CYBERSECURITY

REPORT 2026

ATTACKS ARE ON THE RISE AGAIN – WHAT YOU NEED TO KNOW

ABOUT HORNETSECURITY

Hornetsecurity empowers companies and organizations of all sizes to focus on their core business by protecting M365 workloads, email communications, securing data, and ensuring business continuity and compliance with next-generation cloud-based solutions.

Our flagship product, 365 Total Protection, is the most comprehensive cloud security solution for Microsoft 365 on the market and includes email security, compliance, governance, and backup.

WHAT IS THE CYBERSECURITY REPORT?

The Cybersecurity Report by Hornetsecurity is an annual analysis of the current threat landscape based on real-world data collected and studied by Hornetsecurity's dedicated Security Lab team. Hornetsecurity processes more than 6 billion emails every month. By analyzing the threats identified in these communications, combined with a detailed knowledge of the wider threat landscape, the Security Lab reveals major security trends, threat actor campaigns, and formulates informed projections for the future of Microsoft 365 security threats, enabling businesses to act accordingly. Findings and data from 2025 and projections for 2026 are contained within this report.

WHAT IS THE SECURITY LAB?

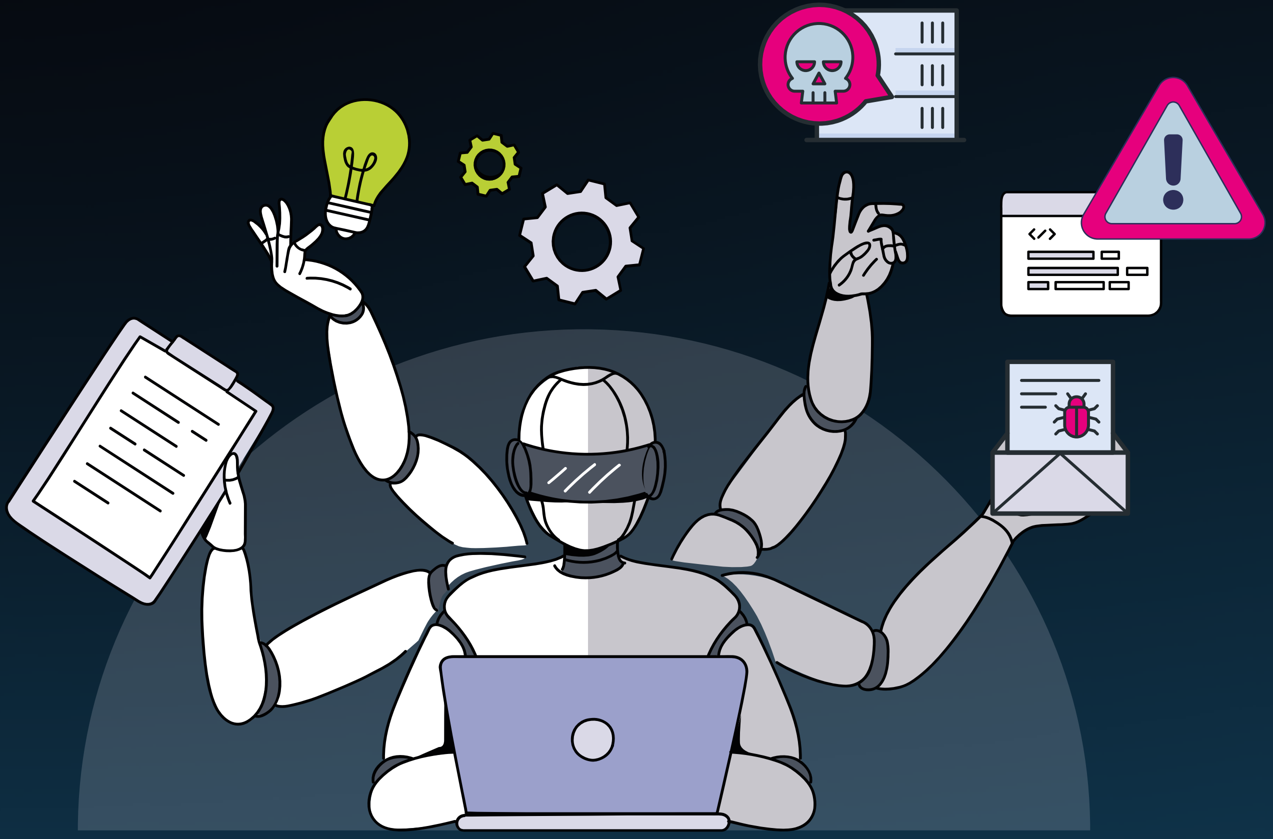
The Security Lab is a division of Hornetsecurity that conducts forensic analysis of the most current and critical security threats, specializing in email security and the Microsoft 365 ecosystem. This multinational team of security specialists has extensive experience in security research, software engineering, and data science.

An in-depth understanding of the threat landscape established through hands-on examination of real-world phishing attacks, malware, ransomware gangs and more, is critical to developing effective countermeasures. The detailed insights uncovered by the Security Lab serve as the foundation for Hornetsecurity's next-gen cyber-security solutions.

HOW TO USE THIS REPORT

This report contains five main sections:

- Chapter 1 is the Executive Summary.
- Chapter 2 focuses on the current threat landscape of the Microsoft 365 platform.
- Chapter 3 covers current concerns and discussions regarding the biggest threats and trends from 2025.
- Chapter 4 contains predictions from the Security Lab about cyber-security threats in 2026, along with advice and guidelines to help protect your business.
- Chapter 5 lists all the references and supporting links used in this report.



BALANCING INNOVATION AND THREAT:
THE DUAL NATURE OF AI

CHAPTER 1

EXECUTIVE SUMMARY

2025 has been a year defined by acceleration. Threat actors embraced automation, artificial intelligence, and social engineering at unprecedented speed, while defenders raced to adapt governance, resilience, and awareness programs to match. What we observed across the Hornetsecurity ecosystem, via our analysis of over 72 billion emails processed, confirms a simple truth: the attack surface is expanding faster than most 72 organizations can secure it.

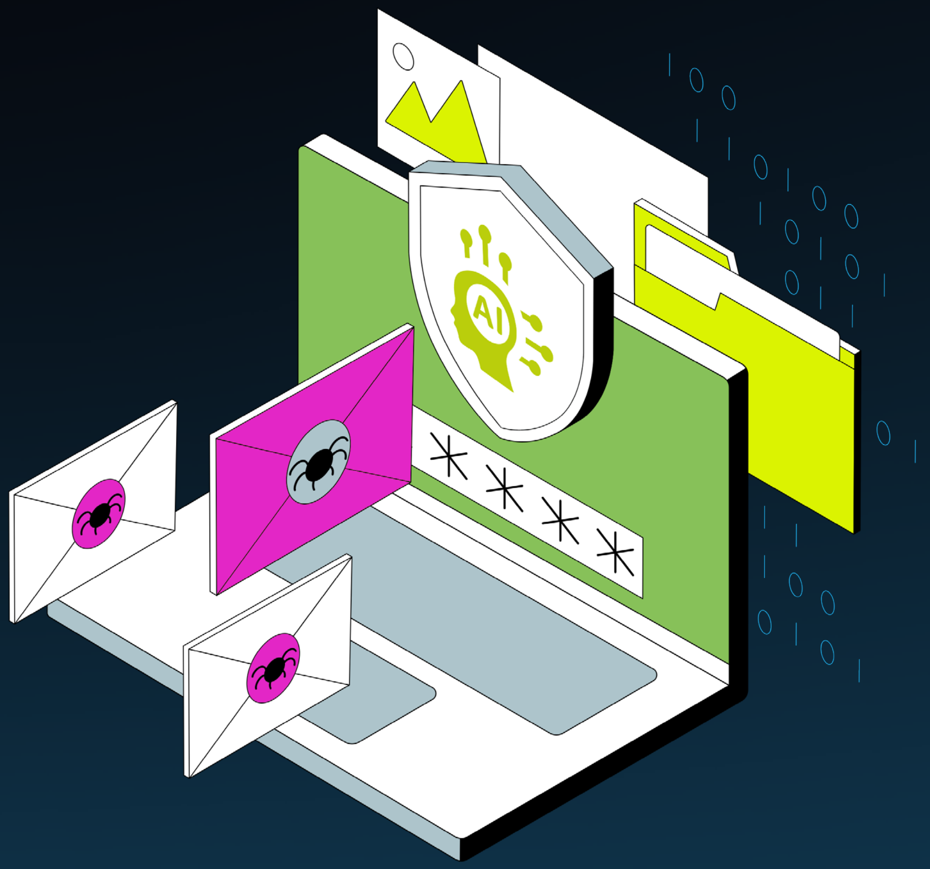
Email remains the most consistent delivery vector for cyber threats, but tactics have evolved. Malware-laden emails surged by **131% year-over-year**, accompanied by a rise in **scams (+34.7%)** and **phishing (+21%)**. Attackers have traded blunt-force volume for precision evasion, leveraging legitimate infrastructure, obfuscated URLs, and stealthy HTML techniques to bypass filters and human visibility alike. Meanwhile, malicious TXT and legacy DOC attachments, once considered to be largely benign or outdated, have re-emerged as primary infection vehicles, highlighting how even “low-risk” file types can no longer be ignored.

Ransomware also made an aggressive comeback in 2025. After several years of relative decline, **24% of organizations** reported being victims. This is a 29% increase from the previous year. While immutable backups and improved disaster recovery planning have lowered ransom payment rates to just **13%** of cases, attackers have responded by diversifying entry points and objectives. Phishing, compromised credentials, and endpoint exploitation now share equal footing as infiltration paths, and new “Ransomware 3.0” variants are beginning to focus less on encryption and more on data integrity manipulation corrupting trust itself rather than just availability.

Artificial Intelligence has reshaped both sides of the security equation. CISOs are optimistic but cautious: **61% believe AI has directly increased ransomware risk**. CISO concerns around AI are vast. They include things like phishing automation to deepfake impersonation and model poisoning. AI’s potential for misuse has become a defining feature of the threat landscape. Yet the defensive side is catching up, with **68% of organizations investing in AI-powered detection and analytics**. The challenge for organizations and security teams in 2026 is governance and working towards harnessing AI’s capabilities without amplifying the risks.

The Hornetsecurity Security Lab forecasts that the coming year will see continued **uncontrolled adoption of AI tools** across enterprises, often faster than legal or security teams can evaluate. This, paired with the **weaponization of agentic AI**, will magnify existing vulnerabilities while introducing new ones that defy traditional containment models. Identity, too, remains the primary battlefield: attacker-in-the-middle kits, compromised browser extensions, and OAuth abuse show that credentials and identity continue to be the weak link in modern cloud ecosystems.

Despite this rising complexity, there are reasons for optimism. Organizations are steadily maturing. The adoption of **Zero Trust principles, immutable backup technologies, and phishing-resistant MFA** are becoming baseline expectations rather than aspirational goals. Security awareness, once a compliance checkbox, is increasingly embedded in company culture. The path forward is clear: resilience, not perfection, is the new metric of success. Those who treat cybersecurity as a core element of business continuity and not **just** an IT issue will be best positioned to thrive in 2026’s evolving threat landscape.



SMART DEFENSE:

HOW AI SHIELDS YOUR INBOX

CHAPTER 2

THE STATE OF SECURITY IN THE INDUSTRY

EMAIL SECURITY TRENDS

Email remains the backbone of business communication and, as our data shows, it also continues to be the primary battleground for attackers. 2025's classification and threat-type shifts reveal two simultaneous realities: attackers are experimenting with new file types and low-effort delivery methods (TXT and legacy DOC surged), and at the same time social engineering remains a consistent lever for compromise.

