
S-RM
fgs global
Cyber Incident Insights Report
2026

# Contents

# Foreword

This report, S-RM's fourth annual Cyber Incident Insights Report, draws on data from over 800 incidents our team responded to globally in 2025. It offers a clear-eyed view of how the threat landscape is evolving and what that means for businesses in the year ahead.

This year we have collaborated with FGS Global, a leading stakeholder strategy firm that advises businesses on communicating with key audiences during cyber incidents and other moments of intense scrutiny. Their perspective on reputation and stakeholder engagement is included throughout.

Ransomware remains the dominant threat, but the ecosystem behind it is fragmenting. S-RM's global cyber team responded to incidents involving 67 distinct ransomware groups, up from 58 the year before, and the influx of newer, less predictable operators has made outcomes harder to predict. The landscape is also shifting: English-speaking threat actors claimed high-profile targets, AI-enhanced communications made established groups and lone operators more effective across borders, and attacks surged across Asia-Pacific. US-based companies remained the primary target, accounting for over 60% of incidents the team responded to.

AI features prominently — not only as a tool for attackers, but as a growing source of organisational risk. The proliferation of AI agents with broad system privileges is creating new attack surfaces many organisations are not yet equipped to defend. Yet familiar patterns persist: unsecured VPNs, misconfigured MFA, and inadequate endpoint protection still account for the majority of successful attacks. Only 22% of ransomware victims S-RM supported had fully deployed and actively monitored EDR.

2025 was the year the C-suite recognised that cyberattacks can derail business plans, causing severe financial and reputational fallout. High-profile attacks on multinationals with complex supply chains and consumer-facing brands showed how quickly a cyber incident becomes a business continuity event, requiring leaders to reassure suppliers, employees, financial stakeholders, regulators, and customers for months.

Many had a plan — few had one that connected the technical response led by CISOs and IT teams with a robust stakeholder communications strategy, leaving them scrambling in real time to contain reputational damage.

Threat actors also became more sophisticated in their communications. AI has made written exchanges more polished and verbal interactions more realistic, but the bigger shift was in tactics: briefing journalists to pressure victims, publicly challenging company statements they deemed misleading, and directly contacting customers, employees, and even crisis management teams to maximise disruption. These developments reinforce why a clear communications response plan has never been more important.

We hope the data, analysis, and insights in the following pages prove useful as you assess your risk posture and prepare for the challenges ahead.

**Jamie Smith**
Global Managing Director, Cyber Security, S-RM
j.smith@s-rminform.com

**Jenny Davey**
Partner and Global Co-Head, Crisis & Issues Management Practice, FGS Global
jenny.davey@fgsglobal.com

# **2025** incidents in numbers

**67** different threat actors encountered, up 16% from 2024

Over **60%** of attacks targeted US-based companies

**24%** of ransomware victims ended up paying a ransom, up from 14% in 2024

**$296,000** was the average ransom paid

**69%** of ransomware victims had "mostly viable"* backups, up from 58% in 2024

Only **22%** of victim organisations had rolled out and actively monitored EDR across their estate

**47%** of BEC victims had not enforced MFA in their M365 enviroment

**$165,000** was the average amount of diverted funds from BEC attacks

The S-RM incident data presented in this report is from Polus Analytics, S-RM's in-house incident data platform. The incidents analysed for this report took place between 1 January and 31 December 2025.

*"Mostly viable" refers to companies whose backups were at least 50% viable.

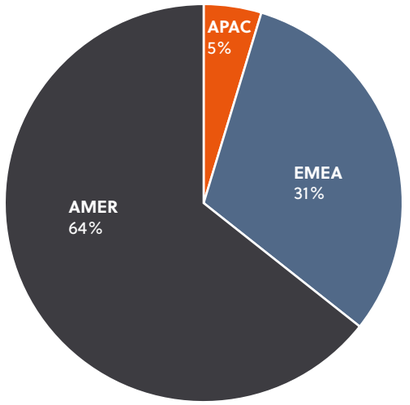
# 01

# Key 2025 stats unpacked



FIGURE 1

**Attack volume by region**




Source: Polus Analytics, 2025

The majority of attacks we responded to in 2025 targeted US-based businesses (figure 1).

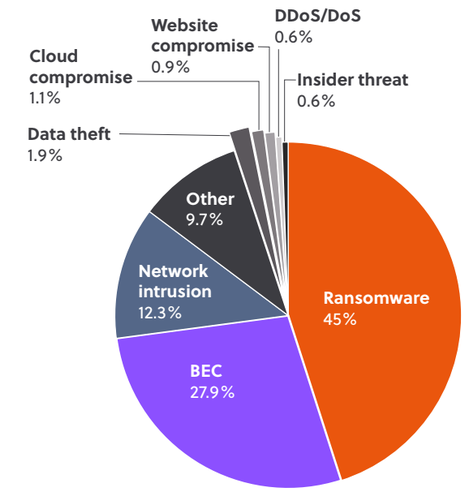
The sheer number of potential targets, the lack of tolerance for business disruption, and the regulatory environment all combine to make the US an attractive hunting ground for a wide range of threat actors. We saw 45 unique threat actors target American companies, more than the rest of the world combined. While there are indications that threat actors are extending their reach (see page 22), we predict the US will remain the primary target for ransomware in 2026 and beyond.

## Attack types

Ransomware attacks continued to dominate the cyber threat landscape in 2025 (figure 2). Our team also responded to a growing number of incidents detected at the network intrusion phase, which often resemble the early stages of a ransomware attack, prior to encryption. In these cases, a quick triage and deployment of counter-measures can make the difference between a devastating attack, and avoiding any encryption or data theft altogether.

FIGURE 2

**Percentage of cases by attack type**



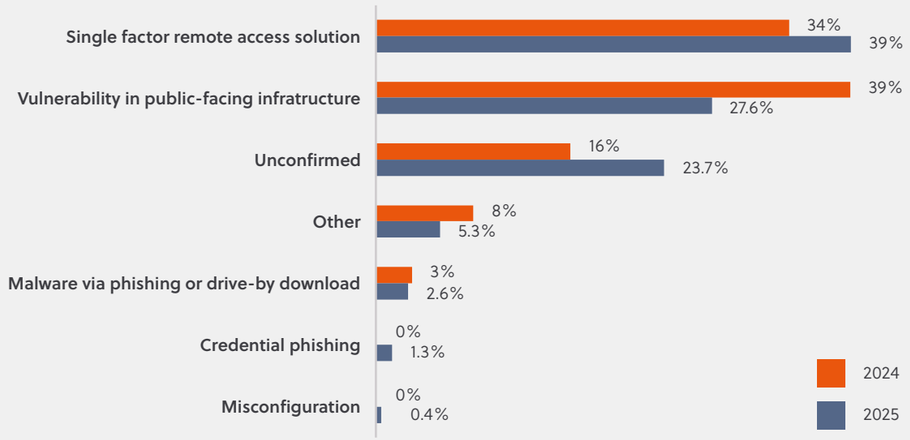

Source: Polus Analytics, 2025

## Method of entry and key controls

Single-factor remote access solutions and vulnerabilities in public-facing infrastructure remain favoured methods of entry amongst ransomware threat groups (figure 3). Despite receiving significant media attention in 2025, social engineering remains a comparatively rare method of entry for ransomware groups. Targeted social engineering attacks are time-consuming and therefore less effective for financially motivated threat actors looking to operate at scale and maximise returns.

