Article

Dec 2025

Cyber Security: five hot takes and key actions

Recently, there's been a wave of cyberattacks battering organisations globally, so what's going on to cause such a flurry?

Craig Archdeacon
Director - APAC

Email craig.archdeacon@waterstons.com

Our APAC General Manager, Craig, takes a look at the five key things he thinks could be behind it.

It's key to note that these businesses were not inherently insecure, decision makers had not knowingly underinvested in cybersecurity, or were aware they were operating under such a high impact unmanaged risk. It's common not to realise has been missed until something happens, even when you've been doing everything right for years, so here are six things to think about...

1. Misplaced confidence

One of the biggest issues? Overconfidence. Companies that think they're 'super secure' are often the ones with the biggest risks. Ironically, the ones that worry they're underprepared are usually the most resilient.

Why? Because they're turning over the rocks, hunting for problems and documenting risk. They're improving step by step, and the presence of concern means they're identifying gaps.

No business will ever be perfect, but being aware of the risks and trying your best to practically address these risks is a great step in the right direction.

Meanwhile, those clinging to a silver bullet solution, a 'great IT guy', or shrugging it off as someone else's problem are sitting ducks.

You don't need to be building stealth bombers to attract threats; even the US military, with its billions in research and top-tier security, can't prevent leaks when a well-resourced adversary is determined.

No business will ever be 100% safe, but looking, learning, and adjusting is what builds resilience.

2. Spending big (but on the wrong things)

Expensive does not equal effective.

People feel safer when investing in something expensive - a flashy 'golden dome idea' or a cyber defence platform that promises to stop everything – but breaches aren't stopped by magic, they're stopped by boring basics, done consistently.

Take the UK Government's Cyber Essentials Scheme: five simple controls that can prevent 80% of common attacks for around £1,500 (excluding remedial work). That's not sexy, but it works.

24/7 SOCs, MDR, XDR, threat intel platforms - they're great, but only when layered with solid hygiene, embedded processes, and a security-aware culture.

It's not about the snazzy tech, but protecting information – yours and your customers' – which means people, process, and technology all pulling in the same direction.

3. Supply chain; your weakest link might not be one of yours

Even companies with the best defences are vulnerable through third-party suppliers.

There's a SaaS tool for everything, but how many companies do real due diligence on suppliers? Who has access to your data? Where is it stored? What's the response plan if they get hit?

The enterprise-grade defences of a Las Vegas aquarium were undone by a $100 smart light plugged into the network. And attackers got in with ease.

One look at a well-known cyber security search engine shows unsecured tech – including webcams, firewalls, and networks with default passwords – in seconds.

Your procurement team might approve a £90 gadget without blinking, but that gadget or supplier might introduce unmeasurable risk, both reputationally and financially. Just ask Maersk – over $800M in revenue and 10 days of operations were lost due to a supply chain attack. Qantas is still counting the impact of its data breach in July.

4. Staff training; tick-box exercises aren't enough

Your people can be your strongest shield or your weakest link. Too often, security training is just an annual compliance video that people open, guess the answers, and forget before they've even closed the browser.

Real engagement is what works. Frequent, targeted micro-learning, simulated phishing, real-life relevance (e.g. how this protects their families, not just their files). If it's boring, it's ignored. But if it's meaningful, it sticks.

We flipped the script with a gamified method - a board game focused not just on security, but resilience: protect, adapt, optimise, innovate. Players run their own businesses with a limited budget; they learn by making mistakes, competing, and improving – not by being lectured.

5. Trusted partners - the good, the bad, and the flattering

Many providers tell clients what they want to hear. They want to land the big contract, so they stroke egos and only show the good stuff.

A true partner is honest, even when it's uncomfortable, and that sometimes means telling clients they're focusing too much on shiny tools and ignoring gaping holes elsewhere. It's about perspective, not perception.

We drew a line in the sand years ago: if you want managed services, you need vulnerability management. Full stop. Over 280,000 vulnerabilities are published annually – you can't ignore that. Some clients walked away, but those who stayed saw 10x the value.

Five actions you need to take:

1. Be humble; no one's perfect but the first step to security is admitting you don't know everything.

2. Start now. Look at Cyber Essentials, the CAF and what they mean to your organisation.

3. Audit your supply chain - if your partners aren't secure, neither are you.

4. Train like you mean it - Use real data, micro-learning, gamification. Make it stick. Make it matter.

5. Choose honest partners - work with people who challenge you, not just cheer you on.

Not sure where to start? That's where we come in. Get in touch and we'll help you turn over those rocks - cyber@waterstons.com