Put simply: quantity and quality are changing. While classic spam volumes have stabilized after normalization, higher-impact categories (Malware, Scam, Phishing, etc.) are growing substantially. That combination (more dangerous content delivered at scale) increases the likelihood that even well-defended organizations will face incidents unless they adjust detection, user awareness, and recovery practices.

Spam, Malware, & Advanced Threat Metrics

The headline numbers are unambiguous: **Malware** saw the largest relative increase (+130.92%), followed by **Scams** (+34.70 %) and **Phishing** (+20.97 %). Those three categories account for the bulk of the risk that results in operational impact (data theft, encryption, business disruption). Meanwhile, categories that traditionally represented lower business risk; legitimate Messages, Transactional, and Commercial Email moved only modestly, indicating that malicious actors are concentrating effort on higher-value attack types.

Key implications:

- **Proliferation of malicious payloads**. A 131% jump in Malware classification means more emails are carrying active payloads (or at least payload indicators) rather than simple noise. Detection strategies must assume malicious intent either way.
- **Scams and advanced social engineering are on the rise**. Scams (+34.7 %) coupled with Phishing (+21.0 %) signals that attackers are refining their lures and ROI. They're making more convincing frauds, and more customized messages, likely enabled by generative AI technologies.
- "**Dirty Commercial**" **growth undermines heuristic filters**. Dirty Commercial Emails (+17.72 %) suggests attackers may be weaponizing lower-quality marketing templates to evade simple content filters and blend in with legitimate marketing traffic.
- **Targeted spear-phishing share is down, but not gone**. Suspect/Spear-Phishing is down (-9.75 %), which likely reflects a shift to more automated/commodity phishing and to credential-theft approaches that bypass classic spear phishing detection. Don't be lulled into complacency: targeted attacks remain high-impact even at lower volume.

EMAIL CLASSIFICATION CATEGORIES

Category	Adjusted YoY Change 2025 vs. 2024
Malware	+130.92 %
Scam	+34.70 %
Phishing	+20.97 %
Dirty Commercial Emails	+17.72 %
Commercial Email	+2.37 %
Legitimate Messages	+3.38 %
Transactional	+3.19 %
Spam	+0.03 %
Social	-8.05 %
Suspect / Spear Phishing	-9.75 %
Pro Commercial Emails	-13.73 %
Bounce	-18.69 %

Note: Calculations take into account and adjust for sample size changes from year to year.

CATEGORY CLASSIFICATION DESCRIPTIONS

Spam
Unsolicited bulk email messages sent to a large number of recipients, typically for advertising or malicious purposes.

Phishing
Fraudulent emails designed to trick recipients into revealing sensitive information such as passwords, credit card numbers, or personal data.

Commercial Email
Legitimate marketing or promotional emails sent by businesses to customers or prospects, often for product announcements or offers.

Legitimate Messages
Authentic, non-promotional emails exchanged between individuals or organizations for normal communication purposes.

Pro Commercial Emails
Professional-grade marketing emails, often highly targeted and personalized, typically used in B2B campaigns.

Transactional
Emails triggered by user actions or system events, such as order confirmations, password resets, or account notifications.

Social
Emails originating from social media platforms, including notifications, friend requests, and activity alerts.

Bounce
Emails that fail to deliver to the recipient's inbox due to invalid addresses, full mailboxes, or server issues.

Dirty Commercial Emails
Marketing emails that violate compliance standards or best practices, often poorly formatted or misleading.

Scam
Emails intended to defraud recipients, often involving fake offers, lottery winnings, or impersonation schemes.

Malware
Emails containing malicious attachments or links designed to install harmful software on the recipient's device.

Suspect/Spear Phishing
Highly targeted phishing attempts aimed at specific individuals or organizations, often using personalized details to appear credible.

ATTACK TECHNIQUES USED IN EMAIL ATTACKS 2025

The 2025 attack-technique landscape shows a clear preference for evasion-first tactics: attackers are less focused on single flashy payloads and more on slipping past filters and human suspicion. The top techniques: header forgery, subtle HTML tricks, use of legitimate hosting, and URL obfuscation are all optimized to blend malicious intent into otherwise benign-looking mail. That shift explains why we're seeing fewer obvious spear-phish samples but more successful credential-theft and multi-stage intrusions: the email is the first step, not the punchline.

Key observations:

- **Header and metadata manipulation dominate**. Fake From and manipulated spam-related headers top the list, demonstrating that spoofing and metadata tampering remain low-cost, high-impact methods to defeat naive filtering and trigger human trust.
- **Abuse of legitimate infrastructure is rising**. Sending campaigns via reputable hosting platforms makes malicious mail appear to come from trustworthy sources. This is a tactic that increases deliverability and reduces immediate filter suspicion.
- **URL obfuscation is ubiquitous**. URL shortening, non-ASCII characters, exotic TLDs (Top Level Domains), and domain fuzzing are all simple ways to hide destination intent and bypass blocklists or visual inspection.
- **HTML/MIME tricks aim to confuse detectors, not readers**. Empty <a> tags, multi-part messages, and zero-(size)-font insertion are designed to mislead signature and keyword-based scanning engines while preserving readability for recipients.
- **Automated, high-volume evasion beats small-scale targeting**. These techniques scale: attackers can roll out many campaigns that individually look benign but collectively yield credential captures, account compromise, or chained downloads.

TOP 10 ATTACK TECHNIQUES USED IN EMAIL ATTACKS IN 2025

Rank	Technique
1	Fake From Header Alteration
2	Fake Spamcause Header Alteration
3	Leverage Legit Hosting Platform to Send Campaign
4	Use of Exotic or Non-Existent TLDs
5	URL Shortening
6	HTML <a> Tag Empty
7	Multi-Parted Emails
8	URL with Non-ASCII Characters
9	Random Domains / URL Fuzzing
10	ZeroFont Technique

TECHNIQUE DESCRIPTIONS

1. *Fake From Header Alteration*
   Attackers forge the "From" header in emails to impersonate trusted senders, tricking recipients into believing the email is legitimate.

2. *Fake Spamcause Header Alteration*
   Manipulation of spam-related headers to bypass spam filters and make malicious emails appear safe.

3. *Leverage Legit Hosting Platform to Send Campaign*
   Using reputable hosting or email services (e.g., cloud platforms) to distribute phishing or malicious campaigns, making detection harder.

4. *Use of Exotic or Non-Existent TLDs*
   Employing unusual or fake top-level domains (e.g., .xyz, .club) to create deceptive URLs that look legitimate.

5. *URL Shortening*
   Using URL shorteners (e.g., bit.ly) to hide the true destination of malicious links, making them harder to detect.

6. *HTML <a> Tag Empty*
   Embedding empty anchor tags in HTML emails to confuse spam filters or hide malicious links.

7. *Multi-Parted Emails*
   Sending emails with multiple MIME parts (e.g., text and HTML) to evade detection by security tools.

8. *URL with Non-ASCII Characters*
   Including special or Unicode characters in URLs to create visually deceptive links (e.g., homoglyph attacks).

9. *Random Domains / URL Fuzzing*
   Generating random or slightly altered domains to bypass domain-based filtering and detection systems.

10. *ZeroFont Technique*
    Inserting zero-size font text in emails to manipulate keyword-based filters while keeping the message readable to humans.

HORNETSECURITY

ATTACHMENT USE AND TYPES IN ATTACKS

Attachment trends in 2025 demonstrate a pronounced pivot in malware delivery strategy. The fastest-growing file carriers are **TXT (+181.39 %)** and **DOC (+118.25 %)**, with ZIP and modern Office formats (DOCX, XLSX) also present but growing more modestly. Legacy or once-popular vectors (HTML, RAR, HTM, XLS) declined, while **ICS** and **SHTML** appear as new entries to our top-ten list. This is a sign attackers are searching for overlooked or under-inspected file types plus calendar files or server-side include vectors.

Key takeaways:

- **TXT and legacy DOC are alarm bells**. TXT files, which are widely treated as "low risk", are being weaponized as staging artifacts (containing obfuscated URLs or scripts). Legacy DOCs (with macro support) remain attractive because many environments still allow or fail to inspect office macros aggressively.
- **Archives STILL matter**. ZIP (+29.82 %) remains a vehicle for payload bundling and evasion; compressed archives continue to be a reliable attacker tactic.
- **Emergence of ICS and SHTML is noteworthy**. Calendar invites (ICS) and server-include variants (SHTML) represent non-traditional vectors that can bypass some mail filters and user expectations. This is especially true for recipients who accept calendar items or preview HTML content.
- **Decline in HTML/HTM/RAR/XLS likely reflects defensive hardening**, but attackers are redirecting to less-monitored channels rather than abandoning email as a vector.

FILE-TYPES FOR MALICIOUS PAYLOADS 2025

File Type	Adjusted YoY Change 2025 vs. 2024
TXT	+181.39%
DOC	+118.25%
ZIP	+29.82%
DOCX	+11.69%
XLSX	+7.85%
PDF	-3.32%
HTML	-27.44%
RAR	-36.93%
HTM	Dropped from top 10
XLS	Dropped from top 10
ICS	New Entry to list in 2025
SHTML	New Entry to list in 2025

Note: Calculations take into account and adjust for sample size changes from year to year.

FILE TYPE DEFINITIONS

PDF
Portable Document Format – Commonly used for documents; attackers often embed malicious links or scripts within PDFs.

DOC
Microsoft Word Document (Legacy) – Older Word file format; can contain macros that execute harmful code.

DOCX
Microsoft Word Document (Modern) – Current Word format; supports embedded macros and scripts that can be exploited.

XLS
Microsoft Excel Spreadsheet (Legacy) – Older Excel format; often targeted for macro-based attacks.

XLSX
Microsoft Excel Spreadsheet (Modern) – Current Excel format; can include malicious macros or links.

TXT
Plain Text File – Simple text files; attackers may use them to deliver phishing content or scripts disguised as text.

HTML
HyperText Markup Language File – Web page format; often used in phishing emails with embedded malicious links.

HTM
HyperText Markup Language File (Variant) – The legacy file extension for HTML files; used for web content and phishing payloads.

SHTML
Secure HTML File – HTML variant supporting server-side includes; can be exploited for malicious redirects.

ZIP
Compressed Archive File – Commonly used to bundle files; attackers hide malware inside compressed archives.

RAR
Compressed Archive File (Alternative) – Similar to ZIP but uses different compression algorithm; often used for malware delivery.

ICS
Calendar File – iCalendar format; attackers use malicious calendar invites to deliver phishing links or payloads.

THE RANSOMWARE RESURGENCE OF 2025

After three consecutive years of decline, ransomware has returned to the forefront of cybersecurity concerns. Hornetsecurity data shows that in 2025, **24 % of organizations reported being victims of a ransomware attack**, up sharply from **18.6 %** in 2024. This reversal shows a flashing red light in the post-pandemic threat landscape and a warning that attackers are evolving with increasing speed.

Despite years of awareness campaigns and training programs, ransomware remains a critical business risk precisely because it adapts to our defenses. Threat actors are now combining **AI-enhanced automation** with tried-and-true social engineering to achieve greater reach, precision, and persistence.

AUTOMATION, AI, AND THE NEW RANSOMWARE PLAYBOOK

Attackers are increasingly leveraging **generative AI and automation** to identify vulnerabilities, craft more convincing phishing lures, and orchestrate multi-stage intrusions with minimal human oversight. This sadly makes ransomware operations more scalable, and more personal.