FIGURE 3

**Ransomware: Method of entry**

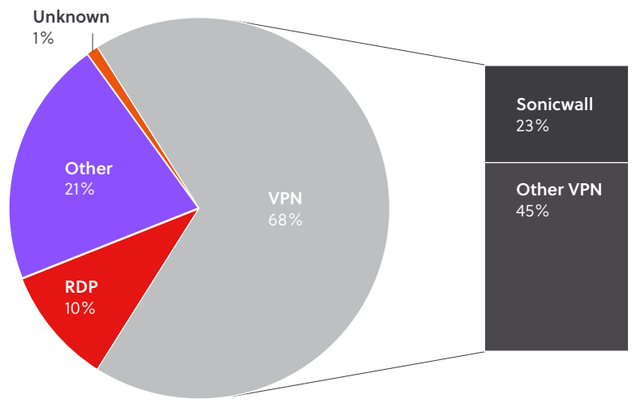



Source: Polus Analytics, 2025

VPN devices were identified as the source of entry in 68% of ransomware cases involving the exploitation of remote access solutions (figure 4). Akira, which remains one of the most prolific ransomware groups in operation, led a particularly targeted campaign against Sonicwall SSL VPN devices. The group was responsible for almost 70% of all the Sonicwall-related incidents we responded to last year.

FIGURE 4

**Remote access solution exploited**

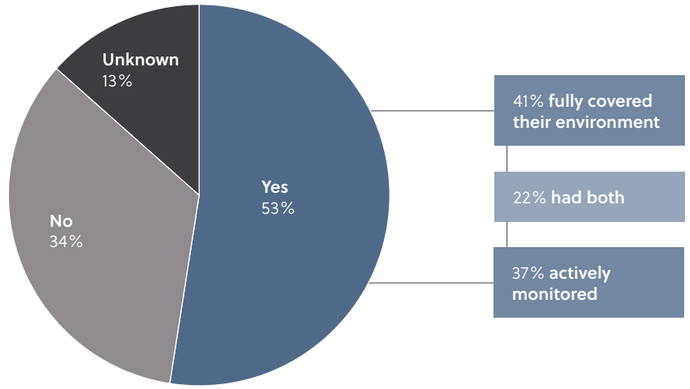



Source: Polus Analytics, 2025

When properly rolled out, EDR is an effective tool for protecting organisations from ransomware. However, proper implementation remains in the minority. Only 22% of ransomware victims had deployed EDR across their entire estate and implemented active monitoring (figure 5).

FIGURE 5

**Ransomware: Was EDR in place prior to the attack?**

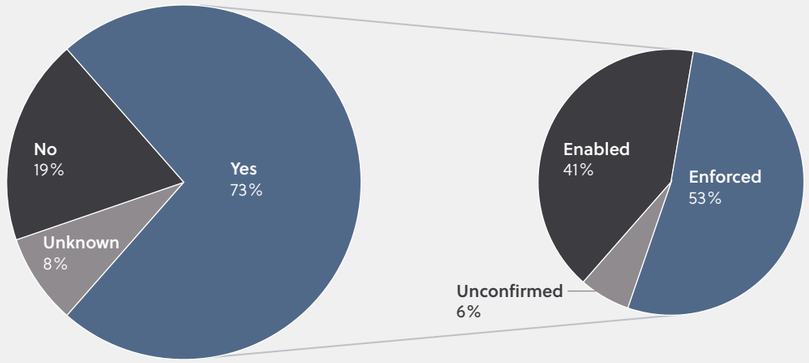



Source: Polus Analytics, 2025

For Business Email Compromise (BEC) cases, credential phishing remains by far the most common method of entry, accounting for 80% of cases in 2025 (where a method of entry could be confirmed). Although 73% of BEC victims had rolled out MFA on their M365 tenant (figure 6), only 53% had fully enforced the control. On the one hand, this demonstrates that misconfiguration of security controls continues to serve as low-hanging fruit for threat actors. On the other, it illustrates the prevalence of token-session theft, which can allow threat actors to bypass MFA entirely.

FIGURE 6

**BEC: Was MFA rolled out on M365?**




Source: Polus Analytics, 2025

## Ransom payments

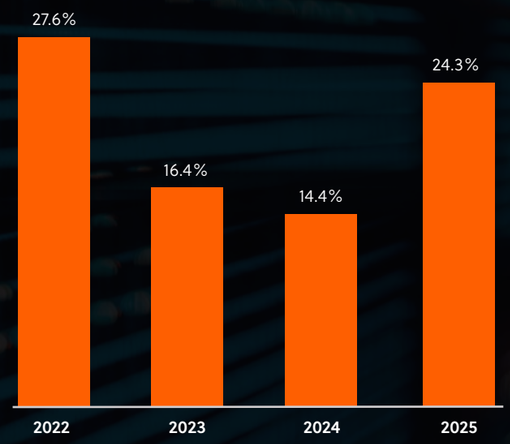
Ransom payments were on the rise again following two years of decline, nearing 2022 levels (figure 7). However, overall payment rates remain compressed.

The average ransom amount paid globally in 2025 came to USD 296,000, with our lowest recorded payment coming in at USD 10,000 and the highest at USD 1,900,000. Payment levels depend on a variety of factors, including the size and revenue of the target, as threat actors are known to tailor their ransom demands to their victim's (perceived) revenue, or the revenue of their parent companies.

Data decryption is no longer the primary motivator for paying ransoms. In 88% of ransomware cases, victims had backups in place, with 70% having mostly viable backups, a picture that has improved for three consecutive years (figure 8). Where viable backups are in place, victims are less likely to end up paying a ransom (figure 9).

