, with around half of those interviewed using encryption.

Chart 110: Cybersecurity technology used by US companies (% of budget in 2014)



Source: Business Sweden et al

Flipside: surveillance debate

There is also a flipside to encryption, whereby some argue that data that cannot be decrypted, preventing spy agencies from reading potential cyber-terrorists' messages and hence foiling an attack. The following highlights the political divide in opinion on the encryption vs. data privacy debate (source: CSIS).

- UK Prime Minister David Cameron wants to ban the use of end-to-end encryption instant message platforms such as WhatsApp, iMessage, fearing government agencies won't be able to tap in what on terrorists' communication.

- US President Barack Obama has a relatively warmer view on strong encryption, believing stakeholders should be allowed to secure the privacy of their data. This view is also likely to be driven by the public's backlash to US government surveillance in a post-Snowden world.

IDs and fintech and payments security

There is a growing security market for identity protection via smart ID cards. In addition, there is rising demand for payments security, which is driven by the rise of fintech – where companies aim to deliver easier, user friendly and mobile payments: (1) moving away from cash transactions; (2) e-commerce penetration; and (3) increased adoption of mobile wallets.

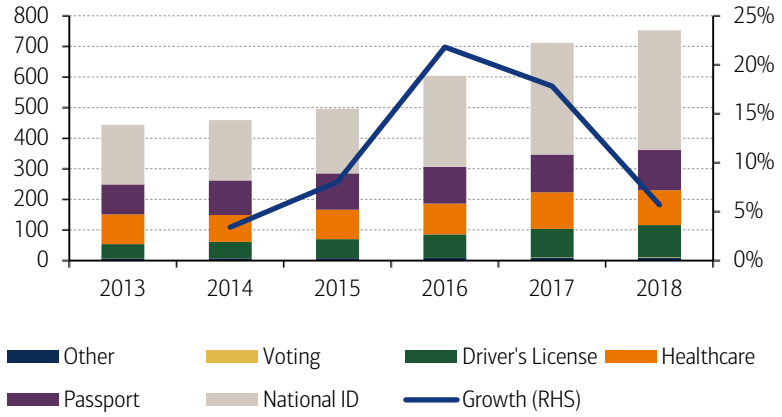
Smart ID Cards: 700mn cards by 2018E

We expect there to be secular demand for smart identity cards driven by new government IDs and enterprise security, among others. Secure, smart electronic documents that are exposed to this trend include: passports, national IDs and driving licences to governments, and access management solutions to enterprises.

Gemalto N.V.: Riding the security wave; reinstate at Neutral, 14 May 2015

We forecast security smart card volumes to top 700mn globally by 2018E (source: BofA Merrill Lynch Global Research, ABI). The lion's share of the smart card market demand is likely to come from national IDs. However, healthcare is another significant portion of the market because its data is increasingly being targeted by cybercriminals.

Chart 111: Security smart card volumes (mn) by type



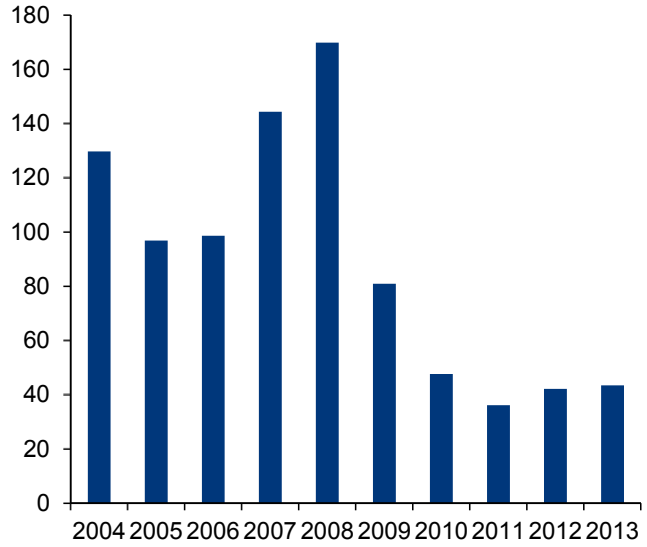
Source: BofA Merrill Lynch Global Research, ABI Research

EMV/NFC payments

Ingenico S.A.: Enabling a cashless future; reinstate at Buy, 14 May 2015

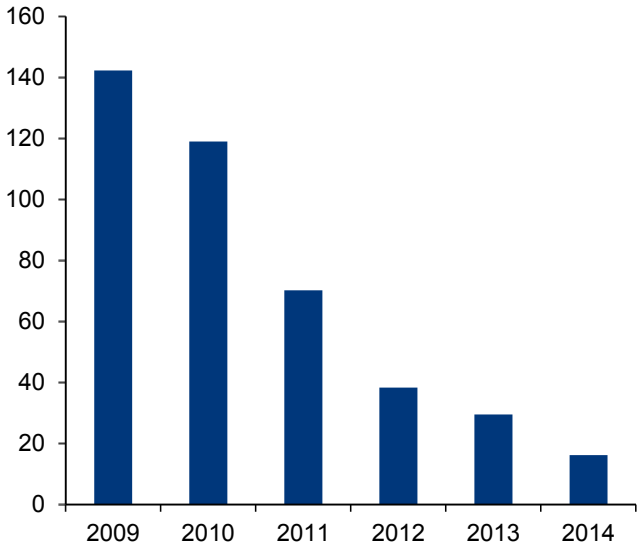
As highlighted by Adithya Metuku and our European Technology team's 'War On Cash' note, the move towards more secure electronic payment systems is a structural growth story, driven by EM demand for card payments, adoption of EMV/NFC (Euro Master Visa / Near-Field Communication) in developed markets and the rapidly expanding mobile point of sale (mPOS) space. EMV cards are tamper proof and nearly impossible to clone, making counterfeit card fraud extremely difficult. Countries such as England, Canada and France that have deployed EMV have seen strong reductions in fraud rates (cf. the US).

Chart 112: : UK counterfeit card fraud cases have dropped by 67% since EMV deployments in 2004



Source: UK cards association

Chart 113: Canada debit losses down significantly, driven by EMV



Source: Interac Association

US regulatory catalysts in 2H15 and 2016

That said, there could be regulatory catalysts in the latter half of 2015 and 2016 that could drive adoption in the underpenetrated US market. Our European Tech team does not assume that all US merchants will be compliant with EMV by the so-called 'fraud liability shift' October 2015 deadline. This essentially means that, after this date, the party in the card acceptance process, either the issuer or the merchant, who does not support EMV, assumes all liability for counterfeit card transactions. Hence, if there are signs of faster-than-expected US EMV penetration vs its estimate of 52% within the existing installed base by October 2015, this could lead to upside to its estimates and would be a positive for investor sentiment.

Table 43: Fraud liability shift key dates

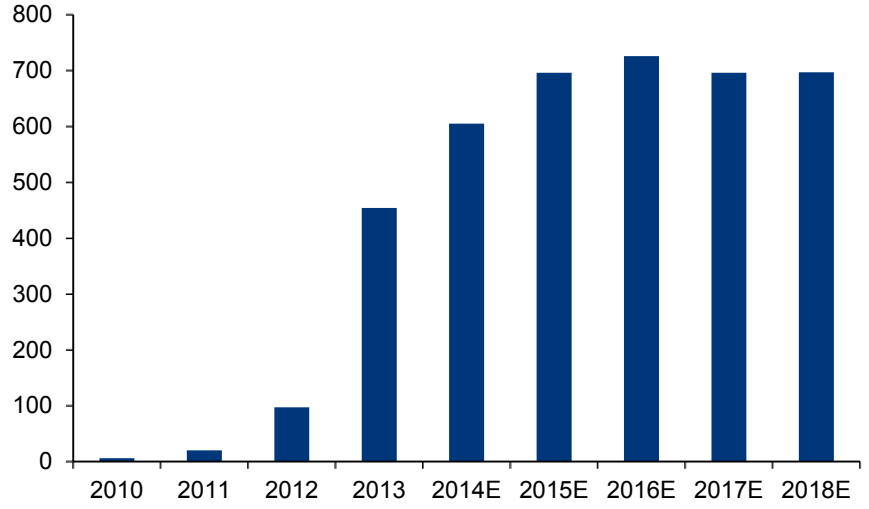
Visa	MasterCard	American Express	Discover
Oct-12	Oct-12		Dec-12
Visa will extend the Technology Innovation Program (TIP) to merchants in the US potentially allowing them to skip the annual PCI DSS validation for any year in which at least 75% of merchant VISA transactions originate from dual-interface EMV chip enabled devices plus other qualification criteria such as being PCI DSS compliant	PCI assessment relief takes effect		Discover will institute Fraud Liability Shift (FLS) for Diners Club International
Apr-13	Apr-13	Apr-13	Apr-13
Acquirers/Processors will be required to support merchant acceptance of EMV chip transactions	Acquirers/Sub-Processor mandate to fully process EMV transactions. Cross border Maestro ATM liability shift to non-EMV ATMs	Processors must be able to support AMEX EMV chip-based contact, contactless and mobile transactions	Discover merchant acquirers, acquiring processors, and merchants with direct connections into its network must be certified as able to support the network data needed in contact and contactless EMV chip card transactions. The mandate applies not only in the U.S., but also in Canada and Mexico.
	Oct-13	Oct-13	Oct-13
	MasterCard Account Data Compromise (ADC) relief takes effect (50%). On this date, if at least 75% of MasterCard transactions originate from EMV-compliant contact and contactless POS terminals, the merchant is relieved of 50% of account data compromise penalties.	Merchants will be eligible to receive relief from PCI Data Security Standard (DSS) reporting requirements if merchants' POS acceptance locations (where 75% of their transactions occur) are enabled to process AMEX EMV chip-based contact and contactless transactions	Discover will grant annual PCI audit waivers for merchants that process 75% of Discover Network transactions via terminals supporting both contact and contactless payments
Oct-15	Oct-15	Oct-15	Oct-15
The party that is the cause of a contact chip transaction not occurring will be financially liable for any resulting card-present counterfeit fraud losses. Does not include automated fuel dispensers (AFD)	MasterCard ADC relief takes effect (100%). On this date, if at least 95% of MasterCard transactions originate from EMV-compliant POS terminals, the merchant is relieved of 100% of account data compromise penalties. MasterCard liability hierarchy takes effect (excluding fuel)	AMEX will institute a Fraud Liability Shift (FLS) policy that will transfer liability for certain types of fraudulent transactions away from the party that has the most secure form of EMV technology	Discover will institute a Fraud Liability Shift in US Canada and Mexico. This FLS policy will be a risk based payments hierarchy that benefits the entity that leverages the highest level of available payments security
	Oct-16		
	Liability will shift for ATM in US from Oct, 2016		
Oct-17	Oct-17	Oct-17	Oct-17
Deadline for automated fuel dispensers (ADF) to comply. Also liability will shift for ATM in US	MasterCard liability hierarchy takes effect for fuel dispensers	FLS takes effect for transactions generated from automated fuel dispensers. Also liability will shift for ATM in US	FLS takes effect for transactions generated from automated fuel dispensers

Source: Verifone company site

China building out electronic payments infrastructure

Similarly, in China, given the large wave of EMV card deployments since 2013 and state support to build out electronic payments infrastructure, there may be upside potential to the 20% unit growth the team currently assumes. China is in the middle of a strong EMV card deployment cycle with card deployments expected to peak in 2016E. Payment terminal growth in China has been robust as retailers prepare to accept EMV cards. However, given the low payment terminal penetration levels and recent EMV card deployments, we expect a strong build-out of payment terminal infrastructure in China over the next few years. A recent MasterCard study found that China is making the shift 'from cash to cashless' far more rapidly than any other country surveyed. Similarly, a recent Nilsson survey found that 71% of shoppers in China's top tier cities prefer paying with bank cards to cash.

Chart 114: China EMV card deployment wave (units mn)

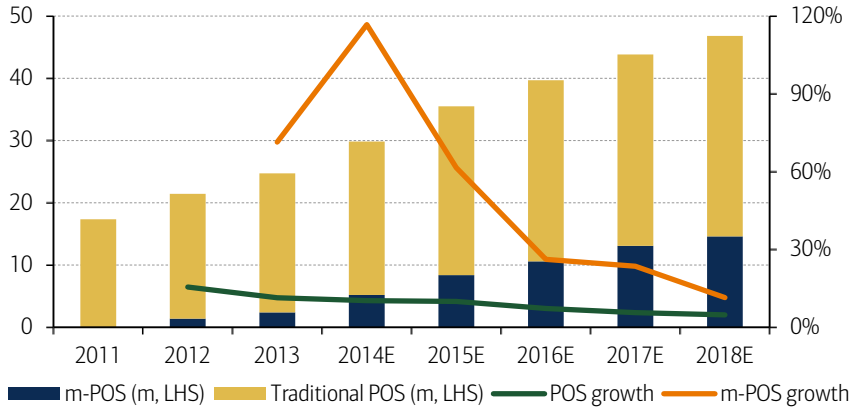


Source: ABI research

PoS terminals: low teens CAGR to 2019E

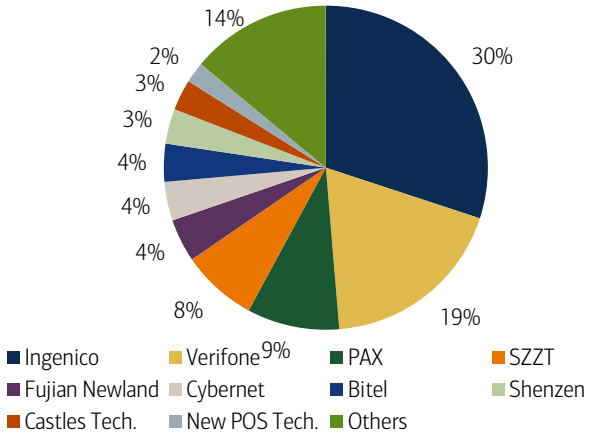
ABI Research expects the payment terminals market to deliver a low-teens CAGR from 2014-19, driven by mid-single-digit rates in the traditional POS business and double-digit growth in the mPOS market.

Chart 115: Traditional POS and m-POS shipments outlook



Source: Nilson report, ABI Research, BofA Merrill Lynch Global Research estimates

Chart 116: Traditional POS market share by volume



Source: Nilson report, data for 2013

MPOS solutions: 100+ players with a range of pricing models

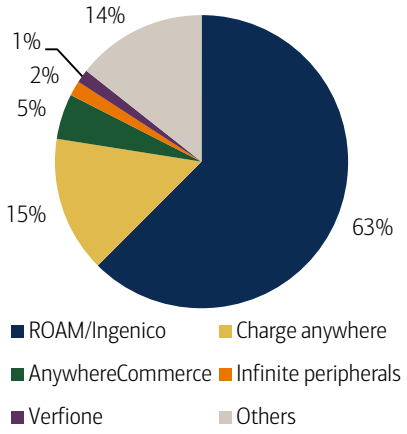
Mobile point of sale (mPOS) solutions have recently attracted increasing interest driven by marketing campaigns by the likes of Square, iZettle etc targeting SMEs. While Square and iZettle are the better-known companies offering mPOS solutions, there are more than 100 players in the mPOS market with a range of pricing models. A number of these companies subsidise the cost of the payment terminal with the idea of recouping this through transaction processing fees.

Table 44: mPOS offerings overview

Company	Customer focus	Pricing
iZettle	Small merchants	Free card reader. 1.5% to 2.75% per swipe
Square	All merchants	Free card reader. 2.75% per swipe
Bank of America Merchant Services	BAMS merchant customers	2.7% per swipe
Intuit	SMEs	1.75% - 2.75% per swipe
Amazon	SMEs	Card reader $10. 2.5% per swipe
WorldPay	Small merchants	1.95-2.75% per swipe
Paypal	All merchants	2.69% per swipe
Payleven	All merchants	Card reader £49. 1.5-2.75% per swipe
Sumup	SMEs	Card reader £59. 2.75% per swipe
Adyen	High volume merchants	Card reader €99. 1.4% per swipe

Source: BofA Merrill Lynch Global Research

Chart 117: mPOS hardware market share by volume



Source: ABI Research, data for 2013

Bank of America Merrill Lynch

Complementary to traditional payment terminals

Traditional POS solutions tend to be more robust and able to handle high card volumes at a much faster speed than mPOS solutions. That said, mPOS solutions should be seen as complementary to traditional payment terminals and one should expect very little cannibalisation for two main reasons:

- We see most mPOS solution providers (eg, Square, iZettle) as essentially payment aggregators that work within the existing payment ecosystem. This means that they are subject to the same economics and have to pay the same fees as other merchants. The key difference from a customer's viewpoint is the change in the pricing model (lack of transparency and generally higher fees).
- We believe this pricing model is likely to work only for merchants with low volumes of card payments. Merchants with a higher turnover of card payments would probably find that the pricing model is better with a traditional merchant account and traditional POS solutions.

Biometrics: next-gen authentication

Biometrics refers to technology that analyses human body characteristics to authenticate a user. Along with NFC technology, the latest generation of consumer devices has introduced biometric authentication into the consumer space, eg, Apple's Touch ID, Siri. We believe the use of biometrics should continue to grow, fuelled by the ongoing growth in mobile device penetration. That said, biometrics is still a relatively new field within the cybersecurity solution space, and widespread public acceptance and testing of the technology remain the fundamental hurdles. For instance, a recent survey by Javelin Strategy and Research showed only a 14% increase vs. 51% negligible effect vis-à-vis consumer propensity to change their online purchasing behaviour if this authentication technology were introduced.

The following are examples of how companies are beginning to adapt this technology and implement it into a user-friendly format for consumers (source: company reports).

- **Halifax** (Lloyds Banking Group) has started testing using Nymi band to capture users' heartbeat rhythms for banking authentication instead of traditional chip & PIN systems.
- **MasterCard** announced in early 2015 that it plans to spend more than US$20mn to roll out a pilot programme that uses a combination of biometrics (facial, voice recognition and fingerprint matching) to authenticate and verify transactions.
- **VOXX Electronics** announced in mid-2015 that it has started to integrate EyeLock's USB-enabled iris ID authentication technology into a Jeep Wrangler, which validates the driver's identity via their retina to authorise the vehicle to start.

Biometrics, fingerprint solutions

O-film: New Buy: Emerging winner, aggressive expansion 02 December 2014

Fingerprint sensor is an electronic component used to capture a digital image of the fingerprint pattern. Fingerprint can be used for security, authentication, website login and other purposes such as payment, which has been a conceptually attractive solution in smartphones. For instance, Apple launched the iPhone 5S in 2013 with a built-in fingerprint sensor and biometric smartphones are becoming the mainstream following

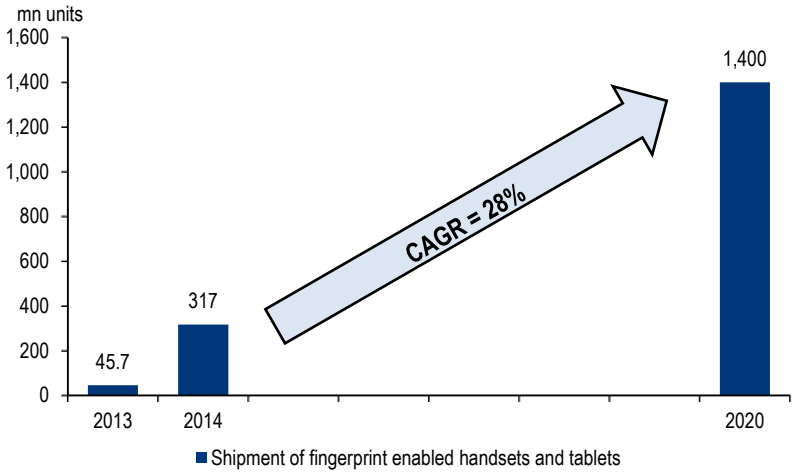
the lead of Apple. New fingerprint-enabled smartphones that have followed suit include brands such as Samsung and HTC.

Exhibit 77: iPhone 5S fingerprint sensor

Source: Apple, BofA Merrill Lynch Global Research

The shipment of fingerprint-enabled devices is forecast to grow 4x by 2020 to 1.4bn units, representing a CAGR of 28% (source: IHS Technology). Given the increasing consumer adoption of fingerprint in mobile devices, we expect this and biometric-related security products to continue to grow and bring large opportunities for players in the market related to this space.

Chart 118: Smartphones and tablets spur the boom in the fingerprint solution market

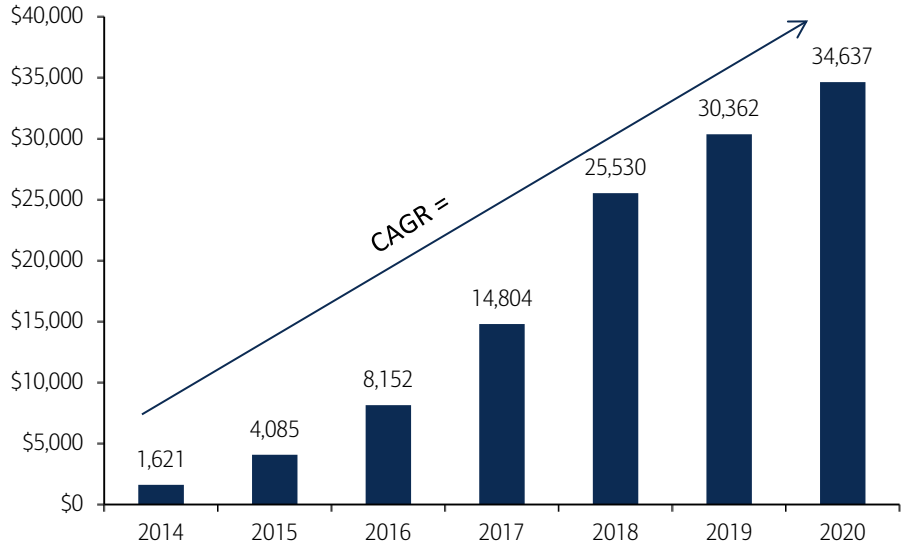


Source: IHS, BofA Merrill Lynch Global Research

$34.6bn mobile biometrics market by 2020E

The mobile biometrics market is forecast to hit US$34.6bn and authenticate nearly 65% of all m-commerce transactions by 2020E (source: Acuity Market Intelligence). This percentage represents 126bn biometric payment transactions, generating more than US$1.1tn in consumer m-commerce purchase value. The main driver of biometric use in devices is expected to come from fingerprint authentication, which should account for roughly half the total market.

Chart 119: Mobile Biometric Revenue (US$mn)



Source: Acuity

Services consulting, US$15.3bn market

Increasingly, information security needs to be managed at the business level. Firms with strong business risk management capabilities can take a more holistic approach. As more data is digitised as it moves through an organisation's various platforms, new opportunities are emerging for consultants with digital practices. The security consulting service market grew from an estimated US$14.2bn in 2013 to US$15.3bn in 2014 at a rate of 8.1% (source: Gartner).

Professional service firms are leading providers

The top 10 information security consultants accounted for 67.2% of the information security consulting market. IBM was ranked second after Deloitte, while EY and PwC moved down to third and fourth, respectively.

Several high-profile information security breaches across the world have made enterprises keen to fortify, prevent and pre-empt criminal access to their organisations. As a result, these incidents have created demand for increased monitoring and response capabilities, which keeps information security consulting as a hot growth area in the services sector.

All information security consultants have reported that client demand focuses on cyber-information-security activities across all industries. In verticals aside from government, cyber-information security is used loosely as a marketing term with which C-levels and business information security buyers are familiar. Providers have been organically or inorganically enhancing their capabilities in information forensics, threat intelligence and cyber-information security resources and technology.

Table 45: Top 10 Information Security Consulting Providers by Market Share, Rank and Revenue, Worldwide, 2014 (Revenue in Millions of Dollars)

2014 Rank	2013 Rank	Rank Change	Vendor	2013 Revenue	2014 Revenue	2014 Market Share (%)	Revenue Growth 2013-2014 (%)
1	1	—	Deloitte	2,159	2,325	15.1	7.7
2	4	2	IBM	1,306	1,815	11.8	39
3	2	-1	EY	1,526	1,744	11.3	14.3
4	3	-1	PwC	1,425	1,524	9.9	6.9
5	5	—	KPMG	1,297	1,396	9.1	7.6
6	6	—	Booz Allen	488	470	3.1	-3.8
7	7	—	HP	365	381	2.5	4.4
8	8	—	Accenture	218	300	1.9	37.8
9	9	—	Atos	201	220	1.4	9.3
10	10	—	EMC (RSA)	183	192	1.3	4.9
			Top 10	9,169	10,366	67.5	13.1
			Others	5,048	4,999	32.5	-0.1
			Total	14,217	15,365	100	8.1

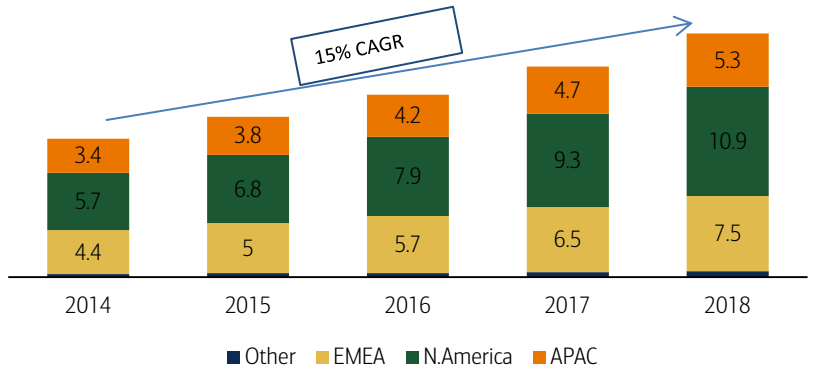
Note: Percentages and numbers may not add up to 100% or totals because of rounding.

Source: Gartner (April 2015)

US$24bn+ managed security services (MSS) market by 2018E

The global market for MSS is forecast to reach US$24.3bn by 2018E with a 15% CAGR between 2014 and 2018 (source: Gartner 2014 et al). The North American market should account for roughly two-fifths of the global MSS market by 2018E. Providers of managed security services (MSS) are essentially third-party companies that have been put in charge of guarding the network security of corporate clients. The players in this outsource market are typically large telecommunication firms.