Some key data points:

- **61 %** of CISOs believe that AI has directly increased the risk of ransomware attacks.
- **77 %** identify **AI-generated phishing** as an emerging and serious threat.
- **68 %** are now investing in **AI-powered detection and protection** capabilities.

The result is an arms race where both sides are using machine learning. For one side the goal is to deceive, the other to defend.

ENTRY POINTS: PHISHING LOSES GROUND, ENDPOINTS RISE

While **phishing remains the leading infection vector at 46 %** of those surveyed, its dominance is slipping. Attackers are diversifying:

Vector	2024	2025	Δ
Phishing/Email-based	52.3 %	46 %	-6,3 pp
Compromised Credentials	~20 %	~25 %	+5 pp
Exploited Vulnerabilities	–	12 %	n/a
Endpoint Compromise	–	26 %	n/a

pp = "Percentage Point"

The data shows a clear pivot toward **credential theft and endpoint compromise**, particularly in hybrid and remote work environments where **BYOD and patch gaps** remain widespread. Ransomware is no longer just an email problem; it's an ecosystem problem.

TRAINING FATIGUE AND THE "FALSE COMPLIANCE" TRAP

Organizations are still investing heavily in awareness training. **74 %** offer it but **42 %** of those feel it's inadequate.

Many programs remain checkbox exercises: annual, unengaging, and quickly forgotten. The result is what Hornetsecurity terms "*false compliance*". This is the illusion of preparedness without meaningful behavioral change.

Small and mid-sized businesses (SMBs) are hit hardest. Many operate with minimal IT staffing and outdated infrastructure, relying on outsourced providers or unpatched cloud tenants. While more **SMBs report having a DR plan**, readiness on paper doesn't always translate into resilience in practice.

RECOVERY AND RESILIENCE: THE SILVER LINING

That said, even as attacks increase, recovery capabilities are quietly improving:

- **62 %** of organizations now use **immutable backup technologies**. These are systems where data cannot be altered or encrypted once the data is written. Not even by administrators or a compromised admin account during an attack.
- **82 %** have implemented a **Disaster Recovery Plan**, which is quickly becoming the new baseline for operational resilience.
- Also in good news, only **13 %** of victims paid the ransom in 2025, down from **16.3 %** in 2024.

The message is clear: organizations are learning to recover without negotiating.

Insurance, however, tells a different story. **Ransomware insurance coverage** dropped from **54.6 %** in 2024 to **46 %** this year, as premiums and exclusions rose and confidence in payouts declined. This market correction suggests that organizations can no longer outsource risk. They must architect security into their systems and build resilience into their culture.

GOVERNANCE: STRATEGY STILL LAGS BEHIND THREAT REALITY

Cybersecurity is now a board-level concern, but many organizations are still catching up to the operational demands of ransomware-era governance. Few boards run cyber crisis **simulations**, and **cross-functional playbooks** remain the exception rather than the rule. As **AI-driven misinformation** and **deepfake extortion** become more plausible, communication readiness is now part of cybersecurity and, thankfully, not a PR afterthought.

OUTLOOK: RESILIENCE IS RISING, BUT SO ARE THE THREATS

The 2025 data paints a nuanced picture: ransomware attacks are increasing, but so is our capacity to recover. The organizations that will weather this new wave are those that **treat resilience as strategy**, not compliance. Immutable backups, well-tested recovery plans, and meaningful user training are no longer optional, they're the minimum viable defense.

Attackers don't stand still, and neither can defenders. The challenge for 2026 won't be preventing ransomware altogether, it will be making sure that when it hits, **business continuity doesn't fail**.

CISO PERSPECTIVES: BALANCING AI PROMISE AND PERIL

Artificial Intelligence is reshaping cybersecurity, and not just as a defensive tool, but as a strategic question. Hornetsecurity's 2025 CISO Insights Poll set out to capture how real-world security leaders are approaching AI: where it's working, where it's risky, and what challenges stand in the way of responsible adoption.

The findings reveal a complex picture. CISOs are enthusiastic, cautious, and in many cases, still experimenting. AI is everywhere but trust, governance, and understanding have, sadly, not yet caught up.

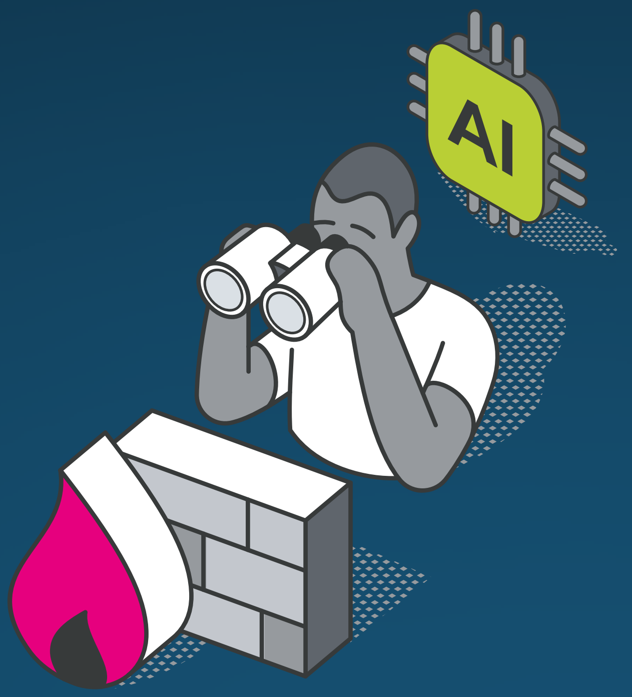
ADOPTION: RAPID GROWTH, UNEVEN GOVERNANCE

Most CISOs surveyed report **significant experimentation with AI**, but structured adoption remains rare. Some organizations are integrating AI into workflows such as triage, enrichment, and ticket management, while others restrict its use entirely.

A CISO from a global finance firm noted, "We're seeing adoption as high as 75 %+ within our organization over the last two years." In contrast, a virtual CISO remarked, "*Two years ago it was open bar on all AI services. This past year, we've started putting in more processes and internal LLMs.*"

The variability shows the core challenge: AI adoption is moving faster than AI governance, like previous innovative trends in the tech space. Many leaders have begun to centralize control and develop internal tools, but others remain in a reactive posture and are chasing compliance rather than leading innovation.

Shadow IT, once a known irritant, has been redefined by AI into Shadow AI Unapproved tools, browser extensions, and SaaS integrations are creating new, opaque risks. As one CISO summarized, "*AI safety concerns have amplified the dangers of shadow IT.*"



END-USER AWARENESS: THE NEW HUMAN RISK FACTOR

If a company is only as strong as its least prepared employee, AI has lowered that bar. CISOs unanimously agree that **end-user awareness of AI risk is dangerously low**. While a few organizations boast strong compliance cultures with some scoring themselves *"5 out of 5"*, most CISOs estimate awareness levels closer to *"1 or 2 out of 5."*

The primary issue? Employees enthusiastically using public AI tools without realizing the security or compliance implications. As one virtual CISO put it, *"People haven't understood the stakes, especially when they share company information in a public AI."*

The consensus: security awareness efforts in-house haven't evolved at the same pace as AI adoption. Focused, scenario-based education is now as important as firewalls and filters.

LEADERSHIP UNDERSTANDING: THE AWARENESS GAP AT THE TOP

CISOs also highlight **a wide disparity in leadership understanding** of AI-related risks. Our polling revealed the broadest spread of responses across this question, ranging from "deep awareness" to "no real understanding." The median answer was a luke-warm "leadership somewhat knows the risks". It's clear that progress is inconsistent and varies widely from business to business.

Some organizations are moving forward collaboratively. A German tech-sector CISO credited joint Legal and Security initiatives for progress: *"Management is beginning to understand the issues related to AI security."* Others, however, report the opposite. *"Management sees the productivity gains but not the risks,"* one virtual CISO said.

This uneven awareness leaves CISOs with dual responsibility: defending against external threats while educating leadership internally.

EMERGING THREATS: DEEPFAKES, MODEL POISONING, AND DATA LEAKS

Nearly all CISOs surveyed agree that **AI misuse will be a major source of cyber risk over the next 12 months**.

The most pressing concerns include:

- **Synthetic identity fraud** using AI-generated documents or credentials
- **Voice cloning and deepfake videos** used for impersonation and fraud
- **Model poisoning**, where malicious data corrupts internal AI systems
- **Sensitive data leakage** through employee misuse of public AI tools

One CISO warned, *"We're most concerned about model poisoning attacks as we run our own models in-house."* Another noted that *"the number one risk of AI is the voluntary leak of company data into public systems."*

AI has become both a tool and a target and the attack surface is clearly expanding faster than many realize.

SECURITY TEAM ADOPTION: CAREFUL, CONTROLLED, AND TACTICAL

Within security operations, AI adoption is measured but growing. CISOs describe limited deployments focused on **specific, low-risk tasks**. For instance, classifying tickets or enriching threat data. One finance-sector CISO shared a practical success story: *"AI turned out great for customer-facing ticket notes. They're concise and bias-free."*

This "cautious optimism" is characteristic of 2025. Security teams are embracing automation but remain wary of overreliance on opaque systems or immature models.

CHALLENGES IN IMPLEMENTATION: THE PRACTICAL BARRIERS

The path to responsible AI adoption is far from smooth. Our CISO poll found that the top barriers include:

- **Uncertainty around AI risks** and potential misuse
- **Compliance and legal constraints**
- **Budget justification and ROI demonstration**
- **Integration challenges** with legacy tools
- **Talent shortages** in AI and data science
- **Leadership buy-in**

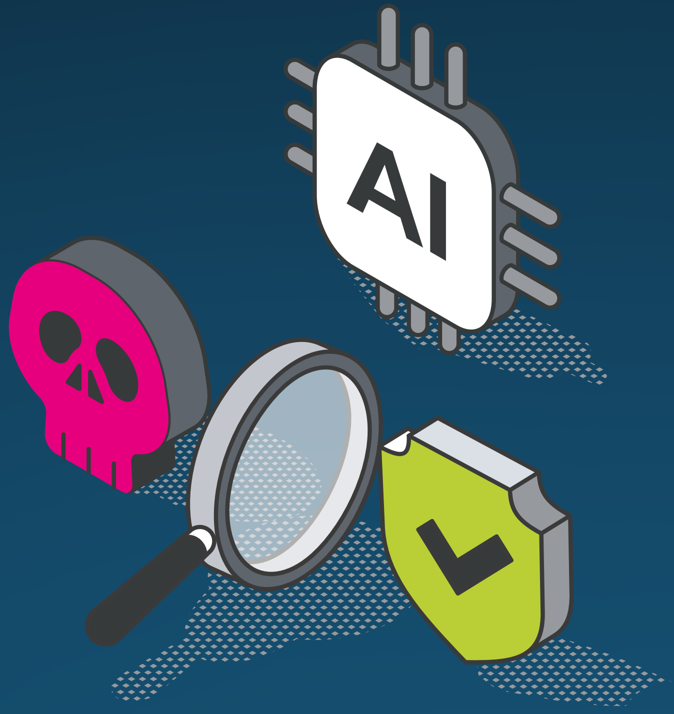
As one CISO summarized, "We still lack skills and specialized experts in AI." Another added, "Detecting a port scan by reading ten lines of logs doesn't bring much value."

Despite the hurdles, CISOs remain pragmatic: AI isn't hype, it's an inevitable evolution. But adoption will remain on a case-by-case basis until transparency, skills, and governance catch up with ambition.

