Happy New WAN: Protecting Data Into 2026

Only a few days away now from New Year's Day again, fireworks and all. Hopefully, it'll be a happy and prosperous one for everyone. Unfortunately, cyber-attacks aren't about fun, prosperity and good will. Of course cyber-criminals might celebrate the new year if their scams and attacks bear them financial rewards, then they really would have something to celebrate. However, most of us don't wish them such luck; we need to ensure that our data and finances are secured.

Amongst the many cyber-attacks that have occurred in 2025, one that stands out was cyber-attack on the Royal Borough of Kensington and Chelsea, Westminster City Council and the London Borough of Hammersmith and Fulham. These London boroughs in England enacted emergency plans after they were hit by a cyber-attack on 26th November 2025.

For example, across the Pond, the State of Nevada declined to pay a ransom on 6th November 2025, as a result of a data breach that was traced by to May. It disrupted services across more than 60 States agencies, exposing thousands of files, and it allegedly caused $1.3m in recovery costs. Furthermore, despite refusing to pay a ransom, no threat actor was identified.

33.7 million customer accounts breached

At the end of the month, Coupang - South Korea's largest e-commerce firm - announced a data breach involving 33.7 million customer accounts. This led to names, emails, phone numbers and some order histories being accessed by an unauthorised part over several months, since June 2025. While no payment details were leaked, affected users were warned that they could fall prey to a phishing attack. The suspect: An insider. Even so, with phishing being a potential issue, the threat to the organisation, its suppliers, its reputation and customers is much wider than an individual.

Such issues just aren't the present that anyone wants just before or even during Christmas, or before the New Year. After all, the festive season isn't immune to cyber-attacks. Infosecurity magazine warns that 'UK Shoppers Lost £11.5m Last Christmas, NCSC Warns.' Phil Muncaster, UK and EMEA news reporter at the magazine adds:

"Scammers have a variety of tools and tactics at their disposal, from advertising non-existent items at knockdown prices, to setting up lookalike web stores promoted by fake ads and phishing messages, which are designed to harvest personal and financial information."

Devastating impact

Any cyber-attack or scam on an individual or an organisation can be devastating. The first thing to avoid thinking is that you're too clever or intelligent to become a victim. The truth is anyone can, and so it's vital to put in place systems and processes to reduce the likelihood of any attack or fraud from succeeding. This includes training, and a means for members of staff to speak up, or to alert others if they see anyone acting suspiciously – including members of internal staff.

What also needs to be borne in mind is that cyber-threats are going to become increasingly sophisticated. Google Cloud therefore advises organisations to plan ahead: "2026 will usher in a new era for cybersecurity. Threat actors will leverage AI to escalate the speed, scope and

effectiveness of their attacks. Simultaneously, defenders will harness AI agents to supercharge security operations and enhance analyst capabilities."

"This transformation introduces new challenges, including "Shadow Agent" risks and the need for evolving identity and access management, all while geopolitical and financial threats continue to accelerate."

AI Arms Race

Well into the New Year, it predict that there will be an AI Arms Race, leading to faster attacks that will be counted with an Agentic Security Operations Centre (SOC). Google AI describes it as being: "An advanced, AI-driven cyber-security model where autonomous AI agents work together to detect, investigate, and respond to threats with minimal human intervention, moving beyond simple automation to independent reasoning, planning and dynamic adaptation for faster, more efficient security." The aim is to predict the next defensive move to avert any potential danger.

Extortion is an old devil. In modern times, it comes in the form of ransomware and data theft, which remain the top threat, and will probably be so in 2026. Various tactics are used to bypass multi-factor authentication. Then there is the Virtualisation Frontline, which is about how attackers are targeting virtualisation infrastructures because this critical layer, says Google Cloud, is a "growing blind spot." With conflicts around the world continuing – including in Ukraine, the activities of some nation states, such as Russia, are often cited as a major cause for concern.

Quantum risk

Cyberlab warns in its 'Top 5 Cyber Security Predictions for 2026' that deepfakes, identity fraud and the human factor will play a significant role in cyber-attacks during the new year. There will also need to be some thought for quantum risk – the risk posed by the increasing use of quantum computers to break current encryption protocols, such as RSA and ECC, which are used to secure data communications.

This threat makes sensitive data particularly vulnerable, and so organisations would be advised to create air gaps for their most vulnerable data. The problem is that bad actors might harvest data now to decrypt it later on, which can lead to financial transactions being compromised or diverted. There could also be national security implications.

With the growth of the Internet of Things (IoT), the risks of this occurring could become more significant, and so there is a need for a Zero Trust Security policy – particularly when it comes to supply chain security, which Cyberlab thinks will become even more of a business requirement than it is today.

Costing UK businesses £14.7bn

Adam Myers, writing for its blog, adds: "In November 2025, the UK Government released a comprehensive report on the economic cost of cyber-crime, which highlights how the average cyber-incident costs a UK business £195,000. Scaling this to an annual UK cost, generates an estimate of £14.7 billion, equivalent to 0.5% of the UK's GDP. The growing threat landscape and significant cost of cyber-crime makes cyber-security a pressing issue for all UK businesses."

Therefore, to prevent any disruption or financial upheaval, it's vital to be able to allow the fireworks to go ahead on 1st January 2026 without having to worry too much about cyber-attacks and data breaches. That's because any mitigations should already be in place to ensure that they can't be successful or, where possible, actually happen at all. If they do occur and they are successful, then service continuity rather than the disaster recovery should already be in place.

Be prepared today

This is achieved through by deploying a multitude of strategies – from the implementation of regular training programmes to prevent staff from clicking on phishing emails, to backing up and - whenever needed - restoring data with WAN Acceleration. The latter uses artificial intelligence (AI) and machine learning (ML) to mitigate the effects of latency and packet loss.

To further accelerate the flow of encrypted data, it also deploys data parallelisation to permit faster backups and restores, while also having the ability obfuscate cyber-criminals. In essence, it's the happy new WAN you want in 2026 – allowing organisations to achieve regulatory compliance, avoid fines caused by data breaches and stay operational. That will help them to save time, money and effort. With that in mind, have a happy and prosperous New Year!