Chart 120: Managed security services market (US$bn)

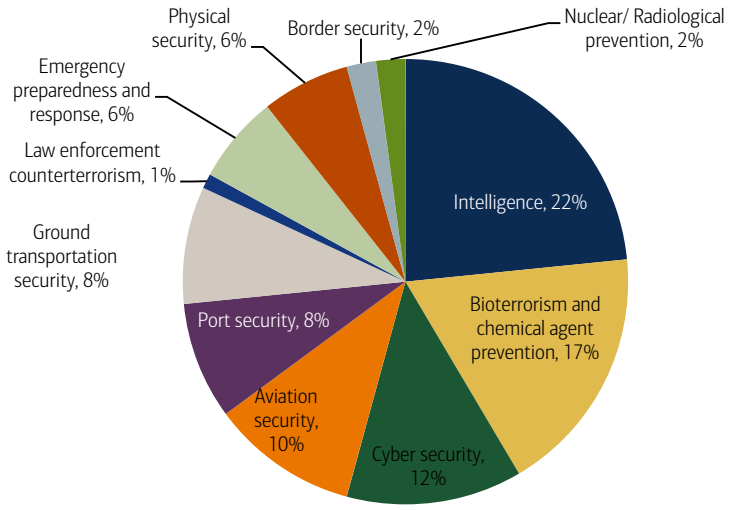


Source: Company disclosures, market research, Gartner 2014

Homeland security & cyber solutions: US$51bn market

Intelligence, law enforcement and counter-terrorism, and bio-terrorism and chemical agent prevention are the three biggest segments in the homeland security market. We believe that the areas of biggest growth will be sectors with cybersecurity focus.

Chart 121: Homeland security market segments

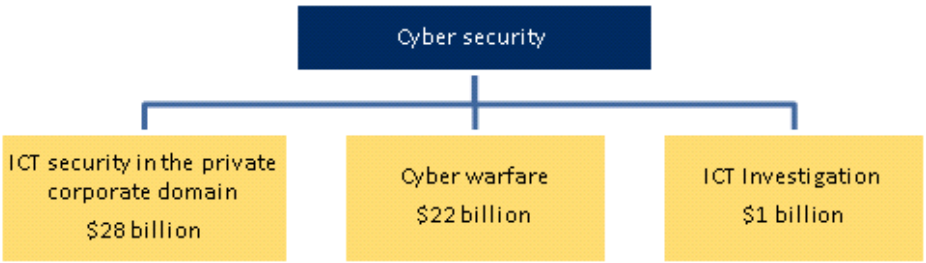


Source: CIVITAS Group, BofA Merrill Lynch Global Research

Rising threat drives growth in $50bn+ cyber homeland market

Reputational damage to firms and governments from the recent spate of cybersecurity breaches continues to drive growth in cybersecurity, despite the overall austerity in defence markets. The market was worth US$51bn in 2014, of which US$28bn was in the corporate domain, US$22bn for cyber warfare and US$1bn from ICT investigations (source: Frost & Sullivan). The key players in this market are Boeing, Lockheed Martin, Raytheon, Thales, Selex SE, Northrop Grumman, BAE, QinetiQ, McAfee, Norton and Symantec.

Exhibit 78: Cyber & homeland security market breakdown



Source: Frost & Sullivan

Fastest growing segments in the next decade

The areas where we anticipate the fastest growth over the coming years are:

- **Cyber & IT systems:** Key towards integrating millions of sensors, screening systems, intelligence sources, databases and operational assets into an effective HLS-HLD infrastructure.

Command Control Communication & Intelligence (C3I) Systems: C3I and net-centric systems will be introduced into most of the local (eg, airports, seaports, smart cities) and government HLS-HLD real-time operational counter terror headquarters.

- **Cybersecurity systems:** The cyber world is becoming a major battlefield in the conflict with terrorism. Cybersecurity systems are becoming major counter-terror tools. The vulnerability of the cyber networks will only increase along with the demand for new counter-terror cyber tools.

- **Biometric Identification systems (eg, e-passport) & bio-detection:** It is estimated that by 2018E, about 2.5bn global residents will have some sort of smart ID document. The EU, India and China are leading this market. However, there are no clear indicators that the biometrics market will follow a similar trajectory in the US.

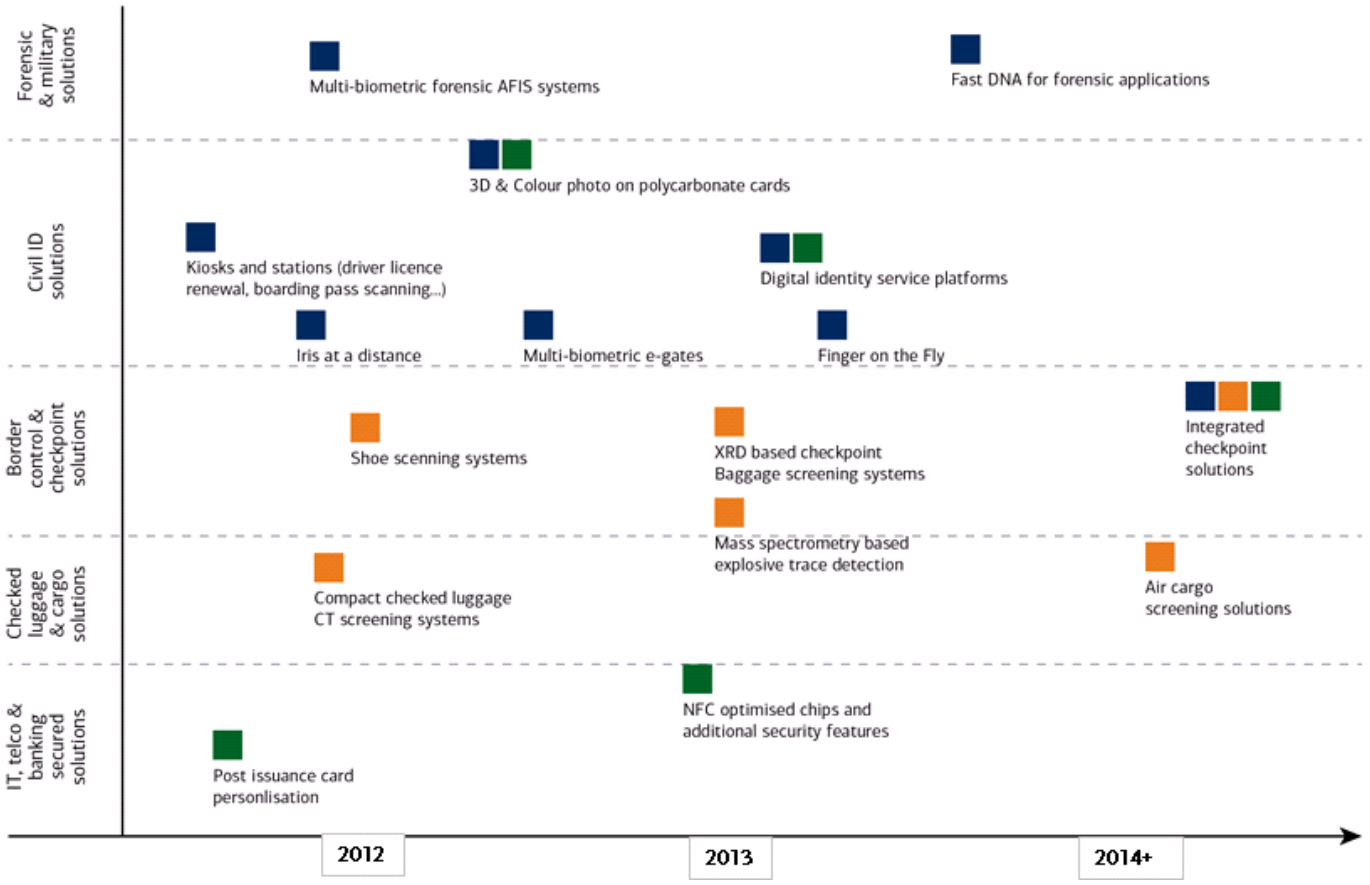
- **Nuclear/radiological logical terror mitigations systems:** This market is forecast to grow rapidly once the technological and managerial issues are resolved.

- **Defending gas-oil energy facilities:** Billions will be allocated by the energy producing states to defend this important energy infrastructure.

- **Border & Maritime Security:** Many important and expensive border protection programmes are currently on the table (Mexico-US, Saudi borders). Global spending will be driven by the increasing occurrence of maritime piracy on larger high-value assets such as cargo ships and oil and gas tankers. Furthermore, the threat of maritime terrorism is very real as groups see the potential to target such potentially explosive targets.

- **Intelligence 'SIGINT' systems:** Surveillance, cyberspace protection and cellular telephones will be used extensively by the world's intelligence communities.

Exhibit 79: Selected breakthrough security solutions roadmap



Source: Safran,, BofA Merrill Lynch Global Research

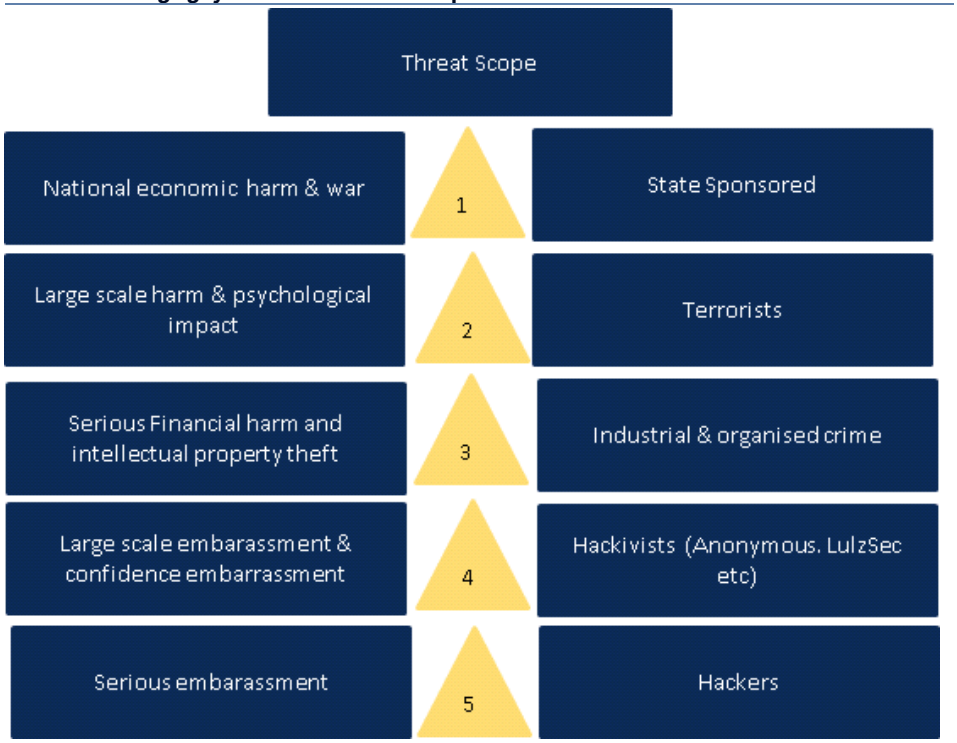
Homeland cyber, specialist solutions & growth

As discussed in the cybersecurity section of the report, the nature of the threatscape is changing constantly in terms of both the volume and magnitude of attacks. Cybersecurity is increasingly becoming a homeland security issue with rising attacks by and on governments, and by governments on companies and citizens. The combination of increasing threats (state-sponsored, terrorist, cyber and narcotics) and growing awareness of the cost impacts of the cyber-security threat is making it a homeland security priority.

Defence companies beginning to focus and specialise in cyber

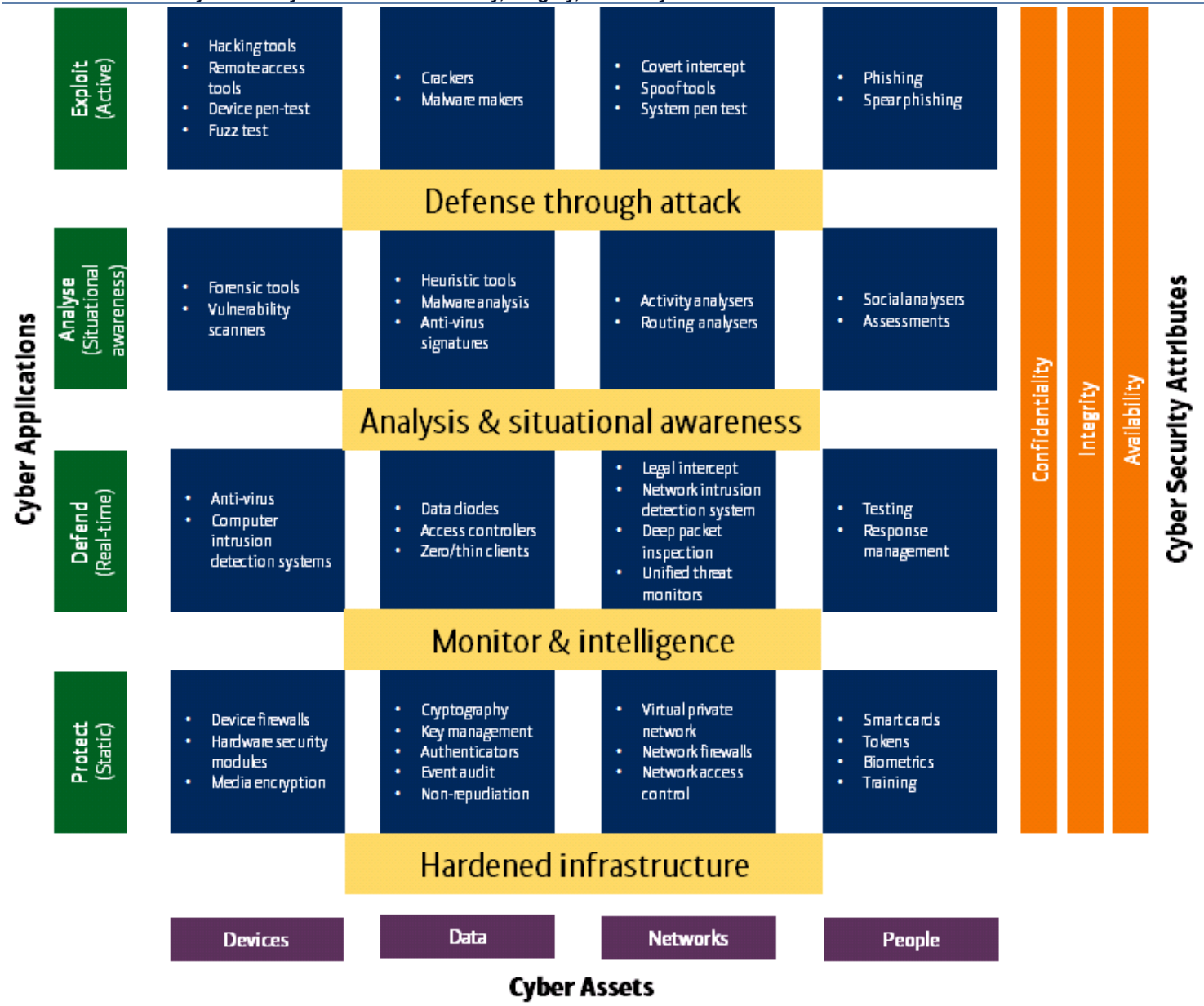
The result is that defence contractors with leading positions in cybersecurity (Ultra, QinetiQ et al) are targeting very specific high-threat, high-barrier-to-entry, niche markets with specialised product solutions – avoiding the high-volume, more commoditised and lower-margin consulting businesses. The volume and frequency of cybersecurity M&A deals in defence has continued to surge as defence contractors look to access the growth in this space.

Exhibit 80: Changing cyber-homeland threatscape



Source: Ultra Electronics

Exhibit 81: Homeland & cyber-security attributes: confidentiality, integrity, availability



Source: Ultra Electronics

High barriers to entry: incumbents continue to benefit

There are incredibly high barriers to entry for the high-threat market of cybersecurity due to: (1) the complexity and expertise necessary; and (2) the nature of confidentiality for the customer. A number of defence contractor cyber solutions focus on product (ie, hardware/software) as opposed to consulting/services, which are lower margin and offer much less opportunity for differentiation and growth.

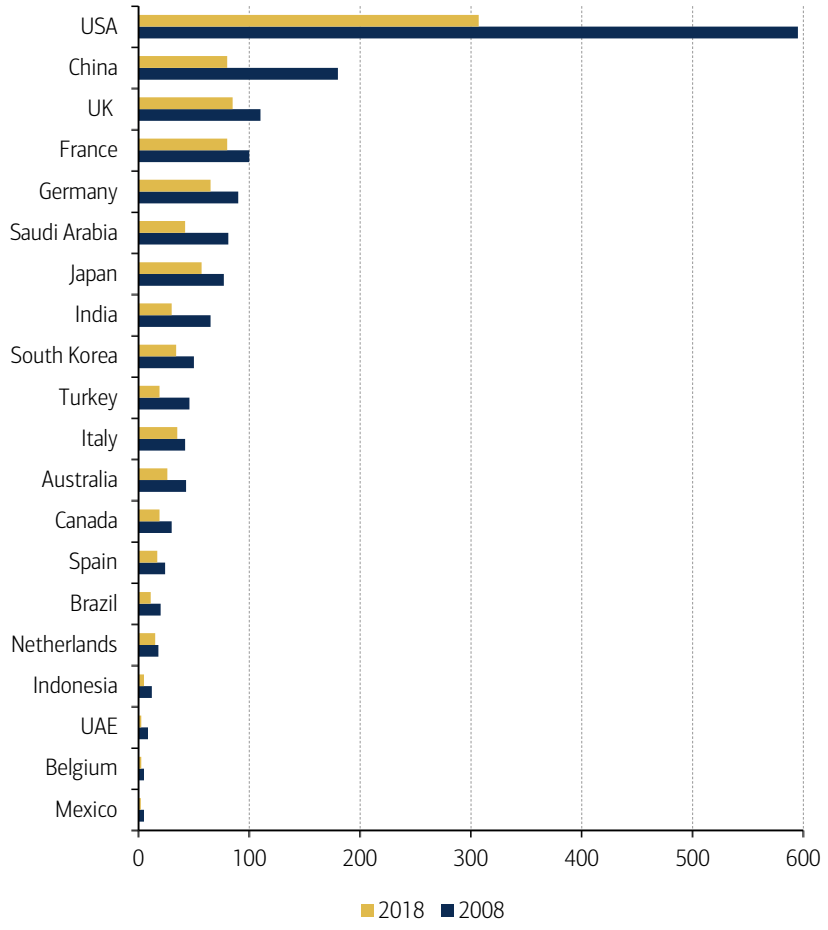
Governments dealing with high-level threats will only operate with contractors offering certified products, which is only achieved through a prior presence/relationship and trust/proven reliability. Customers at the high-threat/top-secret level are unwilling to announce big, public contract competitions as this compromises security.

US$540bn+ global homeland market by 2018E

With the rise in terrorists threats and the 9/11 attack, the homeland security market has grown from just US$30bn in 2000 to an estimated US$415bn in 2013 – encompassing

aviation security, mass trans-cybersecurity, maritime security, critical infrastructure security, cybersecurity, border security, CBRN Security, counter-terror intelligence, IT & C3I, and first responders. It is expected to register a CAGR of 5.54% to reach US$544bn by 2018E (source: marketsandmarkets.com).

Chart 122: National Security Outlay [$Billion]: 2008 & 2018



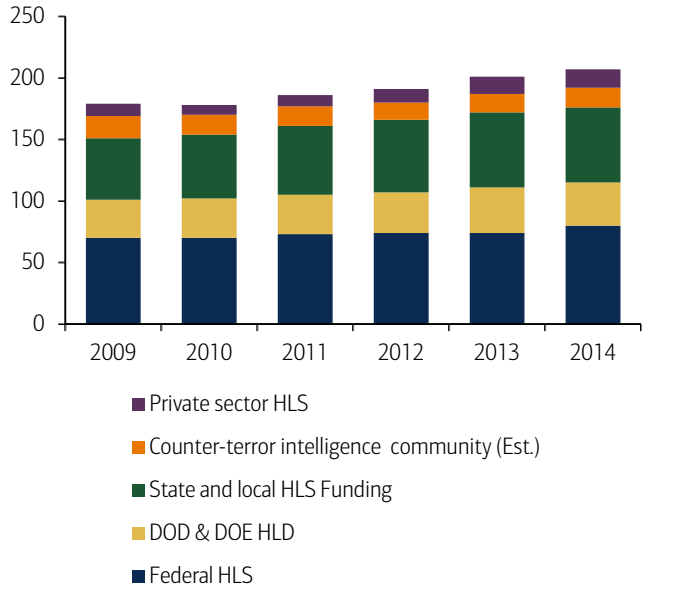
Source: HSRC, BofA Merrill Lynch Global Research

US: #1 homeland market

The combined US market for homeland security products and services – purchased by federal, state and local governments, the intelligence community and the private sector (excluding: HLD and post-warranty revenues) – should increase to US$81-84bn by 2020E, a CAGR of at least 5.9%. The US is expected to remain the dominant player in the homeland security market, with about 35% of the global procurement in this field (source: HSRC).

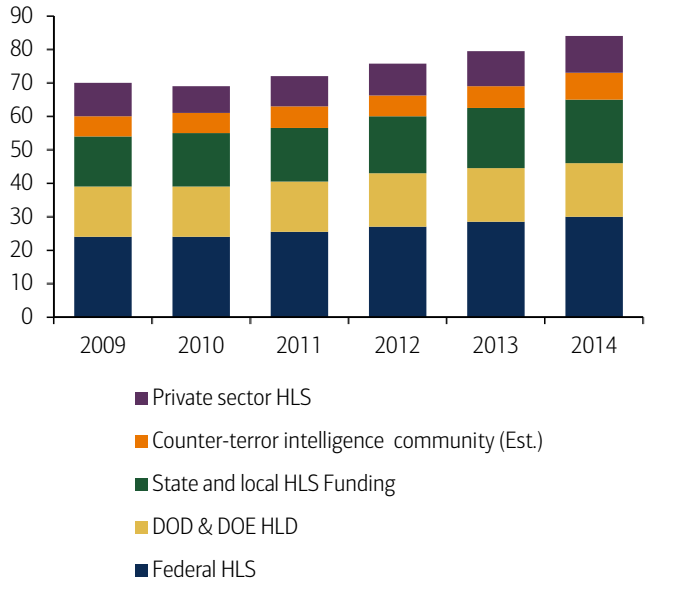
Bank of America Merrill Lynch

Chart 123: US HLS-HLD Funding ($ billion) 2009-2014



Source: HSRC, BofA Merrill Lynch Global Research

Chart 124: US HLS-HLD Market ($ billion) 2009-2014



Source: HSRC, BofA Merrill Lynch Global Research

Europe: homeland spending still important

For defence names, the focus is on high-threat cyber, usually government agencies, critical national infrastructure or large financial institutions. However, as the table below shows, cyber exposure is small as a % of sales for the majority of our companies. In our view, the biggest opportunity lies in commercial cyber, and the best way to play this is through commercial cyber security providers vs. cyber exposure through defence companies. The companies with the largest exposure to commercial cyber are Computer Sciences Corporation, Hewlett Packard, IBM, Intel, SAIC, Symantec, Trend Micro, Kaspersky Lab. There are also pure cyber security companies such as FireEye.

Table 46: Cyber security exposure within our coverage

	Cyber as % FY14 sales	Key cyber solutions	Product/Services mix	Target markets	Main regions
BAE Systems	7%	Data analytics , consulting services	Detica (20% of BAE's Cyber) mainly consulting. US business (80% of cyber)	Government & commercial (mainly financial)	c.75% US, c.25% UK
Finmeccanica	1.50%	Training, threat mgmt, infrastructure protection	Primary consulting, training and services	Government mainly, also large to small institutions	Mainly Italy, also other Europe
QinetiQ**	16%	Data monitoring, consulting expertise	BofAMLe 60% consulting and 40% hardware/software solutions	Governments, critical national infrastructure, SMEs	BofAMLe UK 50%, US 50%
Thales	3%	Encryption, risk assessment, infrastructure security. Have recently entered into strategic partnership with Alcatel	Encryption, risk assessment, infrastructure security	BofAMLe 20-30% consulting and 70-80% hardware/solutions	Global but UK and Europe primarily
Ultra Electronics	25%*	Network security, encryption, lawful intercept	BofAMLe 10% consulting and 90% hardware/software solutions	Government/military 70-80%, critical national infrastructure 20-30%	BofAMLe US 50%, UK 40%, RoW 10%

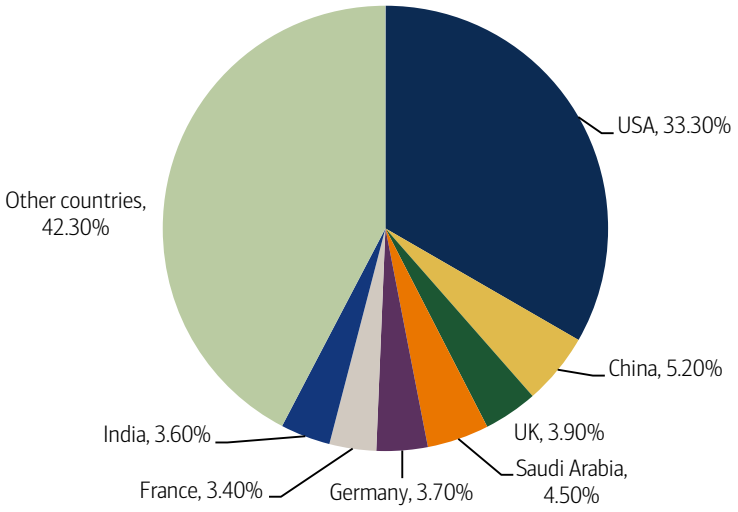
Source: BofA Merrill Lynch Global Research estimates *includes security **BofAMLe, includes C4ISR

EMs homeland markets growing fast

Saudi Arabia is the world's second largest market for homeland security growing out of the need to defend the kingdom and their petro-chemical infrastructure from the threats of home-grown terror. By 2016 China, is expected to surpass Saudi Arabia as the 2nd largest HLD market. After the U.S. China and Saudi Arabia, Britain, Germany, India and France are the next largest players. India, Turkey, and the UAE are also exhibiting

fast market growth on the back of GDP expansion and the increasing threats of terror elaborators (Source: HSRC).

Chart 125: Global HLS-HLD Market 2018 Market Share by Country



Source: HSRC, BofA Merrill Lynch Global Research

Good governance: boardroom engagement, insurance & global governance

The record growth in cybersecurity attacks and the growing cost impacts – IP losses, legal expenses, property losses, reputational losses, time lost, administrative costs et al - mean that cybersecurity risk needs to be included in the range of risks under the purview of boards of directors (i.e. strategic, operational, financial and compliance). This means going beyond the traditional hallmarks of cybersecurity sophistication such as executive leadership, clear, well documented policies and procedures, and integrated tools – and embedding cybersecurity both at board-level and across the board's approach to risk oversight.

