Cyber Security Predictions

for 2026

A look forward to the coming year

Huntsman®

Defence-Grade Cyber Security

Introduction

Each year, as Huntsman Security sets out to forecast what lies ahead, we are reminded of just how difficult it is to predict the course of technology, cyber security, and the world at large. The pace of change is relentless, and the stakes for organisations continue to rise.

Artificial intelligence remains the most visible driver of both opportunity and risk. Just as we saw during the rapid adoption of e-commerce, smartphones, and the cloud, the promise of innovation is shadowed by new avenues for exploitation. While defenders continue to harness AI for automation and detection, adversaries will be equally quick to adapt it for deception and disruption. This tension underpins much of the uncertainty we face in the year ahead in cyber security and beyond.

The broader global environment has also shifted in ways that few anticipated. Last year, when compiling our predictions, we debated the impact of political outcomes in the United States on cyber security and technology markets worldwide. Yet the reality of what has unfolded has been even more complex than expected. Given that much of technology, software and even capital flows originate from the US, changes in leadership there have dislocated international relationships, global supply chains, and ultimately security postures in Europe, Asia, and closer to home.

The past year has also brought no shortage of sobering reminders of the consequences of weak cyber resilience. Attacks that once seemed limited to data theft or website outages have spilled over into highly visible, real-world disruptions - from interrupted services to empty supermarket shelves. Such events have sharpened public awareness of cyber risks, and with visibility comes pressure for organisations to respond more swiftly and effectively.

This year's predictions reflect those realities. They weave together lessons from recent history, today's advances, and tomorrow's uncertainties. We recognise that the future rarely unfolds exactly as we imagine, but by exploring potential scenarios we can help organisations prepare with greater resilience and foresight.

We hope this report not only informs but also equips you with perspective. If any insight here helps you anticipate and mitigate even a single risk, then these predictions will have served their purpose.

Looking to 2026 and beyond, we anticipate the following six areas will have noteworthy impact on the cyber security landscape:

1. **Geopolitical and economic uncertainty becomes the baseline**
2. **The first major AI-driven cyber security breach**
3. **A turning point for cyber security regulation**
4. **Zero tolerance for avoidable breaches**
5. **Ransomware expands its reach: New sectors get noticed**
6. **Secure by Design moves from principle to practice**

Huntsman®

1 Geopolitical and economic uncertainty becomes the baseline

The outlook for 2026 remains clouded by persistent geopolitical and economic volatility. Since the inauguration of the 47th President, policy shifts and economic strategies have been fast-moving.

This always transactional and, at times almost random, pattern of behaviour will continue to make long-term strategic planning difficult. Ongoing global conflicts, including the war in Ukraine, disquiet about the Middle East and conflicts in sub-Saharan Africa show few signs of resolution, while tensions in the Asia–Pacific continue to draw international attention.

For cyber security teams, these prevailing conditions are expected to foster the ongoing threat of state-backed and politically motivated cyber activity. Offensive cyber capabilities are increasingly being spoken of as part of routine geopolitical initiatives, a trend reflected in the world's hot spots and in the rising cyber security budgets of the UK, the EU and others. At the same time, changes in the US administration, such as the refocusing of some key cyber defence agencies, has the potential to reshape intelligence-sharing and defence cooperation.

Economic policy unpredictability adds another layer of complexity to future planning. Sanctions, shifting US tariff positions, and inflationary pressures make strategic planning more challenging for enterprises and global governments too. This has already prompted some organisations in Europe and Canada to diversify their trade arrangements away from US-dominated supply-chains, whether as part of formal government procurement strategies or in response to public sentiment.

In the cyber security market, this may open up opportunities for non-US vendors to gain traction in regions seeking greater certainty in their supply chain independence. Varying levels of jurisdictional impact on the adoption of AI will equally require that technology customers and providers operate with agility and adaptability in the rapidly shifting trade, regulatory, and geopolitical landscapes.
In 2026, uncertainty itself may well prove to be the only constant.

The first major AI-driven cyber security breach

AI technologies have advanced rapidly in recent years, and this momentum is expected to continue into 2026. While innovation continues, controls, safeguards and enabling infrastructure has generally lagged behind, to create potential vulnerabilities.

