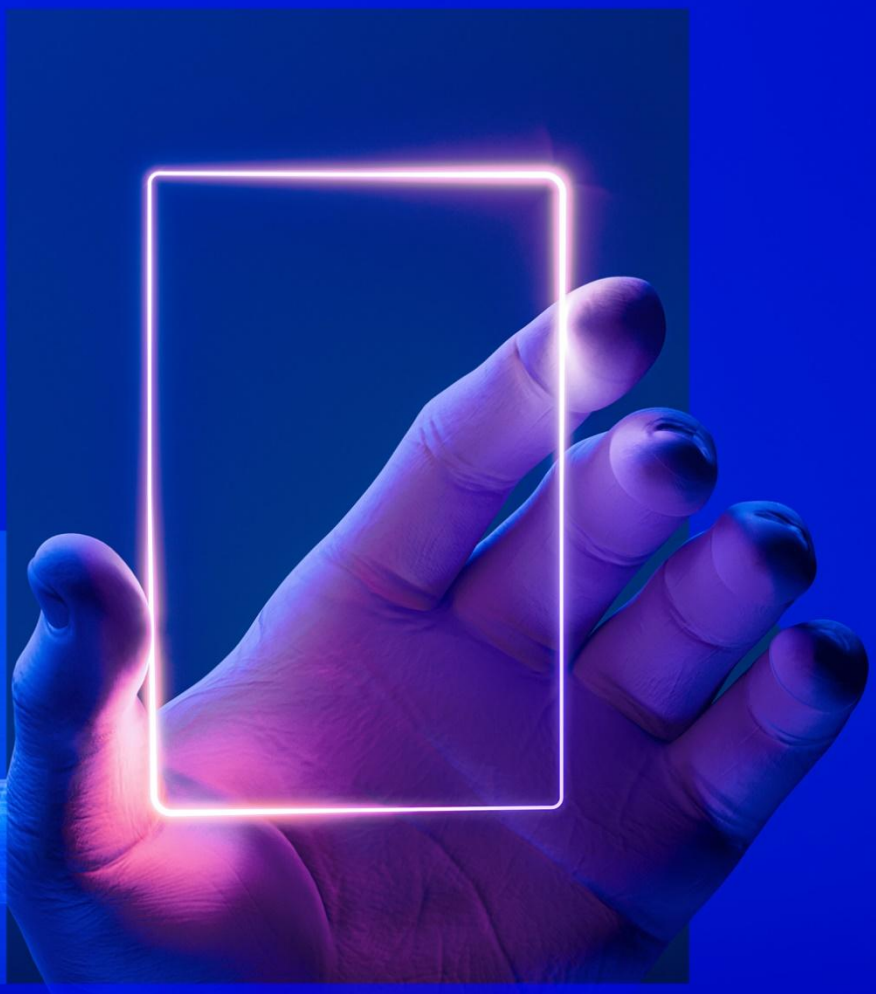
KPMG

2025 Global IR Trend Report

Cyber Incidents and Intelligence

Year-in-Review

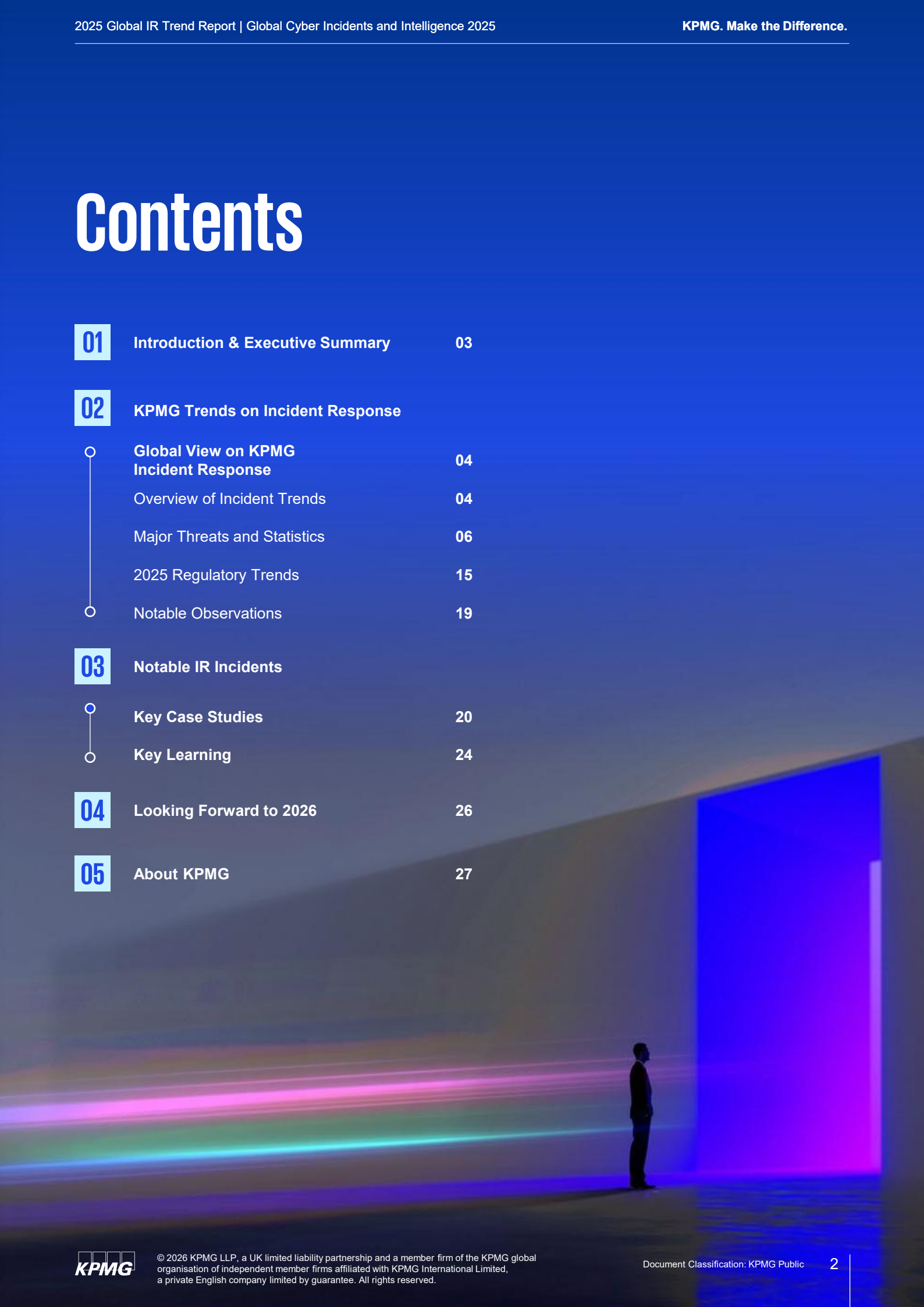
kpmg.com



KPMG. Make the Difference.

May 2026

Contents



01 | Introduction & Executive Summary

Cyber threats are advancing in scale, complexity, and global influence. In 2025, KPMG's **global network of Incident Responders (IR)** noted a significant rise in cross-border threat activity, swift exploitation of high-impact vulnerabilities, and greater operational sophistication among both financially driven and state-affiliated adversaries impacting organizations worldwide.

From KPMG's perspective, 2025 has been defined less by a single dominant ransomware cartel and more by high-volume, fast-moving Ransomware-as-a-Service (RaaS) ecosystems. Groups like **Qilin** and **Akira** continue to show up repeatedly across live cases, typically leveraging compromised credentials, unpatched edge infrastructure, or poorly governed remote access to move quickly to impact. **Cl0p** remains relevant due to its ability to execute large-scale campaigns tied to third-party and data-exfiltration events, while **DragonForce** and similar affiliate-heavy groups are gaining traction by lowering the barrier to entry for attackers. What stands out operationally is the churn: new names appear, rebrand, or disappear rapidly. Threat Actor tradecraft, however, remains consistent: identity abuse, speed over stealth, double-extortion, and pressure on business operations rather than technical persistence.

KPMG's global IR network continues to observe cyber insurance having a material influence on incident response maturity. Organizations increasingly maintain pre-negotiated incident response retainers, breach counsel, and crisis communications pathways, as insurers now expect rapid, disciplined execution within the first 24 – 72 hours.

