

# 2025 CYBER SECURITY PREDICTIONS

## **As we close the doors on 2024, it's an opportune time to evaluate what happened in the cyber security landscape throughout the year and predict what could lie ahead for the industry in 2025.**

It's safe to say 2024 has been a busy year for both defenders and sadly attackers too.

Ransomware continues to be the most damaging threat for organisations, both public and private. We have seen the consequences in the healthcare sector only too clearly.

Nation-states are ramping up cyber espionage campaigns with increasing scale, sophistication and determination in targeting critical infrastructure systems and an unrelenting search for zero day vulnerabilities in network devices and endpoints.

Western security agencies are showing increasing concern about the potential impact of such attacks, not least in the context of Russian hybrid warfare.

Generative AI and sophisticated deep fakery are starting to find their place in supporting increasing compelling social engineering.

Supply chain attacks have made the news worldwide posing new challenges around the management of systemic risks associated with our dependency on digital infrastructure, including ironically cyber security services.

At a time when geopolitical tensions are growing and political blocks are polarising, cyber attacks offer deniable action alongside misinformation and manipulation of the information space to destabilise States.

National cyber security demands national responses, and we have seen the NCSC continue to develop its active defence capabilities as well as working with the NCA to spearhead campaigns to disrupt notorious Russian speaking ransomware groups.

Regulators across all sectors are taking action to drive up cyber security standards, and increase the focus on supply chain resilience.

### **But what else might 2025 bring?**

There are many uncertainties ahead in 2025, and many scenarios in which the world may be a very unsafe place indeed, so with some trepidation lets peer into the crystal ball and speculate on what 2025 may bring.

## **Cyber threats will be driven by aggressive geopolitics**

The world has grown increasingly volatile over the last few years and more polarised too.

The war in the Ukraine has passed its 1000th day, with Russia continuing to ramp up its cyber operations against countries supporting Ukraine as well as turning a blind eye to the scale of organised cyber crime originating from within its borders. We can expect more aggressive cyber attacks against Western infrastructure, as well as increasing attempts to exploit political fault lines amongst European nations. We will see a growing number of sabotage operations in Europe with growing concern over the vulnerability of submarine cables and other digital infrastructure.

The eventual end game for the war between Israel and Iranian proxies is unpredictable, but it seems unlikely that either Israel or Iran will abandon the development of their respective cyber operations capabilities even if they focus on each other as targets.

Perhaps most concerning has been the pace of Chinese cyber espionage development through the rapid build out of attack infrastructure, comprehensive zero day vulnerability research, information collected through use of Chinese technology and a growing focus on exploitation of critical national infrastructure. In 2025, we can expect to see Western nations attribute more offensive cyber operations to China as we have seen with Volt Typhoon and Salt Typhoon recently. There will be a hardening of the US stance on China, and with that a reopening of many debates on dependence on Chinese technology in the US and across Europe.





## **AI will be used by adversaries and defenders in equal measure**

Generative AI has dominated technology conversations in 2024. This will continue in the year ahead with many debates over the ethics of AI adoption including in high risk areas such as law enforcement and surveillance, opinion manipulation and safety critical systems. National regulatory positions on the adoption of AI will diverge as nations seek competitive advantage.

Organisations will get AI adoption wrong in their haste to adopt raising privacy and cyber security concerns, and we will continue to see examples of incidents which could have been avoided had appropriate guardrails been in place.

AI is already being applied to scale social engineering attacks by criminal groups, to identify vulnerable organisations and evade malware detection. This will accelerate in 2025 as AI adoption by organised crime groups becomes mainstream. We can safely predict that AI will soon take on reconnaissance tasks and first stage exploitation of systems independently, allowing attackers to operate with unprecedented speed and scale.

Defenders will also harness AI allowing more sophisticated threat detection, response, analysis and prediction. Caution will remain over fully automated responses to attack, even if there is an inevitability about this development in the near future. Nations will continue to invest in national scale infrastructure to fuse intelligence on attacks and work with technology providers to automate take down and blocking activities. Legal structures will struggle to keep up with the necessity of action at pace, with criminal groups continuing to seek nations who will provide safe cyber havens for their activities.

The cat and mouse race continues, but now enabled by AI.