FROM CURIOSITY TO CAPABILITY

AI in cybersecurity is no longer experimental, but neither is it fully mature. Across industries, the focus is shifting from *"What can AI do?"* to *"How do we govern it?"*

The coming year will define whether security teams can transform AI from a risk into a reliable ally.



NO ONE IS IMMUNE:

THREATS TARGET EVERY ORGANIZATION

CHAPTER 3

AN ANALYSIS OF THE MAJOR SECURITY INCIDENTS AND CYBERSECURITY NEWS OF 2025

It's important to use major cybersecurity incidents that organizations suffer as a learning tool, looking at how your business would have handled a similar attack, and how to improve your resiliency going forward. There's been no shortage of examples since our late 2024 report, here are the top eleven we picked.

OCTOBER 2024 – INTERNET ARCHIVE BREACH AND DDOS ATTACK

In early October 2024, the non-profit Internet Archive (known for the Wayback Machine) suffered a significant data breach affecting over 31 million user accounts. Attackers gained access to a 6.4 GB database containing users' email addresses, usernames, and Bcrypt-hashed passwords, among other details. Around the same time, a hacktivist group dubbed BlackMeta launched a series of distributed denial-of-service (DDoS) attacks against the Archive's websites, temporarily knocking them offline. This incident highlighted vulnerabilities in the Archive's configuration management (an exposed GitLab configuration file was reportedly the attack vector).

There are two takeaways from this one. Even if you're a not-for-profit or "too insignificant to be vulnerable", you're always a target. Additionally you should always check your developer's configuration of their code repositories as sufficient MISconfiguration could negatively impact you down the road.

DECEMBER 2024 – U.S. TREASURY HACK BY CHINESE APT

In late December 2024, the U.S. Department of the Treasury disclosed it had been the victim of a state-sponsored cyberattack attributed to the Chinese government. Attackers linked to a Chinese APT (Advanced Persistent Threat) group exploited a supply-chain weakness by compromising an identity and remote support platform from BeyondTrust, a vendor used by the Treasury. By obtaining a BeyondTrust admin key, the hackers were able to remotely access multiple Treasury employees' workstations and steal unclassified documents. Treasury officials labelled it a "major cybersecurity incident" and notified U.S. cybersecurity authorities (CISA) on December 8, 2024, soon after BeyondTrust alerted them to the intrusion. The breach, coming on the heels of other China-linked attacks on U.S. targets, heightened tensions and prompted urgent reviews of third-party access security and government cyber defenses.

The main lesson here is understanding your threat model, and dependency risks. If you have implemented a security solution, where's the "master key" for that security solution? What happens if it's compromised, and how do you detect that before it's too late?

JANUARY 2025 – CRITICAL VPN ZERO DAY EXPLOITS (IVANTI & SONICWALL)

January 2025 saw attackers actively exploiting critical zero-day vulnerabilities in two popular enterprise remote access products, prompting emergency security alerts worldwide. Ivanti (Pulse Secure) disclosed that its Connect Secure VPN appliance contained a critical authentication bypass flaw that was being exploited in the wild. This zero-day, which allowed remote code execution without login, was used to infiltrate at least 17 organizations (including Nominet, the U.K. domain registry) as early as December 2024. Mandiant researchers linked the Ivanti VPN exploits to a China-based threat actor, given the tools and malware used.

Around the same time, SonicWall warned that a zero-day in its Secure Mobile Access (SMA) 1000 series VPN was similarly exploited by attackers. Microsoft and CISA confirmed that the SonicWall flaw – also allowing unauthenticated remote code execution – had been used in attacks, with incidents later in July as well. These back-to-back VPN security failures revealed the alarming potential for adversaries to abuse trusted remote access systems, leading organizations worldwide to rush out critical patches and mitigations.

These are but two examples of a trend over the last few years, where the very technology you've deployed to protect your network (firewalls, VPN appliances) are so poorly architected and maintained that they instead serve as an easy access point for attackers into your environment. No matter the size of your vendor, you must demand better from them. Procuring security tech to protect you that makes you more vulnerable just isn't acceptable.

MARCH 2025 – JUNIPER NETWORKS ROUTER ESPIONAGE CAMPAIGN

In March 2025, cybersecurity firm Mandiant revealed an ongoing espionage campaign targeting network infrastructure. A China-nexus APT group (UNC3886) had been exploiting a newly discovered vulnerability in Juniper Networks' Junos OS, the operating system for Juniper routers. Starting in mid-2024, the attackers used this zero-day to gain access to enterprise and possibly government routers, then implanted custom backdoor malware on the devices. These stealthy backdoors allowed the hackers to monitor network traffic, and they potentially pivoted further into networks without detection. Juniper patched the flaw once it was discovered, but the incident drew comparisons to past supply chain and infrastructure attacks. It underscored that advanced threat actors are now directly targeting network routers and firewalls to conduct long-term espionage, bypassing traditional endpoint security.

This incident is something you can take directly to your networking team. Routers and switches are part of the "plumbing" of your infrastructure and once deployed tend to be mostly forgotten as long as they work. This also makes them a great place for attackers to hide, particularly as you can't run Endpoint Detection and Response (EDR) on them, so make sure to monitor them for configuration changes, and keep them patched.

JUNE 2025 – UNFI RANSOMWARE ATTACK DISRUPTS FOOD SUPPLY CHAIN

In June 2025, a ransomware attack on United Natural Foods, Inc. (UNFI), a leading food distribution company, demonstrated the real-world impact of cyberattacks on supply chains. UNFI, known as the primary distributor for Whole Foods and other grocers, detected unauthorized activity on its IT systems on June 5. To contain the threat, the company took affected systems offline, which temporarily crippled its ability to process orders and make deliveries. As a result, some grocery retailers experienced product shortages and delivery delays. The disruption continued for multiple days, and UNFI stated that the incident would cause ongoing operational delays and additional costs. The food supply chain impact garnered attention from regulators and highlighted the need for stronger cyber defenses in distribution and manufacturing sectors, as even brief outages can have cascading effects on consumers.

If your business provides a service that's part of larger mesh of companies where an interruption can cause a cascading effect, reaching the public or critical infrastructure, your risk modeling must include this, not only the immediate effect a cyber-attack can have on your own operations. Because in the public's eye (and regulators' view), you'll be held responsible for those wider impacts.

JULY 2025 – SCATTERED SPIDER HACKS (AIRLINES AND RETAIL – QANTAS BREACH)

In some reporting of various incidents over the last few years, "Scattered Spider" has been called a hacking group. This isn't quite accurate, as it's more a loose affiliation of many different actors, with similar tactics, thus it's more accurate to refer to "Scattered Spider-like" techniques. Their approach relies heavily on social engineering, tricking (often outsourced) helpdesk staff to reset credentials. It's less about hacking computers, and more about hacking people. Another notable difference compared to many other threat actors is that they are young, they live in western countries and are native English speakers, predictably leading to many of them being arrested over the last year or two.

Earlier in 2025, Scattered Spider had been linked to attacks on major British retailers (Marks & Spencer, Co-op, Harrods) and insurance firms like Aflac. In July 2025, the group turned its attention to the aviation sector. Qantas Airways, Australia's flag carrier, announced that a third-party contact center platform it uses was compromised, exposing the records of approximately 6 million customers. Stolen data included names, contact details, birth dates, and frequent-flyer numbers, though not financial information. Qantas confirmed it was facing an extortion attempt related to the breach, and cyber investigators noted the attack bore the hallmarks of Scattered Spider's tactics. Around the same time, WestJet (Canada) and Hawaiian Airlines (USA) were also reportedly hit in related incidents.

The main lesson to take from these attacks is to look at your helpdesk procedures, particularly for resetting credentials ("I've lost my phone"), especially for high privilege accounts. All the usual knowledge-based verification details (employee ID, managers name, mother's maiden name etc.) is information that can be gleaned from LinkedIn and other social media and it's not strong enough. As a first step, require anyone recovering a privileged account to do so in person at a company office.

JULY 2025 – INGRAM MICRO RANSOMWARE ATTACK

In the first week of July 2025, Ingram Micro, one of the world's largest IT distribution companies, was knocked offline by a critical ransomware attack. On July 4, reports emerged that Ingram Micro was experiencing a major systems outage; the company soon confirmed it had been hit by a ransomware incident and had proactively taken many systems offline to contain it. The attack disrupted Ingram's operations globally, shuttering its online ordering and logistics systems for nearly a week. By July 10, the distributor had restored all business operations, but not before significantly impacting resellers and partners who rely on Ingram's supply chain services. Cybersecurity journalists identified a relatively new ransomware group called SafePay as the culprit.

Unlike UNFI above, Ingram Micro has no public facing presence, but the lesson here is that if your business is critical to many others operating smoothly, an interruption (in this case for more than a week) will severely impact others, and leading to increased pressure to pay, which is something that you must include in your threat assessment.

JULY 2025 – "TOOLSHELL" ZERO DAY ATTACKS ON MICROSOFT SHAREPOINT

In July 2025, security researchers warned of an ongoing wave of cyberattacks exploiting new zero-day vulnerabilities in on-premises Microsoft SharePoint Servers, collectively dubbed "ToolShell." By July 23, over 400 SharePoint servers worldwide had been compromised via this exploit chain. We published a blog post with more details about this attack here. The attacks allowed unauthorized access and code execution on SharePoint hosts, effectively giving attackers a foothold in victims' corporate networks. A mix of victims were reported, including private sector firms and at least a few U.S. government agencies; even the U.S. Department of Energy confirmed it was "minimally impacted". Microsoft's threat intelligence teams attributed the activity to multiple Chinese state-sponsored groups (codenamed Linen Typhoon, Violet Typhoon, and Storm-2603) that rapidly adopted the exploits once they became known. Separately, criminals linked to a new ransomware called Warlock also leveraged ToolShell to infiltrate organizations and deploy malware. Microsoft released patches for the SharePoint flaws, and, along with agencies like CISA, urged all organizations to update immediately.

The take-aways here are to carefully evaluate whether you still want to rely on on-premises software (from any vendor) as that's often not the focus of the vendor in favor of their SaaS offerings, and if you must, make sure these systems aren't publicly accessible. Protect them with a VPN, or better yet, a cloud-based SASE solution. You must also make sure to have a patch program in place to keep these servers up to date.

AUGUST 2025 – SALESLOFT+DRIFT

In late August 2025 it became evident that Salesloft, an integration for Salesforce (and Slack / Pardot) had been compromised, and Salesforce disabled the Drift integration to these systems. The attack actually started in June 2025, with the Salesloft GitHub account being compromised, followed by access to their AWS environment, where the threat actors obtained OAuth tokens to Drift's customers environments. This type of supply chain attack where compromising a single vendor can potentially give the attackers access to hundreds of victim's organizations is particularly dangerous. OAuth tokens are incredibly powerful, and once they're in the criminal's possession, only revoking them and the integration itself will protect you, not MFA or resetting credentials (unlike with compromised user credentials). The list of victims is long, and includes BeyondTrust, CloudFlare, CyberArk, Nutanix, Palo Alto Networks, Qualys, Rubrik, Tenable and Zscaler.

Incident response is challenging because if you're impacted, you must establish what data the integration had access to, what additional credentials for other systems might be available in that data (and so on) and then reset all of those credentials. There's also the risk of exposure, or fines, depending on the content of the data that was exfiltrated. The lesson here is exactly what we highlighted in last year's report, non-human identities and integrations via APIs and OAuth across cloud and your different SaaS vendors must be monitored for anomalous activity. It's part of the identity fabric, not supervised, and incredibly attractive to attackers because of it.