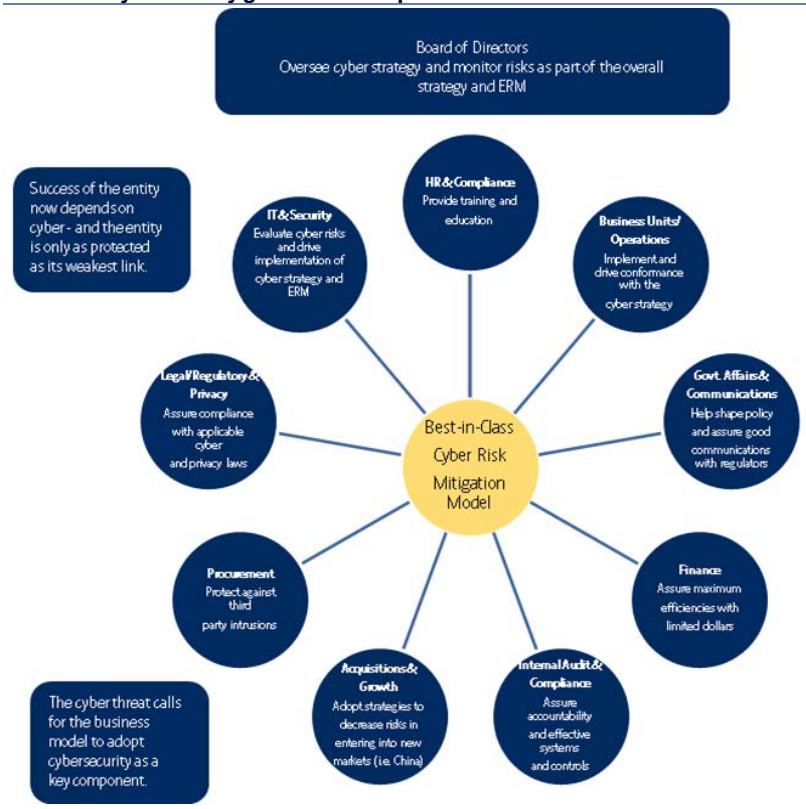
We believe that companies and boards still have a long way to go on cybersecurity. For instance, an 2015 NYSE Governance Services-Veracode survey of 200 directors of public companies across sectors, 66% are "less than confident" their companies are properly secured against cyberattacks. A June 2015 Ponemon Institute survey of board members and IT security professionals showed that only 43% of IT security professionals think that their board is informed about threats facing the organisation (vs. 70% of board members who thought this), and only 18% believe their boards cybersecurity governance measures are effective.

With the average cost of cybercrimes skyrocketing, we anticipate a growing market for cyber insurance. The cyber insurance market saw US$2.4bn in premiums in 2014 with US companies accounting for up to 90% of market - and financials, tech & communications and healthcare sectors accounting for 50% of premiums (source: Lloyd's). With the number of cyber attacks up to 80-90mn+ per year, the global cyber insurance market could grow to US$85bn, according to a number of insurer members at Lloyd's. The key challenge in the market's growth remains business leaders' lack of awareness on corporate cybersecurity, including the fact that they are often unaware that cyber is an insurable risk.

The increasing interconnectivity and aggregation of cybersecurity risks is increasingly rendering the borders of organisations and nation-states irrelevant – with attacks that originate in one location affecting multiple jurisdictions. As a result, a holistic and global approach to cybersecurity risk is thus vital. Despite some recent progress at the international and regional levels on norms and confidence-building measures, a comprehensive and functional regime of global cyber security governance remains clearly lacking (source: ESADEgeo-Zurich Insurance).

> "Boards that choose to ignore, or minimize, the importance of cybersecurity responsibility do so at their own peril." - SEC Commissioner Luis A. Aguilar

Exhibit 82: Cybersecurity governance components



Source: The Conference Board

- ## Better boardroom engagement is key

With cost, litigation, regulation and reputation making cybersecurity a critical business risk, we believe that boards and corporates show that they are insufficiently prepared to deal with the issue.

> "In the modern economy, every company runs on IT. That makes security the business of every person in the organization, from the chief executive to the newest hire, and not just personnel with "security" in their title or job description. Everyone should be accountable, and learn how not to be a victim." – Cisco

Companies & boards have a long way to go on governance

For instance an 2015 NYSE Governance Services-Veracode survey of 200 directors of public companies across sectors, 66% are "less than confident" their companies are properly secured against cyberattacks. A June 2015 Ponemon Institute survey of board members and IT security professionals showed that only 43% of IT security professionals think that their board is informed about threats facing the organisation (vs. 70% of board members who thought this), and only 18% believe their boards cybersecurity governance measures are effective.

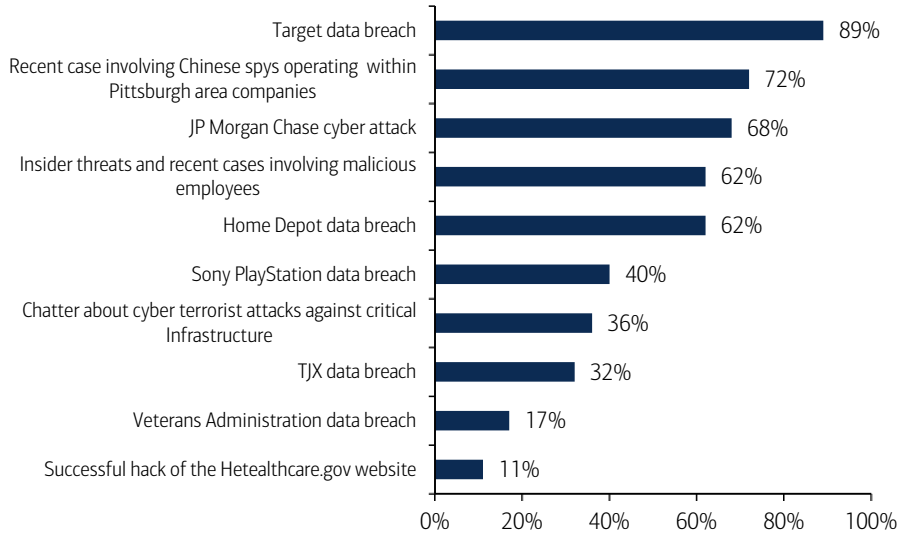
Responsibility is being seen as a broad business issue

According to the 2015 Cisco Security Capabilities Benchmark Study, 91% of organisations have an executive with direct responsibility for security. When cybersecurity breaches do occur, boards are most likely to hold CEOs accountable, followed by CISOs, and the entire executive team. CISOs only ranked fourth on the accountability ladder which can be seen as positive sign that cyberattacks are being seen as a broad board issue rather than an IT issue (source: NYSE Governance Services).

The Target breach has been a game changer in getting the C-Suite's attention

The 2014 Target breach has been key to the C-Suite and boardroom seeing cybersecurity risks as critical (source: Ponemon Institute).

Chart 126: How have cybersecurity incidents impacted boards involvement in cyber governance?

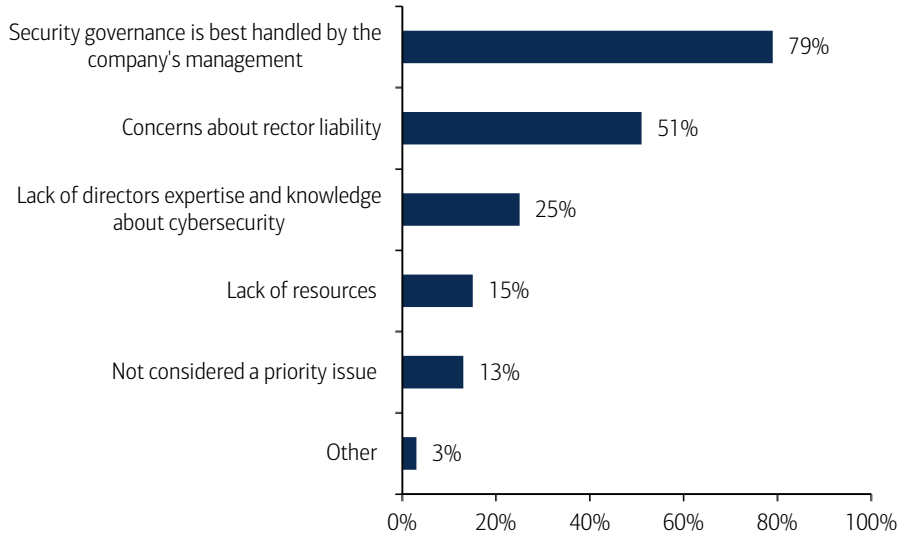


Source: Ponemon Institute

Cyber is becoming a topic for boardroom discussions

Between 65-80% of directors say cybersecurity topics are discussed at board meetings - but alarmingly – up to 35% say cybersecurity is not on their agenda, and c20% only held such discussions after the fact (i.e. post-an internal incident or incident at a competitor) (source: NYSE Governance Services, Ponemon Institute).

Chart 127: Why cybersecurity is not on the board's agenda

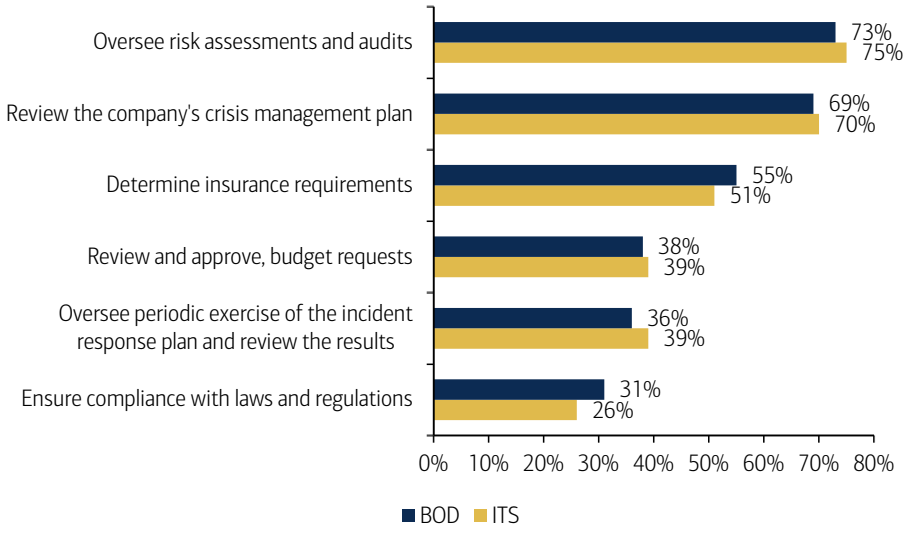


Source: Ponemon Institute

Board oversight & management may be insufficient to address the threatscape

Most boards are engaged in overseeing risk assessments and audits, reviewing the crisis management plan and determining insurance requirements. However, oversight activities that would make more of a contribution to the cybersecurity strategy of an organisation are rarely on the board's agenda such as ensuring compliance with laws and regulations (source: Ponemon Institute).

Chart 128: Top cybersecurity oversight activities

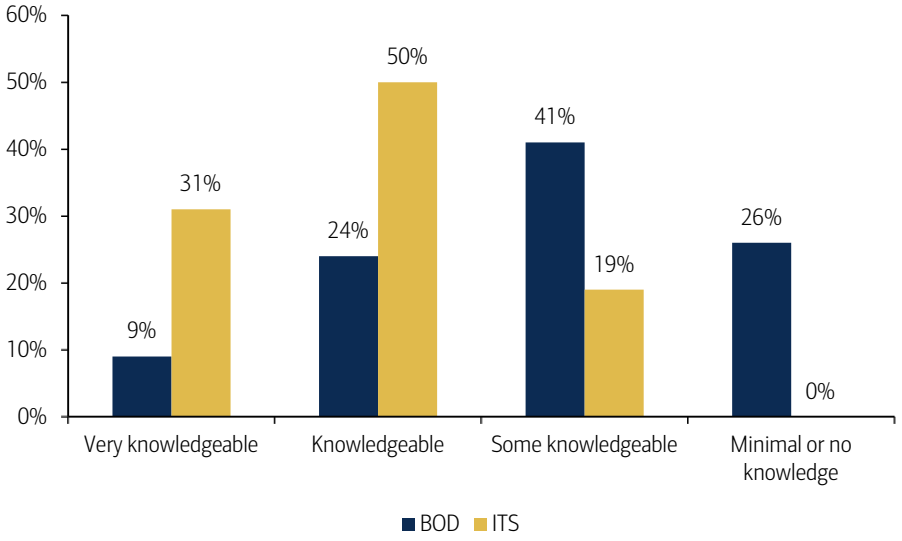


Source: Ponemon Institute

Board members knowledge is limited & IT security professionals sceptical

Only 33% of board members say they are very knowledgeable about cybersecurity meaning that boards may lack the information needed to make decisions about cyber governance and meaningfully communicate with IT professionals about risks. IT security professionals do not trust that boards are effective in dealing with cybersecurity governance issues due to knowledge and visibility gaps. Only 18% believe that their practices are very effective (vs. 59% of board members themselves) (source: Ponemon Institute).

Chart 129: How knowledgeable are you about cybersecurity?

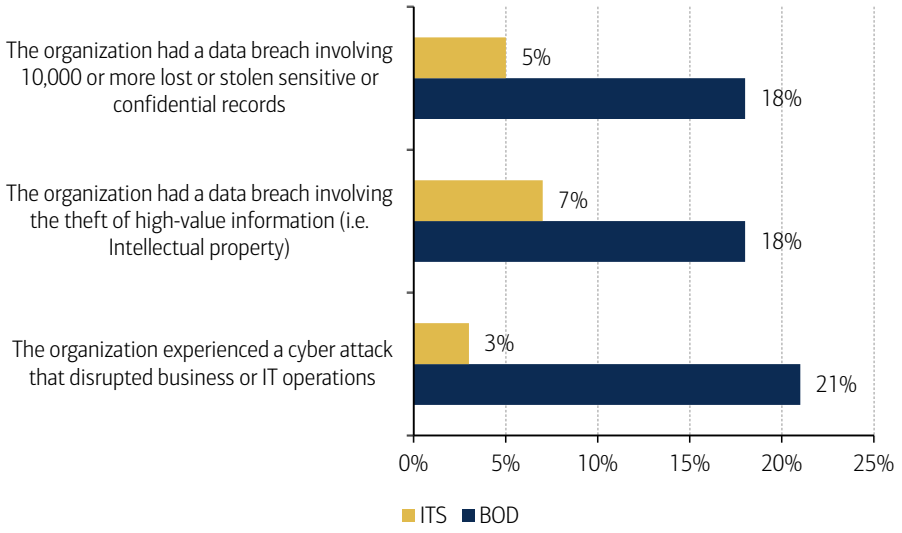


Source: Ponemon Institute

Board members are often in the dark about the theft of high value information

Board members may not be receiving information and breaches about cyber and data breaches - with only 59% of them aware of breaches, only 23% believing the their company has a breach involving IP and 18% unsure. There is also a significant gap in awareness between the board and IT security professionals about attacks (source: Ponemon Institute).

Chart 130: Uncertainty about cyber attacks and data breaches in the past 2Y

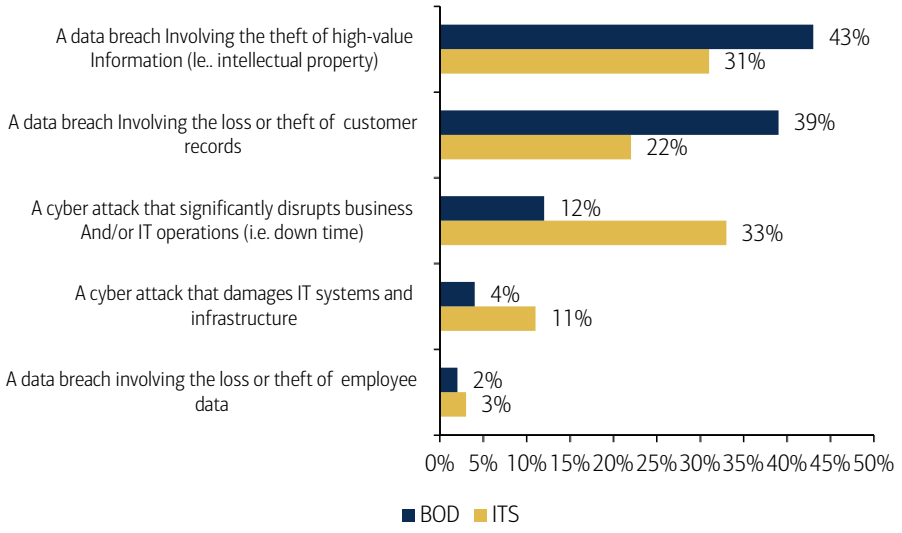


Source: Ponemon Institute

Directors top concerns differ widely from cyber professionals

In terms of cybersecurity fears, 44% of directors rank brand damage due to customer loss as their #1 fear, followed by the cost of responding to a breach, the loss of competitive advantage due to corporate espionage, and regulatory and compliance violations (source: NYSE Governance Services). In contrast, IT security professionals are focused on a cyber attack that significantly disrupts business and/or IT operations (downtime) (source: Ponemon Institute).

Chart 131: What worries board members & IT security professionals



Source: Ponemon Institute

Belief that cybersecurity blocks innovation –

46% of CFOs, 50% of CIOs, 51% of CEOs, and 70% of CTOs believe that internal cybersecurity policies block innovation to some extent (source: CEBR),

Don't understand the impacts of their products & services

Cybersecurity ranked 2nd to last on directors' list of concerns when introducing a new product and service to market (after revenue potential, competitive differentiation, and development costs). There was in fact a reluctance to add cybersecurity features because of their perceived inconvenience on customers and partners. (source: NYSE Governance Services).

3rd-party software & supply chain risk are of substantial concern

72% of surveyed directors are either "very concerned" or "concerned" about risk from third-party software in their supply chains (source: NYSE Governance Services).

Biggest barriers to innovation is HR

72% of surveyed directors said that finding and hiring people with the right skills is the largest roadblock to keeping up with the pace of innovation (source: NYSE Governance Services).

Adding cybersecurity talent & expertise is key

With only 11% of public company boards in the U.S. reporting a high level of understanding of cybersecurity (source: NACD), many companies and boards need to add employees and members with technology and cybersecurity expertise to truly understand the scope of cybersecurity issues that affect the organisation. Positively, in recent years, companies have been

- **Adding board members with cybersecurity knowledge** - such as AIG, Blackberry, CMS Energy, Delta Airlines, Ecolab, GM, Parsons, and Wells Fargo, among others.
- **Taking on cybersecurity experts to advise the CEO and board** – such as JPMorgan's recent hire of the former Chief of Staff to the US Army, General Odierno, to provide strategic advice to the CEO on a range of issues including evolving issues of physical and cyber security.

> Target did not have a CISO or CSO at the time it experienced a major attack in 2014.

Asking tougher questions on cybersecurity

Boards also need to start asking tough questions about cybersecurity. According to the National Cyber Security Alliance, key questions include:

- Is there a Board committee assigned to address cybersecurity? Do we need a separate risk committee?
- Does someone serving on the Board have expertise in cybersecurity and information technology?
- What are the company's cybersecurity risks and what cyberattacks have occurred?
- How is the company managing cyber risk?
- Does the company have a chief security officer who reports to a senior executive outside the information technology division?
- How is the organization using counsel and outside consultants?

- Do the company's outsourced providers and contractors have cyber controls and policies in place? Do they align with the company's expectations?
- What is the cybersecurity budget? Is it adequate?
- How will management respond to a cyberattack? What are circumstances when law enforcement will be notified?
- What constitutes a material cybersecurity breach? How will those events be disclosed to investors?
- Does the company have cyber insurance? If a cyber insurance policy is in place, is it adequate?
- Is there an annual company-wide awareness campaign established around cybersecurity?

Cyber-insurance: growing market for hack coverage

With the average cost of cybercrimes for US companies reaching a record US$12.7mn in 2014 and cybercrime costing the global economy up to US$575bn annually – we anticipate a growing market for cyber insurance. The cyber insurance market saw US$2.4bn in premiums in 2014 with US companies accounting for up to 90% of market - and financials, tech & communications and healthcare sectors accounting for 50% of premiums (source: Lloyd's). With the number of cyber attacks up to 80-90mn+ per year, the global cyber insurance market could grow to US$85bn, according to a number of insurer members at Lloyd's. The key challenge in the market's growth remains business leaders' lack of awareness on corporate cybersecurity, including the fact that they are often unaware that cyber is an insurable risk.

US$2.4bn in premiums in 2014

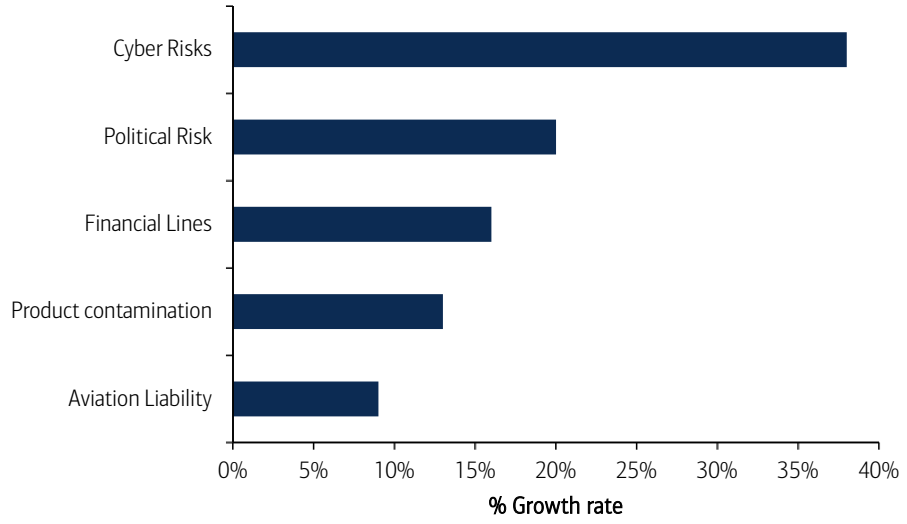
In 2014, the insurance industry took in US$2.4bn in premiums on policies to protect companies from cybersecurity losses. That was up from US$1.3bn in 2013 and US$1bn in 2013 and US$600mn in 2012 (source: Lloyd's).

According to Net Diligence's 2014 cyber claims study:

- The average payout for crisis services was US$366,484
- The average claim payout was US$733,109
- The average claim payout for a large company was US$2.9mn

Insurance cover for cyber risks grew at a CAGR of 38% between 2009 and 2014, according to Aon's own global risk insight platform, making it the company's fastest growing product during that period – greater than insuring against political risk and financial lines.

Chart 132: Total premium - CAGR 2009-2013



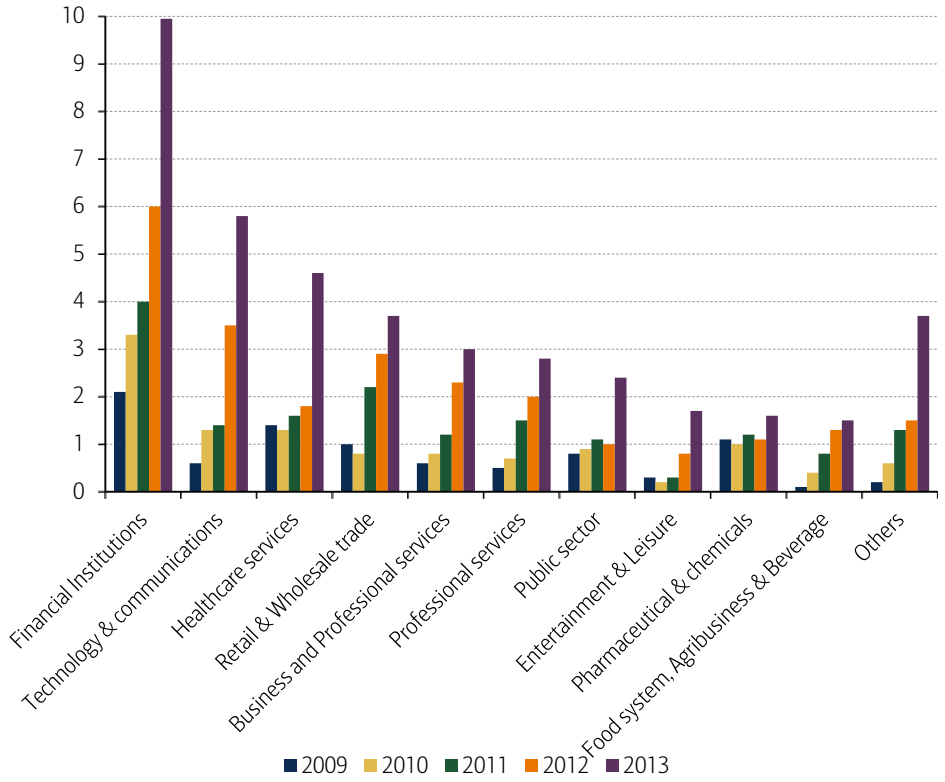
Source: Aon

Financials, tech & comms and HCA: top 3 sectors taking out premiums

Financial institutions, technology and communications and healthcare sectors were the top three sectors that took out premiums accounting for nearly 50% of the total cyber premium market globally (source: Aon).