In breaches, the difference between a contained event and a business-wide crisis comes down to preparedness, clear decision rights, tested playbooks, and the ability to produce defensible forensic evidence quickly. Post-incident, insurers scrutinize root cause and control failures, feeding directly into security investment decisions. The net effect is that cyber insurance is becoming embedded in enterprise risk governance, not just to pay for breaches, but to actively reduce their likelihood, scope, and impact. It has become a forcing function for better security hygiene, not a passive financial backstop. From active breach engagements, the most common root causes in insured incidents remain consistent: Multi Factor Authentication (MFA) gaps, over-privileged identities, misconfigured Endpoint Detection and Response (EDR) deployments, weak logging, and poor patch discipline. Organizations are responding by aligning security roadmaps directly to insurer expectations, tightening identity and access management, validating backup and recovery procedures, improving asset visibility, and operationalizing detection rather than relying on tools alone. Premiums, coverage limits, and claim eligibility are now tied to whether these controls work in practice, not merely whether they exist on paper.

This report offers a global perspective on the cyber incidents investigated by KPMG member firms worldwide, highlighting major trends, threat actor behaviors, and industry-specific insights observed throughout 2025. Developed collaboratively by KPMG's global network of Incident Responders and Cyber Threat Intelligence analysts, the report provides data-driven analysis, strategic lessons learned, and forward-looking considerations to help organizations enhance their security posture.

Findings are derived from real incidents handled by KPMG's global network of cyber incident responders in 2025. While the nature of these events are accurately reflected, identifying information has been removed to preserve confidentiality.

02 | KPMG Trends on Incident Response

02.01 | Global View on KPMG Incident Response

Overview of Incident Trends

2025 Incidents by Regions

We now pivot from the strategic overview of a rapidly advancing threat landscape to the hard data. This section examines key trends from KPMG's 2025 frontline incident response engagements globally, from the dominance of Ransomware-as-a-Service (RaaS) to the exploitation of foundational control gaps. Our granular analysis of geographic and industry threat landscape and adversary tactics offers perspective to help global leaders benchmark risk and fortify their defenses.

Europe

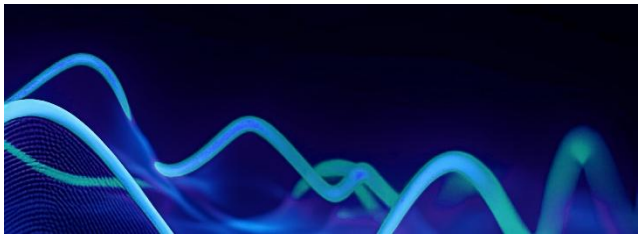
In Europe, incident complexity and cost are magnified by the continent's intense regulatory pressure, where the primary driver of an engagement is often the immense risk of non-compliance. For instance, a data breach at a multi-national financial services firm requires a response where technical recovery is only the start. The bulk of the effort, which pushes the average cost over €250K, is a legally-driven transformation to manage mandatory 72-hour breach disclosures across multiple countries and mitigate the threat of crippling GDPR fines. This has fundamentally shifted our response model beyond standard IR to integrate legal, compliance, and crisis management, ensuring full and defensible business resilience.

Europe continues to account for the largest share of recorded incidents, shaped by its diverse industrial landscape, digital interconnectedness, evolving regulatory environment, and current geopolitical climate. Heightened tensions, particularly across Eastern Europe and the broader European Union (EU), have made organizations increasingly attractive to both financially motivated and state-aligned threat actors. In 2025, KPMG's Incident Responders observed high-tempo ransomware activity driven by established RaaS ecosystems, with engagements frequently involving actors linked to **Qilin**, **Akira**, and **Scattered Spider-style** affiliates moving quickly through identity compromise and edge infrastructure exposure. Manufacturing, retail, and financial services remain heavily targeted, with attacks prioritizing speed to encryption and data theft. Regulatory complexity and cross-border impact add further friction, which adversaries actively exploit to increase extortion leverage.

Asia Pacific

In the Asia Pacific region, the narrative of cost and complexity is one of operational survival for the significant volume of mid-tier companies under attack. For these businesses, the immediate, existential threat is not a regulatory fine but a paralyzed production line from a ransomware attack or a halted logistics network. These victims require a uniquely rapid and efficient response model that prioritizes business continuity. Our approach has therefore evolved into a pragmatic transformation focused on speedy recovery, rebuilding core systems, and ensuring immediate operational resilience to get these businesses back on their feet.