FIGURE 7

**Percentage of extortion cases resulting in payment,** by year




Source: Polus Analytics, 2025

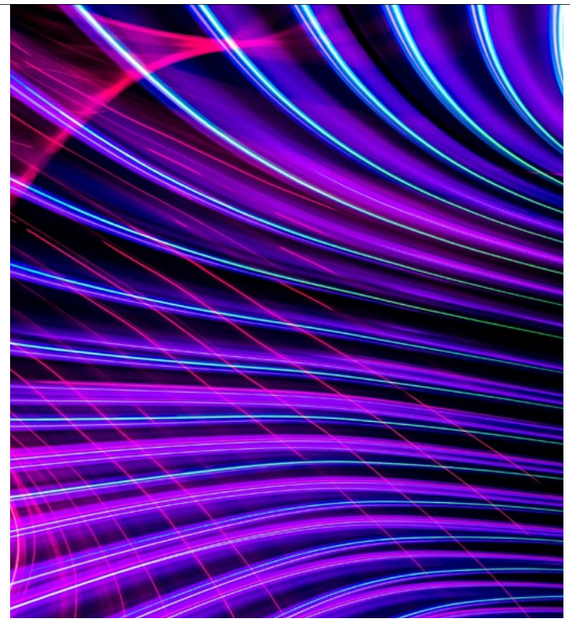
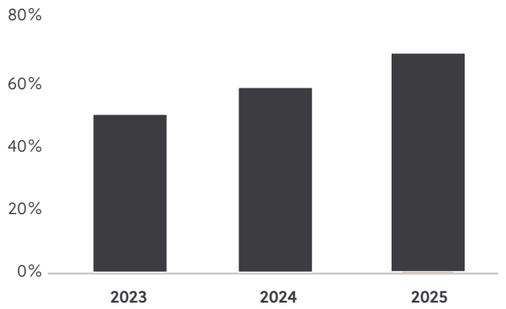


FIGURE 8

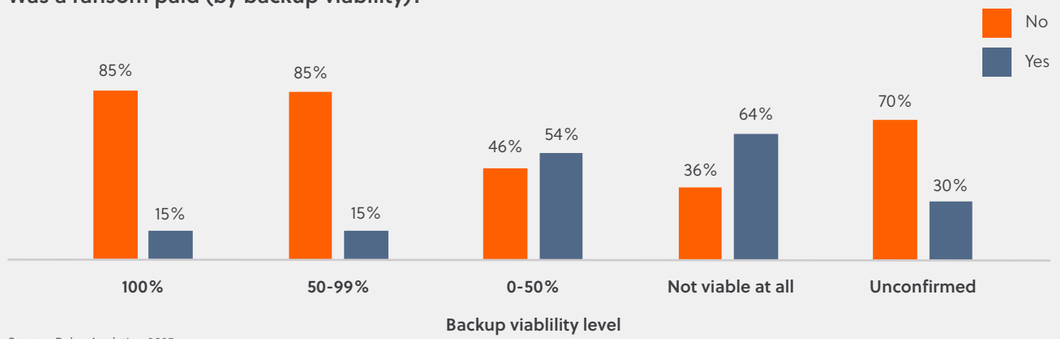
**Incidents where backups were over 50% viable**




Source: Polus Analytics, 2025

FIGURE 9

**Was a ransom paid (by backup viability)?**

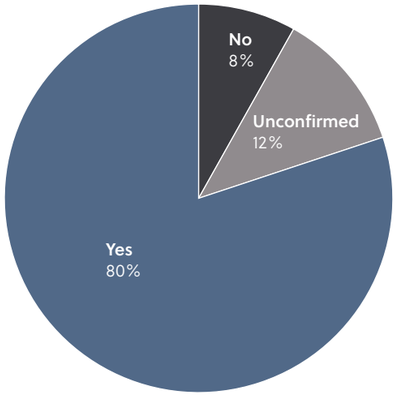



Source: Polus Analytics, 2025

With organisations continually improving their backup posture, it is unsurprising that data exfiltration has become a go-to tactic for threat actors, enabling them to 'double-extort' their victims (figure 10). In many cases, we now see separate ransom demands for decryption, data suppression, and cessation of further pressure tactics.

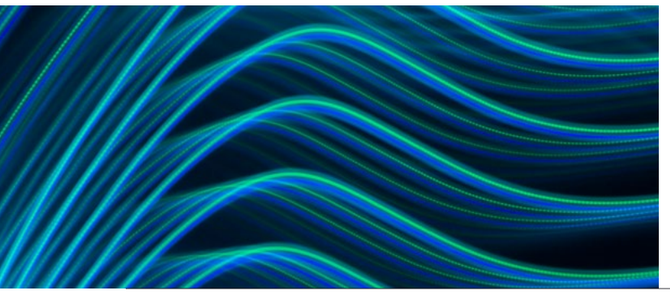
FIGURE 10

**Was data exfiltrated as part of the ransomware attack?**




Source: Polus Analytics, 2025

Threat actor engagement has also evolved. Rather than engaging purely to negotiate a ransom, victims increasingly communicate with threat actors to gather information about what may have been exfiltrated, or to buy time while they recover or prepare for a data leak. Our data shows that although 60% of victims choose to engage with a threat actor, only 41% of those ultimately pay a ransom.



## Sector insights

In 2025, the top 5 sectors (figure 11) reporting the most cases were:

1 **Financial services:** Of all sectors, financial services had by far the highest prevalence of cases where victim organisations did not have EDR rolled out at all – 56% compared to an average of 34%.

2 **Professional services:** Law firms in particular see a higher-than-average prevalence of BECs (49% of cases compared to an average of 28%). As lawyers regularly receive and share links to document-sharing sites with clients, they are particularly vulnerable to convincing phishing attacks.