Bank of America Merrill Lynch

Chart 133: Cyber Risk - Total premiums by Industry



Source: Aon

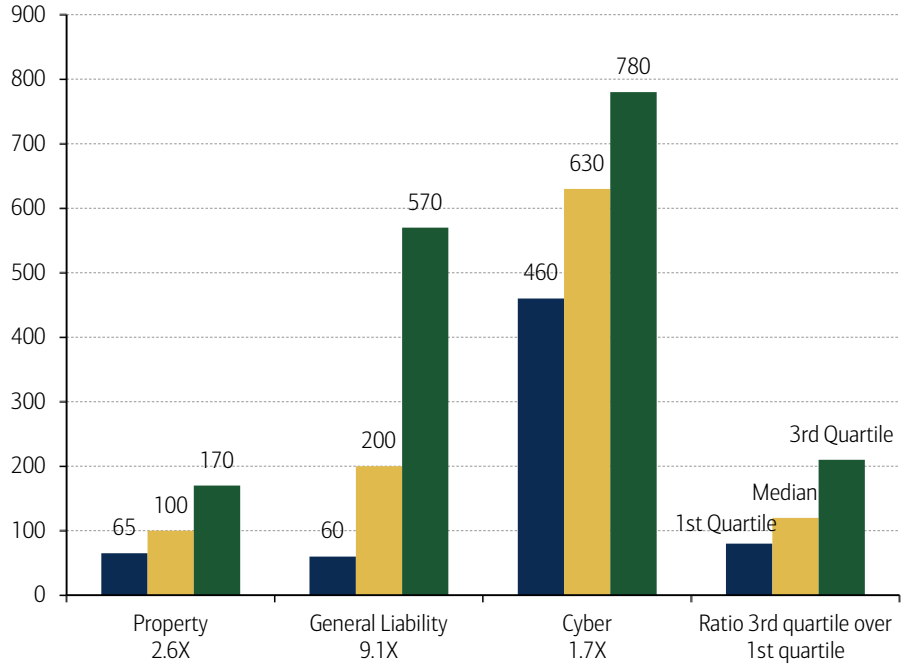
US companies are ahead of the curve: up to 90% of premiums

The exact number of companies that have a cyber insurance policy is difficult to determine given that individual surveys poll different numbers and types of respondents, often from a varied distribution of industry groups. But Lloyd's, estimates that up to 90% of insurance is being purchased by U..S. firms. The U.S. cyber insurance market was estimated to be worth US$1bn in 2014 vis-a-vis gross written premiums and is forecast to double to US$2bn by 2015 year-end (source: Marsh & McLennan).

Premiums priced towards the high end

The non-physical nature of cyber risks makes it possible for insurers to suffer losses from a vast number of clients spread across different geographies as a result of a single event. Hence in the case of cyber insurance, the price of the premium is driven by uncertainty over the risk compared to more traditional covers, where more historical data is available and incident cases are more predictable. As a result, we are seeing much flatter pricing for cyber across firms than for other lines of insurance; the difference between third and first quartile pricing is 1.7x for cyber, 9.1x for general liability, and 2.6x for property (source: UK Cybersecurity, Marsh & McLennan).

Chart 134: Pricing analysis, relative pricing index, property = 100



Source: UK Cybersecurity, Marsh & McLennan

Underwriters are conservative about cyber risk

The combination of a higher absolute price and lower price differentiation suggests that cyber is early in its development and that underwriters are more conservative about the risk, creating a challenge to a core role of insurance – namely, that high pricing discourages take up, and flat pricing provides no incentive for firms to reduce their cyber risk and save on premiums (source: UK Cybersecurity, Marsh & McLennan)

Companies have a long way to go on cyber insurance

As we have discussed throughout the report, there remains significant room for improvement in terms of companies and boards of directors' taking cybersecurity risk into account. This includes the need for better understanding the damages to an organisation from a cyber attack which can be categorised across multiple losses (see table below) which go well beyond the frequent focus on the single point of a data breach.

Table 47: Loss Categories Deriving From Cyber Attacks And Non-Malicious It Failures

Loss Category	Description
Intellectual property (IP) theft	Loss of value of an IP asset, expressed in terms of loss of revenue as a result of reduced market share.
Business interruption	Lost profits or extra expenses incurred due to the unavailability of IT systems or data as a result of cyber attacks or other non-malicious IT failures.
Data and software loss	The cost to reconstitute data or software that has been deleted or corrupted.
Cyber extortion	The cost of expert handling for an extortion incident, combined with the amount of the ransom payment.
Cyber crime/cyber fraud	The direct financial loss suffered by an organisation arising from the use of computers to commit fraud or theft of money, securities, or other property.
Breach of privacy event	The cost to investigate and respond to a privacy breach event, including IT forensics and notifying affected data subjects. Third-party liability claims arising from the same incident. Fines from regulators and industry associations.
Network failure liabilities	Third-party liabilities arising from certain security events occurring within the organisation's IT network or passing through it in order to attack a third party.
Impact on reputation	Loss of revenues arising from an increase in customer churn or reduced transaction volumes,

Table 47: Loss Categories Deriving From Cyber Attacks And Non-Malicious It Failures

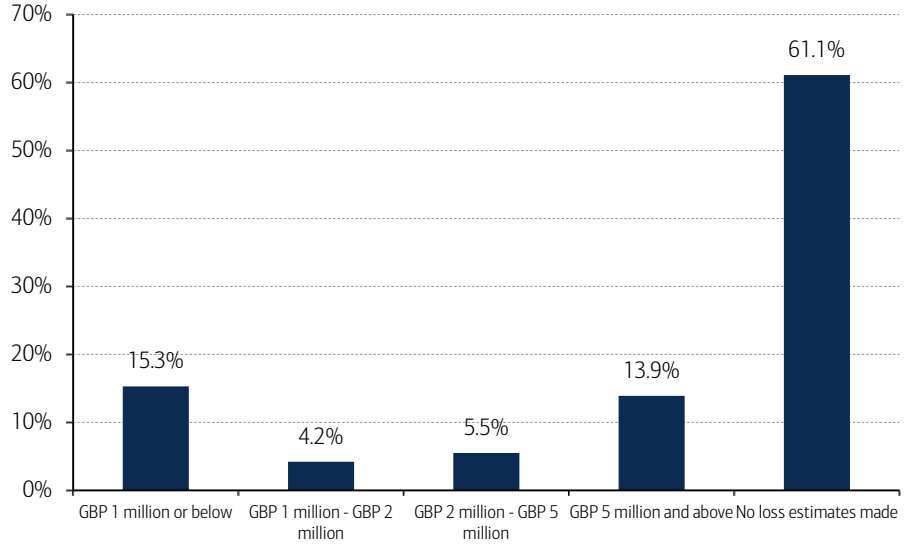
Loss Category	Description
	which can be directly attributed to the publication of a defined security breach event.
Physical asset damage	First-party loss due to the destruction of physical property resulting from cyber attacks.
Death and bodily injury	Third-party liability for death and bodily injuries resulting from cyber attacks.
Incident investigation and response costs	Direct costs incurred to investigate and "close" the incident and minimise post-incident losses. Applies to all the other categories/events.

Source: Marsh & McLennan

61% of UK companies have not attempted to estimate the financial impacts

For example, a recent survey by Marsh showed that 61.1% of UK organisations have not yet made any attempt to estimate or calculate the financial loss stemming from a cyber attack and only 13.9% estimate a worst case scenario of >£5mn in losses.

Chart 135: Has your organisation conducted or estimated the financial impact of a cyber-attach? What is the worst loss value?



Source: Marsh & McLennan

Over 50% of CEOs believe they have cyber insurance vs. <10% who actually do

This extends to cyber insurance with 52% of UK CEOs believing that they have insurance cover for cyber, whereas in fact less than 10% actually do (source: Marsh & McLennan).

> "52% of CEOs in the UK believe that they have insurance cover for cyber, whereas in fact only less than 10% do" - Marsh & McLennan

Cyber risks continue to be misunderstood at board level

Cyber risks continue to be misunderstood at the boardroom level with a recent survey conducted by Marsh & McLennan showing only 19.4% of boardrooms at UK organisations taking primary responsibility for the review and management of cyber risks with a worrying 55.5% allocating their IT department as the leading stakeholder.

Companies failing to account for risks vis-à-vis customers & suppliers

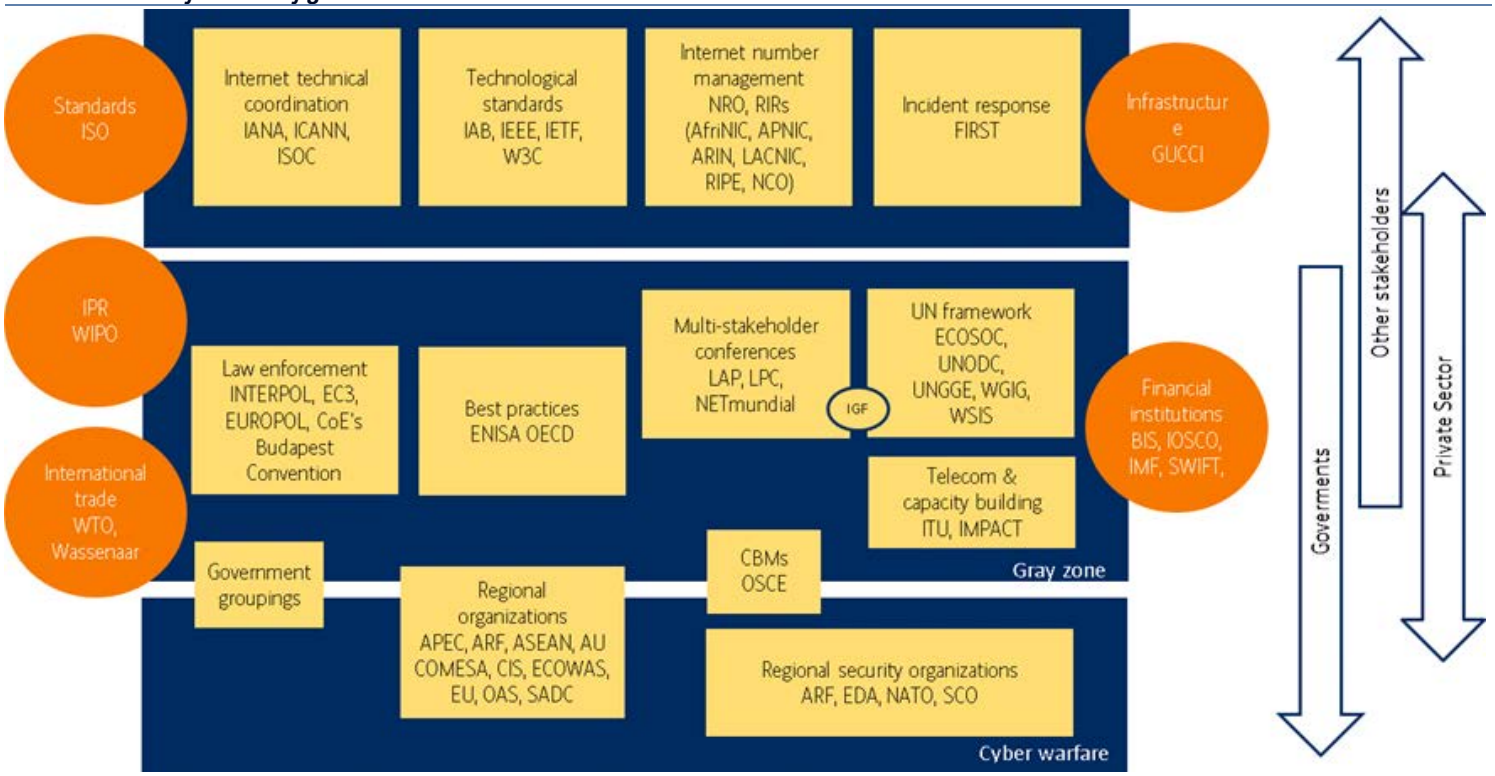
Nearly 70% of UK companies do not assess their suppliers and/or customers for cyber risks, which is worrying given the likely impacts on their business (source: Marsh & McLennan).

Need for better global cybersecurity governance

The increasing interconnectivity and aggregation of cybersecurity risks is increasingly rendering the borders of organisations and nation-states irrelevant – with attacks that originate in one location affecting multiple jurisdictions. As a result, a holistic and global approach to cybersecurity risk is thus vital. Despite some recent progress at the international and regional levels on norms and confidence-building measures, a comprehensive and functional regime of global cyber security governance remains clearly lacking (source: ESADEgeo-Zurich Insurance).

> "We are fast approaching a defining moment for global cyber governance. The ubiquity of the internet and impact of emerging technology present huge opportunities for global growth. But at the same time, cyber risks are becoming both more systemic and more interconnected. An effective cyber
> governance framework is vital." - ESADEgeo-Zurich Insurance

Exhibit 83: Global cybersecurity governance institutions



Source: ESADEgeo

Global cybersecurity governance challenges

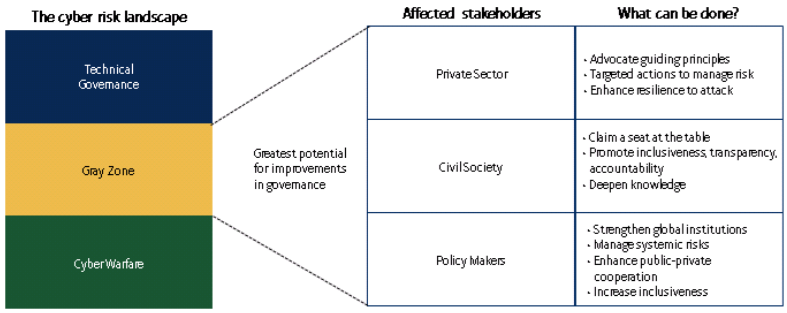
A detailed mapping of the rules, institutions, and procedures that govern the relationships among the different agents operating in the cybersecurity governance sphere reveals a number of challenges including

- **Three layers of cybersecurity governance** – technical governance (private to private and international organisations (IOs); grey zone: private to private (and IOs), private to government, and IOs, government to government (and IOs); and cyberwarfare (government to government).

Bank of America Merrill Lynch

- **Ideological differences preclude strong and effective institutions** – there exists no unanimously-accepted set of values to clearly guide global cyber governance.
- **Current governance framework does not adequately reflect the global nature of cyberspace** – with the framework primarily focused on WEur and NAm (source: ESADEgeo-Zurich Insurance).

Exhibit 84: Improving global cybersecurity governance



Source: Zurich Insurance Group

Towards a new global governance framework

Both the private sector and policymakers need to take measures to improve global cybersecurity governance:

- **Actions for private sector** – championing common values, sharing information to mitigate cyber risk, improving risk management, and resilience
- **Actions for policymakers** – strengthening global institutions, managing systemic cybersecurity risks, (eg Cyber WHO) enhancing public-private cooperation, and increasing inclusiveness (source: ESADEgeo-Zurich Insurance).

Table 48: Recommendations to private sector and policymakers to improve global cybersecurity governance

Recommendation	Proposed mechanism
Business	
Greater information-sharing to mitigate cyber risk.	Insurance industry via the CRO forum. Anonymized business loss reporting via private sector-led initiatives, e.g., FS-ISAC, public-private bodies e.g., ENISA.
Champion common values for global cyber governance in absence of governments' consensus.	Lobby through institutions, particularly privately-led initiatives, e.g., CRO forum and multi-stakeholder dialogue forums, such as WEF.
Take targeted actions to manage cyber risk.	Adopt SANS 20 Critical Security Controls. Further actions needed for larger organizations.
Enhance general resilience to cyber risk.	Built-in redundancy, incident response and business continuity planning, scenario planning and exercises.
Policymaker	
Strengthen those aspects of global governance that have worked properly and isolate them from geopolitical tensions.	Develop informal global cyber networks. Adopt a 'build it and they will come' approach.
Create a system-wide institution for incident response.	G20+20 Cyber Stability Board.
Enhance crisis management to deal with a potential systemic cyber crisis.	Cyber WHO (World Health Organization).
Seek greater public-private cooperation.	Incentivize alignment of public/private interests on cyber security.
Reinforce protection of critical information infrastructures.	Cyber stress tests.

Source: ESADEgeo-Zurich Insurance

Regulations: early days but still a long way to go

Governments are introducing new cybersecurity legislation in the face of growing risks. They are also tweaking or updating their IT and criminal laws to reflect the changing nature and damage of cyber-attacks. With each country around the world differing in terms of IT infrastructure maturity, each one is dealing with the emergence of national cybersecurity at different stages of their economic development, meaning countries are tackling this issue in many different approaches.

On the flipside of recent reforms in cybersecurity laws is the issue of data privacy and state surveillance. On the one hand there is the argument that the government should be able to do whatever it takes to secure the general welfare of its citizens, including spying on them, in the interests of national homeland security. On the other hand, some believe that civil liberties shouldn't be sacrificed whatever the costs. Hence there is somewhat a contradiction in ensuring the "bad guys" don't get hold of someone's personal data but the government's ability to read private text messages is seen as legitimate hacking.

US, lack of federal regulation & coordination

President Obama is on record as stating that cyber-attacks are the "most serious economic and national security" challenge America faces. However, there remain few federal cybersecurity regulations (ex-those focusing on specific industries) that really punish those who attack the US.

> Cyber-attacks are the "most serious economic and national security" challenge America faces today - US President Obama

In February 2013, President Obama proposed the Executive Order Improving Critical Infrastructure Cybersecurity which seeks to enhance information flow between DHS and critical infrastructure companies. And in January 2015 this was updated with his Executive Order that "encourages the private sector to share appropriate cyber threat information with the Department of Homeland Security's National Cybersecurity and Communications Integration Center" (source: White House)

The spotlight on legislation has been also augmented with the recent Sony Pictures and OPM hacks which were sourced to North Korea and China respectively. The former set the ball rolling on using economic sanctions to tackle cyber attacks coming from nation-state. By April 2015, Obama introduced an Executive order that froze the property and assets of persons engaging in significant malicious cyber-enabled activities. It allowed the US Treasury Dept. to freeze assets and bar other financial transactions of entities engaged in destructive cyber attacks.

No single standard for private-sector companies

In addition, although a frequent topic of discussion on, no single standard for private-sector cybersecurity programs has yet to emerge among the main US federal departments. The National Institute of Standards and Technology (NIST) Cybersecurity Framework is often considered foremost among existing guidance, but several other agencies are also expressing views, including the following recent guidance from the Department of Justice (DOJ), the Securities and Exchange Commission (SEC) and the Federal Trade Commission (FTC). The following are the latest guidance notes from each one (source: Sidley Austin LLP):

- **DOJ** - has issued helpful cybersecurity guidance notes for companies "to assist organizations in preparing to respond to a cyber incident". This guidance is voluntary in nature and is not a binding regulation per se.

- **FTC** – was granted the legal right to police and sue corporates if their cybersecurity practices failed in protecting their customer data under Section 5 of the Federal Trade Commission Act "which prohibits unfair and deceptive acts or practices". As a result, the FTC has brought more than 50 lawsuits against companies over lax cybersecurity, most of which have resulted in settlements. Hence there is growing concern from the corporate space that litigation will be brought upon them even if data breaches were initiated by cyber attackers.

- **SEC** - recently issued a guidance update, building on its initial investigation, for registered investment advisers and investment companies underscoring the need for them to continuously review their cybersecurity preparedness. The SEC makes clear that the failure to implement adequate cybersecurity protections could raise serious regulatory compliance issues.

Europe, regulation tightening

In 2013 the EU published a new cybersecurity strategy including a proposed directive. Networking and Information Security (NIS) which would impose a legal obligation on companies to ensure they have suitable Cybersecurity systems in place, require notification of potential security risks and for actual incidents to be reported to cybersecurity authorities that will be established across Europe.

Proposed EU cybersecurity directive

The Directive could mean a ramping up of spend in the space with operators of critical infrastructures in some sectors (financial services, transport, energy, health), enablers of information society services (notably: app stores e-commerce platforms, Internet payment, cloud computing, search engines, social networks) and public administrations obliged to adopt risk management practices and report major security incidents on their core services. As of June 2015, the directive's principles are being finalized into legally binding regulations, with negotiation and implementation looking set for 2016.

The Directive does not cover breaches of personal data, but rather systemic cyber attacks that compromise data systems. So, while European institutions are still trying to find an agreement regarding the general data protection regulation, capable of equipping the EU with a set of rules fit for the 21st century on the protection of personal data, the Directive will in parallel ensure that deleting, damaging, deteriorating, altering or suppressing computer data on an information system, or rendering such data inaccessible, intentionally and without right, will be punishable as a criminal offence.

Table 49: EU Cybersecurity Maturity Dashboard (2015)

# QUESTION	Austria	Belgium	Bulgaria	Croatia	Cyprus	Czech Republic	Denmark	Estonia	Finland	France	Germany	Greece	Hungary	Ireland	Italy	Latvia	Lithuania	Luxembourg	Malta	Netherlands	Poland	Portugal	Romania	Slovakia	Slovenia	Spain	Sweden	United Kingdom
LEGAL FOUNDATIONS																												
1. Is there a national cybersecurity strategy in place?	✓	✓	✗	✗	✓	✓	✗	✓	✓	✓	✓	✗	✓	✗	✓	✓	✓	✓	✗	✓	✓	Draft	✓	✓	✗	✓	✗	✓
2. What year was the national cybersecurity strategy adopted?	2013	2012	-	-	2013	2011	-	2014	2013	2011	2011	-	2013	-	2014	2014	2011	2013	-	2013	2013	-	2013	2008	-	2013	-	2011
3. Is there a critical infrastructure protection (CIP) strategy or plan in place?	✓	⊙	⊙	✗	✗	✓	✗	✓	✓	✗	✓	✓	⊙	✗	✓	✗	⊙	✗	⊙	✓	✓	✗	✓	✓	✓	✓	✓	✓
4. Is there legislation/policy that requires the establishment of a written information security plan?	✗	✗	✗	✗	✗	✓	⊙	✓	⊙	✗	✗	⊙	✓	✗	✗	✗	✗	✗	⊙	⊙	⊙	✗	✗	⊙	✗	✗	✓	⊙
5. Is there legislation/policy that requires an inventory of "systems" and the classification of data?	✓	✓	✓	✓	⊙	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	⊙	⊙	✓	✓	✓	✓	✓	✓	✓	✓	✓
6. Is there legislation/policy that requires security practices/ requirements to be mapped to risk levels?	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✗	✓	✗	✓	✓	✓	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓
7. Is there legislation/policy that requires (at least) an annual cybersecurity audit?	✓	✗	✗	✗	✗	✗	✗	✓	✓	✗	Draft	✗	✗	✗	✗	✓	⊙	⊙	⊙	⊙	✗	⊙	✗	✗	⊙	⊙	✗	✗
8. Is there legislation/policy that requires a public report on cybersecurity capacity for the government?	⊙	✗	✗	⊙	✗	✓	✗	✓	✓	✗	Draft	✗	✓	✗	✓	✗	⊙	✗	✗	✓	✗	⊙	✗	⊙	✗	✗	✗	⊙
9. Is there legislation/policy that requires each agency to have a chief information officer (CIO) or chief security officer (CSO)?	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗
10. Is there legislation/policy that requires mandatory reporting of cybersecurity incidents?	✗	⊙	✗	✗	✓	✓	✗	✓	✗	✗	✓	✗	✗	✗	✗	✓	✓	✗	✓	✗	✓	✗	✓	✗	✓	✗	✗	✗
11. Does legislation/policy include an appropriate definition for critical infrastructure protection (CIP)?	✓	✓	✓	✗	✗	✓	✓	✓	✓	✗	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓
12. Are requirements for public and private procurement of cybersecurity solutions based on international accreditation or certification schemes, without additional local requirements?	✓	⊙	N/A	N/A	N/A	⊙	✓	✓	✓	⊙	✓	✓	✓	N/A	✓	⊙	⊙	⊙	N/A	✓	⊙	N/A	⊙	✗	N/A	✓	✓	⊙
OPERATIONAL ENTITIES																												
1. Is there a national computer emergency response team (CERT) or computer security incident response team (CSIRT)?	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	⊙	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2. What year was the computer emergency response team (CERT) established?	2008	2008	2008	2009	-	2011	2009	2008	2014	2008	2012	2009	2013	-	2014	2006	2006	2011	2002	2012	2008	2008	2011	2009	2010	2008	2003	2014
3. Is there a national competent authority for network and information security (NIS)?	⊙	✓	✓	✓	⊙	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	⊙	✓	⊙	⊙	✓	✓	✓	✓	✓	✓	✓
4. Is there an incident reporting platform for collecting cybersecurity incident data?	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
5. Are national cybersecurity exercises conducted?	✓	✓	✓	⊙	⊙	⊙	✓	✓	✓	✓	✓	✓	⊙	✓	✓	✓	⊙	⊙	⊙	✓	⊙	⊙	⊙	✓	⊙	⊙	✓	✓
6. Is there a national incident management structure (NIMS) for responding to cybersecurity incidents?	✓	✗	⊙	✗	✗	✓	⊙	⊙	✗	✗	✗	✗	✓	✗	✓	✓	⊙	⊙	✗	✓	✓	⊙	⊙	✗	✗	✓	⊙	✓
PUBLIC PRIVATE PARTNERSHIPS										✗																		
1. Is there a defined public private partnership (PPP) for cybersecurity?	✓	⊙	⊙	⊙	⊙	✗	✗	⊙	⊙	✗	✓	✗	⊙	✗	⊙	✗	✗	✗	⊙	✓	✗	⊙	✗	✗	✗	✓	⊙	✓
2. Is industry organised (i.e. business or industry cybersecurity councils)?	✓	✓	⊙	✗	✗	✗	✓	⊙	✓	✗	✓	✗	⊙	✓	⊙	✗	⊙	✗	✗	✓	⊙	✗	⊙	⊙	⊙	✓	⊙	✓
3. Are new public private partnerships in planning or underway (if so, which focus area)?	✓	✗	✗	✗	✗	⊙	✗	✗	✗	⊙	✓	✗	✗	✗	⊙	⊙	⊙	⊙	✗	-	✗	✗	✓	✗	✗	-	✗	-
SECTOR SPECIFIC CYBERSECURITY PLANS																												
1. Is there a joint public private sector plan that addresses cybersecurity?	✓	✗	✗	⊙	⊙	✗	✗	✗	⊙	✓	✗	✗	⊙	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✓	✗	✓
2. Have sector specific security priorities been defined?	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	⊙	✗	⊙
3. Have any sector cybersecurity risk assessments been conducted?	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
EDUCATION																												
1. Is there an education strategy to enhance cybersecurity knowledge and increase cybersecurity awareness of the public from a young age?	✓	⊙	⊙	✗	✗	✓	✗	✓	✓	✓	⊙	✗	✓	⊙	✓	✓	✓	✓	✗	✓	✓	✗	✓	✓	✗	✓	✗	✓

Source: BSA

€100m potential fine for companies

The EU General Data Protection Regulation (GDPR) is expected to add new requirements for breach notification to individuals, require organizations that handle personal data to conduct risk assessments and audits, and increase fines for compromised businesses. It is hoped that the new breach notification requirements may increase disclosure of security incidents in Europe, where in the US, state data-breach notification statutes have resulted in the disclosure of a significant number of security breaches which in turn has raised the consciousness around cybersecurity issues (source: PwC)

Table 50: Actual vs. potential fines under the EU scenario

Company	Date	Fine paid (€m)	Revenue (€m)	% revenue	EU 2% scenario (€m)	EU 5% scenario (€m)
Sony	Jan-2013	0.29	53,800 (2012)	< 0.001%	1,076	2,690
Google	Jan-2014	0.15	11,400 (2013)	0.00%	228	570
Thomas Cook	Jul-2014	0.19	11,115 (2013)	0.00%	222	556

Source: Schroders

The updated data protection framework would inflict strict sanctions on companies breaching data privacy laws, including a fine of up to €100m or 5% of a company's global annual turnover (source: European Commission). Hence if we compare recently imposed fines on companies, either after significant data breaches or failures to comply with data regulations, these fines would actually have a greater material impact on companies' revenues under the new EU scenario. For instance, Thomas Cook was fined only €190, 000 in 2014 after million of banking details were stolen in 2014 which is immaterial compared to the new €100m or 5% threshold imposed by the EU (source: Schroders).