SEPTEMBER 2025 - JAGUAR LAND ROVER

On Monday the 1st of September 2025 Jaguar Land Rover (JLR) production ground to a halt across their UK, Slovakia, Brazil and Indian factories. As this is an ongoing situation, and only limited production has resumed at the time of writing four weeks later, this ransomware attack has had a huge impact across JLR themselves and their suppliers. Technical details aren't available yet, but most of JLR's IT systems were outsourced to Tata Consultancy Services (TCS), part of the Tata Group, JLR's owners since 2008.

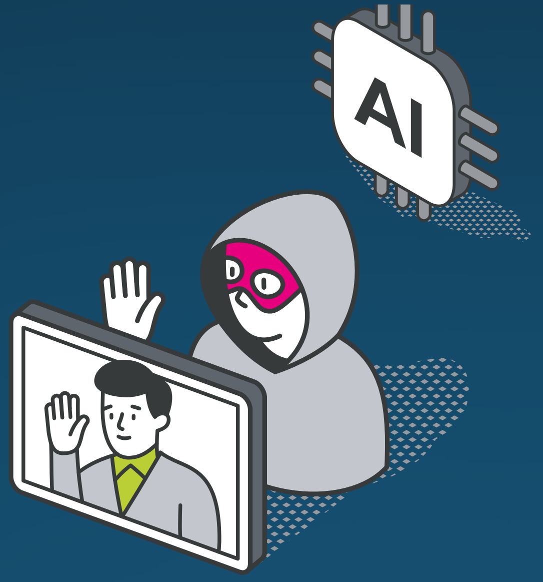
Many manufacturing industries, including car manufacturing, are moving towards fully automated supply chains, with parts arriving "just in time" and completely digital design and manufacturing workflows. This can of course be very efficient, but understanding the complex web of interdependence in such a huge system and ensuring that cybersecurity is incorporated at every weak point is crucial. While JLR has huge cash reserves the UK government has underwritten a £1.5 billion loan to help them deal with the fallout. The overall financial impact is expected to be £1.9 billion, with over 5000 organizations impacted by the attack. JLR employs over 34,000 people, with 120,000 throughout their supply chain, some of those suppliers are expected to go bankrupt. It also looks like JLR didn't have cybersecurity insurance and thus had to foot the entire bill for this disaster.
The lesson here is clear, the call for digital transformation in every industry has been loud for the last decade, and while this is important for any business, not taking appropriate steps to mitigate cyber security weaknesses in every part of the overall system brings huge risks. And make sure you have cybersecurity insurance commensurate to your risk profile. The last sobering take away is that with the government bailout, it's likely that future attacks will target UK companies, as they're more likely to pay up.

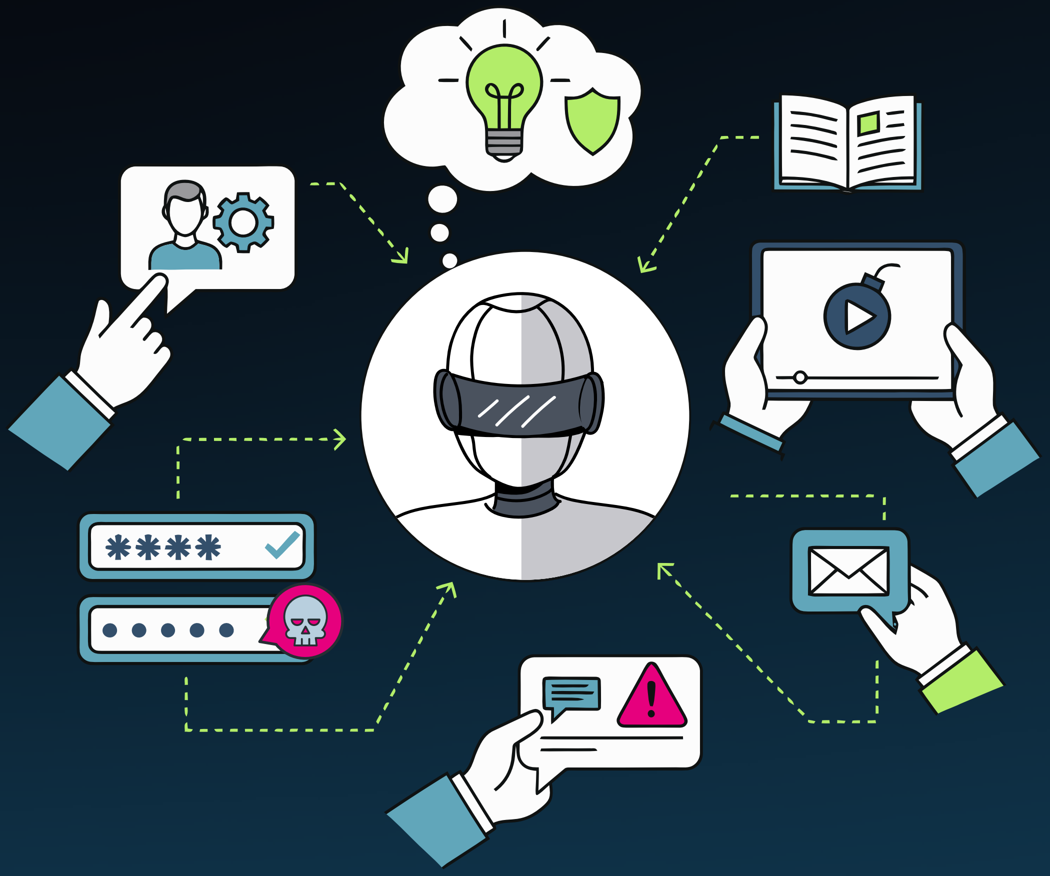
OCTOBER 2025 – F5 COMPLETE COMPROMISE

In October 2025, F5 Networks (a major vendor of application delivery controllers and network security gear) disclosed that it had been breached by a highly sophisticated nation-state threat actor. Subsequent investigation indicated that the attackers likely gained initial access in late 2023 by exploiting an F5 system that was mistakenly left exposed online, bypassing internal security policies. This lapse allowed the hackers to establish a foothold and maintain long-term, stealthy access to F5's internal network for at least 12 months without detection. The breach was only uncovered in August 2025, after which F5 made it public in mid-October, highlighting serious supply-chain security concerns given F5's products are deeply embedded in many organizations' infrastructure.

Once inside, the intruders leveraged a custom malware backdoor (dubbed "BRICKSTORM") to move laterally through F5's virtualized environment while evading security controls. BRICKSTORM, attributed to a China-linked espionage group known as UNC5221, enabled the attackers to remain almost invisible. There were, at one point, even lying dormant for over a year, likely to outlast F5's log retention period and erase traces of the initial compromise. When they reactivated, the attackers exfiltrated extremely sensitive files, including portions of the proprietary BIG-IP source code and internal reports on undisclosed (zero-day) vulnerabilities in F5's products. This stolen data effectively gave the hackers insight into security flaws that were not yet patched or public, a cache of information that experts likened to a "master key" for potential future attacks against F5 devices worldwide. The incident underscored how a single well-executed breach of a core technology provider can pose broad risks, since F5's platforms are used to protect and load-balance critical applications across government and enterprise networks globally.

The lesson here is an uncomfortable one and echoes the SolarWinds breach back in 2020: even the largest cyber security vendor can be compromised by a determined attacker, and without adequate monitoring and logging can remain undetected for a very long time. This is a developing story and while we don't have enough technical details yet to predict the outcome over the months to come, if your network relies on F5 equipment you need to update everything, including all credentials.





AI-DRIVEN THREATS:
WHEN INNOVATION BECOMES EXPLOITATION

CHAPTER 4

FORECASTING THE THREAT LANDSCAPE IN 2026

DID WE GET LAST YEAR'S PREDICTIONS RIGHT?

In last year's report we made some predictions of what 2025 would bring for cybersecurity, and overall, we were spot on. Unsurprisingly we talked about the risk of Large Language Model (LLMs) based Generative AI (GenAI) in the hands of attackers. While we can't say for sure that a particular phishing email or other scam was helped along by attackers fine tuning the lure to make it as enticing as possible, both OpenAI and Anthropic have continued to put out reports of cases where they've spotted malicious use of their tools (and subsequently blocked those accounts).

Novel uses include Claude Code being used to automate reconnaissance, harvesting credentials and penetrating networks. The exfiltrated financial data was also analyzed by AI to decide on ransom amounts. North Korean IT workers are now a widespread threat, and they used both Claude and ChatGPT to create fake personas, automate resume generation, complete technical and coding assessments during the hiring process as well as delivering work once employed. Whilst this was an easy prediction and we got it right, it's interesting to see how attackers experiment with different uses of AI during various phases of their attacks.

We also predicted the use of more convincing deepfakes for spear-phishing and influence operations (IO) and again this has been borne out over the last 12 months. New releases of video creation tools have brought a deluge of AI "slop" that's blurring ordinary user's ability to separate fact from fiction, a reality that societies (and businesses) around the world are already struggling with.

Last year's report also predicted legal cases around AI, and, again we were spot on, including the $1.5 billion class action lawsuit against Anthropic. Due to politically changing winds the US is unlikely to rein in the worst excesses of AI companies there, but the EU has passed the AI Act.

The relentless march of new and updated regulatory frameworks continues across most of the world and our prediction that this will increase the workload and challenges for businesses (and their suppliers) was also accurate, with the NIS2 Directive taking budget from recruitment and emergency reserves, whereas the Digital Operational Resilience Act (DORA) and the UK's Prudential Regulation Authority (PRA) compliance costs businesses over a €1million.

Our look at the free and open-source software ecosystem (FOSS) was also quite prescient, with regular reports of hundreds or thousands of malicious packages reported across NuGet, PyPI, RubyGems and npm (35,000 malicious packages in npm in August 2025 taking the top spot) in the last year. This seems to be a worsening trend and if your business develops software in-house, you must track these malicious packages before they are included in your applications. The days of nerds worldwide contributing code to FOSS for the benefit of humanity at large voluntarily may be coming to an end.

Our final prediction around the adoption of memory safe languages (Rust/Swift) appears also to be accurate, although it's slower going. Rust is appearing in Windows third-party drivers, in the OS kernel (where about 70 % of all CVE's come from memory safety issues), as well as Hyper-V, Azure and Microsoft 365. Linux is also incorporating Rust, as is Android, where it's led to a 52 % reduction in memory vulnerabilities over the last six years. Apple meanwhile is charting a slightly different route, as they've got control over all of the hardware and software, with their Memory Integrity Enforcement but the result is the same – avoid exploitable memory issues.

Overall, all of our predictions have materialized, which says more about the predictability of cyber security criminals than our power to prophesize.

THE SECURITY LAB'S 2026 PREDICTIONS

Uncontrolled Adoption of AI Tools

As AI tools continue to mature, adoption across organizations is accelerating, often more quickly than governance or security frameworks can adapt. This acceleration is led by both management-led initiatives as well as grassroots experimentation by employees, and new AI solutions are being deployed daily in some cases. The pace of innovation has outstripped the ability of legal, IT, and security teams to evaluate each implementation, leaving critical visibility gaps.

Uncontrolled adoption effectively expands the organizational attack surface. Many AI tools, particularly those powered by large language models (LLMs), lack the separation between code and data inherent in more traditional applications. This introduces new vectors for prompt injection, data leakage, and unintended disclosure of sensitive corporate data. The rise of agentic AI compounds this risk, as autonomous actions can occur without human oversight or established approval chains.