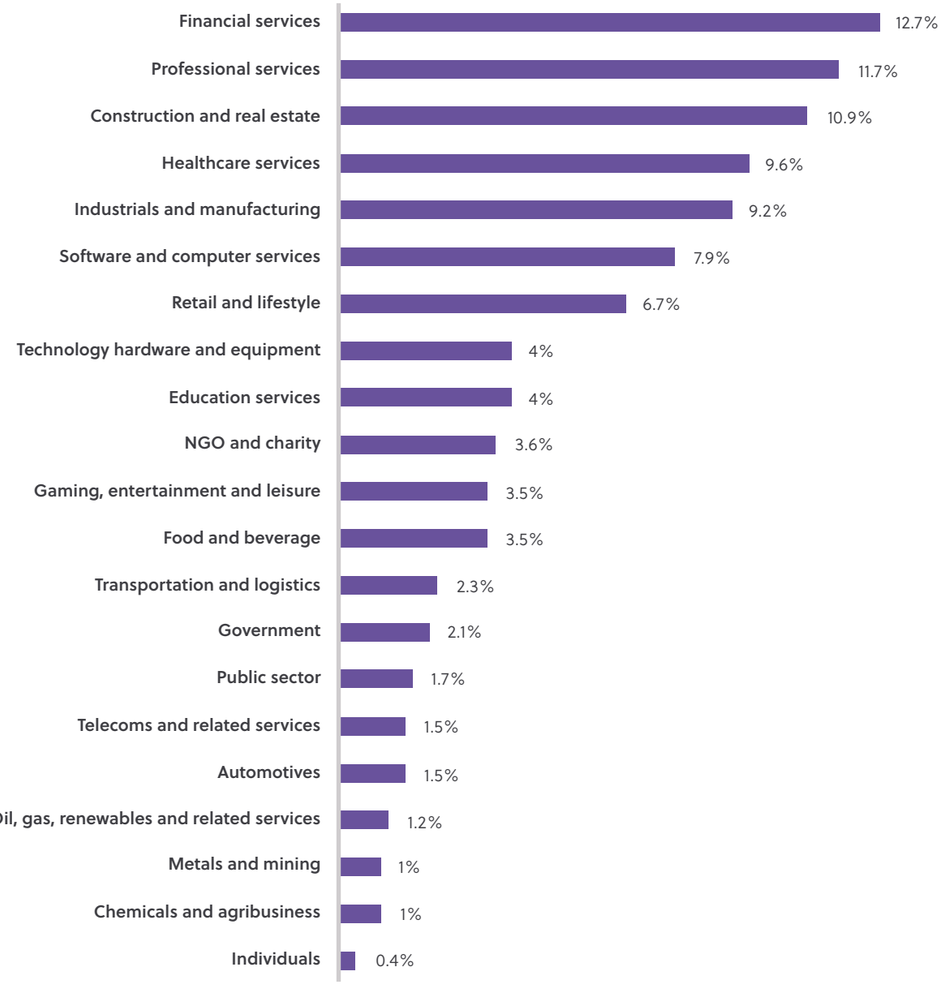
3 **Construction & real estate:** The construction and real estate sector had a higher-than-average prevalence of VPN-related attacks – 87% compared to the average of 68%.

4 **Healthcare services:** Healthcare services were attacked by the highest number of unique threat actors – 21 in total. Notably, this sector also struggled with MFA rollout on remote access solutions compared to others.

5 **Industrials & manufacturing:** Industrials and manufacturing companies have the greatest ransom payment rate (37%) out of the top five sectors (versus an average of 24%), likely due to the high impact of operational disruption caused by ransomware attacks.

FIGURE 11

**Percentage of incidents by sector**




Source: Polus Analytics, 2025

# FGS GLOBAL PERSPECTIVE

## Reputation and ransoms

Deciding whether or not to pay a ransom is a complex process, fraught with risk. Companies are reluctant to make a payment to a criminal operation, while the risk of inadvertently paying a sanctioned entity is a major concern for legal teams. There is also a reputational consideration – payments can become public, either through law enforcement action against ransomware gangs, data leaks following takedowns, or insider disclosures when groups splinter.

As a result, most companies won't pay unless the financial or human cost of disruption outweighs the risk. These decisions are difficult to make in the heat of a crippling attack, so an "it depends" policy isn't enough. At a minimum, boards need to:

- Understand how quickly they could restore operations after a severe attack, which is often the key factor in deciding whether to pay.
- Agree in advance who the decision-makers will be, including the role of independent non-executive or supervisory board members and any delegated authority thresholds.
- Build a decision-making framework that reduces reliance on ego or anecdote in the boardroom.

For organisations that cannot or will not pay, such as government-controlled entities, a clear plan for managing the consequences, including sensitive data leakage and prolonged operational disruption, is essential.
Given the reputational, legal, regulatory, operational, and technical dimensions of the pay/don't pay decision, a short workshop with key advisers to rehearse the arguments gives companies a significant head start — versus educating themselves under pressure during a live incident.

# 02

# The divided threat landscape

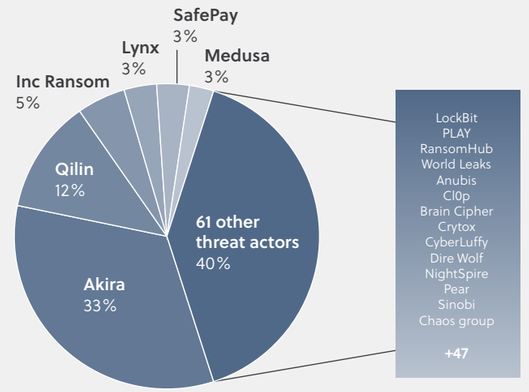




The ransomware ecosystem in 2025 was defined less by the emergence of novel tactics and more by expansion and structural instability. S-RM responded to incidents involving 67 distinct ransomware groups, up from 58 in 2024, underscoring the continued diversification of the threat landscape (figure 12).

FIGURE 12

**Percentage of incidents by threat actor**
(where threat actor was identified)




Source: Polus Analytics, 2025

Incident volume continued to be driven by established ransomware-as-a-service (RaaS) operations, such as Akira and Qilin, which between them accounted for 45% of the incidents we responded to. These operations are structured and commercially oriented, with developers, affiliates, and access brokers forming a loosely organised but highly active ecosystem.

Beyond the well-known groups, however, the field becomes less predictable, and we observed a proliferation of new threat actors operating with varying degrees of effectiveness and sophistication.

**Several key themes emerged from the fragmented threat actor landscape:**

1. **High impact:** Inexperienced threat actors can still cause significant harm. Despite lacking operational maturity, they often inflict disproportionate damage. In one incident, the group BlackCard accidentally wiped servers during data exfiltration.

2. **Ephemeral operations:** Many emerging cybercriminal groups are short-lived due to internal conflicts and scams. For example, the VanHelsing operation quickly collapsed after a developer absconded with funds and decryption keys. Attempts to mitigate damage by releasing malware source code failed, and activity under their new identity, Global, was short-lived.

3. **Ditching the script:** The ransomware ecosystem typically follows established norms, with groups using a repeatable attack methodology and playbooks for negotiations. However, 2025 saw inexperienced groups deviating significantly from expectations, sometimes to their own detriment. NightSpire, for instance, issued unrealistic deadlines and prematurely published data during negotiations, reducing their chances of securing settlements.