Overall, the EU's pipeline of cybersecurity legislation is now expected to be fully enforced sometime in 2017, according to numerous law firms specialising in this space. Given that the European Council has stated that "the timely adoption of … the Cybersecurity Directive is essential for the completion of the Digital Single Market by 2015", we expect cybersecurity to remain high on the agenda of the European Parliament going forwards.

RoW, regulation catching up

With cybersecurity increasingly becoming a global phenomenon, rather than just an issue confined to the West, the rest of the world also need to implement cybersecurity regulation, in our view. Considering APAC enterprises spent $230 billion to deal with cybersecurity breaches in 2014, the highest for any region globally, there remains huge scope to reduce this cost with better laws governing cyber activity (source: Marsh & McLennan). Below are examples of the latest legislation either introduced or pending for each country:

- **Singapore** - the 2014 introduction of the Personal Data Protection Act (PDPA) highlights several new stringent requirements, such as suggesting organizations having cyber insurance in place and be able to produce a comprehensive history of all security incidents.

  Organizations that do not fully comply with this act are subject to financial penalties of up to US$788,995 or SGD$1 million (Source: Singapore Personal Data Protection Commission, PwC).

- **South Korea -** implementation of the Personal Information Protection Act in September 2011, considered among the toughest in Asia. In April 2013, the government announced the National Anti-Cyberterrorism Act escalating the issue to a matter of national security in the context of purported North Korean attacks,

- **India –** the Information Technology Act of 2000 addressed cybercrimes such as email scams, identity theft, however in 2013 the government introduced a National Cyber Security Policy in order to enhance protection to public and private infrastructure and sovereign data.
- **Taiwan** - Computer-Processed Personal Data Protection Law was amended and renamed the Personal Information Protection Act (PIPA) in 2010, and came into full effect in October 2012
- **Japan** – a draft proposal was first discussed in June 2013 and by mid-2015, the government adopted a revised draft cybersecurity strategy in the wake of a huge personal data breach in the Japan Pension Service. It proposes for the NISC to monitor independent administrative agencies and other government-linked organizations for cyberattacks.
- **Philippines** - enactment the Cybercrime Prevention Act in 2012 criminalizes "cyber squatting", online libel and slander among others

Russia, data localisation would cost $6bn

Russian President Vladimir Putin signed the nation's new data localisation law in July 2015 in an effort to prevent Russian citizens from getting hacked, although some human rights groups believe it was designed to give government more control of Internet use in the country. The recently introduced law in would effectively require foreign businesses and web services to house Russian data inside the country as opposed to outside e.g. Google storing data they've collected in Russian servers rather than repatriated back to the US. According to the ECIPE's analysis, data localisation would cost the Russian economy over $6bn, with Russian GDP falling $ 3.2 billion, while foreign investment could tumble $2.9 billion.

China, the Great Firewall 2.0?

Similar to Russia, China has also begun to draft its very own data localisation law, proposing its own national cybersecurity law in mid-2015. If the draft law is enacted, it will also require foreign internet companies that operate within China to store this information within the country rather than their own domiciled servers. The draft law states that its objectives are to: (1) safeguard China's cyber sovereignty; (2) protect against cyber-attacks; (3) augment internet security and safety (4) regulate the use of personal data. (source: NPC China). However, unlike the Russian law there remains scope for interpretation as the clauses are more vague in capturing specificities.

Global trade, "arms-like" control on cyber technology

China and Israel aren't parties to the Wassenaar Agreement

Amid growing cyber-security and homeland defence concerns, the 41 arms-exporting country signatories to the Wassenaar Agreement – which regulates exports of military hardware and "dual-use" equipment – agreed in December 2013 that export controls should be established for "Internet Protocol (IP) network surveillance systems or equipment, which, under certain conditions, may be detrimental to international and regional security and stability." Efforts to place controls on devices and software could create substantial challenges for cybersecurity-exposes businesses that outsource software or hardware development or that do not currently need export licences for sales abroad (Source: WilmerHale).

EU implemented proposal: US moving towards stricter version

In October 2014, the European Commission adopted a delegated Regulation updating the EU list of dual-use items subject to EU export controls. It came into force on 31 December 2014. The delegated Regulation introduces numerous changes, including controls on new categories of items such as IT intrusion software, or spyware, and

telecommunication and internet surveillance equipment. The updated list reflects growing security concerns regarding the use of surveillance technology and cyber-tools that could be misused in violation of human rights or against the EU's security.

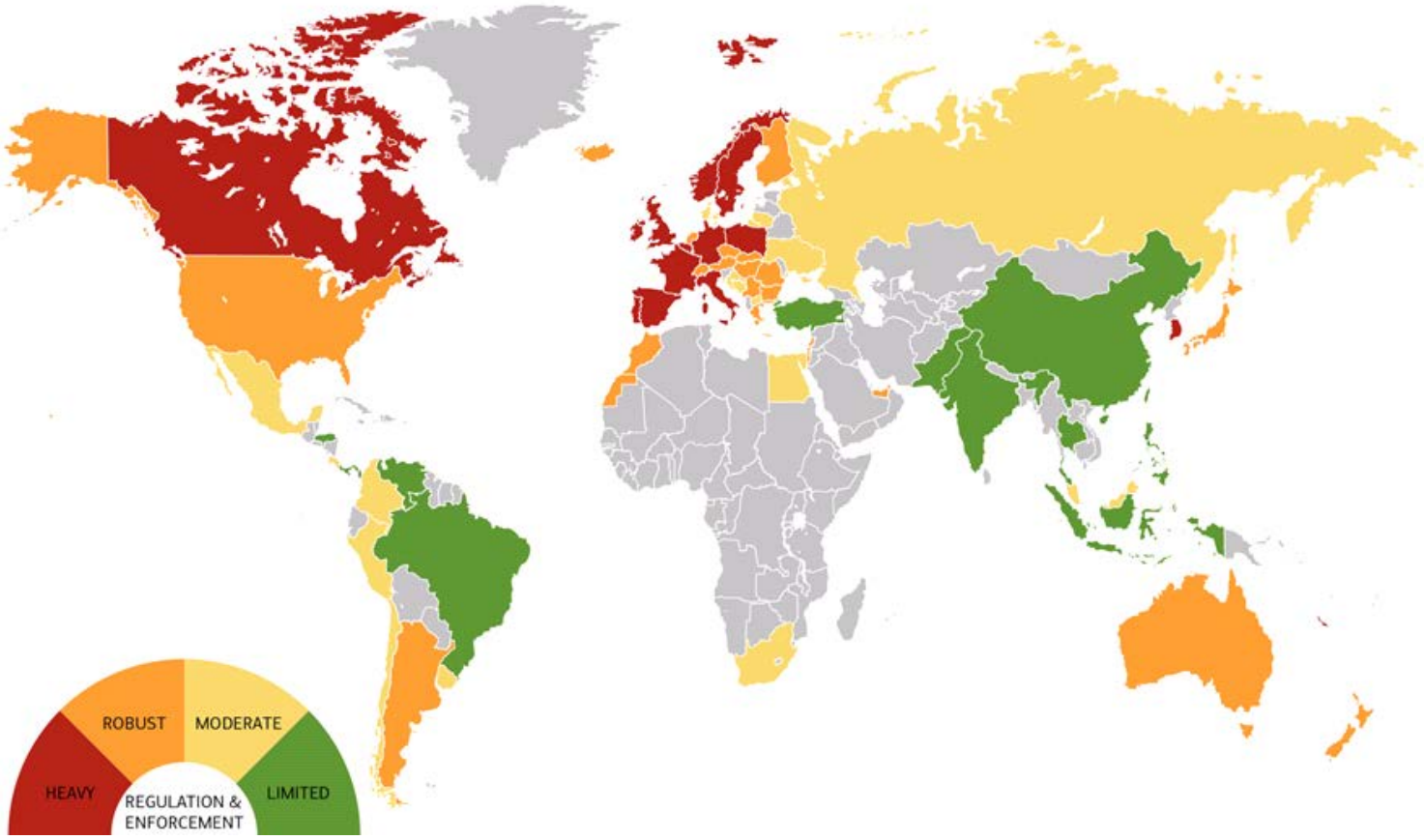
The US already imposes export controls for equipment, software and technologies that provide penetration capabilities for attacking, denying, disrupting or otherwise impairing the use of cyber infrastructure or networks – and Congress is considering new export controls on cybersecurity technologies and offensive cyber "weapons." The 2014 “National Defense Authorization Act” (NDAA) would require that federal departments suppress the trade in cyber tools and infrastructure that can be used for criminal, terrorist or military activities (ex-legitimate purposes of self-defence), and ask the President to study ways to contain the proliferation of "cyber weapons." In 2015, the U.S. Department of Commerce's Bureau of Industry and Security (BIS) published a proposal to implement the Wassenar agreement. The proposal caused alarm among major players in the security market because it proposed licensing restrictions on exporting and transfer of intrusion software and security research.

Privacy & civil liberty concerns

On the flipside of recent reforms in cybersecurity laws is the issue of data privacy and state surveillance. On the one hand there is the argument that the government should be able to do whatever it takes to secure the general welfare of its citizens, including spying on them, in the interests of national homeland security. On the other hand, some believe that civil liberties shouldn’t be sacrificed whatever the costs. Hence there is somewhat a contradiction in ensuring the “bad guys” don’t get hold of someone’s personal data but the government’s ability to read private text messages is seen as legitimate hacking.

Hence legislation not only pertains to cybercrime but also increasingly matters pertaining to privacy driven by the escalation in the number of data breaches. DLA Piper’s map below shows how data privacy vis-à-vis regulation and enforcement differs globally. On one side of the spectrum Europe has one of the most severe laws in place whilst on the other side EMs such as China, India and Brazil have more limited rules governing data protection.

Exhibit 85: Global data protection laws by severity



Source: DLA Piper

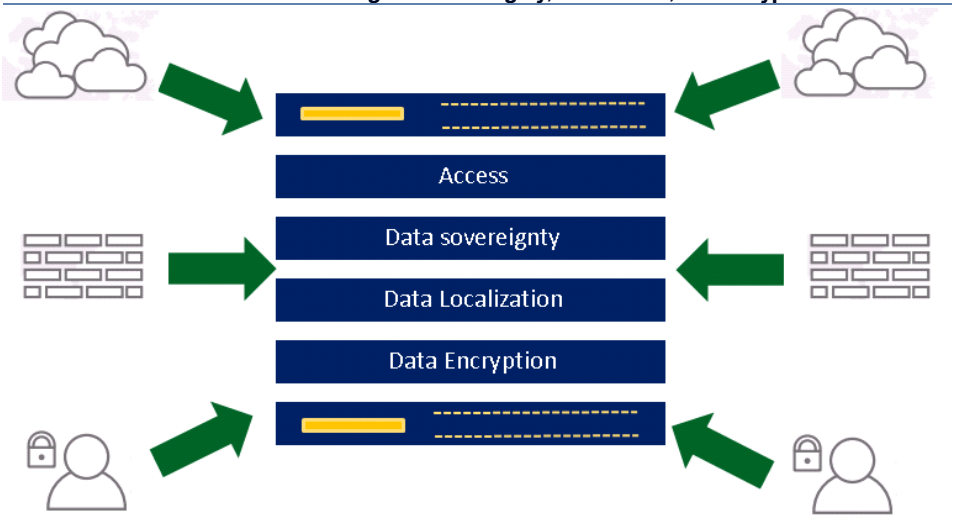
Consumer data privacy

Whilst consumers online have been victimized by cyber-threats in the form of malware and identity theft, they are increasingly facing the challenge of determining which companies to trust in holding their personal information amidst the escalation in data breaches.

> 1 in 3 consumers admitted they provide false information in order to protect their privacy - Symantec

According to a survey by Symantec, 57% of respondents are worried their data is not safe at all. In addition, 88% say data protection this is an important factor when choosing a company to do business with—more important than the quality of the product (86%) or the customer service experience (82%)..

Exhibit 86: The Conundrum of Balancing Data Sovereignty, Localization, and Encryption



Source: Cisco

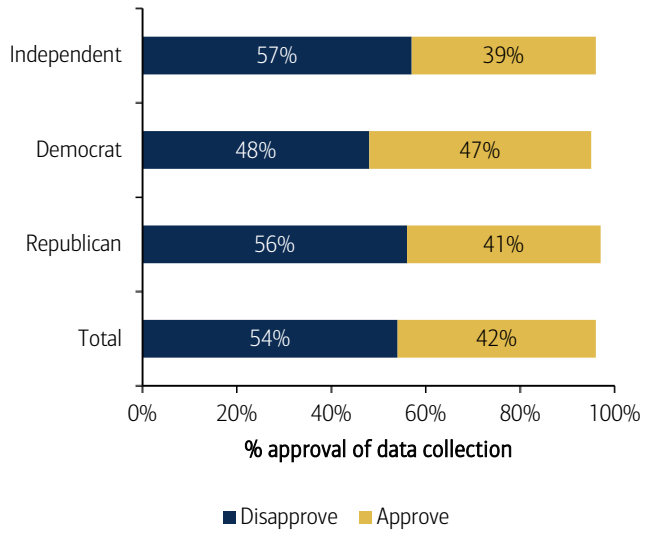
Amazon most trusted company for data privacy

According to Ponemon Institute's annual study that tracks consumers' rankings of organizations that collect and manage their personal information, Amazon was the #1 trusted company in terms of data privacy overall. It was followed by: American Express, PayPal, Hewlett Packard and IBM respectively from second to fifth place. It is interesting to note that names like Facebook, Apple and Google among others did not rank in the top five of this study, given the current scrutiny vis-à-vis their links with government agencies.

US - what is more important: data privacy or national security?

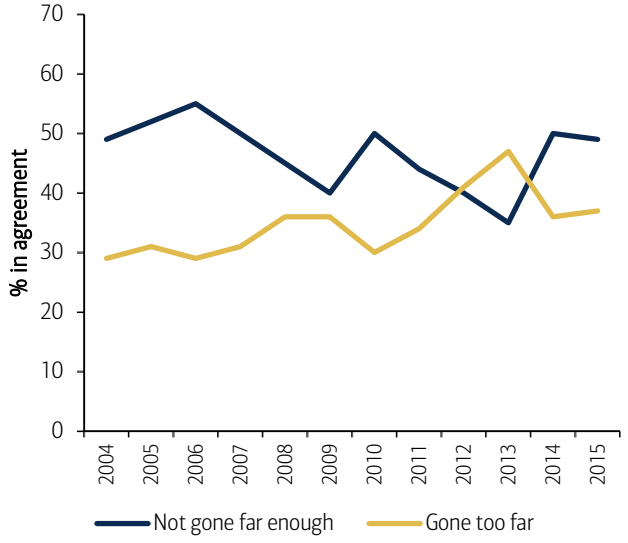
The case studies of WikiLeaks and Edward Snowden have brought to the forefront the extent with which Western national governments were willing to spy on their citizens. In a recent Pew Research survey, it showed 54% of Americans disapproved of the US government's collection of data as part of anti-terrorism efforts. However that said, while many have concerns about government surveillance, Americans also say anti-terrorism policies have not gone far enough to adequately protect them. In 2015, 49% say the latter is their bigger concern than the restriction in civil liberties (37%). Furthermore this preference for national security has pretty much held constant in the decade, with only the Snowden leaks in 2013 reversing this view briefly.

Chart 136: Americans' views of NSA surveillance



Source: Pew research

Chart 137: Concern over countries protection over Civil Liberties



Source: Pew research

Overall, there is growing traction in US Congress to pass legislation permitting sharing of cyber threat information between companies and the government, especially after the OPM cyber attack in early 2015. For instance, in April 2015, Congress passed the Protecting Cyber Networks Act (PCNA). Sponsored by the House Intelligence Committee, the legislation aims to defend against cyber-attacks through the creation of a framework for the voluntary sharing of cyber threat information between private entities and the federal government, and it includes liability protection for those companies that choose to participate (source: US Congress, ISACA)

EU - data protection is stricter

Whilst America takes a more ad-hoc approach to data protection, often relying on a combination of public regulation, private self-regulation, and legislation; the EU in contrast has a more stringent approach. Data protection in the EU stems largely from a bill passed in 1995, dubbed the "Data Protection Directive" This law, reaffirming European nations' respect for all citizens' "private and family life," places far more power in the hands of the individual. By granting users the right to both remove and correct any personal information about them online, as well as by barring companies from transferring data either to another company or across national borders, consumers in Europe have broad safeguards to ensure their digital privacy.

Bank of America Merrill Lynch

Skills & talent crisis: closing the gap

A perfect storm is brewing in demand for cybersecurity professionals with challenges including: the changing face of ICT and cybersecurity (rising sophistication of threats, larger ICT footprints, adoption of nextgen cybersecurity technologies), human resources issues (demand outstripping supply, wage strains), and a lack of prioritisation by corporates (business conditions, lack of understanding, spending, training).

The greatest shortages are being experienced by the healthcare, education and retails sectors, while cash-strapped governments are finding it hard to keep up with the private sector. By 2020E, it is estimated that the shortfall in the global information security workforce will reach 1.5mn (source: Frost & Sullivan).

Training on cybersecurity remains a weak link with only 51% of companies having employee cybersecurity awareness training programmes in place, and only 57% requiring staff to complete training on privacy policies (source: PwC). This is extremely worrying given that it is thought that more than a decade of cybersecurity research experience is needed to acquire the skills to defend against modern-day attacks (source: Websense). Cloud computing and BYOD are two of the priority areas for training going forward (source: Frost & Sullivan).

Chart 138:Impact of cybersecurity workforce shortages: very great & great impacts

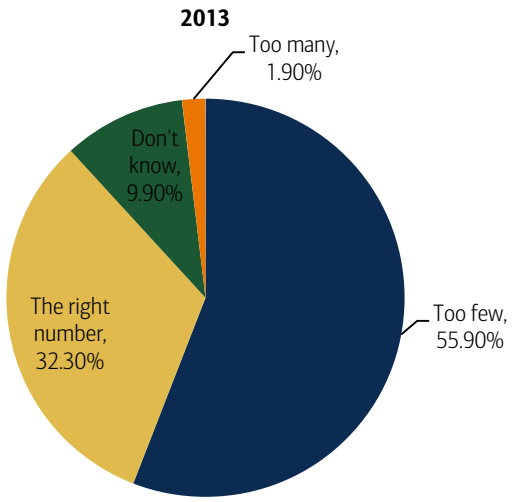
Source: Frost & Sullivan, BofA Merrill Lynch Global Research

Not enough cyber pros: 1.5mn person gap by 2020E

According to Frost & Sullivan's 2015 Global Information Security Workforce Study, 62% of 14,000 survey respondents globally stated that their organisations have too few information security professionals (vs. 56% in the 2013 survey).

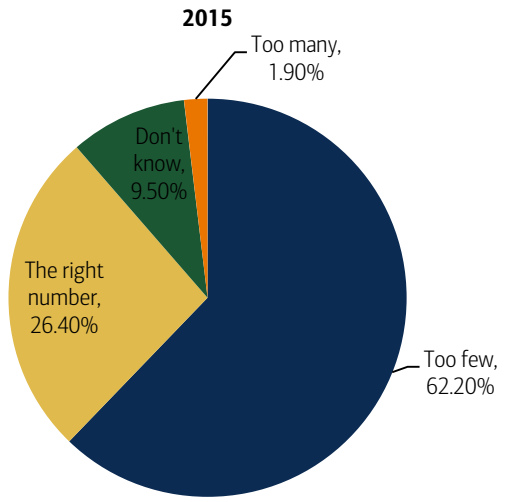
A huge 62% of 14,000 survey respondents said that their organisations have too few information security professionals, up from 56% in 2013. By 2020E, it is estimated that the shortfall in the global information security workforce will reach 1.5mn (source: Frost & Sullivan).

Chart 139: Does your organization have the right number of cybersecurity professionals? (% of survey respondents) - 2013



Source: Frost & Sullivan

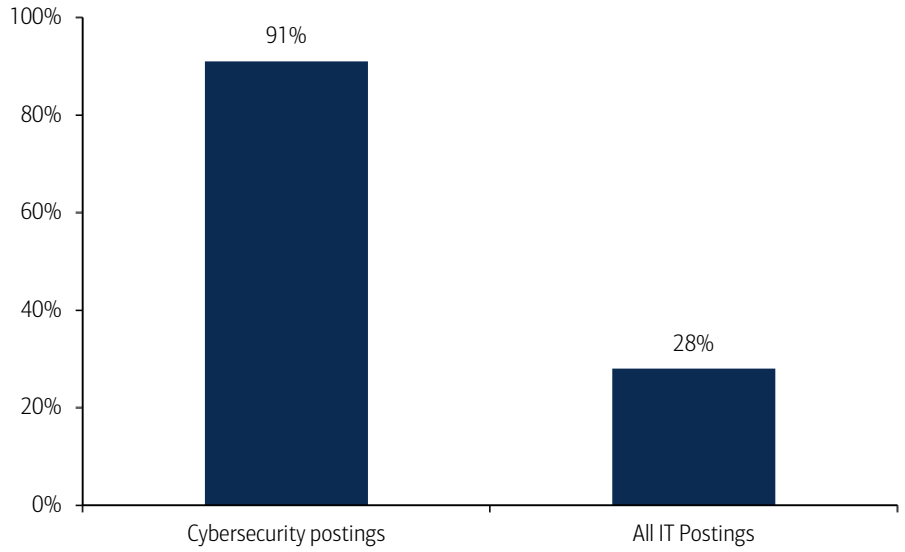
Chart 140: Does your organization have the right number of cybersecurity professionals? (% of survey respondents) - 2015



Source: Frost & Sullivan

We are seeing multiple signs that demand is outstripping supply, including that postings for cybersecurity jobs have grown three times as fast as openings for IT jobs overall (source: burningglass).

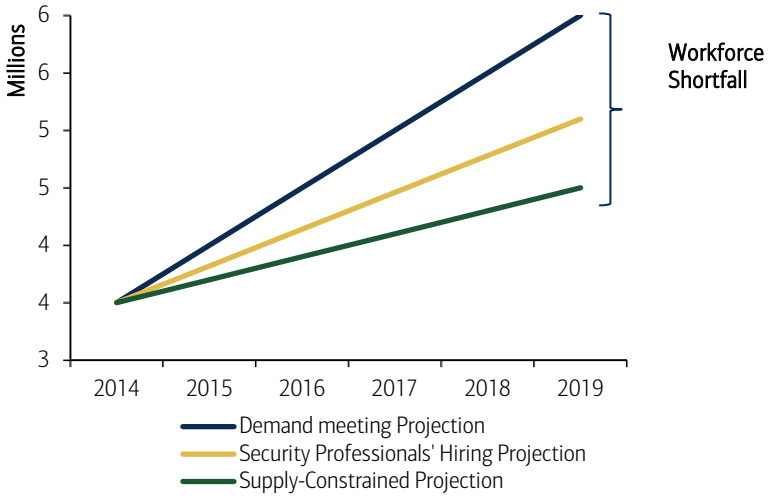
Chart 141: Growth in job postings (2010-2014)



Source: burning glass

By 2020E, it is estimated that the shortfall in the global information security workforce will reach 1.5mn (source: Frost & Sullivan).

Chart 142: Projected Information Security Workers Globally

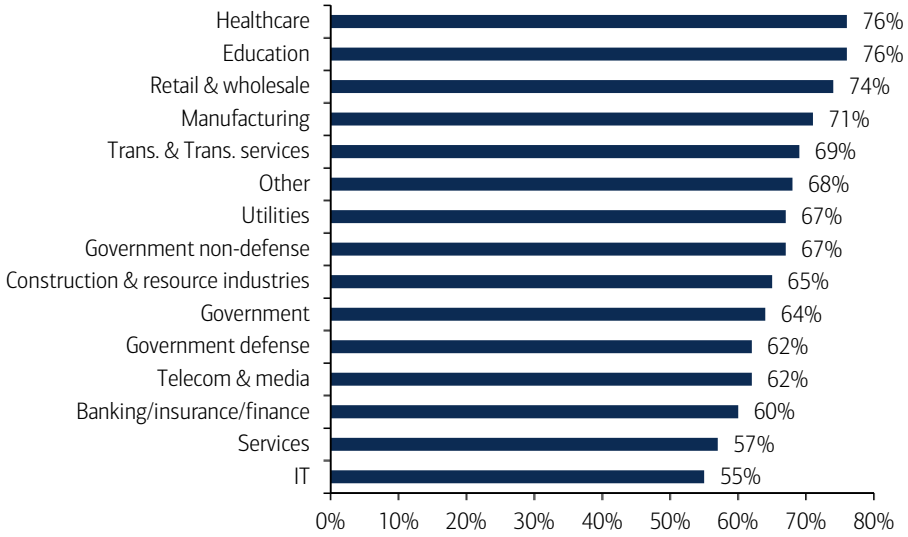


Source: Frost & Sullivan

Healthcare, education & retail being hit hardest

The greatest reported shortages of cybersecurity professionals are in the healthcare, education and retail sectors. While IT had the lowest percentage of respondents, it is interesting that more than 50% of IT sector cybersecurity professionals report that their organisations have too few people in the space (source: Frost & Sullivan).