There have already been incidents involving data privacy, the provenance of AI models and their training data as well as the quality of outputs. At the same time, cyber attackers are increasingly leveraging AI to craft more sophisticated phishing campaigns, identify security weaknesses and even automating exploit development.

The recognised gap that is emerging between cyber threats and our collective ability to defend against them; may well mark 2026 as the year of the first major AI-driven cyber security breach. Given the gaps that remain around AI governance and the challenges many organisations face in maintaining strong security postures, it is increasingly plausible that AI-enabled attacks will exploit vulnerabilities in our defences. With significant data loss, operational disruption, or impacts to the availability of critical infrastructure services being just the start.

Reports indicate that AI-enhanced malicious tools have already reached customers, and researchers continue to assess the capabilities of AI-powered attackers.

While AI promises to enhance defensive capabilities as well, the dual-use nature of this technology means that both defenders and adversaries will likely see performance gains—heightening the stakes across the cyber security landscape – unless the efforts of defenders are better supported.

A turning point for cyber security regulation

Several significant cyber security and operational resilience measures in Australia, the UK, and Europe are expected to move from transitional status to active enforcement. While timelines have shifted in recent years due to consultation processes, legislative steps, and governance reviews, many frameworks now appear to be nearing full implementation.

For organisations, this is likely to mean a narrowing window for preparation. Those that have already invested in governance structures, control frameworks, and reporting mechanisms will probably find the transition smoother. Although, some may find that their new regulatory obligations don't perfectly match their current cyber security framework, and need to accelerate efforts to align with evolving requirements.

These developments are likely to drive broader adoption of objective, evidence-based risk management practices, as well as more structured reporting and oversight. For leadership teams, the ability to demonstrate compliance, and identify areas of emerging threat exposure, will become increasingly important in maintaining trust with regulators, partners, and customers.

While the exact timing and scope of enforcement will depend on finalised regulations and rollout schedules, the direction is clear: expectations around cyber governance are rising. Businesses that embed routine proactive, transparent risk management into their operations in 2026 will be better positioned to navigate both regulatory scrutiny and an evolving threat landscape.

EU: DORA	Took effect 17 January 2025
EU: Cyber Resilience Act	Mandatory reporting starts 11 September 2026 Most provisions apply from 11 December 2027
EU: Cyber Solidarity Act	Took effect 4 February 2025
Australia: Security of Critical Infrastructure Act	Positive reporting obligations delayed to September 2025 Telecoms rules live April 2025 March 2026 smart device standard in force
Australia: APRA – CPS230	Took effect in July 2025
UK: Cyber Security & Resilience Bill (NIS)	Likely to be enacted in 2026
UK: Defence Cyber Certification (DCC)	Audit scheme goes live in 2025. Likely to appear in new contracts 2026
Japan Active Cyber Defense Law	Enacted May 2025
Ireland: National Cyber Security Bill (NIS2)	Expected to be enacted by end of 2025
UN Convention Against Cybercrime	Ratification from late 2025

Zero tolerance for avoidable breaches

By 2026, tolerance for preventable cyber security breaches is expected to reach an inflection point, where for the majority of mainstream players, evidence of cyber security posture will become a precondition of commercial arrangements.

Over the past year, incidents in retail, healthcare, and the leisure and hospitality sectors (leading to downtime, data loss, or service disruption) have reinforced the nature and debilitating impact of basic, and sometimes familiar, security lapses. Weak remote access controls, missed patches, reused passwords, and unsecured administrative accounts remain amongst the most common root causes of attack.

Frustration is growing across business leadership, consumers, regulators, and the cyber security community that some organisations continue to fail to uphold their cyber security responsibilities as a routine part of their operations. Certainly, regulators' increasing demand for accountability, and holding organisations responsible for the performance of their 3rd party suppliers will bring change. So too will the growing level of digital connection and recognition of the operational disruption caused by poor cyber hygiene.

Demands for improved performance will increasingly galvanise like-minded partners; with those that cannot, or will not, keep up having their participation in supply chains and access to the broader economy curtailed. The commercial reality is that the non-negotiable price of a commercial relationship will become, at least in part, an evidence-based cyber bill of health.