4. **Inconsistency among incumbents:** Large extortion operations experienced instability due to law enforcement pressure and internal churn. This led to less predictability among established groups, such as Akira and Qilin. We responded to multiple incidents whereby victim data was not published despite non-payment, and others in which victims later identified their data on unrelated extortion sites.

## Closer to home?

For organisations operating in Western Europe and North America, there was a shared sense in 2025 that the ransomware threat was edging closer to home. Attacks on big-name brands carried out by English-speaking threat actors such as Scattered Spider made the headlines, but beyond this, groups previously understood to be operating out of Russia and affiliated countries seemed to have fine-tuned their approach. Communications appeared more deliberate, deadlines and threats more precisely articulated, and arguments more coherently framed.

What explains this shift? For the more established RaaS threat groups, use of large language models (LLMs) has likely improved their capabilities. While AI has featured across multiple stages of the attack chain, its impact during communications and negotiations has been particularly visible. Messaging has become more professional in tone and, at times, more psychologically calibrated.

In addition, while the geographical base of these operations may not have shifted out of the Russia and CIS region, their effectiveness at operating further afield has improved. There is growing evidence that affiliates and facilitators are no longer based in the same jurisdictions as core operators, suggesting that the threat actor ecosystem is expanding beyond its more established jurisdictions.

For the newer groups that claimed responsibility for high-profile attacks last year, proximity to their victims was a distinct advantage. These attacks leveraged social engineering, helpdesk manipulation, and abuse of identity recovery processes – all of which required a strong command of English and cultural familiarity with the individuals targeted.

The net effect is clear – cyber threat actors are increasingly empowered to operate beyond borders. It is harder for victim organisations to spot malicious actors, and even when they do, those actors are better placed to evade defences or negotiate favourable outcomes. Expect the proliferation of anglophone threat actors – whether genuine or aided by AI – to continue in 2026.



FGS GLOBAL PERSPECTIVE

### New entrants present new risks

The increasingly fragmented threat actor landscape is making stakeholder communications harder to control during a ransomware attack.

Ransomware groups are growing more sophisticated in manipulating the media. Last year, we witnessed threat actors briefing reporters at major news organisations and trade press via Telegram about stolen data and system vulnerabilities. They scrutinise company statements, exposing attempts to downplay an attack or misrepresent what data was affected. The Co-op, one of the UK's largest food retailers, experienced this firsthand in 2025. Meanwhile, the rise of new and emerging threat actors makes their tactics harder to predict.

The motivations are also shifting. Over the past year in the US, higher education became a notable target for alleged "hacktivists" not seeking ransom payments but reputational damage by exposing internal policies on DEI or admissions practices.

Companies need to be prepared for a wider range of scenarios. With responses under greater scrutiny than ever, developing detailed scenario plans and clear, consistent communications is essential to reassure stakeholders about the steps being taken without over-sharing or drawing premature conclusions about an incident's scope.

# 03

# All eyes to the East:
# The rise of ransomware in the Asia Pacific region

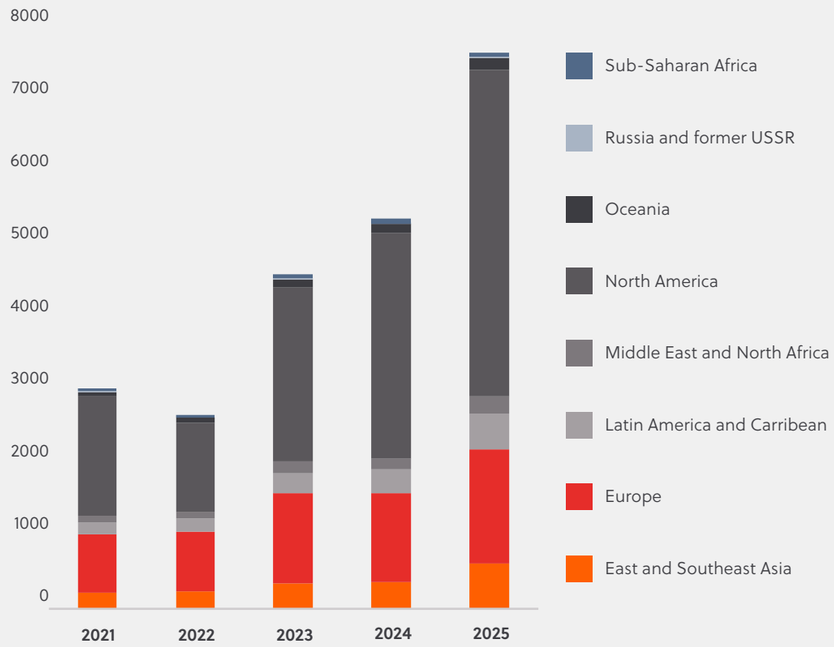




For years, cyber threat actors have focused their activities on Western Europe and North America. In 2025, however, the biggest increase in observed ransomware attacks was in Asia-Pacific* (figure 13). Over 760 organisations across the region were named on ransomware leak sites, 59% more than the previous year. Within this, East and South East Asia saw the largest increase, at 71%, more than any other region globally.

FIGURE 13

**Number of publicly disclosed ransomware attacks 2021 to 2025 by region**




Source: ecrime.ch

Ransomware accounted for 64% of all incidents we responded to in Asia-Pacific, considerably higher than our global average of 45%. Financial services was the most impacted sector, accounting for 20% of the cases.

*Bangladesh, Cambodia, China (including Hong Kong), India, Indonesia, Japan, Laos, Malaysia, Mongolia, Myanmar, Nepal, Papua New Guinea, Philippines, Singapore, South Korea, Sri Lanka, Taiwan, Thailand, Timor-Leste, Vietnam and Oceania

## An attractive target

Rapid and far-reaching digitalisation across Asia has created a large attack surface for threat actors, ultimately increasing the pool of potential victims. Even small businesses are adopting online infrastructure and cloud-based services, and most lack the cyber maturity to defend adequately against evolving ransomware tactics.

At the same time, the introduction and enforcement of stricter privacy and data-breach regulations across Asia has given threat actors additional leverage. Attackers now frequently threaten not only to encrypt data, but also to expose sensitive information in ways that could trigger regulatory penalties and cause reputational damage. This is a familiar pattern – threat actors deployed similar tactics following the introduction of the GDPR in Europe and other data privacy legislation in North America.

## Old actors, new actors

Qilin was the most active ransomware group targeting Asia-based organisations in 2025. This was no surprise – Qilin was one of the most active ransomware groups globally last year, with a total of 1,153 publicly disclosed victims, 9% of which were in Asia.