Chart 143: Too few cybersecurity workers by sector (% of survey respondents)

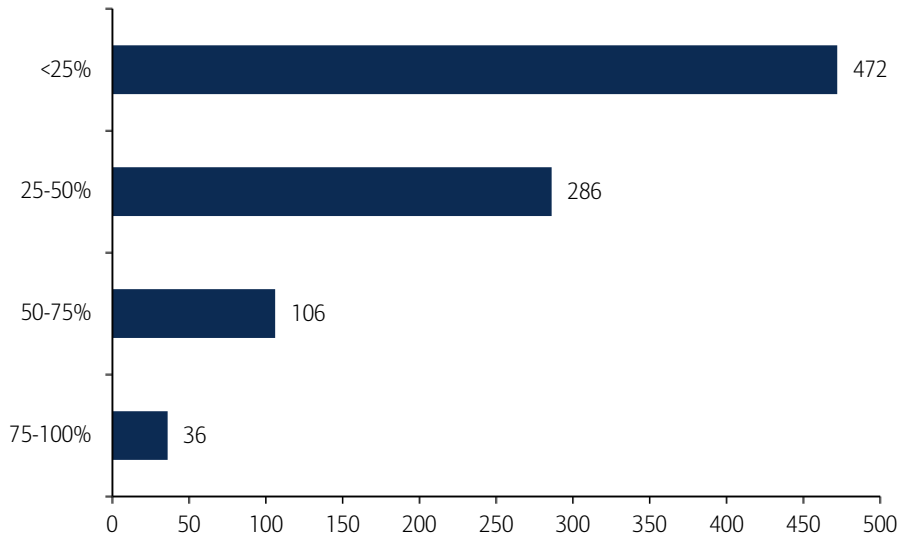


Source: Frost & Sullivan

Insufficient pool of suitable candidates

An insufficient pool of suitable candidates is causing the cyber talent shortfall. The ISACA-RSA State of Cybersecurity 2015 survey found that over 50% of respondents reported that fewer than 25% of applicants are truly qualified for open positions. The largest gaps were thought to exist in the ability to understand the business, followed by technical skills and communication.

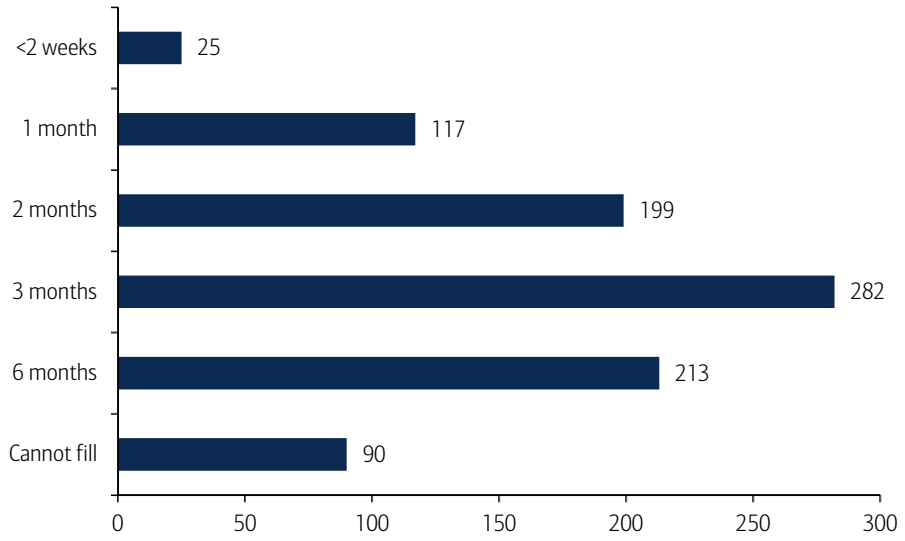
Chart 144: On average, how many cybersecurity applicants are qualified?



Source: ISACA-RSA

The same survey found that it takes 53% of organisations between three and six months to fill a position, while 10% cannot fill them at all (source: ISACA-RSA).

Chart 145: Time taken to hire a skilled cybersecurity professional (% of survey respondents)



Source: ISACA-RSA

Rising retention difficulties: 20% turnover

In 2014, nearly one in five cybersecurity professionals changed employers or employment status – marking the highest level in the past five years. 14% changed employers while still employed, with the rising churn additional proof of the scarcity of cybersecurity professionals (source: Frost & Sullivan).

It's not about the money (this time)

The reasons for the hiring shortfall are not about money as more organisations are making the budget available to hire more personnel and the shortage means that pressure on price (salaries) is increasing. Cybersecurity workers can command an average salary premium of US$9,000, or 9% more than other IT workers (source: burningglass).

Hiring will not stop: 195,000 to be hired in 2015

This projected workforce shortfall does not mean cyber hiring will stop. Frost & Sullivan predicts a global increase of 195,000 cyber security professionals in the next year: a rise of nearly 6% over 2014.

> "There is going to be a Black Friday–like buying frenzy for cybersecurity talent throughout 2015 … Some organizations will be left high and dry." - Jon Oltsik

Training is the weak link

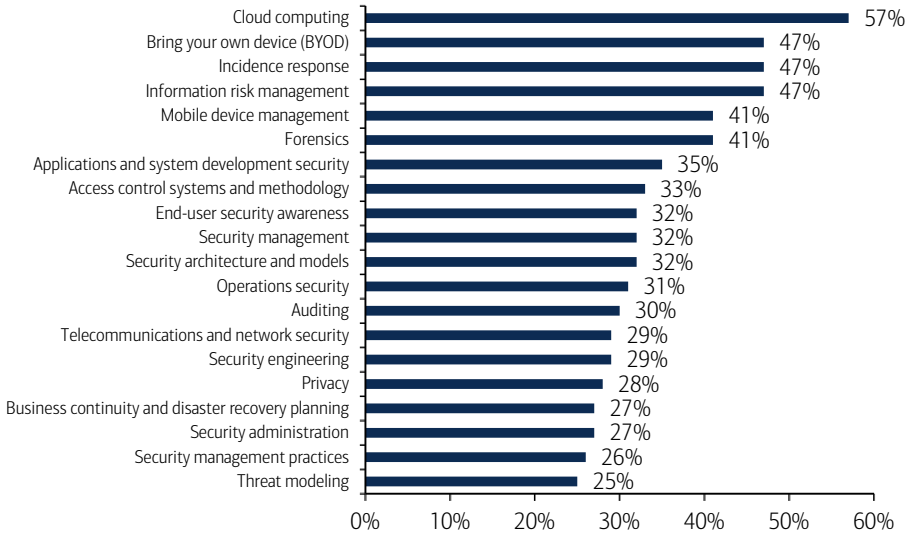
Employee training and awareness should be a key component of company HR given that the weakest link in the cybersecurity chain is often human. While 90% of companies have regular security training in place for security employees (source: Cisco), we are not seeing similar success across organisations. According to PwC's Global State of Information Security Survey 2015, only 51% of surveyed companies have employee security awareness training programmes in place. A slightly higher number, 57%, say they require employees to complete training on privacy policies.

> "It takes 11 years alone of security research experience to acquire the skills needed to defend against modern day attacks" - Websense

Top areas for training: cloud and BYOD

31% of organisations plan to increase cybersecurity training budgets, with the top areas for training and development for cybersecurity professionals over the next three years being dominated by technologies requiring protection such as cloud computing and bring-your-own-device (BYOD). Other priority areas include information risk management, applications and systems development, and access control (source: Frost & Sullivan).

Chart 146: Areas seeing growing 3Y demand for cyber training (% of survey respondents)



Source: Frost & Sullivan

Governments: falling behind the private sector in the race

Governments are also facing a cybersecurity skills and talent gap as they struggle to deal with intrusions into their own systems and attacks against critical infrastructure, and protect ICT networks.

> "The cyber world is the wild, wild west and to some degree [the federal government] is asked to be the sheriff." – U.S. President Obama

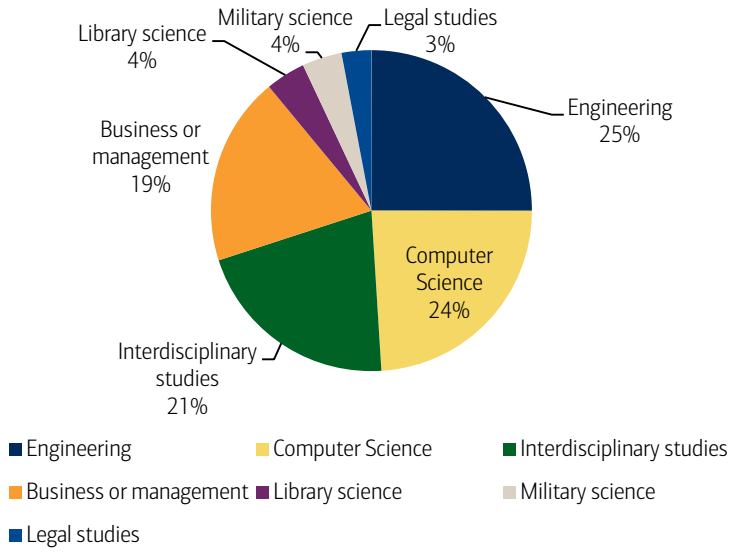
Booz Allen Hamilton, a major government contractor, argues that the US federal government has fallen behind in the race for highly qualified cybersecurity talent and that, without the skilled workforce in place to protect the integrity of systems, the nation will be highly vulnerable:

- **The government lacks a master cyber workforce strategy** to attract and retain top talent.
- **The federal government struggles to compete for skilled cyber workers** who are in high demand.
- **Government loses top candidates** to a slow and ineffective hiring process.
- **Agency cyber training and development Is uneven**.
- **Government compensation isn't competitive**, especially for experienced talent

Education sector has a key role to play

The higher education sector has a key role to play in tackling the skills and talent gap, including teaching cybersecurity as part of all of computing degrees, at a minimum. Cybersecurity as a dedicated academic subject in higher education is still a nascent concept, with the issue spanning many disciplines. Engineering (25%) is the #1 academic department where cyber is likely to be situated at a university followed by Computer Science (24%) and Interdisciplinary (21%) (source: Ponemon Institute).

Chart 147: Academic department where cybersecurity is most likely situated



Source: Ponemon Institute

Bank of America Merrill Lynch

Top US post-secondary schools for cybersecurity

The leading US institution for an education in cybersecurity is the University of Texas, San Antonio, according to a study by Ponemon Institute.

Table 51: Data used for meta ranking for top rated educational institutions

Institutes	# of ratings	# of 1st choice ratings	Average survey score
University of Texas, San Antonio	98	90	9.4
Norwich University	69	63	9.2
Mississippi State University	78	67	9
Syracuse University	78	70	8.8
Carnegie Mellon University	80	69	8.8
Purdue University	63	44	9
University of Southern California	116	57	8.8
University of Pittsburgh	71	66	8.6
George Mason University	91	75	8.6
West Chester University of Pennsylvania	57	45	8.6
U.S. Military Academy, West Point	21	13	9
University of Washington	81	40	8.4

Source: Ponemon Institute

Appendix – Cybersecurity Glossary

Table 52: Cybersecurity glossary of commonly used terms

Term	Definition
Acceptable interruption window	The maximum period of time that a system can be unavailable before compromising the achievement of the enterprise's business objectives
Access control list (ACL)	An internal computerized table of access rules regarding the levels of computer access permitted to logon IDs and computer terminals
Advanced Encryption Standard (AES)	A public algorithm that supports keys from 128 bits to 256 bits in size
Advanced persistent threats (APTs)	A targeted cyberespionage or cybersabotage attack that is usually sponsored by a nation state with the goal of stealing information from an organization. The motivation behind an advanced persistent threat is to gain information for military, political, or economic advantage.
Adware	A software package that automatically plays, displays or downloads advertising material to a computer after the software is installed on it or while the application is being used
Analog	A transmission signal that varies continuously in amplitude and time and is generated in wave formation
Android (droid)	Google's brand name for its Linux-based operating system for mobile devices (smartphones and tablets).
Anti-malware	A technology widely used to prevent, detect and remove many categories of malware, including computer viruses, worms, Trojans, keyloggers, malicious browser plug-ins, adware and spyware
Antispam	A type of application that defends against the threats that spam poses (such as viruses, phishing attempts, and denial-of-service attacks) and reduces the amount of spam entering an email system.
Antivirus software	An application software deployed at multiple points in an IT architecture. It is designed to detect and potentially eliminate virus code before damage is done and repair or quarantine files that have already been infected
Architecture	Description of the fundamental underlying design of the components of the business system, or of one element of the business system (e.g., technology), the relationships among them, and the manner in which they support enterprise objectives
Asymmetric key (public key)	A cipher technique in which different cryptographic keys are used to encrypt and decrypt a message
ATM skimming	A type of fraud or theft that occurs when an ATM is compromised with a skimming device. A card reader that can be disguised to look like a part of the machine. The card reader collects victims' account information and personal identification numbers (PIN).
Attack mechanism	A method used to deliver the exploit. Unless the attacker is personally performing the attack, an attack mechanism may involve a payload, or container, that delivers the exploit to the target.
Attack vector	A path or route used by the adversary to gain access to the target (asset)
Attacks	Security events that have been identified by correlation and analytics tools as malicious activity attempting to collect, disrupt, deny, degrade, or destroy information system resources or the information itself. Security events such as SQL Injection, URL tampering, denial of service, and spear phishing fall into this category.
Attenuation	Reduction of signal strength during transmission
Audit trail	A visible trail of evidence enabling one to trace information contained in statements or reports back to the original input source
Authentication	1. The act of verifying identity (i.e., user, system) 2. The act of verifying the identity of a user and the user's eligibility to access computerized information
Backdoor	Computer programmers often build backdoors into software applications so they can fix bugs. If hackers or others learn about a backdoor, the feature may pose a security risk. It can also be referred to as a trap door.
Backup	A backup is a duplicate copy of data made for archiving purposes or for protection against damage and loss. A backup is usually kept physically separate from the originals for recovery when originals are damaged or lost.
Bandwidth	The range between the highest and lowest transmittable frequencies. It equates to the transmission capacity f an electronic line and is expressed in bytes per second or Hertz (cycles per second).
Bastion	System heavily fortified against attacks
Biometrics	A security technique that verifies an individual's identity by analyzing a unique physical attribute, such as a handprint
Black hat hackers	Hackers who gain unauthorized access into a computer system or network with malicious intent. They may use computers to attack systems for profit, for fun, for political motivations, or as part of a social cause. Such penetration often involves modification and/or destruction of data, as well as distribution of computer viruses, Internet worms, and delivery of spam through the use of botnets.
Blacklist	A list of known sources of unwanted email used for filtering spam. A blacklist can also be a list of websites that are considered to be dangerous because they exploit browser vulnerabilities or send spyware and other unwanted software to users.
Blended threat	A general description for malicious programs that combine elements of multiple types of malware: viruses, worms, Trojans, etc.
Block cipher	A public algorithm that operates on plaintext in blocks (strings or groups) of bits
Bluetooth	A wireless technology commonly used to wirelessly link phones, computers, and other network devices over short distances. It can also be used to exchange data over short distances.
Bot	Short for "robot," a computer that has been infected with malicious software without the user's knowledge. Once the computer has been affected, a cybercriminal can send commands to it and other infected machines over the Internet. Since the compromised computers blindly follow the commands of the cybercriminals, infected machines are also called zombies.
Botnet (bot network)	Short for "robot network," a botnet is a network of hijacked computers controlled remotely by a hacker. The hacker can use the network to send spam and launch Denial of Service (DoS) attacks, and may rent the network to other cybercriminals. A single computer in a botnet can automatically send thousands of spam messages per day. The most common spam messages come from zombie computers.
Boundary	Logical and physical controls to define a perimeter between the organization and the outside world
Breach or compromise	An incident that has successfully defeated security measures and accomplished its designated task.
Bridge	Data link layer device developed in the early 1980s to connect local area networks (LANs) or create two separate LAN or wide area network (WAN) network segments from a single segment to reduce collision domains
Bring your own device (BYOD)	An enterprise policy used to permit partial or full integration of user-owned mobile devices for business purposes
Browser hijacker	A type of malware that alters your computer's browser settings so that you are redirected to websites that you had no intention of visiting. Most browser hijackers alter browser home pages, search pages, search results, error message pages, or other browser content with unexpected or unwanted content.
Brute force attack	Repeatedly trying all possible combinations of passwords or encryption keys until the correct one is found
Buffer overflow	Occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold
Bug	An unintentional fault, error, failure, or mistake in a software program that can produce an incorrect or unexpected result or cause a program to behave in unintended ways.
Business impact analysis/assessment (BIA)	Evaluating the criticality and sensitivity of information assets. An exercise that determines the impact of losing the support of any resource to an enterprise, establishes the escalation of that loss over time, identifies the minimum resources needed to recover, and prioritizes the recovery of processes and the supporting system
Cache	Pronounced like "cash," a cache stores recently used information in a place where it can be accessed extremely fast. Computers have a disk cache; this stores information that the user has recently read from the hard disk. Web browsers also use a cache to store the pages, images, and URLs of recently visited websites on the user's hard drive. When users visit web pages that they have been to recently, the pages and images don't have to be downloaded again.
Caller ID spoofing	This is the practice of causing the telephone network to display a false number on the recipient's caller ID. A number of companies provide tools that facilitate caller ID spoofing. Voice over Internet Protocol (VoIP) has known flaws that allow for caller ID spoofing. These tools are typically used to populate the caller ID with a specific bank or credit union, or just with the words "Bank" or "Credit Union."
Carding	A technique used by thieves to verify the validity of stolen card data. The thief will use the card information on a website that has real-time transaction processing. If the transaction is processed successfully then the thief knows the card is still good. The purchase is usually for a small amount to avoid using the card's limit and to avoid attracting the attention of the card owner.

Table 52: Cybersecurity glossary of commonly used terms

Term	Definition
Certificate (Certification) authority (CA)	A trusted third party that serves authentication infrastructures or enterprises and registers entities and issues them certificates
Certificate revocation list (CRL)	An instrument for checking the continued validity of the certificates for which the certification authority (CA) has responsibility
Chain of custody	A legal principle regarding the validity and integrity of evidence. It requires accountability for anything that will be used as evidence in a legal proceeding to ensure that it can be accounted for from the time it was collected until the time it is presented in a court of law.
Checksum	A mathematical value that is assigned to a file and used to "test" the file at a later date to verify that the data contained in the file has not been maliciously changed
Chief Information Security Officer (CISO)	The person in charge of information security within the enterprise
Child identity theft	When a thief steals the identities of children to use for fraudulent financial transactions. It can take years before the theft is discovered, often the victims discover this when they engage in their first financial transactions. The dangers associated with child identity theft include damaged credit and income tax liability.
Cipher	An algorithm to perform encryption
Ciphertext	Information generated by an encryption algorithm to protect the plaintext and that is unintelligible to the unauthorized reader.
Cleartext	Data that is not encrypted. Also known as plaintext
Cloud computing	Convenient, on-demand network access to a shared pool of resources that can be rapidly provisioned and released with minimal management effort or service provider interaction
Collision	The situation that occurs when two or more demands are made simultaneously on equipment that can handle only one at any given instant (Federal Standard 1037C)
Common Attack Pattern Enumeration and Classification (CAPEC)	A catalogue of attack patterns as "an abstraction mechanism for helping describe how an attack against vulnerable systems or networks is executed" published by the MITRE Corporation
Compartmentalization	A process for protecting very-high value assets or in environments where trust is an issue. Access to an asset requires two or more processes, controls or individuals.
Computer emergency response team (CERT)	A group of people integrated at the enterprise with clear lines of reporting and responsibilities for standby support in case of an information systems emergency. This group will act as an efficient corrective control, and should also act as a single point of contact for all incidents and issues related to information systems.
Computer forensics	The application of the scientific method to digital media to establish factual information for judicial review
Consumerization	A new model in which emerging technologies are first embraced by the consumer market and later spread to the business
Contactless payment	A noncash payment transaction that doesn't need a physical connection between the payment device, which can be a number of things ranging from traditional plastic cards to mobile phones, and the physical point-of-sale terminal (for example, a cash register).
Content filtering	Controlling access to a network by analyzing the contents of the incoming and outgoing packets and either letting them pass or denying them based on a list of rules
Cookie	Small amounts of data generated by a website and saved by your web browser. Websites use cookies to identify users who revisit their sites, and are most commonly used to store login information for a specific site. When a server receives a browser request that includes a cookie, the server can use the information stored in the cookie to customize the website for the user. Whenever a user checks the box "Remember me on this computer," the website will generate a login cookie once the user successfully logs in. Each time users revisit the site, they may only need to enter their password or may not need to login at all. Cookies can be used to gather more information about a user than would be possible without them.
Crimeware	Malicious software such as viruses, Trojan horses, spyware, and other programs used to commit crimes on the Internet including identity theft and fraud.
Criminal identity theft	When a criminal fraudulently identifies himself to police as another individual at the point of arrest. In some cases criminals have previously obtained state-issued identity documents using credentials stolen from others, or have simply presented fake identification.
Critical infrastructure	Systems whose incapacity or destruction would have a debilitating effect on the economic security of an enterprise, community or nation.
Criticality	The importance of a particular asset or function to the enterprise, and the impact if that asset or function is not available
Criticality analysis	An analysis to evaluate resources or business functions to identify their importance to the enterprise, and the impact if a function cannot be completed or a resource is not available
Cross-site scripting (XSS)	A type of injection, in which malicious scripts are injected into otherwise benign and trusted web sites
Cryptosystem	A pair of algorithms that take a key and convert plaintext to ciphertext and back
Cyberbullying	Bullying that takes place in cyberspace. This includes the Internet and mobile phone communication. It may involve harassing, threatening, embarrassing, or humiliating someone online.
Cybercop	An investigator of activities related to computer crime
Cyberespionage	Activities conducted in the name of security, business, politics or technology to find information that ought to remain secret. It is not inherently military.
Cybergangs	Cybergangs are groups of hackers, crackers, and other cybercriminals that pool their resources to commit crimes on the Internet. Organized crime is often involved in cybergang activity.
Cybersecurity architecture	Describes the structure, components and topology (connections and layout) of security controls within an enterprise's IT infrastructure
Cybersquatting	Registering, trafficking in, or using a domain name with malicious intent to profit from the goodwill of a trademark or brand name belonging to someone else. The cybersquatter then offers to sell the domain to the person or company who owns a trademark contained within the name at an inflated price. Cybersquatters also sometimes register variations of popular trademarked names as a way of distributing their malware.
Cyberwarfare	Activities supported by military organizations with the purpose to threat the survival and well-being of society/foreign entity
DAT files	Also known as a data file, these files are used to update software programs, sent to users via the Internet. .DAT files contain up-to-date virus signatures and other information antivirus products use to protect your computer against virus attacks. .DAT files are also known as detection definition files and signatures.
Data custodian	The individual(s) and department(s) responsible for the storage and safeguarding of computerized data
Data Encryption Standard (DES)	An algorithm for encoding binary data
Data leakage	Siphoning out or leaking information by dumping computer files or stealing computer reports and tapes
Data owner	The individual(s), normally a manager or director, who has responsibility for the integrity, accurate reporting and use of computerized data
Database	A stored collection of related data needed by enterprises and individuals to meet their information processing and retrieval requirements
Decentralization	The process of distributing computer processing to different locations within an enterprise
Decryption	A technique used to recover the original plaintext from the ciphertext so that it is intelligible to the reader. The decryption is a reverse process of the encryption.
Decryption key	A digital piece of information used to recover plaintext from the corresponding ciphertext by decryption
Defacement	A change made to the home page or other key pages of a website by an unauthorized individual or process, usually unknown to the website owner.
Defense in depth	The practice of layering defenses to provide added protection. Defense in depth increases security by raising the effort needed in an attack. This strategy places multiple barriers between an attacker and an enterprise's computing and information resources.
Demilitarized zone (DMZ)	A screened (firewalled) network segment that acts as a buffer zone between a trusted and untrusted network
Denial of service (DoS)	An attack specifically designed to prevent a system from functioning properly as well as denying access to the system by authorized users. Hackers can cause denial-of-service attacks by destroying or modifying data or by overloading the system's servers until service to authorized users is delayed or prevented.
Denial-of-service attack (DoS)	An assault on a service from a single source that floods it with so many requests that it becomes overwhelmed and is either stopped completely or operates at a significantly reduced rate
Dialers	Dialers include software programs that redirect Internet connections to a party other than the user's default ISP and are designed to run up additional connection charges for a content provider, vendor, or other third party.
Dictionary attack	Method of breaking into a password-protected computer, mobile device, or online account by entering every word in a dictionary as a password.
Digital certificate	A piece of information, a digitized form of signature, that provides sender authenticity, message integrity and non-repudiation. A digital signature is generated using the sender's private key or applying a one-way hash function.