This shift will accelerate the adoption of advanced protection capabilities such as Continuous Threat Exposure Management (CTEM), and a newer generation of more reliable data-driven threat exposure management platforms that will replace obsolete manual processes. Unlike older scanning or survey tools, these solutions offer continuous visibility, reporting and remediation guidance.

The tightening of enforcement across a growing number of sectors, and the mandatory reporting of ransomware payments (and the pending outright prohibition in the UK), will shift demonstrable cyber security from a "nice-to-have" to a must have in 2026. This will fundamentally raise the baseline of what constitutes acceptable cyber risk management and what is no longer fit for purpose.

Ransomware expands its reach: new sectors get noticed

Until recently, industries like retail were often viewed as lower-profile cyber targets. Important, but not as critical as finance, energy, or healthcare.

That perception shifted in 2025, when a series of UK retail sector breaches caused online systems to go dark with a major disruption and empty shelves, in some stores, for weeks. The incidents dominated public discussion for some time, and showed how even in sectors not traditionally considered as "risky" a ransomware attack can quickly escalate to a critical incident.

The same applies to other seemingly lower-priority industries too: clothing, DIY goods, passenger transport, and the support services that many organisations depend on. Well targeted malware attacks can reward the hacker with profitable data theft and unsettle public confidence – all at the same time.

Recent expansions of regulatory frameworks such as NIS2, DORA, and SOCI already acknowledge the critical role of online service providers, cloud platforms, and payment processors. However, sectors not yet covered by such regulation should monitor their cyber posture and not become a soft target. Personal information continues to be prized by hackers and high-profile attacks can be quickly leveraged for profit by ransomware and other malicious actors.

In 2026, this growing awareness is likely to translate into increased threat activity targeting industries that previously sat outside the traditional "critical infrastructure" spotlight.

For organisations in these sectors, as higher profile targets address their threat exposure, less obvious targets too will need to strengthen their cyber resilience to avoid becoming victim to a high-profile incident that puts them on the front page.

Secure by Design moves from principle to practice

"Secure by Design" will continue to gain traction as both a regulatory expectation and a market differentiator.

While some pillars are already being adopted by both customers and vendors, the coming year is likely to bring greater emphasis on secure product design, development and operation and the rigour and quality of those processes.

These shifts are being shaped by evolving legislation, procurement standards, and a growing focus from both governments and enterprises on vendor management and supply chain integrity. "Secure by Design" principles go beyond code quality, to embrace the governance of design processes, development environments, operational integrity and assurance processes that validate product resilience over its lifecycle.

For technology producers, this will mean tighter security controls across the design and manufacturing environment, more rigorous development oversight, and higher assurance levels across all parts of the product value-chain.

For buyers and end users, the impact may be less visible, but the products and services they rely on should be more resilient and fit for purpose, with fewer vulnerabilities and reduced risk of compromise at the source.

While much of this work will happen behind the scenes, 2026 has the potential to be the year when investment in secure product design begins to embed itself into industry norms, quietly but fundamentally bringing the performance parameters for security technology into sharper focus in the years ahead.

Huntsman Security

Cyber Security Predictions for 2026

1 Geopolitical and economic uncertainty becomes the baseline

2 The first major AI-driven cyber security breach

3 A turning point for cyber security regulation

4 Zero tolerance for avoidable breaches

5 Ransomware expands its reach: New sectors get noticed

6 Secure by Design moves from principle to practice

2026
Huntsman

About Huntsman Security

Since 1999, Huntsman Security has been on the cutting-edge of cyber security software development, serving some of the most sensitive and secure intelligence, defence and criminal justice environments in the world.

Huntsman®

HUNTSMAN | TIER-3 PTY LTD

ASIA PACIFIC

t: **+61 2 9419 3200**
e: **info@huntsmansecurity.com**

Level 2,
11 Help Street
Chatswood NSW 2067

EMEA

t: **+44 845 222 2010**
e: **ukinfo@huntsmansecurity.com**

7-10 Adam Street,
Strand
London WC2N 6AA

NORTH ASIA

t: **+81 3 5953 8430**
e: **info@huntsmansecurity.com**

GINZA EAST SQUARE 4F
3-12-7 Kyobashi Chuoku, Tokyo
Japan 104-003

huntsmansecurity.com

linkedin.com/company/tier-3-pty-ltd

twitter.com/Tier3huntsman