We also observed a host of new ransomware groups in 2025 for whom Asian companies made up a disproportionately large share of victims (table 1). These groups appear to have made Asia-Pacific a strategic focus.

TABLE 1

**New ransomware groups in Asia in 2025**

| Threat actor | First seen | Total number of victims | Number of victims in Asia | Percentage of victims in Asia |
|---|---|---|---|---|
| NightSpire | March 2025 | 101 | 34 | 34% |
| Dire Wolf | May 2025 | 56 | 28 | 50% |
| Gentlemen | September 2025 | 77 | 24 | 31% |
| Crypto24 | April 2025 | 33 | 14 | 42% |
| WALocker | June 2025 | 19 | 8 | 42% |
| Gunra | April 2025 | 21 | 7 | 33% |
| Obscura | August 2025 | 19 | 6 | 32% |

Source: ecrime.ch

TABLE 2

**Number of ransomware cases by country** in 2024 and 2025

| Country | Ranking in 2025 | Victims in 2025 | Victims in 2024 | Percentage Change |
|---|---|---|---|---|
| United States | 1 | 4,057 | 2,783 | 46% |
| Canada | 2 | 420 | 300 | 40% |
| Germany | 3 | 312 | 169 | 85% |
| United Kingdom | 4 | 278 | 266 | 5% |
| Italy | 5 | 170 | 145 | 17% |
| France | 6 | 168 | 125 | 34% |
| Spain | 7 | 153 | 107 | 43% |
| **Australia** | **8** | **130** | **102** | **27%** |
| Brazil | 9 | 127 | 121 | 5% |
| India | 10 | 113 | 105 | 8% |

Source: ecrime.ch

## Focus on Australia

An outlier in the Asia-Pacific region historically, Australia has consistently been targeted by ransomware actors. Last year it placed eighth in the global standings and saw a year-on-year increase in ransomware attacks of 27% (table 2).

**Indiscriminate targeting:** Organisations of all sizes in Australia were hit over the course of the year. The national flag carrier, Qantas, suffered a data breach impacting millions of customers, prompting the company to lower bonus payments to senior executives amid a significant public backlash. However, it was SMEs that accounted for the majority (78%) of Australian companies named on ransomware leak sites. The Australian Cyber Security Centre's annual threat report found that the cost of these incidents for SMEs had increased by 14% to AUD 56,000.

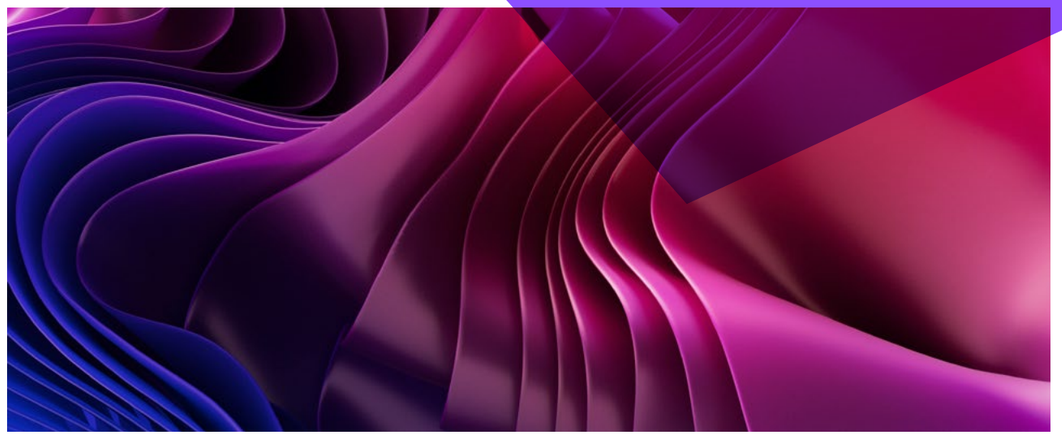
**Mandatory ransomware reporting:** 2025 was also a significant year for the regulatory landscape in Australia. The Cyber Security Act, the first of its kind globally, has introduced mandatory reporting requirements for ransom payments to the Australian Signals Directorate within 72 hours. The threshold for reporting was set relatively low, covering all organisations with an annual turnover of AUD 3 million or more, and included all organisations with business operations in Australia, not just Australian-owned entities.

# 04

# ThreatGPT:
# Emerging risks from AI







AI dominated security headlines again in 2025, with popular narratives warning of fully autonomous cyberattacks in which swarms of AI agents would breach networks, steal data, and encrypt systems at will.

The reality is more measured. While threat actor adoption of AI attracts the most attention, the more immediate risk lies in insecure AI adoption within enterprises themselves. As organisations embed AI agents into workflows, they introduce new non-human identities, expand privileged access, and create novel attack surfaces that are not yet fully understood. At the same time, AI is accelerating existing adversarial capabilities, compressing attack timelines and lowering the barrier to entry across the attack lifecycle.

**Threat Actors' use of AI –** the dawn of fully automated ransomware?

In 2025, reporting from the AI company Anthropic highlighted a case in which its Claude chatbot was allegedly used to carry out automated end-to-end ransomware attacks. An attacker was reportedly able to leverage the agentic capabilities of the AI chatbot to identify targets, harvest credentials, and even extort ransoms.

This case study has added to the general public's concern that cybercriminals are leveraging AI to create autonomous, self-adapting, or even AI-driven attacks. In practice, though, fully autonomous attacks are not yet driving financially motivated incidents at scale. While threat actors are using AI to support tasks like reconnaissance, vulnerability discovery, content generation, and code development, they are largely optimising existing tactics rather than introducing fundamentally new ones.

AI has accelerated existing threats: attacks play out more quickly, at a greater scale, and are becoming more accessible to amateur threat actors with lower levels of technical capability.

- Emerging malware families are starting to use LLMs to dynamically generate scripts, modify command sequences, and tailor content in real-time to evade detection, indicating a shift towards more adaptive tools.
- AI capabilities are being rapidly operationalised, with developer productivity tools being repurposed for offensive activities like credential harvesting and espionage within months of release rather than years.

- The discovery and exploitation of new software vulnerabilities are accelerating; for instance, AI-assisted coding expedited the exploitation of the React2Shell vulnerability, leading to immediate active exploits and a flood of non-functional AI-generated exploits on GitHub.
- State-linked actors are employing AI in various activities such as reconnaissance, social engineering, and malware development, with AI increasingly integrated into espionage operations targeting tech companies, financial institutions, and governments.