Table 52: Cybersecurity glossary of commonly used terms

Term	Definition
Digital forensics	The process of identifying, preserving, analyzing and presenting digital evidence in a manner that is legally acceptable in any legal proceedings
Digital signature	A piece of information, a digitized form of signature, that provides sender authenticity, message integrity and non-repudiation
Disaster recovery plan (DRP)	A set of human, physical, technical and procedural resources to recover, within a defined time and cost, an activity interrupted by an emergency or disaster
Discretionary access control (DAC)	A means of restricting access to objects based on the identity of subjects and/or groups to which they belong
Distributed denial of service (DDos)	A type of denial-of-service (DoS) attack in which more than one traffic generator directs traffic to a targeted URL. Traffic-generating programs are called agents, and the controlling program is the master. DoS agents receive instruction from a master to carry out an attack, which is designed to disable or shut down the targeted URL.
Domain name	This is a name that identifies a website; for example, mcafee.com is the domain name of McAfee's website. Each domain name is associated with an IP address. Domain names are used in URLs to identify particular web pages.
Domain name system (DNS)	A hierarchical database that is distributed across the Internet that allows names to be resolved into IP addresses (and vice versa) to locate services such as web and e-mail servers
Drive-by download	A program that is automatically downloaded to your computer without your consent or even your knowledge. It can install malware or potentially unwanted programs merely by your viewing an email or website.
Droppers	Malicious software designed to install other malicious software on a target.
Dumpster diving	The practice of sifting through commercial or residential trash in the hopes of finding information to steal or commit fraud.
Dynamic ports	Dynamic and/or private ports--49152 through 65535: Not listed by IANA because of their dynamic nature.
Egress	Network communications going out
Encryption algorithm	A mathematically based function or calculation that encrypts/decrypts data
Encryption key	A piece of information, in a digitized form, used by an encryption algorithm to convert the plaintext to the ciphertext
Ethernet	A popular network protocol and cabling scheme that uses a bus topology and carrier sense multiple access/collision detection (CSMA/CD) to prevent network failures or collisions when two devices try to access the network at the same time
Exploit	Full use of a vulnerability for the benefit of an attacker
False negative	An error that occurs when antivirus software fails to detect that an infected file is truly infected. False negatives are more serious than false positives, although both are undesirable. False negatives are more common with antivirus software because they may miss a new or a heavily modified virus.
False positive	An error that occurs when antivirus software wrongly claims that a virus is infecting a clean file. False positives usually occur when the string chosen for a given virus signature is also present in another program.
File Transfer Protocol (FTP)	A protocol used to transfer files over a Transmission Control Protocol/Internet Protocol (TCP/IP) network (Internet, UNIX, etc.)
Firewall	A system or combination of systems that enforces a boundary between two or more networks, typically forming a barrier between a secure and an open environment such as the Internet
Freeware	Software available free of charge
Gateway	A device (router, firewall) on a network that serves as an entrance to another network
Geolocation	Term used to describe the capability to detect and record where you and other people are located. Geolocation information can be obtained in a number of ways, including using data from a user's IP address, MAC address, RFID, Wi-Fi connection location, or GPS coordinates.
Geotagging	Process of adding geographical identification data to various types of media, such as a photograph or video taken with your camera or mobile device. This data usually consists of latitude and longitude coordinates, and they can also contain altitude, bearing, distance, and place names.
Grey hat hackers	Skilled hackers who sometimes act legally, sometimes in good will and sometimes not. They are a hybrid between white and black hat hackers. They usually do not hack for personal gain or have malicious intentions, but may or may not occasionally commit crimes during the course of their technological exploits.
Hash function	An algorithm that maps or translates one set of bits into another (generally smaller) so that a message yields the same result every time the algorithm is executed using the same message as input
Hashing	Using a hash function (algorithm) to create hash valued or checksums that validate message integrity
Hijacking	An exploitation of a valid network session for unauthorized purposes
Hole	A vulnerability in the design software and/or hardware that allows the circumvention of security measures.
Honeypot	A specially configured server, also known as a decoy server, designed to attract and monitor intruders in a manner such that their actions do not affect production systems
Host	A term often used to describe the computer file to which a virus attaches itself. Most viruses run when the computer or user tries to use the host file.
Hotspot	A hotspot is a site that offers Internet access over a wireless connection. Hotspots typically use Wi-Fi technology and are generally found in coffee shops and various other public locations.
Hub	A common connection point for devices in a network, hubs are used to connect segments of a local area network (LAN)
Human firewall	A person prepared to act as a network layer of defense through education and awareness
Hyperlink (link)	A clickable word, phrase, or image on a website that once clicked takes the user from one web page to another, or to another resource on the Internet. They are typically underlined or set apart by a different color. When you move your cursor over a hyperlink, whether text or image, the arrow should change to a small hand pointing at the link.
Hypertext Transfer Protocol (HTTP)	A communication protocol used to connect to servers on the World Wide Web. Its primary function is to establish a connection with a web server and transmit hypertext markup language (HTML), extensible markup language (XML) or other pages to client browsers
Hypertext Transfer Protocol Secure (HTTPS)	A protocol for accessing a secure web server, whereby all data transferred are encrypted.
Imaging	A process that allows one to obtain a bit-for-bit copy of data to avoid damage of original data or information when multiple analyses may be performed.
Impact analysis	A study to prioritize the criticality of information resources for the enterprise based on costs (or consequences) of adverse events. In an impact analysis, threats to assets are identified and potential business losses determined for different time periods. This assessment is used to justify the extent of safeguards that are required and recovery time frames. This analysis is the basis for establishing the recovery strategy.
In the wild (ITW)	A virus is "in the wild" (ITW) if it is verified as having caused an infection outside a laboratory situation. Most viruses are in the wild and differ only in prevalence.
Inadvertent actor	Any attack or suspicious activity sourcing from an IP address inside a customer network that is allegedly being executed without the knowledge of the user.
Incident response	The response of an enterprise to a disaster or other significant event that may significantly affect the enterprise, its people, or its ability to function productively. An incident response may include evacuation of a facility, initiating a disaster recovery plan (DRP), performing damage assessment, and any other measures necessary to bring an enterprise to a more stable status.
Incident response plan	The operational component of incident management
Information harvesters	People who supply stolen data but do not necessarily use it to commit fraud. The information obtained by harvesters is sold to criminal networks that trade the information in Internet back alleys.
Infrastructure as a Service (IaaS)	Offers the capability to provision processing, storage, networks and other fundamental computing resources, enabling the customer to deploy and run arbitrary software, which can include operating systems (OSs) and applications
Ingestion	A process to convert information extracted to a format that can be understood by investigators
Ingress	Network communications coming in
Inherent risk	The risk level or exposure without taking into account the actions that management has taken or might take (e.g., implementing controls)
Injection	A general term for attack types which consist of injecting code that is then interpreted/executed by the application. (OWASP)
Integrity	The guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity
International Mobile Equipment Identity (IMEI)	A number 15 or 17 digits in length that is unique to each mobile phone and tablet. It is used to identify users on the Global System for Mobile Communications (GSM) and the Universal Mobile Telecommunications System (UMTS). It is usually found printed inside the battery compartment of the phone. If a mobile phone is lost or stolen, the owner can call the network provider and instruct them to blacklist the phone based on the IMEI number and make it useless on the network.

Table 52: Cybersecurity glossary of commonly used terms

Term	Definition
International Mobile Subscriber Identity (IMSI)	A unique identification associated with all Global System for Mobile Communications (GSM) and Universal Mobile Telecommunications System (UMTS) network mobile phone users. The IMSI is a unique number identifying a GSM subscriber stored inside the subscriber identity module (SIM).
International Standards Organization (ISO)	The world's world s largest developer of voluntary International Standards
Internet Assigned Numbers Authority (IANA)	Responsible for the global coordination of the DNS root, IP addressing, and other Internet protocol resources
Internet Control Message Protocol (ICMP)	A set of protocols that allow systems to about communicate information the state of services on other systems
Internet protocol (IP)	Specifies the format of packets and the addressing scheme
Internet Protocol (IP) address	An IP address is a unique numerical label assigned to a device, such as a computer or other device on a network, including the Internet. IP addresses allow computers, routers, printers, and other devices to identify one another to communicate.
Internet Protocol (IP) packet spoofing	An attack using packets with the spoofed source Internet packet (IP) addresses
Internet service provider (ISP)	A third party that provides individuals and enterprises with access to the Internet and a variety of other Internet-related services
Intrusion detection system (IDS)	Inspects network and host security activity to identify suspicious patterns that may indicate a network or system attack
Intrusion prevention system (IPS)	A system designed to not only detect attacks, but also to prevent the intended victim hosts from being affected by the attacks
IOS	Apple's brand name for its mobile operating system.
IP Security (IPSec)	A set of protocols developed by the Internet Engineering Task Force (IETF) to support the secure exchange of packets
IT governance	The responsibility of executives and the board of directors; consists of the leadership, organizational structures and processes that ensure that the enterprise's IT sustains and extends the enterprise's strategies and objectives
Jailbreaking	Process of removing limitations imposed by Apple on devices running the iOS operating system (iPhone, iPad, and iPod). Users do this to gain root access to the operating system to be able to install apps obtained through means other than the official App Store. While this can allow the user greater control of what is installed on the device, it can also cause data corruption and make the device less secure.
Kernel mode	Used for execution of privileged instructions for the internal operation of the system. In kernel mode, there are no protections from errors or malicious activity and all parts of the system and memory are accessible.
Key length	The size of the encryption key measured in bits
Key risk indicator (KRI)	A subset of risk indicators that are highly relevant and possess a high probability of predicting or indicating important risk
Keylogger	Software used to record all keystrokes on a computer
Keylogger (keystroke logging)	Software that tracks or logs the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that their actions are being monitored. This is usually done with malicious intent to collect information including instant messages, email text, email addresses, passwords, credit card and account numbers, addresses, and other private data.
Latency	The time it takes a system and network delay to respond
Legacy system	Outdated computer systems
Local area network (LAN)	Communication network that serves several users within a specified geographic area
Location-based services (LBS)	A service accessible by mobile devices that uses information on the geographical position of the mobile device. Applications like this can help locate the nearest coffee shop or ATM, receive a warning about a nearby traffic jam, or see an ad for a local sale or promotion.
Log	To record details of information or events in an organized record-keeping system, usually sequenced in the order in which they occurred
Logical access	Ability to interact with computer resources granted using identification, authentication and authorization
Logical access controls	The policies, procedures, organizational structure and electronic access controls designed to restrict access to computer software and data files
MAC header	Represents the hardware address of an network interface controller (NIC) inside a data packet
Mail bomb	An excessively large email (typically many thousands of messages) or one large message sent to a user's email account. This is done to crash the system and prevent genuine messages from being received.
Mail relay server	An electronic mail (e-mail) server that relays messages so that neither the sender nor the recipient is a local user
Mainframe	A large high-speed computer, especially one supporting numerous workstations or peripherals
Malicious app	A mobile application (app) disguised as a legitimate app that can contain viruses, worms, Trojan horses, malware, spyware, or any other items that may harm user devices or personal data. Once a malicious app is downloaded, it can wreak havoc in multiple ways including sending text messages to premium-rate numbers, taking control of the infected device, and downloading the user's contact lists. Cybercriminals distribute malicious apps through legitimate app stores like Google Play by masquerading as a legitimate app.
Malicious code	A term used to describe software created for malicious use. It is usually designed to disrupt systems, gain unauthorized access, or gather information about the system or user being attacked. Third party software, Trojan software, keyloggers, and droppers can fall into this category.
Malvertising	This is usually executed by hiding malicious code within relatively safe-looking online advertisements. These ads can lead a victim to unreliable content or directly infect a victim's computer with malware, which may damage a system, access sensitive information, or even control the computer through remote access.
Malware	Short for malicious software. Designed to infiltrate, damage or obtain information from a computer system without the owner's consent
Mandatory access control (MAC)	A means of degrees of requirements for restricting access to data based on varying security information contained in the objects and the corresponding security clearance of users or programs acting on their behalf
Man-in-the-middle attack	An attack strategy in which the attacker intercepts the communication stream between two parts of the victim system and then replaces the traffic between the two components with the intruder's own, eventually assuming control of the communication
Masking	A computerized technique of blocking out the display of sensitive information, such as passwords, on a computer terminal or report
Media access control (MAC) address	A unique identifier assigned to network interfaces for communications on the physical network segment
Medical identity theft	This occurs when someone uses a person's name and sometimes other parts of their identity—such as insurance information—without the person's knowledge or consent to receive benefits such as treatments, prescriptions, or other medical services in another person's name. The dangers of medical identity theft include being denied health coverage, or being given the wrong treatment. (The doctor could be given the wrong medical history, such as a different blood type.)
Message authentication code	An American National Standards that is Institute (ANSI) standard checksum computed using Data Encryption Standard (DES)
Message digest	A smaller extrapolated version of the original message created using a message digest algorithm
Message digest algorithm	Message digest algorithms are SHA1, MD2, MD4 and MD5. These algorithms are one-way functions unlike private and public key encryption algorithms
Metropolitan area network (MAN)	A data network intended to serve an area the size of a large city
Miniature fragment	Using this method, an attacker fragments the IP packet into smaller ones and pushes it through the firewall, in the hope that only the first of the sequence of fragmented packets would be

Table 52: Cybersecurity glossary of commonly used terms

Term	Definition
attack	examined and the others would pass without review.
Mirrored site	An alternate site that contains the same information as the original
Mobile malware	Software with a malicious purpose that commonly performs actions without a user's knowledge. It may be designed to disable your phone, remotely control your device, send unsolicited messages to the user's contact list, make charges to the user's phone bill, or steal valuable information. Mobile malware uses the same techniques as PC malware to infect mobile devices.
Mobile payment	An alternative payment where a consumer can use their mobile phone to make a payment, instead of using cash or credit cards. This is sometimes referred to as a mobile wallet.
Mobile phone spam	Also known as SMS spam, text spam, or mobile spamming. Mobile phone spam is unsolicited and generally unwanted commercial advertisements that are sent to a user's mobile phone by way of text messaging.
Mobile site	The use of a mobile/temporary facility to serve as a business resumption location. The facility can usually be delivered to any site and can house information technology and staff.
Monitoring policy	Rules outlining or delineating the way in which information about the use of computers, networks, applications and information is captured and interpreted
Multifactor authentication	A combination of more than one authentication method, such as token and password (or personal identification number [PIN] or token and biometric device).
Multimedia messaging service (MMS)	A standard way to send messages that includes multimedia content to and from mobile phones. The most popular use is to send photos, but it can also be used for delivering videos, text pages, and ringtones.
Near-field communications (NFC)	A set of standards for smartphones and similar devices to establish radio communication with each other by touching them together or bringing them into close proximity, usually no more than a few inches or centimeters. This technology is currently being used for contactless payment transactions and data exchange.
Network	A network can consist of two or more computers, mobile devices (phones and tablets), gaming devices, Internet connected TVs, etc. connected to each other. Networks can be connected by cables or wirelessly. The purpose of a network is to share files and information.
Network basic input/output system (NetBIOS)	A program that allows applications on different computers to communicate within a local area network (LAN).
Network interface card (NIC)	A communication card that when inserted into a computer, allows it to communicate with other computers on a network
Nonintrusive monitoring	The use of transported probes or traces to assemble information, track traffic and identify vulnerabilities
Normalization	The elimination of redundant data
Obfuscation	The deliberate act of creating source or machine code that is difficult for humans to understand
Open Web Application securityproject (OWASP)	An open community dedicated to enabling organizations to conceive, develop, acquire, operate, and maintain applications that can be trusted
Operating system (OS)	A master control program that runs the computer and acts as a scheduler and traffic controller
Outcome measure	Represents the consequences of actions previously taken; often referred to as a lag indicator
Outsiders	Any attacks sourced from an IP address external to a customer's network.
Packet	Data unit that is routed from source to destination in a packet-switched network
Packet filtering	Controlling access to a network by analyzing the attributes of the incoming and outgoing packets and either letting them pass, or denying them, based on a list of rules
Packet switching	The process of transmitting messages in convenient pieces that can be reassembled at the destination
Passive response	A response option in intrusion detection in which the system simply reports and records the problem detected, relying on the user to take subsequent action
Password attack	An attempt to obtain or decrypt a user's password for illegal use. Hackers can use cracking programs, dictionary attacks, and password sniffers in password attacks. Defense against password attacks is rather limited but usually consists of a password policy including a minimum length, unrecognizable words, and frequent changes.
Password cracker	A tool that tests the strength of user passwords by searching for passwords that are easy to guess
Password sniffing	The use of a sniffer (software or a device that monitors a network and makes a copy of data sent over a network) to capture passwords as they cross a network. The network could be a local area network, or the Internet itself.
Password stealer (PWS)	Malware specifically used to transmit personal information, such as usernames and passwords.
Patch	Fixes to software programming errors and vulnerabilities
Patch management	An area of systems management that involves acquiring, testing and installing multiple patches (code changes) to an administered computer system in order to maintain up-to-date software and often to address security risk
Payload	The section of fundamental data in a transmission. In malicious software this refers to the section containing the harmful data/code.
Peer-to-peer (P2P) networking	A distributed system of file sharing in which any computer on the network can see any other computer on the network. Users can access each others' hard drives to download files. This type of file sharing is valuable, but it brings up copyright issues for music, movies, and other shared-media files. Users are also vulnerable to viruses, Trojans, and spyware hiding in files.
Penetration testing	A live test of the effectiveness of security defenses through mimicking the actions of real-life attackers
Personal identification number (PIN)	A type of password (i.e., a secret number assigned to an individual) that, in conjunction with some means of identifying the individual, serves to verify the authenticity of the individual
Personally identifiable information (PII)	Any information that, by itself or when combined with other information, can identify an individual.
Pharming	The process of redirecting traffic to a fake website, often through the use of malware or spyware. A hacker sets up a fraudulent website that looks like a legitimate website in order to capture confidential information from users.
Phishing	This is a type of electronic mail (e-mail) attack that attempts to convince a user that the originator is genuine, but with the intention of obtaining information for use in social engineering
Piggyback	The practice of gaining unauthorized access to a system by exploiting an authorized user's legitimate connection without their explicit permission or knowledge.
Plain old telephone service (POTS)	A wired telecommunications system.
Platform as a Service (PaaS)	Offers the capability to deploy onto the cloud infrastructure customer-created or -acquired applications that are created using programming languages and tools supported by the provider
Port (Port number)	A process or application-specific software element serving as a communication endpoint for the Transport Layer IP protocols (UDP and TCP)
Port scanning	The act of probing a system to identify open ports
Potentially unwanted program (PUP)	Often legitimate software (nonmalware) that may alter the security state or the privacy of the system on which they are installed. This software can, but not necessarily, include spyware, adware, keyloggers, password crackers, hacker tools, and dialer applications and could be downloaded in conjunction with a program that the user wants.
Principle of least privilege/access	Controls used to allow the least privilege access needed to complete a task
Protocol	The rules by which a network operates and controls the flow and priority of transmissions
Proxy server	A server that acts on behalf of a user
Public key encryption	A cryptographic system that uses two keys: one is a public key, which is known to everyone, and the second is a private or secret key, which is only known to the recipient of the message
Public key infrastructure (PKI)	A series of processes and technologies for association of cryptographic keys with the entity to whom those keys were issued
Quick response (QR) code	A two-dimensional code that can be scanned with a QR barcode reader or a camera-enabled smartphone with QR reader software. Once a QR code is scanned, it can direct a user to just about anything: a web page, call a phone number, or an SMS text message. QR codes provide organizations with a quick and easy way to direct their customers to online content. QR codes are often found in magazines, product packaging, on advertisements, online, and in other marketing collateral.

Table 52: Cybersecurity glossary of commonly used terms

Term	Definition
Radio-frequency identification (RFID)	A generic term to describe a system that transmits the identity (in the form of a unique serial number) of an object or person wirelessly using radio waves.
Ransomware	Malicious software created by a hacker to restrict access to the computer system that it infects and demand a ransom paid to the creator of the malicious software for the restriction to be removed. Some forms of ransomware may encrypt files on the system's hard drive, while others may simply lock the system and display messages to coax the user into paying.
Reciprocal agreement	Emergency processing agreement between two or more enterprises with similar equipment or applications
Recovery	The phase in the incident response plan that ensures that affected systems or services are restored to a condition specified in the service delivery objectives (SDOs) or business continuity plan (BCP)
Recovery time objective (RTO)	The amount of time allowed for the recovery of a business function or resource after a disaster occurs
Redundant site	A recovery strategy involving the duplication of key IT components, including data or other key business processes, whereby fast recovery can take place
Registered ports	Registered ports--1024 through 49151: Listed by the IANA and on most systems can be used by ordinary user processes or programs executed by ordinary users
Registration authority (RA)	The individual institution that validates an entity's proof of identity and ownership of a key pair
Remote access service (RAS)	Refers to any combination of hardware and software to enable the remote access to tools or information that typically reside on a network of IT devices
Remote administration tool (RAT)	Software designed to give an administrator remote control of a system. Hackers can install malicious RAT software on a computer without the user's knowledge and take control of it remotely without the user's knowledge. RATs can be installed by opening an infected attachment, clicking links in a popup window, or through any other software that poses as legitimate.
Removable media	Any type of storage device that can be removed from the system while is running
Repeaters	A physical layer device that regenerates and propagates electrical signals between two network segments
Replay	The ability to copy a message or stream of messages between two parties and replay (retransmit) them to one or more of the parties
Replication	The process by which a virus makes copies of itself to carry out subsequent infections. Replication is one of the major criteria separating viruses from other computer programs.
Residual risk	The remaining risk after management has implemented a risk response
Resilience	The ability of a system or network to resist failure or to recover quickly from any disruption, usually with minimal recognizable effect
Return-oriented attacks	An exploit technique in which the attacker uses control of the call stack to indirectly execute cherry-picked machine instructions immediately prior to the return instruction in subroutines within the existing program code
Risk acceptance	If the risk is within the enterprise's risk tolerance or if the cost of otherwise mitigating the risk is higher than the potential loss, the enterprise can assume the risk and absorb any losses
Risk avoidance	The process for systematically avoiding risk, constituting one approach to managing risk
Rogue program	Any program intended to damage programs or data, or to breach a system's security. It includes Trojan horse programs, logic bombs, and viruses.
Root cause analysis	A process of diagnosis to establish the origins of events, which can be used for learning from consequences, typically from errors and problems
Rooting	A way that users of mobile devices (mobile phones, tablet PCs, and other devices running the Android operating system) hack their devices to gain privileged access to the operating system. This gives the user the ability to alter or replace system applications and settings, run apps that require administrator permissions, or perform operations that otherwise would have not been possible.
Rootkit	A software suite designed to aid an intruder in gaining unauthorized administrative access to a computer system
Rootkits	A stealthy type of malware that is designed to hide the existence of certain processes or programs from normal methods of detection and enable continued privileged access to a computer. Rootkits are the hardest type of invasive software to detect and nearly impossible to remove. As alluded to in the name, they dig into the root of a hard drive. They are designed to steal passwords and identifying information.
Router	A networking device that can send (route) data packets from one local area network (LAN) or wide area network (WAN) to another, based on addressing at the network layer (Layer 3) in the open systems interconnection (OSI) model
RSA	A public key cryptosystem developed by R. Rivest, A. Shamir and L. Adleman used for both encryption and digital signatures
Scareware	A common trick cybercriminals use to make users think that their computer has become infected with malware to get them to purchase a fake application. Often the fake application that the user is tricked into purchasing is actually a malicious program which can disable real antivirus software and wreak havoc on a user's machine.
Secure Electronic Transaction (SET)	A standard that will ensure that credit card and associated payment order information travels safely and securely between the various involved parties on the Internet.
Secure Multipurpose Internet Mail Extensions (S/MIME)	Provides cryptographic security services for electronic messaging applications: authentication, message integrity and non-repudiation of origin (using digital signatures) and privacy and data security (using encryption) to provide a consistent way to send and receive MIME data.
Secure Shell (SSH)	Network protocol that uses cryptography to secure communication, remote command line login and remote command execution between two networked computers
Secure Sockets Layer (SSL)	A protocol that is used to transmit private documents through the Internet
Security as a Service (SecaaS)	The next generation of managed security services dedicated to the delivery, over the Internet, of specialized information-security services.
Security event	An event on a system or network detected by a security device or application.
Security metrics	A standard of measurement used in management of security-related activities
Security perimeter	The boundary that defines the area of security concern and security policy coverage
Security device	Any device or software designed specifically to detect and/or protect a host or network from malicious activity. Such network-based devices are often referred to as intrusion detection and/or prevention systems (IDS, IPS or IDPS), while the host-based versions are often referred to as host-based intrusion detection and/or prevention systems (HIDS or HIPS).
Segregation/separation of duties (SoD)	A basic internal control that prevents or detects errors and irregularities by assigning to separate individuals the responsibility for initiating and recording transactions and for the custody of assets
Service delivery objective (SDO)	Directly related to the business needs, SDO is the level of services to be reached during the alternate process mode until the normal situation is restored
Service level agreement (SLA)	An agreement, preferably documented, between a service provider and the customer(s)/user(s) that defines minimum performance targets for a service and how they will be measured
Shareware	Software provided to users without payment on a trial basis and is usually offered with limited features. Shareware requires payment to the author for full rights. If, after trying the software, you do not intend to use it, you simply delete it. Using unregistered shareware beyond the evaluation period is pirating. Also known as trialware or demoware.
Short code	Telephone numbers shorter than full telephone numbers that can be used only for messaging on mobile phones. They are designed to be easier to read and remember. Short codes are widely used for value-added services such as television program voting, ordering ringtones, charity donations, and mobile services. Messages sent to a short code can be billed at a higher rate than a standard text message and may even subscribe a customer to a recurring monthly service that will be added to the their mobile phone bill until the user texts the word "STOP"(for example) to terminate the service.
Short message service (SMS)	A form of text messaging on mobile phones.
Shoulder surfing	The use of direct observation techniques, such as looking over someone's shoulder, to get information. A criminal can get access to your personal identification number (PIN) or password by watching over your shoulder as you use an automated teller machine (ATM) or type on your computer.
Signature files	Data files containing detection and/or remediation code that antivirus or antispyware products use to identify malicious code.