Recent vulnerabilities such as **Echoleak in M365 Copilot (Aim Labs)** really show the seriousness of these risks. Unlike buffer overflows or code injections, LLM-based exploits don't have straightforward mitigations. Even following best practices from the **OWASP LLM01:2025 Prompt Injection** guidance, organizations face residual exposure due to the unpredictability of AI model behavior. Reports such as "*Detecting and Countering Misuse of AI*" (August 2025, Anthropic) further confirm that even state-of-the-art models remain susceptible to manipulation and abuse.

Weaponization of Agentic AI

It should come as no surprise then that agentic AI systems (autonomous models capable of executing multi-step goals) are already being weaponized. The line between automation and orchestration has blurred. Attackers can now script, adapt, and launch multi-vector campaigns with minimal expertise, lowering the barrier of entry. These models can support every stage of the attack lifecycle, from reconnaissance to exploitation to impact, following the MITRE ATT&CK framework end-to-end.

One doesn't have to look very far in online search to find cases where agentic AI has started to make an impact on threat-actor operations. These cases contain techniques like crafting phishing lures, bypassing CAPTCHA gates, or impersonating humans through voice and video deepfakes. These findings confirm what many defenders already suspect: AI is amplifying both the accessibility and velocity of cybercrime.

Despite safety claims from major vendors, misuse persists. Anthropic's own August 2025 threat report (listed above) acknowledged ongoing model abuse for reconnaissance and payload generation, validating the concern that agentic AI systems will continue to outpace safeguards. With LLMs capable of "vibe coding" entire attack chains autonomously, the barrier to entry for sophisticated exploitation has all but vanished.

RANSOMWARE 3.0: LLM-DRIVEN AND INTEGRITY-FOCUSED

As discussed above in our 2025 ransomware survey findings, ransomware operations are entering a new evolutionary phase. This phase is defined by automation, autonomy, and data corruption. In 2026, we expect to see the emergence of LLM-driven orchestration, where large language models coordinate reconnaissance, payload generation, and adaptive evasion. Simultaneously, attackers are shifting from encryption or exfiltration to data integrity manipulation: altering, corrupting, or subtly falsifying records to create doubt in the trustworthiness of data itself.

Historically, ransomware has evolved in response to defender resilience. Think encryption-only attacks (Ransomware 1.0) to double extortion (Ransomware 2.0). With widespread adoption of immutable backups and cyber insurance, direct encryption attacks are yielding diminishing returns. The next logical step for cybercriminals is to compromise trust rather than access. Manipulated data in financial systems, medical records, or industrial controls creates prolonged chaos, regulatory exposure, and reputational damage.

Academic research has already demonstrated proof-of-concept ransomware campaigns autonomously orchestrated by AI. A 2025 NYU Tandon School of Engineering study showed that LLMs could execute complete attack chains autonomously. This included reconnaissance, exfiltration, encryption, and adaptation, and it was all done without human intervention. Adding data corruption to that process is a natural and dangerous progression.

ATTACKER-IN-THE-MIDDLE WILL MAKE PHISHING RESISTANT MFA MANDATORY

The move to MFA for stronger authentication over the last decade has been a good one, but attackers have evolved alongside our defenses. Attackers use phishing kits, including the open source Evilginx to set up fake sign-in pages, mimicking Microsoft's, Google's or Okta's pages and then trick users via phishing emails or Teams messages into clicking a link to it. Users sign in to the fake page, and their username, password, and MFA prompts are passed to the legitimate sign in page behind the scenes, while the attacker steals the resulting token, and can then access everything the user can, known as Attacker-in-the-Middle (AiTM).

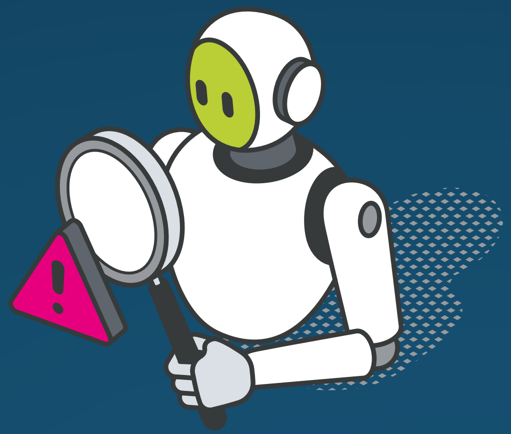
The ability to manage the MFA prompt is now a "standard feature" in these phishing kits. The only good defense is phishing resistant MFA technologies such as FIDO2 hardware keys, Windows Hello for Business, Certificate based Authentication (CBA) and Passkeys, as these are tied to the legitimate sign in page, and won't work on the fake one, even if the user has been tricked. However, not only do you need to deploy phishing resistant MFA, you must also mandate it as the only sign in method, because most phishing kits now will also force a downgrade from a stronger MFA method to a less secure one.

PASSKEY ADOPTION WILL BE SLOWED BY CONFUSING USER EXPERIENCES

While hardware FIDO keys are a great option for phishing resistant MFA, it's an added cost for every user to budget for. Passkeys, where the security chip in your modern smartphone is used instead, are an alternative, and we predicted that their adoption this year would accelerate, which it has, but not to the extent we expected. The main reason for this is a fragmented user experience, it looks differently on an iPhone, an Android phone or a Windows / MacOS laptop. Furthermore, there are two flavors, with consumer ones being "syncable", meaning they're stored in your Apple or Google consumer account so you can use them on different devices. Storing corporate credentials in end users' personal cloud accounts isn't acceptable for most businesses, so they generally enforce non-syncable passkeys. Those are locked to the smartphone where they were created, and in the case of Microsoft 365, the only app that's accepted is Microsoft Authenticator. Add to this the confusing experience where you're signing in to a service on your laptop and then have to scan a QR code with your phone, and then complete the sign in flow on your phone. Passkeys are the future of phishing resistant MFA but the tech giants need to get together and harmonize the overall experience for both consumer and business users.

IDENTITY VERIFICATION AND RESET PROCESSES WILL CONTINUE TO COMPROMISE ORGANIZATIONS

Several of the very large breaches we've seen recently were due to (often outsourced) help desk staff being tricked into resetting accounts for administrative user accounts. Remember, your authentication strength isn't measured by which technology you use when everything is working normally, but by how hard it is to subvert your enrolment and recovery processes. How do you validate that new hires are actually the people you expect (and not a North Korean infiltrator) in today's remote working world? What's your process for recovering accounts for users who have lost their phone, FIDO key, forgotten their password and whose laptop just died? Do you have a more secure process for high privilege accounts? (Including the requirement for an in-person validation at a company office). Identity is the new firewall, but you must look holistically at mitigating risks in your entire identity workflow, starting from when the job offer is made to the last day of work.



SAAS APPS ARE THE NEW ATTACK SURFACE

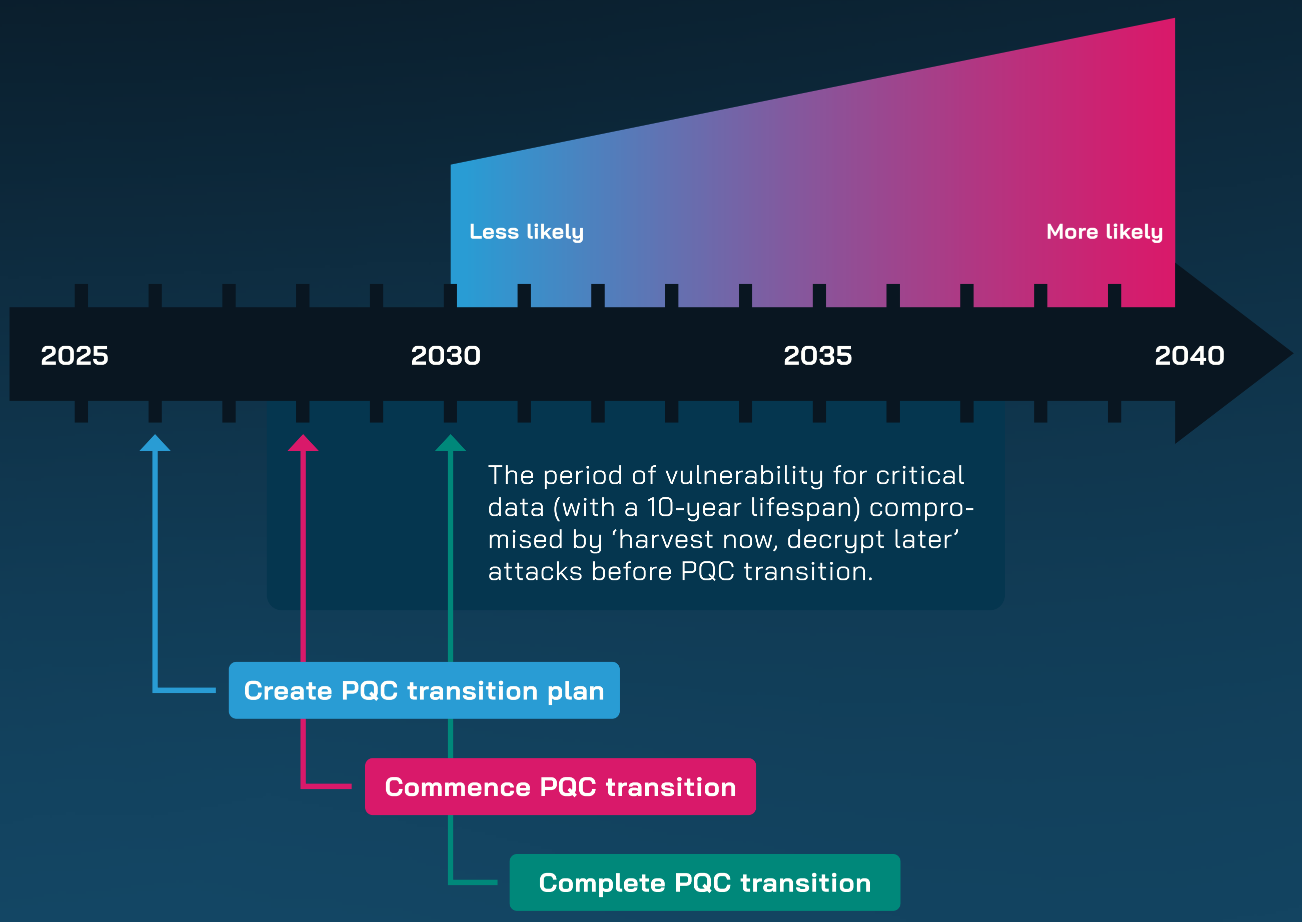
Certain enterprise compromises over the last few years are interesting because they completely bypass the traditional "compromise a normal user – pivot in the internal network – compromise administrator accounts". As businesses become more and more reliant on SaaS services, new types of attacks that only compromise cloud data and identities are becoming more prevalent. Normal defenses such as EDR are mostly blind to these attacks, because while they're taking place in the browser, there's no malicious files or activity that endpoint protection can detect. As a matter of fact, so much of modern business computing now happens in a browser, which is opaque to EDR, that using an enterprise browser and/or specialized software for protection in the browser is our strong recommendation. Mitre even has an ATT&CK MATRIX for different SaaS attacks.

BROWSER EXTENSIONS WILL COMPROMISE MORE BUSINESSES IN THE COMING YEAR

Modern browsers are complex applications, almost like entire operating systems in themselves, and full of protection that keep us mostly safe from dangers on the internet, both in our personal life and at work. But most of us also use browser extensions, often for productivity or convenience, but sometimes these come with hidden risks. In some cases, they're vulnerable in some way, degrading the protection of the browser itself, in other cases they're intentionally malicious. This could be by having a similar name to a popular add-in, or by criminals buying a previous benign extension and then weaponizing it.