## **The dangers of autonomy –** are AI agents inherently insecure?

As AI becomes embedded into day-to-day operations, organisations are introducing more workflows using AI agents with the ability to make decisions autonomously. This expands the attack surface in ways that are not yet fully understood. Even if malicious human actors are taken out of the equation, if non-human identities are given highly privileged access to systems, there is an inherent risk that they will act in undesirable ways.

A widely-cited use case for AI agents is to assist with mailbox management, summarising the content of emails and even automatically responding. The problem from a security perspective is that this exposes the agent to prompt injection attacks, in which an attacker can hide a malicious instruction in data to be reviewed by the agent.* There are now many real-world examples of AI agents being manipulated into exfiltrating sensitive data or even facilitating account takeover via prompt injection.

The same characteristics that make AI agents powerful productivity tools (autonomy, contextual reasoning, and access to integrated systems) also make them high-value targets in an attack chain. In 2026, organisations will do well to apply the same identity, privilege, and monitoring discipline to AI systems that they apply to human users.

*This stems from an inherent vulnerability in the way LLMs function. LLMs are non-deterministic, meaning their output is never guaranteed to be the same even with the exact same input. This unpredictability complicates traditional assurance and control models. At their core, LLMs treat all inputs as 'tokens', which are used to generate output, so it is not possible to fully and meaningfully separate 'data', such as emails in your mailbox you might ask the agent to summarise or websites the agent might read when completing a research task, from 'instructions', like a command to click on a phishing link and enter your password. Mitigations exist, but no model can fully distinguish malicious instructions embedded within trusted data sources.



## **OpenClaw and AI agent security –** A lobster in the coalmine?

In the race to advance AI, security is often treated as an afterthought. This is apparent when AI is used to quickly develop and release new tools with minimal oversight and human input, often referred to as 'vibe coding'. This trend increases the likelihood that long-established security principles are bypassed in the rush to deploy code as quickly as possible to stay ahead of the competition.

The launch of OpenClaw (aka Clawdbot, aka Moltbot) in January 2026 should serve as a warning. OpenClaw is an open-source autonomous AI agent that can be installed locally to take actions on behalf of users, such as managing email or booking flights. The tool was riddled with vulnerabilities and widely decried as a security nightmare: agents were tricked into divulging passwords and API keys, and even downloading malware. Despite the clear risks, it has been installed hundreds of thousands of times.

Even without malicious intent, AI agents risk acting in insecure ways and exposing sensitive information – raising serious questions about accountability. Guardrails can reduce risk, but AI agents should be treated as untrusted identities. They require least-privilege access, continuous monitoring, and explicit segmentation from sensitive systems. Without this discipline, AI adoption risks creating privileged, opaque intermediaries that attackers can manipulate rather than breach directly.

# 05

# Looking ahead:
## What to expect in 2026





### AI adoption will result in more attacks and complicate incident response

As organisations deploy AI agents, automated workflows, and API-driven integrations, they're creating new categories of non-human identities with broad privileges. When these systems are compromised, responders face unfamiliar challenges: mapping what an AI agent accessed, what actions it took, and what data it exposed. Traditional forensic playbooks for compromised user accounts don't translate well to automation systems that interact with dozens of services and process thousands of transactions autonomously.

Security teams will need new approaches to logging, monitoring, and auditing non-human identities, as well as new frameworks for containing incidents when those identities are compromised.

### Extortion will become more targeted, personal, and harder to ignore

Ransomware groups are moving beyond generic threats of data publication. While searching for insurance policies, financial documents, and sensitive communications is already standard, attackers are getting better at identifying the most damaging material — customer data, intellectual property, regulatory violations, and anything that triggers additional legal liability.

AI-assisted review of stolen data is accelerating this shift, helping groups rapidly categorise and weaponise what they've taken. The result: extortion tailored to maximise pressure, with specific, personalised leverage designed to make victims fear the consequences of non-payment.

### Established ransomware groups will face disruption, but operators will rebrand — not disappear

A handful of dominant groups — Akira, Qilin, Scattered Spider/ShinyHunters — will continue to lead in victim counts, while smaller newcomers try to gain a foothold. This top-heavy consolidation with constant turnover at the bottom is now the norm in organised cybercrime, with new names representing both genuine entrants and rebrands of disrupted operations.

Among established players, Akira has drawn serious law enforcement attention. Given its trajectory, we expect some disruption to its operations in 2026. But history shows takedowns fragment groups rather than eliminate them. Operators often regroup under new banners with modified infrastructure. The knowledge, relationships, and capabilities that made them successful survive any single brand. Individual group names will come and go; the overall threat level won't meaningfully change.

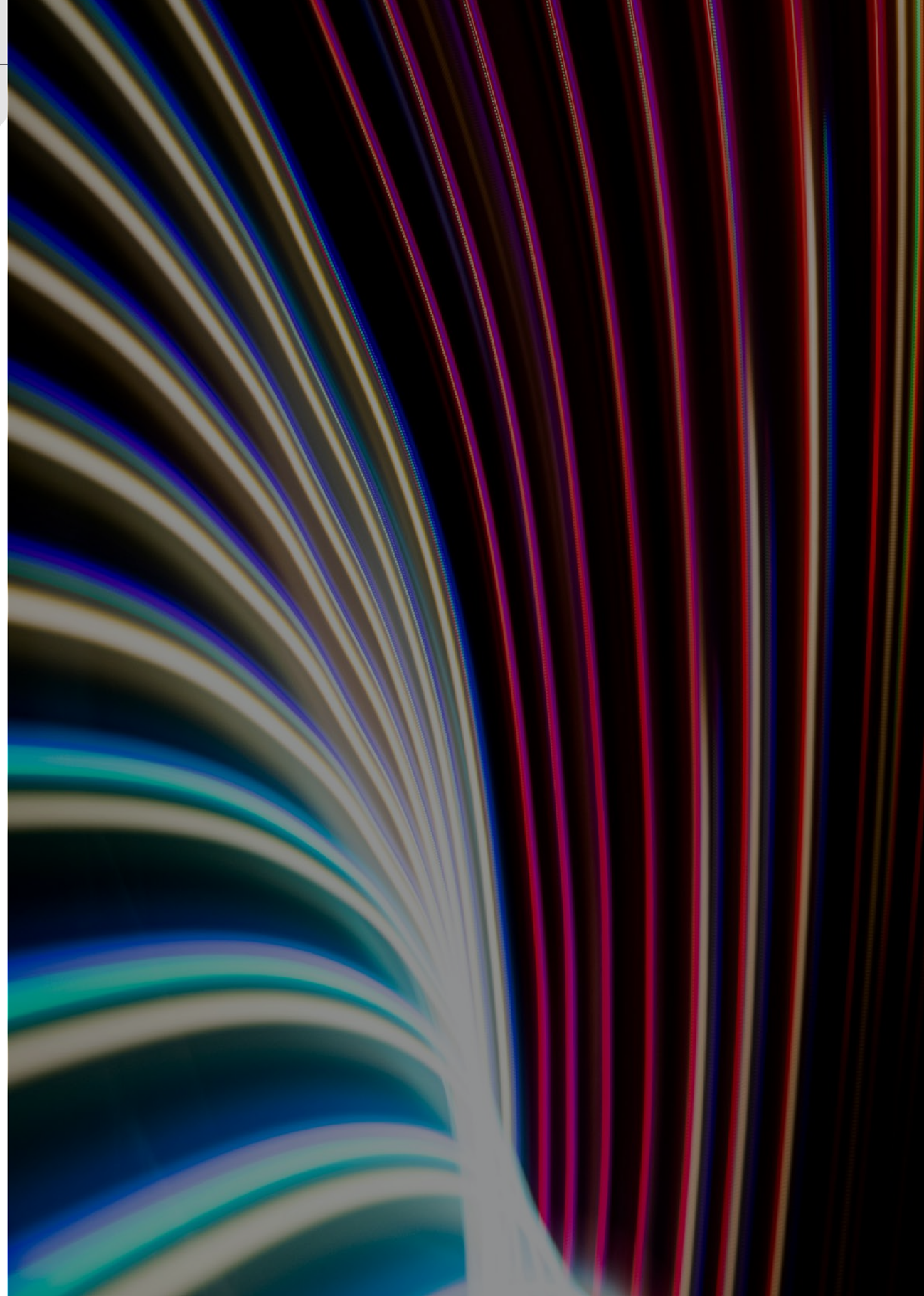
## Ransomware attacks will get faster; EDR may struggle to keep up