Table 52: Cybersecurity glossary of commonly used terms

Term	Definition
SIM (subscriber identity module) card	A small electronic card, approximately the size of a postage stamp, that is placed underneath a mobile phone's battery. The SIM card stores data such as user identity, location phone number, network authorization data, personal security keys, contact lists, and stored text messages.
Simple Mail Transfer Protocol (SMTP)	The standard electronic mail (e-mail) protocol on the Internet
Single factor authentication (SFA)	Authentication process that requires only the user ID and password to grant access
Smart card	A small electronic device that contains electronic memory, and possibly an embedded integrated circuit
SMiShing	The act of using social engineering techniques similar to phishing but via text messaging. The name is derived from "SMS (Short Message Service) phishing." SMS is the technology used for text messages on mobile phones. SMiShing uses text messages to try and get you to divulge your personal information. The text message may link to a website or a phone number that connects to automated voice response system.
Sniffer	Software or device that monitors network traffic. Hackers use sniffers to capture data transmitted over a network.
Social engineering	An attack based on deceiving users or administrators at the target site into revealing confidential or sensitive information
Software as a service (SaaS)	Offers the capability to use the provider's applications running on cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., webbased e-mail).
Source routing specification	A transmission technique where the sender of a packet can specify the route that packet should follow through the network
Spam	Computer-generated messages sent as unsolicited advertising
Spear phishing	An attack where social engineering techniques are used to masquerade as a trusted party to obtain important information such as passwords from the victim
Spim	A type of spam specific to instant messaging. The messages can be simple unsolicited ads or fraudulent phishing mail.
Splog	A combination of the words spam and blog that has been created for the purpose of distributing spam. Splogs contain fake articles created for search engine spamming. Splogs are created to attract people to spam sites, primarily via search engines.
Spoofed website	A website that mimics a real company's site—mainly financial services sites—in order to steal private information (passwords, account numbers) from people tricked into visiting it. Phishing emails contain links to the counterfeit site, which looks exactly like the real company's site, down to the logo, graphics, and detailed information.
Spoofing	Faking the sending address of a transmission in order to gain illegal entry into a secure system
Spyware	Software whose purpose is to monitor a computer user's actions (e.g., web sites visited) and report these actions to a third party, without the informed consent of that machine's owner or legitimate user
SQL injection	Results from failure of the application to appropriately validate input. When specially crafted user-controlled input consisting of SQL syntax is used without proper validation as part of SQL queries, it is possible to glean information from the database in ways not envisaged during application design.
Stateful inspection	A firewall architecture that tracks each connection traversing all interfaces of the firewall and makes sure they are valid.
Statutory requirements	Laws created by government institutions
Supervisory control and data acquisition (SCADA)	Systems used to control and monitor industrial and manufacturing processes, and utility facilities
Suspicious activity	These are lower priority attacks or suspicious traffic that could not be classified into one single type of category. They are usually detected over time by analyzing extended periods of data.
Sustained probe/scan	Reconnaissance activity usually designed to gather information about the targeted systems such as operating systems, open ports, and running services.
Switches	Typically associated as a data link layer device, switches enable local area network (LAN) segments to be created and interconnected, which has the added benefit of reducing collision domains in Ethernet-based networks.
Symmetric key encryption	System in which a different key (or set of keys) is used by each pair of trading partners to ensure that no one else can read their messages
System development life cycle (SDLC)	The phases deployed in the development or acquisition of a software system.
System hardening	A process to eliminate as many security risks as possible by removing all nonessential software programs, protocols, services and utilities from the system
Tablet	A portable computer that uses a touchscreen as its primary input device. Most tablets are small and weigh less than the average laptop.
Telnet	Network protocol used to enable remote access to a server computer
Tether	Process of connecting your mobile phone to a laptop or similar data device using a data cable or wirelessly via Bluetooth. This is commonly done to connect a device, such as a laptop, to the Internet using a mobile phone.
Threat agent	Methods and things used to exploit a vulnerability
Threat analysis	An evaluation of the type, scope and nature of events or actions that can result in adverse consequences identification of the threats that exist against enterprise assets
Threat event	Any event during which a threat element/actor acts against an asset in a manner that has the potential to directly result in harm
Threat vector	The path or route used by the adversary to gain access to the target
Time bomb	A malicious action triggered at a specific date or time.
Timelines	Chronological graphs where events related to an incident can be mapped to look for relationships in complex cases
Token	A device that is used to authenticate a user, typically in addition to a username and password
Topology	The physical layout of how computers are linked together
Transmission Control Protocol (TCP)	A connection-based Internet protocol that supports reliable data transfer connections
Transmission Control Protocol/Internet Protocol (TCP/IP)	Provides the basis for the Internet; a set of communication protocols that encompass media access, packet transport, session communication, file transfer, electronic mail (e-mail), terminal emulation, remote file access and network management
Transport Layer Security (TLS)	A protocol that provides communications privacy over the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery.
Triggered event	An action built into a virus that is set off by a specific condition. Examples include a message displayed on a specific date or reformatting a hard drive after the 10th execution of a program.
Triple DES (3DES)	A block cipher created from the Data Encryption Standard (DES) cipher by using it three times
Trojan (Trojan horse)	Malicious programs disguised as legitimate software. Users are typically tricked into loading and executing it on their systems. One key factor that distinguishes a Trojan from viruses and worms is that Trojans don't replicate.
Trojan horse	Purposefully hidden malicious or damaging code within an authorized computer program
Tunnel mode	Used to protect traffic between different networks when traffic must travel through intermediate or untrusted networks. Tunnel mode encapsulates the entire IP packet with and AH or ESP header and an additional IP header.
Tunneling	A virus technique designed to prevent antivirus applications from working correctly. Antivirus programs work by intercepting the operating system before it can execute a virus. Tunneling viruses try to intercept the actions before the antivirus software can detect the malicious code. New antivirus programs can recognize many viruses with tunneling behaviour.
Two-factor authentication	The use of two independent mechanisms for authentication, (e.g., requiring a smart card and a password) typically the combination of something you know, are or have
Typosquatting	Also known as URL hijacking, it relies on mistakes such as typographical errors made by Internet users when inputting a website address into a browser. If the user accidentally enters the incorrect website address, they are lead to an alternative website that usually is designed for malicious purposes.

Table 52: Cybersecurity glossary of commonly used terms

Term	Definition
Unauthorized access	This usually denotes suspicious activity on a system or failed attempts to access a system by a user or users who does not have access.
Uniform resource locator (URL)	The string of characters that form a web address
User Datagram Protocol (UDP)	A connectionless Internet protocol that is designed for network efficiency and speed at the expense of reliability
User interface impersonation	Can be a pop-up ad that impersonates a system dialog, an ad that impersonates a system warning, or an ad that impersonates an application user interface in a mobile device.
User provisioning	A process to create, modify, disable and delete user accounts and their profiles across IT infrastructure and business applications
Value	The relative worth or importance of an investment for an enterprise, as perceived by its key stakeholders, expressed as total life cycle benefits net of related costs, adjusted for risk and (in the case of financial value) the time value of money
Vertical defense-in depth	Controls are placed at different system layers – hardware, operating system, application, database or user levels
Virtual local area network (VLAN)	Logical segmentation of a LAN into different broadcast domains
Virtual private network (VPN)	A secure private network that uses the public telecommunications infrastructure to transmit data
Virtualization	The process of adding a "guest application" and data onto a "virtual server," recognizing that the guest application will ultimately part company from this physical server
Virus	A program with the ability to reproduce by modifying other programs to include a copy of itself
Virus signature file	The file of virus patterns that are compared with existing files to determine whether they are infected with a virus or worm
Vishing	The criminal practice of posing as a legitimate source to obtain information over the telephone system (phishing via phone/ voicemail). It is facilitated by Voice over IP because it can spoof (fake) caller ID to gain access to personal and financial information.
Voice over Internet protocol (VoIP)	Telephone service that uses the Internet as a global telephone network. Skype is an example of a VoIP offering for both regular and mobile phones.
Volatile data	Data that changes frequently and can be lost when the system's power is shut down
War dialling	Process in which a computer is used to automatically call a list of telephone numbers, usually dialling every number in a local area code to search for computers and fax machines that can successfully make a connection with the computer. When each call is made, the program makes a list of which numbers made a successful connection with a computer and a fax machine. That list can be later used by hackers for various reasons, including hacking a wireless access point with an unprotected login or an easily cracked password to gain access to a network.
War driving	The act of stealing personal information by driving around looking for unsecured wireless connections (networks) using a portable computer or a personal digital assistant (PDA). If your home wireless connection is not secured, thieves can access data on all the computers you have connected to your wireless router, as well as see information you type into your banking and credit card sites.
Warm site	Similar to a hot site but not fully equipped with all of the necessary hardware needed for recovery
Web hosting	The business of providing the equipment and services required to host and maintain files for one or more web sites and provide fast Internet connections to those sites
Web server	Using the client-server model and the World Wide Web's HyperText Transfer Protocol (HTTP), Web Server is a software program that serves web pages to users.
Well-know ports	Well-known ports--0 through 1023: Controlled and assigned by the Internet Assigned Numbers Authority (IANA), and on most systems can be used only by system (or root) processes or by programs executed by privileged users. The assigned ports use the first portion of the possible port numbers. Initially, these assigned ports were in the range 0-255. Currently, the range for assigned ports managed by the IANA has been expanded to the range 0-1023.
Whaling	A type of scam in which phishers find the name and email address of a company's top executive or team of executives (information often freely available on the web), and craft an email specific to those people and their role at the company. The email attempts to lure the executives into clicking on a link that will take them to a website where malware is downloaded onto their machines to copy keystrokes or ferret out sensitive information or corporate secrets.
White hat hackers	Also known as "ethical hackers," white hat hackers are computer security experts who specialize in penetration testing and other testing methodologies to ensure that a company's information systems are secure. These security experts may utilize a variety of methods to carry out their tests, including social engineering tactics, use of hacking tools, and attempts to evade security to gain entry into secured areas.
Whitelist	A list of legitimate email addresses or domain names that is used for filtering spam. Messages from whitelisted addresses or domains are automatically passed to the intended recipient.
Wide area network (WAN)	A computer network connecting different remote locations that may range from short distances, such as a floor or building, to extremely long transmissions that encompass a large region or several countries
Wi-Fi protected access (WAP)	A class of systems used to secure wireless (Wi-Fi) computer networks.
Wi-Fi protected access II (WPA2)	Wireless security protocol that supports 802.11i encryption standards to provide greater security. This protocol uses Advanced Encryption Standards (AES) and Temporal Key Integrity Protocol (TKIP) for stronger encryption.
Wiper	Malicious software designed to erase data and destroy the capability to restore it.
Wired Equivalent Privacy (WEP)	A scheme that is part of the IEEE 802.11 wireless networking standard to secure IEEE 802.11 wireless networks (also known as Wi-Fi networks)
Wireless local area network (WLAN)	Two or more systems networked using a wireless distribution method
Worm	A programmed network attack in which a self-replicating program does not attach itself to programs, but rather spreads independently of users' action
Write blocker	A devices that allows the acquisition of information on a drive without creating the possibility of accidentally damaging the drive
Write protect	The use of hardware or software to prevent data to be overwritten or deleted
Zero-day threats, zero-day vulnerabilities	Also known as zero-hour threats and vulnerabilities, they include threats that take advantage of a security hole before the vulnerability is known. The security hole is usually discovered the same day the computer attack is released. In other words, software developers have zero days to prepare for the security breach and must work as quickly as possible to fix the problem.
Zero-day-exploit	A vulnerability that is exploited before the software creator/vendor is even aware of it's existence
Zombie	A computer that has been compromised by a virus or Trojan horse that puts it under the remote control of an online hijacker. The hijacker uses it to generate spam or makes the computer unusable to the owner, and the user is usually unaware that their computer has been compromised. Generally, a compromised machine is only one of many in a botnet, and will be used to perform malicious tasks under remote direction.
Zoo	A collection of viruses used for testing by researchers. See also: in the wild, zoo virus.
Zoo virus	A virus found only in virus laboratories that has not moved into general circulation.

Source: ISACA, IBM, Kaspersky, BofA Merrill Lynch Global Research

Disclosures

Important Disclosures

FUNDAMENTAL EQUITY OPINION KEY: Opinions include a Volatility Risk Rating, an Investment Rating and an Income Rating. *VOLATILITY RISK RATINGS*, indicators of potential price fluctuation, are: A - Low, B - Medium and C - High. *INVESTMENT RATINGS* reflect the analyst's assessment of a stock's: (i) absolute total return potential and (ii) attractiveness for investment relative to other stocks within its *Coverage Cluster* (defined below). There are three investment ratings: 1 - Buy stocks are expected to have a total return of at least 10% and are the most attractive stocks in the coverage cluster; 2 - Neutral stocks are expected to remain flat or increase in value and are less attractive than Buy rated stocks and 3 - Underperform stocks are the least attractive stocks in a coverage cluster. Analysts assign investment ratings considering, among other things, the 0-12 month total return expectation for a stock and the firm's guidelines for ratings dispersions (shown in the table below). The current price objective for a stock should be referenced to better understand the total return expectation at any given time. The price objective reflects the analyst's view of the potential price appreciation (depreciation).

Investment rating	Total return expectation (within 12-month period of date of initial rating)	Ratings dispersion guidelines for coverage cluster*
Buy	≥ 10%	≤ 70%
Neutral	≥ 0%	≤ 30%
Underperform	N/A	≥ 20%

* Ratings dispersions may vary from time to time where BofA Merrill Lynch Research believes it better reflects the investment prospects of stocks in a Coverage Cluster.

***INCOME RATINGS*, indicators of potential cash dividends, are: 7 - same/higher (dividend considered to be secure), 8 - same/lower (dividend not considered to be secure) and 9 - pays no cash dividend.** *Coverage Cluster* is comprised of stocks covered by a single analyst or two or more analysts sharing a common industry, sector, region or other classification(s). A stock's coverage cluster is included in the most recent BofA Merrill Lynch Comment referencing the stock.

BofA Merrill Lynch Research personnel (including the analyst(s) responsible for this report) receive compensation based upon, among other factors, the overall profitability of Bank of America Corporation, including profits derived from investment banking revenues.

Other Important Disclosures

Officers of MLPF&S or one or more of its affiliates (other than research analysts) may have a financial interest in securities of the issuer(s) or in related investments.
From time to time research analysts conduct site visits of covered companies. BofA Merrill Lynch policies prohibit research analysts from accepting payment or reimbursement for travel expenses from the company for such visits.
BofA Merrill Lynch Global Research policies relating to conflicts of interest are described at http://www.ml.com/media/43347.pdf.
"BofA Merrill Lynch" includes Merrill Lynch, Pierce, Fenner & Smith Incorporated ("MLPF&S") and its affiliates. Investors should contact their BofA Merrill Lynch representative or Merrill Lynch Global Wealth Management financial advisor if they have questions concerning this report. "BofA Merrill Lynch" and "Merrill Lynch" are each global brands for BofA Merrill Lynch Global Research.
Information relating to Non-US affiliates of BofA Merrill Lynch and Distribution of Affiliate Research Reports:
MLPF&S distributes, or may in the future distribute, research reports of the following non-US affiliates in the US (short name: legal name): Merrill Lynch (France): Merrill Lynch Capital Markets (France) SAS; Merrill Lynch (Frankfurt): Merrill Lynch International Bank Ltd., Frankfurt Branch; Merrill Lynch (South Africa): Merrill Lynch South Africa (Pty) Ltd.; Merrill Lynch (Milan): Merrill Lynch International Bank Limited; MLI (UK): Merrill Lynch International; Merrill Lynch (Australia): Merrill Lynch Equities (Australia) Limited; Merrill Lynch (Hong Kong): Merrill Lynch (Asia Pacific) Limited; Merrill Lynch (Singapore): Merrill Lynch (Singapore) Pte Ltd.; Merrill Lynch (Canada): Merrill Lynch Canada Inc; Merrill Lynch (Mexico): Merrill Lynch Mexico, SA de CV, Casa de Bolsa; Merrill Lynch (Argentina): Merrill Lynch Argentina SA; Merrill Lynch (Japan): Merrill Lynch Japan Securities Co., Ltd.; Merrill Lynch (Seoul): Merrill Lynch International Incorporated (Seoul Branch); Merrill Lynch (Taiwan): Merrill Lynch Securities (Taiwan) Ltd.; DSP Merrill Lynch (India): DSP Merrill Lynch Limited; PT Merrill Lynch (Indonesia): PT Merrill Lynch Indonesia; Merrill Lynch (Israel): Merrill Lynch Israel Limited; Merrill Lynch (Russia): OOO Merrill Lynch Securities, Moscow; Merrill Lynch (Turkey I.B.): Merrill Lynch Yatirim Bank A.S.; Merrill Lynch (Turkey Broker): Merrill Lynch Menkul Değerler A.Ş.; Merrill Lynch (Dubai): Merrill Lynch International, Dubai Branch; MLPF&S (Zurich rep. office): MLPF&S Incorporated Zurich representative office; Merrill Lynch (Spain): Merrill Lynch Capital Markets Espana, S.A.S.V.; Merrill Lynch (Brazil): Bank of America Merrill Lynch Banco Multiplo S.A.; Merrill Lynch KSA Company, Merrill Lynch Kingdom of Saudi Arabia Company.
This research report has been approved for publication and is distributed in the United Kingdom to professional clients and eligible counterparties (as each is defined in the rules of the Financial Conduct Authority and the Prudential Regulation Authority) by Merrill Lynch International and Bank of America Merrill Lynch International Limited, which are authorized by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority, and is distributed in the United Kingdom to retail clients (as defined in the rules of the Financial Conduct Authority and the Prudential Regulation Authority) by Merrill Lynch International Bank Limited, London Branch, which is authorised by the Central Bank of Ireland and subject to limited regulation by the Financial Conduct Authority and Prudential Regulation Authority - details about the extent of our regulation by the Financial Conduct Authority and Prudential Regulation Authority are available from us on request; has been considered and distributed in Japan by Merrill Lynch Japan Securities Co., Ltd., a registered securities dealer under the Financial Instruments and Exchange Act in Japan; is distributed in Hong Kong by Merrill Lynch (Asia Pacific) Limited, which is regulated by the Hong Kong SFC and the Hong Kong Monetary Authority is issued and distributed in Taiwan by Merrill Lynch Securities (Taiwan) Ltd.; is issued and distributed in India by DSP Merrill Lynch Limited; and is issued and distributed in Singapore to institutional investors and/or accredited investors (each as defined under the Financial Advisers Regulations) by Merrill Lynch International Bank Limited (Merchant Bank) and Merrill Lynch (Singapore) Pte Ltd. (Company Registration No.'s F 06872E and 198602883D respectively). Merrill Lynch International Bank Limited (Merchant Bank) and Merrill Lynch (Singapore) Pte Ltd. are regulated by the Monetary Authority of Singapore. Bank of America N.A., Australian Branch (ARBN 064 874 531), AFS License 412901 (BANA Australia) and Merrill Lynch Equities (Australia) Limited (ABN 65 006 276 795), AFS License 235132 (MLEA) distributes this report in Australia only to 'Wholesale' clients as defined by s.761G of the Corporations Act 2001. With the exception of BANA Australia, neither MLEA nor any of its affiliates involved in preparing this research report is an Authorised Deposit-Taking Institution under the Banking Act 1959 nor regulated by the Australian Prudential Regulation Authority. No approval is required for publication or distribution of this report in Brazil and its local distribution is made by Bank of America Merrill Lynch Banco Múltiplo S.A. in accordance with applicable regulations. Merrill Lynch (Dubai) is authorized and regulated by the Dubai Financial Services Authority (DFSA). Research reports prepared and issued by Merrill Lynch (Dubai) are prepared and issued in accordance with the requirements of the DFSA conduct of business rules.
Merrill Lynch (Frankfurt) distributes this report in Germany. Merrill Lynch (Frankfurt) is regulated by BaFin.
This research report has been prepared and issued by MLPF&S and/or one or more of its non-US affiliates. MLPF&S is the distributor of this research report in the US and accepts full responsibility for research reports of its non-US affiliates distributed to MLPF&S clients in the US. Any US person receiving this research report and wishing to effect any transaction in any security discussed in the report should do so through MLPF&S and not such foreign affiliates. Hong Kong recipients of this research report should contact Merrill Lynch (Asia Pacific) Limited in respect of any matters relating to dealing in securities or provision of specific advice on securities. Singapore recipients of this research report should contact Merrill Lynch International Bank Limited (Merchant Bank) and/or Merrill Lynch (Singapore) Pte Ltd in respect of any matters arising from, or in connection with, this research report.
General Investment Related Disclosures:
Taiwan Readers: Neither the information nor any opinion expressed herein constitutes an offer or a solicitation of an offer to transact in any securities or other financial instrument. No part of this report may be used or reproduced or quoted in any manner whatsoever in Taiwan by the press or any other person without the express written consent of BofA Merrill Lynch.
This research report provides general information only. Neither the information nor any opinion expressed constitutes an offer or an invitation to make an offer, to buy or sell any securities or other financial instrument or any derivative related to such securities or instruments (e.g., options, futures, warrants, and contracts for differences). This report is not intended to provide personal investment advice and it does not take into account the specific investment objectives, financial situation and the particular needs of any specific person. Investors should seek

financial advice regarding the appropriateness of investing in financial instruments and implementing investment strategies discussed or recommended in this report and should understand that statements regarding future prospects may not be realized. Any decision to purchase or subscribe for securities in any offering must be based solely on existing public information on such security or the information in the prospectus or other offering document issued in connection with such offering, and not on this report.

Securities and other financial instruments discussed in this report, or recommended, offered or sold by Merrill Lynch, are not insured by the Federal Deposit Insurance Corporation and are not deposits or other obligations of any insured depository institution (including, Bank of America, N.A.). Investments in general and, derivatives, in particular, involve numerous risks, including, among others, market risk, counterparty default risk and liquidity risk. No security, financial instrument or derivative is suitable for all investors. In some cases, securities and other financial instruments may be difficult to value or sell and reliable information about the value or risks related to the security or financial instrument may be difficult to obtain. Investors should note that income from such securities and other financial instruments, if any, may fluctuate and that price or value of such securities and instruments may rise or fall and, in some cases, investors may lose their entire principal investment. Past performance is not necessarily a guide to future performance. Levels and basis for taxation may change.

This report may contain a short-term trading idea or recommendation, which highlights a specific near-term catalyst or event impacting the company or the market that is anticipated to have a short-term price impact on the equity securities of the company. Short-term trading ideas and recommendations are different from and do not affect a stock's fundamental equity rating, which reflects both a longer term total return expectation and attractiveness for investment relative to other stocks within its Coverage Cluster. Short-term trading ideas and recommendations may be more or less positive than a stock's fundamental equity rating.

BofA Merrill Lynch is aware that the implementation of the ideas expressed in this report may depend upon an investor's ability to "short" securities or other financial instruments and that such action may be limited by regulations prohibiting or restricting "shortselling" in many jurisdictions. Investors are urged to seek advice regarding the applicability of such regulations prior to executing any short idea contained in this report.

Foreign currency rates of exchange may adversely affect the value, price or income of any security or financial instrument mentioned in this report. Investors in such securities and instruments, including ADRs, effectively assume currency risk.

UK Readers: The protections provided by the U.K. regulatory regime, including the Financial Services Scheme, do not apply in general to business coordinated by BofA Merrill Lynch entities located outside of the United Kingdom. BofA Merrill Lynch Global Research policies relating to conflicts of interest are described at http://www.ml.com/media/43347.pdf.

Officers of MLPF&S or one or more of its affiliates (other than research analysts) may have a financial interest in securities of the issuer(s) or in related investments.

MLPF&S or one of its affiliates is a regular issuer of traded financial instruments linked to securities that may have been recommended in this report. MLPF&S or one of its affiliates may, at any time, hold a trading position (long or short) in the securities and financial instruments discussed in this report.

BofA Merrill Lynch, through business units other than BofA Merrill Lynch Global Research, may have issued and may in the future issue trading ideas or recommendations that are inconsistent with, and reach different conclusions from, the information presented in this report. Such ideas or recommendations reflect the different time frames, assumptions, views and analytical methods of the persons who prepared them, and BofA Merrill Lynch is under no obligation to ensure that such other trading ideas or recommendations are brought to the attention of any recipient of this report.

In the event that the recipient received this report pursuant to a contract between the recipient and MLPF&S for the provision of research services for a separate fee, and in connection therewith MLPF&S may be deemed to be acting as an investment adviser, such status relates, if at all, solely to the person with whom MLPF&S has contracted directly and does not extend beyond the delivery of this report (unless otherwise agreed specifically in writing by MLPF&S). MLPF&S is and continues to act solely as a broker-dealer in connection with the execution of any transactions, including transactions in any securities mentioned in this report.

Copyright and General Information regarding Research Reports:

Copyright 2015 Merrill Lynch, Pierce, Fenner & Smith Incorporated. All rights reserved. iQmethod, iQmethod 2.0, iQprofile, iQtoolkit, iQworks are service marks of Bank of America Corporation. iQanalytics®, iQcustom®, iQdatabase® are registered service marks of Bank of America Corporation. This research report is prepared for the use of BofA Merrill Lynch clients and may not be redistributed, retransmitted or disclosed, in whole or in part, or in any form or manner, without the express written consent of BofA Merrill Lynch. BofA Merrill Lynch Global Research reports are distributed simultaneously to internal and client websites and other portals by BofA Merrill Lynch and are not publicly-available materials. Any unauthorized use or disclosure is prohibited. Receipt and review of this research report constitutes your agreement not to redistribute, retransmit, or disclose to others the contents, opinions, conclusion, or information contained in this report (including any investment recommendations, estimates or price targets) without first obtaining expressed permission from an authorized officer of BofA Merrill Lynch.

Materials prepared by BofA Merrill Lynch Global Research personnel are based on public information. Facts and views presented in this material have not been reviewed by, and may not reflect information known to, professionals in other business areas of BofA Merrill Lynch, including investment banking personnel. BofA Merrill Lynch has established information barriers between BofA Merrill Lynch Global Research and certain business groups. As a result, BofA Merrill Lynch does not disclose certain client relationships with, or compensation received from, such companies in research reports. To the extent this report discusses any legal proceeding or issues, it has not been prepared as nor is it intended to express any legal conclusion, opinion or advice. Investors should consult their own legal advisers as to issues of law relating to the subject matter of this report. BofA Merrill Lynch Global Research personnel's knowledge of legal proceedings in which any BofA Merrill Lynch entity and/or its directors, officers and employees may be plaintiffs, defendants, co-defendants or co-plaintiffs with or involving companies mentioned in this report is based on public information. Facts and views presented in this material that relate to any such proceedings have not been reviewed by, discussed with, and may not reflect information known to, professionals in other business areas of BofA Merrill Lynch in connection with the legal proceedings or matters relevant to such proceedings.

This report has been prepared independently of any issuer of securities mentioned herein and not in connection with any proposed offering of securities or as agent of any issuer of any securities. None of MLPF&S, any of its affiliates or their research analysts has any authority whatsoever to make any representation or warranty on behalf of the issuer(s). BofA Merrill Lynch Global Research policy prohibits research personnel from disclosing a recommendation, investment rating, or investment thesis for review by an issuer prior to the publication of a research report containing such rating, recommendation or investment thesis.

Any information relating to the tax status of financial instruments discussed herein is not intended to provide tax advice or to be used by anyone to provide tax advice. Investors are urged to seek tax advice based on their particular circumstances from an independent tax professional.

The information herein (other than disclosure information relating to BofA Merrill Lynch and its affiliates) was obtained from various sources and we do not guarantee its accuracy. This report may contain links to third-party websites. BofA Merrill Lynch is not responsible for the content of any third-party website or any linked content contained in a third-party website. Content contained on such third-party websites is not part of this report and is not incorporated by reference into this report. The inclusion of a link in this report does not imply any endorsement by or any affiliation with BofA Merrill Lynch. Access to any third-party website is at your own risk, and you should always review the terms and privacy policies at third-party websites before submitting any personal information to them. BofA Merrill Lynch is not responsible for such terms and privacy policies and expressly disclaims any liability for them.

Subject to the quiet period applicable under laws of the various jurisdictions in which we distribute research reports and other legal and BofA Merrill Lynch policy-related restrictions on the publication of research reports, fundamental equity reports are produced on a regular basis as necessary to keep the investment recommendation current.

Certain outstanding reports may contain discussions and/or investment opinions relating to securities, financial instruments and/or issuers that are no longer current. Always refer to the most recent research report relating to a company or issuer prior to making an investment decision.

In some cases, a company or issuer may be classified as Restricted or may be Under Review or Extended Review. In each case, investors should consider any investment opinion relating to such company or issuer (or its security and/or financial instruments) to be suspended or withdrawn and should not rely on the analyses and investment opinion(s) pertaining to such issuer (or its securities and/or financial instruments) nor should the analyses or opinion(s) be considered a solicitation of any kind. Sales persons and financial advisors affiliated with MLPF&S or any of its affiliates may not solicit purchases of securities or financial instruments that are Restricted or Under Review and may only solicit securities under Extended Review in accordance with firm policies.

Neither BofA Merrill Lynch nor any officer or employee of BofA Merrill Lynch accepts any liability whatsoever for any direct, indirect or consequential damages or losses arising from any use of this report or its contents.