Asia Pacific is driven by rapid digital transformation and accelerated adoption of emerging technologies. Incident volumes are comparable to Europe, though the complexity and scale of breaches are notably smaller. KPMG's Incident Responders observed a combination of global ransomware operators and regionally concentrated campaigns, with groups such as **Qilin** and **Makop** surfacing regularly, exploiting credential reuse, unmanaged remote access, and delayed patching. Aggressive double-extortion tactics are common, with attackers assuming lower response maturity and slower decision cycles. APAC organizations are no longer opportunistic targets; they are deliberate, repeat targets due to scale, data value, and uneven security governance.



02 | KPMG Trends on Incident Response (Cont.)

The Americas

In the Americas, the incident response landscape is driven by the sheer scale and complexity of incidents, particularly within the mature U.S. market. Engagements frequently involve deeply embedded threat actors within large, multinational corporations, making the response a massive program of work. This complexity of moving from simple containment to painstakingly hunting an adversary across a vast network inherently creates a longer and more costly incident response cycle. Consequently, our approach has evolved to include deep, transformative requirements and enterprise-wide resilience-building, turning what was once a short-term IR event into a prolonged and necessarily expensive strategic recovery effort.

The region exhibited incident activities that are consistently targeted across both public and private sectors, with a mix of high severity complex engagements. In 2025, KPMG's frontline responders repeatedly encountered **Akira**, **Qilin**, **Cl0p**, **RansomHub**, and affiliate-driven crews operating at scale. Initial access typically involved compromised credentials, VPNs, RDP, or third-party compromise, with execution that was fast and business-impact focused. A defining characteristic of 2025 activity is churn: groups rebrand, splinter, or merge, but the playbook remains consistent. From an IR perspective, incidents increasingly blur the line between ransomware, data extortion, and supply-chain fallout, underscoring the need for cross-sector collaboration and scalable response frameworks.

Oceania

The Oceania landscape is defined by its position as a high-value target for sophisticated, globally-operating cybercrime syndicates. A ransomware attack on a major Australian retailer, for instance, is rarely a simple encryption event; it's often a multi-faceted crisis involving 'double extortion,' where sensitive customer data is also stolen and threatened to be leaked. This tactic is what drives response costs well over $750K, as engagements must expand beyond technical recovery to include crisis communications, potential extortion negotiations, and managing intense public and regulatory scrutiny. Our approach is therefore a comprehensive transformation aimed at hardening defenses against these persistent, globally-orchestrated criminal campaigns.

While Oceania reports the lowest incident volume, this may reflect reduced reporting frequency as much as reduced exposure. In 2025, KPMG's frontline responders observed consistent activity from the same global ransomware groups impacting Australia and New Zealand, particularly **Qilin** and **Akira**. Tactics mirror those seen in larger regions: rapid lateral movement, cloud and identity abuse, and pressure via data exposure. The operational impact, however, can be outsized due to smaller teams and concentrated infrastructure. The key frontline takeaway is that Oceania is not insulated; attackers treat it as part of the global operating theatre, not a secondary market.

Mapping incident response activity by region reveals not just where threats concentrate, but how consistent the underlying patterns are. Regardless of geography, the same actor groups, initial access vectors, and exploitation playbooks appear repeatedly. For CISOs and security leaders, the implication is that no region operates in isolation. Cyber risk is globally distributed, and so must be the response.

Major Threats and Statistics

2025 Data Events by Industry

Europe (EU)

In 2025, Europe continued to demonstrate a pronounced concentration of cyber incidents within **industrial and manufacturing (30%),** and **financial services (18%),** reflecting sustained targeting of the region's industrial base and critical economic infrastructure.

Consumer-facing organizations (17%) and **professional services (11%)** also reported notable incident volumes, highlighting broad exposure across commercial operations and persistent risk to customer data, business continuity, and third-party relationships.

Technology & Media, Healthcare & Life Sciences, and **Government & Education sectors** each comprised **8%** of reported incidents, demonstrating that threat activity in Europe remains distributed across essential services and digitally dependent functions.

Beyond the direct impact of cyber threats, organizations operating in Europe have faced additional challenges stemming from macroeconomic and regulatory developments. The introduction of new trade restrictions, particularly in response to geopolitical tensions, has led to increased operational costs and uncertainty for many industrial and manufacturing firms. These pressures, in some cases, have resulted in reduced spending on security initiatives and workforce reductions, which can hinder the ability to respond to and recover from cyber incidents effectively.