Ransomware operators are executing at unprecedented speed — what once took weeks now takes days, and what took days now takes hours. Better tooling, more experienced operators, streamlined playbooks, and selective use of AI for reconnaissance and lateral movement are all driving this acceleration. For defenders, the detection and response window is shrinking fast, putting greater pressure on preventative controls and rapid detection.

Making matters worse, threat actors are investing heavily in understanding and circumventing EDR products — disabling security agents, exploiting monitoring blind spots, and developing purpose-built evasion techniques. Speed and stealth are converging, and defenders need to assume both will keep improving.

## Unsecured VPNs will remain the easiest door in for attackers

Despite years of warnings and high-profile breaches, many SMEs still run VPN infrastructure with known vulnerabilities, weak authentication, or slow patching cycles. This isn't ignorance, but the reality of limited resources, competing priorities, and the complexity of maintaining secure remote access at scale. Until VPN security becomes dramatically simpler or organisations fully adopt zero-trust architectures, this will remain one of the most reliable entry vectors for threat actors.



## FGS GLOBAL PERSPECTIVE

### Cyber to remain a boardroom priority

Cyber will remain near the top of the risk register in 2026, but for evolving reasons. Companies face higher expectations from investors, employees, and customers in how they respond to incidents. Meanwhile, the combination of more targeted attacks on sensitive company data; with rapid adoption and scaling of AI tools, is rapidly changing the cyber risk profile for businesses.

Business interruption, already operationally challenging, can now be as reputationally damaging as disclosing a large data breach. The attack on car manufacturer Jaguar Land Rover in 2025 laid bare the reputational challenges of widespread business disruption, with its key suppliers scrambling to understand the impact on their own businesses; amid a perfect storm of interest from media, government, regulators, employees and business partners.

Organisations also face a speed paradox: communicate quickly to maintain trust, but risk acting on incomplete information, or wait for certainty and appear paralysed. In 2026, reputations will hinge on detection speed and the transparency, timeliness, and accuracy of a company's response. Preparing for how to manage the stakeholder fallout from a cyber attack has never been more important.

Ultimately, the companies that emerge relatively unscathed in 2026 will be those that treat security posture, business resilience and stakeholder engagement as inseparable.



## Contributors


### S-RM

**Aditya Ganjam Mahesh**
Senior Analyst, Incident Response

**Daniel Caplin**
Director, Incident Response, Americas

**James Tytler**
Senior Associate, Incident Response

**Kyle Schwaeble**
Head of Incident Response, APAC

**Lawrence Copson**
Associate, Incident Response

**Melissa DeOrio**
Global Cyber Threat Intelligence Lead

**Tom Crooke**
Senior Associate, Incident Response

**Virginia Romero**
Global Delivery Lead, Incident Response

### FGS Global

**Jenny Davey**
Partner and Global Co-Head, Crisis & Issues Management Practice

**Kelly Kimberly**
Partner and Co-Head, Cybersecurity & Data Privacy Practice

**Charles O'Brien**
Partner and Head of Crisis Paris

**Johannes Steger**
Managing Director, Crisis & Issues Management Practice

**Kelly Langmesser**
Managing Director, Crisis & Issues Management Practice

**Oli Sherwood**
Managing Director, Crisis & Issues Management Practice

**Alex Felton**
Director, Crisis & Issues Management Practice

**Tom Grant**
Director, Crisis & Issues Management Practice


## Editors


**Casey O'Brien**
Global Head of Incident Response, S-RM

**Lenoy Barkai**
Director, Cyber Security, S-RM

# Contact us


## S-RM

**Jamie Smith**
Global Managing Director,
Cyber Security
j.smith@s-rminform.com

**Paul Caron**
Global Managed Services Lead & Head of
Cybersecurity, Americas
p.caron@s-rminform.com

**Lester Lim**
Regional Head, APAC, Cyber Security
l.lim@s-rminform.com

## FGS Global

**Jenny Davey**
Partner and Global Co-Head, Crisis
& Issues Management Practice
jenny.davey@fgsglobal.com

**Kelly Kimberly**
Partner and Co-Head, Cybersecurity
& Data Privacy Practice
kelly.kimberly@fgsglobal.com

**Ben Richardson**
Partner and Head of Asia
ben.richardson@fgsglobal.com


---

### About S-RM

S-RM is a cyber security and corporate intelligence consultancy. We provide intelligence, resilience and response solutions to organisation worldwide. Founded in 2005, we have 400+ experts across nine international offices, serving clients across all regions and major sectors. Find out more at www.s-rminform.com

### About FGS Global

FGS Global is the world's leading stakeholder strategy firm, with over 1,500 professionals across 31 offices worldwide. We advise clients on integrated strategies that build and protect reputation, activate stakeholders, and achieve business-critical outcomes in today's complex environment. Find out more at www.fgsglobal.com