Picture credit: AdobeStock

TAKING STOCK

Trevor Dearing *outlines the lessons learnt in his cyber security round up of the past 12 months*

2025 has been a year of cyber disruption like no other. Whether it's our favourite supermarkets, our most relied on social services or our means to travel domestically and abroad, this year has shown us the inescapable truth that breaches are inevitable. And with 88 percent of organisations worldwide experiencing at least one ransomware attack, no sector is immune.

Despite increased investment in cyber security, attacks are more frequent and severe. Organisations can no longer stand by and be passive. The imperative is clear: build operational resilience to ensure that critical operations continue during an active attack. To do this, a proactive and organisation wide approach is vital.

This year has seen some standout cyber incidents. Recently, both the Co-op and Harrods were struck by ransomware that disabled core systems and Jaguar Land Rover was forced to halt production for multiple weeks, causing staff to apply for Universal Credit. Yet, it isn't just household names that have suffered.

As well as organisations themselves being targeted, there have also been risks posed to complex webs of suppliers. In North America, United Natural Foods (UNFI) suffered an attack that brought down its electronic ordering systems and caused major disruption across supermarket supply chains. JLR's smaller suppliers have spoken of possible bankruptcy as the production delay stretches on.

Even more recently, airports across Europe, including Heathrow, Brussels, Berlin and Dublin, have had to deal with mass disruptions when a third-party supplier was compromised. Passengers were stranded as airlines scrambled to revert to manual check-in and baggage processes. As organisations grow more connected, the potential for one incident to domino into a disaster has increased.

Airports across Europe had to deal with mass disruptions when a third-party supplier was compromised

Healthcare has also been a prime target. Major organisations such as DaVita disclosed that over 2.7-million patient records were compromised during a ransomware attack. The breach affected insurance information, clinical data and personal records. In the healthcare sector, cyber takes on an extra layer of urgency with concerns over cyber impacts on patient safety in addition to regulatory compliance and reputational damage.

Public services proved equally vulnerable. In July, the city of St. Paul in Minnesota, declared a state of emergency after ransomware crippled municipal systems. In the UK, Transport for London also was impacted by a group of malicious actors.

The breaches of this year have made one thing clear: cyber attacks now carry tangible, operational consequences. They are no longer limited to stealing data. They are engineered to cause maximum disruption, halt operations and impact business continuity. Yet, for all their sophistication, 2025's most damaging attacks have exposed surprisingly consistent patterns of organisational vulnerability. Below are the key lessons where defences repeatedly fail and what must change.

It always seems fitting to start lessons with the basics. A consistent theme of 2025 has been that many organisations still overlook fundamental security hygiene. That means unpatched systems, misconfigurations and weak access controls, which leave critical gaps for attackers to exploit. In just over half of ransomware cases, attackers exploited unpatched systems to move laterally and escalate system privileges. Remote Desktop Protocol (RDP) compromises also remain a top entry point, accounting for 33 percent of how ransomware is unleashed. These are the basics of security hygiene, which when overlooked lead to serious consequences. Without these foundations in place, organisations will remain exposed. It doesn't matter how many advanced tools you have if these simple security steps are neglected.

Let's take the recent TfL breach as an example of the importance of security controls, which focus on limiting the impact. Stronger segmentation between critical systems, combined with identity-based access controls, would have made it harder for attackers to move laterally. It also would have made traffic monitoring between systems far easier and could have provided early warning of suspicious activity. These are straightforward measures, yet their absence continues to leave organisations vulnerable.

Another key factor in many breaches is a lack of understanding over environments and what's talking to what. The majority of businesses monitor traffic across their hybrid estate, yet nearly 40 percent of traffic lacks sufficient context for investigation. Visibility without context is meaningless. We saw this with the Storm-0501 ransomware campaign, which spread by exploiting misconfigurations across hybrid Active Directory and Entra ID environments. Another threat group called ShinyHunters was able to target Salesforce customers like Allianz Life by abusing overlooked permissions.

The pattern is clear: attackers move laterally through environments that organisations can't properly see or understand. To close the gap, organisations must think more like attackers. Adversaries don't see network boundaries or departmental silos, they see pathways. They map relationships between compromised accounts, vulnerable systems, and misconfigured access points to plan their next move. Just like attackers, organisations should look for the relationships that allow lateral movement where malicious actors jump from one compromised account to another.

CONTAINMENT STRATEGIES SHOULD ASSUME THAT A THIRD PARTY MIGHT BE COMPROMISED

The key here is observability, not just visibility. Graph-based security models reinforced with AI provide the clarity defenders lack today. They can turn a suspicious login from just another low-level alert into a high-priority warning when correlated correctly. AI-powered graphs reveal how a vulnerable cloud configuration could be exploited via a weak identity in another. Instead of drowning in noise, analysts see the real attack paths adversaries are likely to exploit.

The past year has seen governments act to strengthen organisational security. Europe's Digital Operational Resilience Act (DORA) imposes stricter operational standards on financial services, while the UK's proposed Cyber Resilience Bill seeks cross-sector requirements such as mandatory ransomware reporting and transparency. Meanwhile, the NIS2 Directive also put in place greater requirements for critical infrastructure including 24-hour incident reporting. These initiatives provide necessary baselines, but should not be seen as the sole driver of security transformation.

ENISA guidance reveals the difficulties sectors face around legacy systems, under-resourced teams and complex supply chains when complying with the NIS Directive. It is proving to be both an operational and resource intensive challenge. The same can be said for organisations complying with DORA.

A poignant lesson for organisations is to not look at compliance as the goal in itself and instead focus on the bigger picture. Passing an audit won't stop ransomware, look instead at the content of what these regulators are asking. DORA, NIS2 and other policies are all asking organisations to become more resilient. Yes, they provide a necessary baseline to start the journey, but true resilience comes from adopting a risk-based approach to both meet regulatory obligations and strengthen an organisation's security posture in tandem. Doing this effectively means identifying and prioritising protection of critical assets and systems and embedding resilience into all operations. Regulatory audits should be seen as a validation of this pursuit and not the driving force behind them.

Resilience doesn't just sit within the IT team. To be effective, it must become part of an organisation's culture. Too often, organisations treat incident response as an exercise in blame. In some cases, analysts are more afraid of the stigma of 'getting it