Make sure your business has a way of tracking extensions that are installed in your user's browsers, easy ways of blocking ones that are found to be malicious (Intune or AD GPOs can do this) and educating your users about the risks.

Estimated likelihood of achieving CRQC



The period of vulnerability for critical data (with a 10-year lifespan) compromised by 'harvest now, decrypt later' attacks before PQC transition.

PREDICTIONS REGARDING QUANTUM COMPUTING

Most threats we look at in this report are current, while the advent of a Cryptographically Relevant Quantum Computer (**CRQC**) is still some years away. This day, known as Q-Day, is when these types of computers have sufficient scale (number of Qubits – the equivalent to bits in a classical computer), and low enough cost that they can use Shor's algorithm to break asymmetric encryption such as RSA and Diffie-Hellman. Or Grover's algorithm to halve the strength of symmetric cryptography (AES-128 becomes AES-64).

Many different tech companies, including the usual suspects (Google, IBM, Microsoft) are pouring millions into different flavors of quantum computers, seeing which technological approach is going to provide enough stable qubits. The problem is noise, if you have lots of qubits, but use up most of them for error correction; the overall number of logical qubits available to run your calculations are minimized. Quantum computers will not replace our current computers; instead they'll be used for very specific types of calculations, including breaking our current encryption algorithms.

While CRCQs are still 5 to 15 years away, you can't wait until they arrive. Your organization should start planning now, if you store any Personally Identifiable Information (PII), Personal Health Information (PHI) and intend to (or you're compelled to by regulation) to keep it for longer than five years, you need to start using quantum resistant algorithms for the encryption now. This is because several agencies around the world are using Harvest Now, Decrypt Later (HDNL) to store data that they can't decrypt now but will be able to with CRCQs. Furthermore, it's a huge project; you need to find every system, device and part of your network that uses encryption, which algorithm is used and what type of data is stored or transmitted. Sometimes it'll be easy to add quantum resistant algorithms, in other cases you'll need to replace the system entirely, or re-architect your processes.

NIST has standardized three quantum resistant algorithms:

- FIPS 203 defines a cryptographic scheme called Module-Lattice-Based Key-Encapsulation Mechanism (**ML-KEM**), which is derived from the CRYSTALS-KYBER submission.
- FIPS 204 is the Module-Lattice-Based Digital Signature Algorithm (**ML-DSA**), based on the CRYSTAL-Dilithium submission.
- FIPS 205 specifies the Stateless Hash-Based Digital Signature Algorithm (**SLH-DSA**), which is derived from the SPHINCS+ submission.

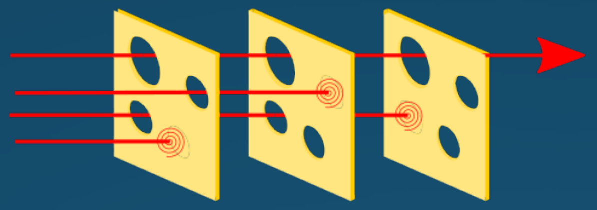
They rely on Transport Layer Security (TLS) version 1.3 so start by rolling that out everywhere you can in your environment.

As for Operating Systems, preview versions of Windows 11 and Windows Server have updated versions of SymCrypt, the same library that's used across Azure and Microsoft 365. ML-KEM and ML-DSA are already available in SymCrypt, both on Windows and Linux. SymCrypt-OpenSSL also offers the same support for OpenSSL. Apple is also including PQC in their CryptoKit for developers, and iMessage in iOS and TLS 1.3 in iOS26 are already incorporating PQC.

If you write your own applications in-house aim for crypto agility so that you can swap out cipher suites, or entire algorithms as updates are delivered.

RISKS FOR ORGANIZATIONS IN 2026

Cybersecurity isn't a technology problem, it's a people and process problem. As so often happens when you're deep into the latest technology and seeing rapid developments in GenAI, or Machine Learning, or Agentic AI, the solutions you see are tech based ("when you only have a hammer, every problem looks like a nail"). But organizations rarely get breached based on technology failures alone, it's more likely a combination of people, process and technology failures. The Swiss cheese model illustrates this clearly:



In other words, if you build cyber resiliency into your organization, through layers of protection and processes, you'll be more likely to avoid a devastating breach.

No matter the size of your business, you will be a target of cyber security attacks in 2026. As you can see in our data, being a small organization / a not-for-profit / "not having anything worth attacking" isn't a defense against criminals. If your business has sensitive data and cash reserves, you are a target. Build a cyber resiliency program based on the Zero Trust principles:

- Assume breach – obviously you build strong, layered protections, but they will eventually fail. At some point the holes will line up, and a breach will happen. Do you have detections in place to spot that quickly? Do you have isolated networks and only the required permissions assigned to minimize the blast radius? Do you have the people and the processes in place to react to the alerts and evict the attackers quickly before they can do major damage?
- Least privilege – this is possibly the hardest thing to get right, give people only the permissions they need to do their job, and regularly review them so they don't accumulate over time.
- Verify each connection – have a strong policy engine in place (Conditional Access in Entra ID) that verifies each login and access to applications, files and other resource to ensure that access isn't allowed by default, but rather only permitted when the right conditions are met.

Before spending money on advanced security tools that solve specific problems, start by taking care of security hygiene basics based on the above principles:

- Implement MFA for everyone. Given the huge increase in Attacker-in-The-Middle (AiTM) kits having MFA bypass built in, you need to move to phishing resistant MFA. This includes hardware OAuth keys, Windows Hello for Business, Certificate based Authentication and Passkeys, which doesn't allow authentication to fake login pages, even if the user themselves has been tricked.
- Have a strong endpoint protection solution on all devices where that's possible, and integrate that with identity, cloud applications and an email hygiene solution for comprehensive eXtended Detection and Response (XDR).
- Train your users to spot phishing attempts, whether in email, Teams, Zoom or WhatsApp but more importantly – build a security culture. Assuming that IT or the security team is taking care of all cyber security so everyone else in the business don't have to worry about it is like saying "only the workplace health and safety staff needs to worry about accidents". No – everyone needs to speak up when they spot something dangerous, whether that's balancing precariously on a rickety chair to replace a light bulb, or someone about to click on a link that they shouldn't.
- Patch your software, but unless you want to double the size of your IT department, do it in a smart way. Apply Continuous Threat Exposure Management (CTEM) principles to protect your business-critical systems that have exploitable vulnerabilities first rather than trying to patch everything, everywhere, which is impossible.
- Look at your supply chain. Several large breaches in recent months have been due to outsourced helpdesk organizations being socially engineered (hacking people instead of computer systems). Understand all your outsourced processes, remembering that you can outsource a function, but not the risk associated with it. And investigate all the supply chains that make your business operate, and build in resilience for when they are disrupted, either through cybersecurity attacks or for other reasons.

A CYBER RESILIENT ORGANIZATION

Because cyber security is a people and process problem, the solution isn't more technology, it's about changing the culture of your business.

We can learn a lot from the aviation industry, where every incident and accident is thoroughly investigated, not to assign blame, but to identify all the different people, process and technology factors that contributed to it. And then take those lessons and incorporate more / different training, changing processes and technologies to make sure it doesn't happen again.

It starts with fostering a safety culture where everyone feels safe to speak up when they see something that's not right. This only happens when people aren't blamed individually when an incident happens – it's about improving the processes so that people aren't as likely to make those mistakes. In turn, this means that cybersecurity is everyone's responsibility, not just the IT or security department – because various parts of the business make technology decisions that bring risks that everyone, not just IT needs to manage. We in cybersecurity must also do better when it comes to communicating with other stakeholders, translating "geek speak" into business risk language.

As you build resiliency in every part of your business, keep up with the changes in the threat landscape as attackers are ever innovative in finding cracks in our systems to exploit.

A HOLISTIC SECURITY STRATEGY

We've mentioned it earlier but it bears repeating – start with the basics. Foundational cyber security hygiene processes and technology will serve your organization's defenses much better than the latest cyber security point solution. You need multiple layers of protections (remember the Swiss cheese model):

Next-Gen Spam/Malware detection with ATP for behavioral analysis to protect against the contin¬ued barrage of email-based threats we see in this industry

End-User Security Awareness Training to train end-users to spot social engineering attacks and spear-phishing attacks

Backup and recovery capabilities for BOTH on-premises data and data that lives in cloud services such as M365 for recovery purposes should a ransomware attack get through

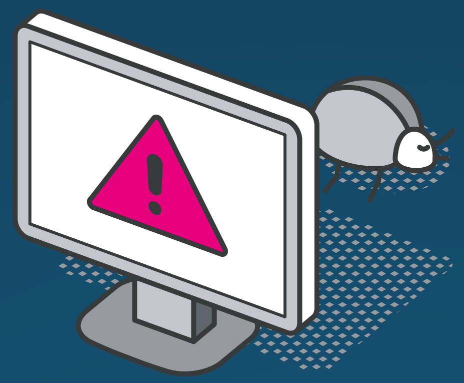
Compliance and governance features that help protect against accidental data leakage and ensure that compliance controls are met

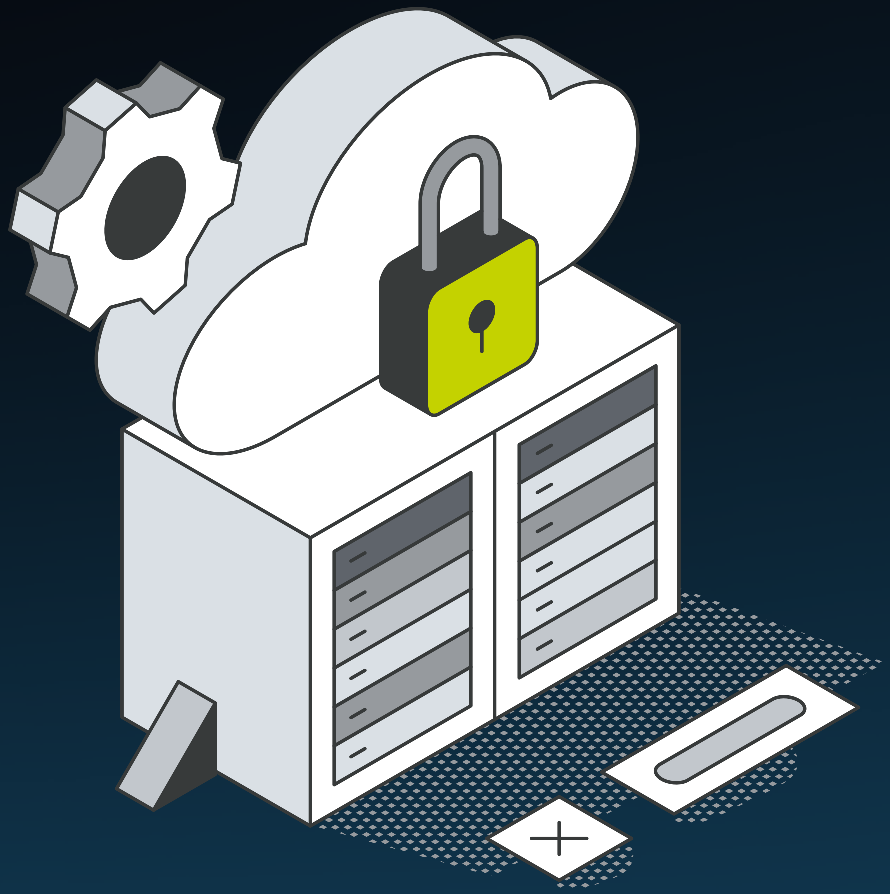
Least privilege and sharing control for your sensitive corporate data stored in SharePoint and OneDrive for Business

AI powered cyber assistant for Email and Teams protection, helping every user stay safe

Learn More
Cybersecurity is just one of the many challenges facing businesses today but not prioritizing it enough can lead to catastrophic outcomes (just ask Jaguar Land Rover).