## **Supply chain attacks will demonstrate the dangers of ubiquitous software**

CrowdStrike was undoubtedly the biggest third-party cyber incident to take place in 2024, demonstrating as it did the complexity of digital supply chains but also the complex trade off between rapidly countering cyber threats and the risks of upgrading systems at pace. It also prompted many firms to review just which third parties could implement changes directly into their operational environments.

Of course we will see more supply chain incidents in 2025, whether accidental or malicious acts by cyber criminals and states. We can also expect to see these incidents create unexpected consequences for digital society.

Governments are now assembling a more accurate view of the nature of supply chain dependencies and systemic risks, and in doing so discovering the extent to which critical infrastructure providers are dependent on unregulated digital service providers.

Expect supply chain risk to be a focus area for regulatory action in 2025. Some we know already – the implementation of the EU Digital Operational Resilience Act (DORA), the EU Network and Information Systems (NIS) 2 directive and the Bank of England's critical third party regime. More is to come as the UK government seeks to bring managed service providers within scope of regulation.

While EU and UK regulation is likely to be broadly aligned, expect that the US regulatory position will be more complex given the political landscape. There will also be an interesting dynamic as competition regulators seek to open up closed system architectures, while cyber security regulators seek to drive security improvements and even establish liability for failure or compromise.

Improving supply chain security will be on the agenda for many organisations, public and private, in 2025.



## Disinformation and deep fakes will spur financial fraud and political unrest

Truth and fiction will blur even more in 2025. Deep fakes have become increasingly convincing and we have now crossed the threshold where we can reasonably expect citizens to distinguish reality from AI generated constructs.

The debate on the responsibilities of social media platforms will continue into 2025, with UK and EU regulators attempting to intervene and growing pressure on AI developers to flag AI generated content and on media channels to identify and remove fakes. In a world of rapid innovation and powerful social media platforms we can expect major public and political debate, but also little international consensus.

Cyber criminals will replicate the appearance, voice, and behaviours of high-profile figures with startling accuracy, and we will see some high profile examples of fakery as part of sophisticated social engineering, business email compromise and fraud campaigns. Financial institutions will be forced to play a growing role in countering these fraud campaigns, as regulators increasingly seek to place responsibility on banks for protecting customers against the consequences of fraud.

States will increasingly resort to manipulation of the information space to further their political ends, looking for creative ways to divide and polarise political opinions in democratic societies. All of this is becoming just part of projecting power in a modern digital world.

Cyber security has become far more than just protecting networks and information systems, with people (as ever) being key to security.

## 2025 will be the busiest year on record for a growing number of regulated firms

2025 will be a year of significant regulatory change.

DORA enters into force on the 17th January 2025. Transposition of the EU NIS 2 directive continues across many countries with implementation to follow. Many critical infrastructure providers are reviewing their security and resilience posture in 2025 as national regulations become clearer. The EU Cyber resilience regulation came into force on the 23rd October 2024, starting the implementation clock for product cyber security, while the first set of EU AI regulations will come into force in February 2025 prohibiting use of AI systems which pose unacceptable risks.

The UK government's Cyber Security and Resilience bill will be tabled in Parliament in the midst of a climate of growing concern over state cyber attack, while we also wait to see the final form of the Digital Information and Smart Data bill with the promised modernisation and strengthening of the Information Commissioner's Office.

The regulatory environment at Federal level in the US will be less certain as the Trump administration strikes its balance between free market innovation and heavy weight regulation, but we can expect to see key states such as New York and California continue to develop their cyber security regimes. Globally it seems to be open season on cyber regulation with nations worldwide strengthening their critical infrastructure protection, developing their concept of national sovereignty in cyberspace and worrying about protection of their information space and the hearts and minds of their citizens.

Global companies will face the daunting task of adopting cyber security policies that can cater to the diverse requirements in varying regions, such as the EU, US, Asia, and the Far East; while also trying to genuinely manage cyber risk rather than focussing purely on regulatory compliance.




**These are Beyond Blue's cyber security predictions for 2025.**

**There will undoubtedly be some surprises along the way!**

**One thing seems certain, cyber security, privacy and resilience will feature on board agenda for some time to come.**





BEYOND  
blue