Just as many businesses outsource parts of their operations to specialists in that area – take advantage of the deep knowledge and skills we at Hornetsecurity have developed since 2007. Partner with us to keep your business safe.





365 TOTAL PROTECTION

AI-POWERED, ALL IN ONE M365 SECURITY, BACKUP & GRC

PLAN 1

- SPAM & MALWARE PROTECTION
- EMAIL ENCRYPTION
- EMAIL SIGNATURES & DISCLAMER

PLAN 2

INCLUDES 1

- ADVANCED THREAT PROTECTION
- EMAIL ARCHIVING
- EMAIL CONTINUITY

PLAN 3

INCLUDES 1 + 2

- AUTOMATIC BACKUP O M365 DATA
- GRANULAR RECOVERY WITH END USER SELF SERVICE
- UNLIMITED STORAGE IN ONE ALL-INCLUSIVE FEE

PLAN 4

INCLUDES 1 + 2 + 3

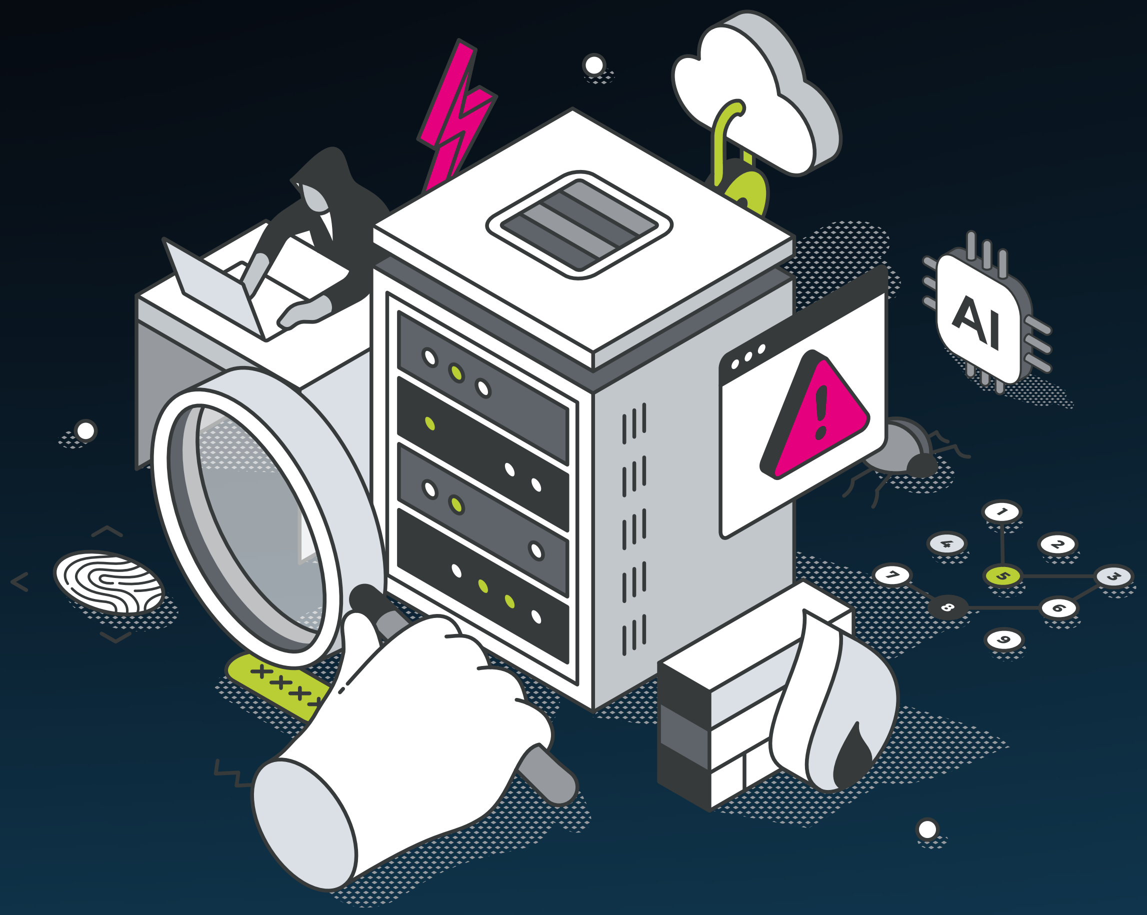
- SECURITY AWARENESS
- PERMISSION MANAGEMENT
- DMARC REPORTING & MANAGEMENT

POWERED BY AI CYBER ASSISTANT

- AI RECIPIENT VALIDATION
- TEAMS PROTECTION
- AI EMAIL SECURITY ANALYST

START YOUR FREE TRIAL

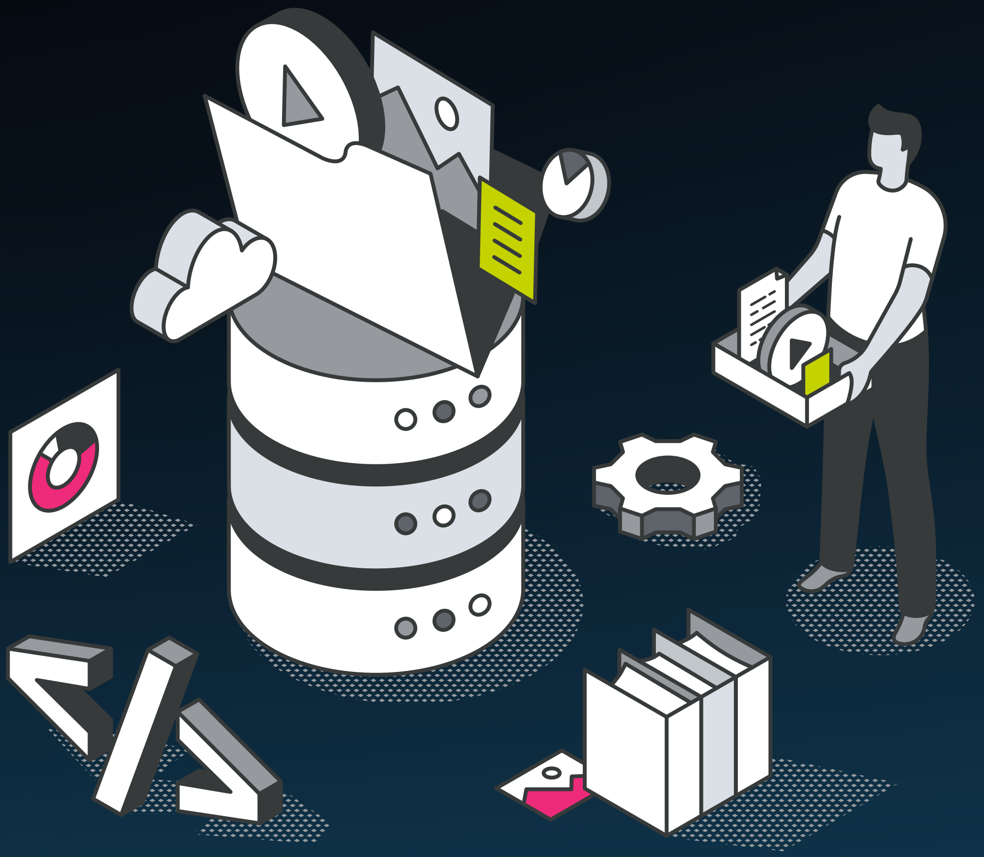
HORNETSECURITY



CHAPTER 5

RESOURCES

- https://www.hornetsecurity.com/en/blog/ransomware-impact-report-2025-press-release/
- https://www.hornetsecurity.com/en/blog/ciso-insights/
- https://www.hornetsecurity.com/en/blog/sharepoint-vulnerability/
- https://openai.com/global-affairs/disrupting-malicious-uses-of-ai-june-2025/
- https://www.anthropic.com/news/detecting-countering-misuse-aug-2025
- https://openai.com/global-affairs/disrupting-malicious-uses-of-ai-october-2025/
- https://www.cnbc.com/2025/09/25/judge-anthropic-case-preliminary-ok-to-1point5b-settlement-with-authors.html
- https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence
- https://www.hornetsecurity.com/en/blog/nis2-directive/
- https://www.infosecurity-magazine.com/news/nis2-compliance-strain-budgets/
- https://www.infosecurity-magazine.com/news/dora-compliance-costs-soar/
- https://ossf.github.io/malicious-packages/stats/
- https://techcommunity.microsoft.com/blog/windowsdriverdev/towards-rust-in-windows-drivers/4449718
- https://www.youtube.com/watch?v=uDtMuS7BExE
- https://pentiumsoak.com/the-rise-of-rust-in-the-linux-kernel-transforming-security-stability-in-2025/
- https://medium.com/cybersecurity-and-iot/how-googles-switch-to-rust-programming-is-redefining-android-s-security-a-52-drop-in-memory-29620cd46e0a
- https://security.apple.com/blog/memory-integrity-enforcement/
- https://www.aim.security/post/echoleak-blogpost
- https://genai.owasp.org/llmrisk/llm01-prompt-injection/
- https://arxiv.org/abs/2508.20444v1
- https://github.com/kgretzky/evilginx2
- https://www.proofpoint.com/us/blog/threat-insight/dont-phish-let-me-down-fido-authentication-downgrade
- https://en.wikipedia.org/wiki/North_Korean_remote_worker_scheme
- https://attack.mitre.org/matrices/enterprise/cloud/saas/
- https://postquantum.com/post-quantum/crqc/
- https://en.wikipedia.org/wiki/Shor%27s_algorithm
- https://en.wikipedia.org/wiki/Grover%27s_algorithm
- https://github.com/microsoft/SymCrypt-OpenSSL
- https://developer.apple.com/videos/play/wwdc2025/314/
- https://en.wikipedia.org/wiki/Cryptographic_agility
- https://en.wikipedia.org/wiki/Swiss_cheese_model
- https://community.isc2.org/ijoyk78323/attachments/ijoyk78323/industry-news/5604/1/g21f.pdf
- https://en.wikipedia.org/wiki/Continuous_Threat_Exposure_Management
- https://www.hornetsecurity.com/en/blog/supply-chain-attacks/
- https://www.hornetsecurity.com/en/services/advanced-threat-protection/
- https://www.hornetsecurity.com/en/services/security-awareness-service/
- https://www.hornetsecurity.com/en/services/365-total-backup/
- https://www.hornetsecurity.com/en/services/vm-backup/
- https://www.hornetsecurity.com/en/services/365-total-protection/
- https://www.hornetsecurity.com/en/services/365-permission-manager/
- https://www.hornetsecurity.com/en/services/ai-cyber-assistant/
- https://www.hornetsecurity.com



ABOUT THE AUTHORS

WRITTEN BY

ANDY SYREWICZE

Andy has over 20 years' experience in providing technology solutions across several industry verticals. He specializes in Infrastructure, Cloud, and the Microsoft 365 Suite.

Andy holds the Microsoft MVP award in Security.

PAUL SCHNACKENBURG

Paul Schnackenburg started in IT when DOS and 286 processors were the cutting edge. He runs Expert IT Solutions, an MSP on the Sunshine Coast in Australia.

Paul is a well-respected technology author and active in the community, writing in-depth technical articles, focused on cybersecurity, Microsoft 365 and related cloud services.

He holds MCSE, MCSA, MCT certifications.