Furthermore, evolving regulatory requirements, such as the EU's Digital Operational Resilience Act (DORA) and amendments to the Cybersecurity Act are driving organizations to reassess their incident response and reporting capabilities. While these regulations aim to strengthen cyber resilience, they also necessitate extra investment in compliance, reporting infrastructure, and skilled personnel. For sectors already contending with budget constraints or reduced headcounts, meeting these new standards can be particularly challenging, potentially increasing risk exposure and elongating recovery timelines.

Key Takeaway

In Europe, incident complexity and cost are magnified by the continent's intense regulatory pressure, where the primary driver of an engagement is often the immense risk of non-compliance. For instance, a data breach at a multi-national financial services firm requires a response where technical recovery is only the start. The bulk of the effort, which pushes the average cost over $500k, is a legally-driven transformation to manage mandatory 72-hour breach disclosures across multiple countries and mitigate the threat of crippling GDPR fines. This has fundamentally shifted our response model beyond standard IR to integrate legal, compliance, and crisis management, ensuring full and defensible business resilience.

Taken together, these factors underscore the importance of strategic investment in security controls, workforce development, and regulatory readiness. CISOs and IT leaders should prioritize initiatives that deliver measurable improvements in resilience and response capability, while also advocating for sustained funding and cross-functional collaboration to address the evolving risk landscape in Europe.

Percentage of events reported in Europe (generalized)

Industrial & Manufacturing

30%

Manufacturing, Construction, Engineering, Heavy Industry

Financial Services

18%

Banking, Insurance, Financial Institutions

Consumer & Retail

17%

Retail, Food & Beverage, Hospitality, Consumer Goods

Professional Services

11%

Consulting, Business Services

Technology & Media

8%

IT, Communications, Media

Healthcare & Life Sciences

8%

Healthcare, Pharmaceuticals, Research

Government & Education

8%

Public Sector, Education, Social Services

Major Threats and Statistics (Cont.)

2025 Data Events by Industry

Asia Pacific (APAC)

In 2025, the Asia Pacific region exhibited a broad and diverse distribution of cyber incident activity, underscoring an increasingly complex and interconnected threat landscape. **Industrial and manufacturing organizations** accounted for **18%** of reported incidents, reflecting sustained exposure to attacks targeting operational technology, supply chains, and critical infrastructure. **Professional services**, **healthcare and life sciences**, and **consumer and retail** organizations each represented **17%** of incidents, highlighting the continued targeting of service-driven and customer-facing sectors that rely heavily on digital platforms, sensitive data, and extensive third-party ecosystems.

The widespread distribution of incidents across industries reflects the rapid expansion of the region's digital footprint, which has materially increased exposure to cyber threats. Key trends observed during the period include a marked rise in automated attacks, the emergence of cross-border advanced persistent threat (APT) campaigns, and increased targeting of critical infrastructure – such as transportation networks, public-facing web portals, and municipal services – often exacerbated by ineffective security controls. Phishing and fraud activity also continued to escalate, further complicating the regional threat environment.

Technology and media, along with financial services organizations, each account for **14%** of incidents, reinforcing the persistent focus by threat actors on digitally dependent and data-intensive industries. Attacks in these sectors frequently exploit sector-specific vulnerabilities, including intellectual property theft, data breaches, and financial fraud. While **government and education entities** represented a smaller proportion of incidents at **3%,** their involvement remains significant given their role in delivering essential public services and managing critical systems.

Despite the growing scale and sophistication of cyber activity, transparency around cyber incidents remains limited across many Asia Pacific jurisdictions. Comprehensive incident reporting is inconsistent, with details often reconstructed from fragmented sources such as local CERTs, law enforcement disclosures, or media reporting. This lack of visibility constrains organizations' ability to benchmark risk, share lessons learned, and coordinate effective response strategies. Collectively, these factors reinforce the need for organizations across APAC to strengthen incident response frameworks, enhance cross-sector collaboration, and continuously mature their cyber resilience to address an evolving and multifaceted risk landscape.

Key Takeaway

In the Asia Pacific region, the narrative of cost and complexity is one of operational survival for the significant volume of mid-tier companies under attack. For these businesses, the immediate, existential threat is not a regulatory fine but a paralyzed production line from a ransomware attack or a halted logistics network. These victims require a uniquely rapid and efficient response model that prioritizes business continuity. Our approach has therefore evolved into a pragmatic transformation focused on speedy recovery, rebuilding core systems, and ensuring immediate operational resilience to get these businesses back on their feet.

Percentage of events reported in Asia Pacific (generalized)

Industrial & Manufacturing

18%

Manufacturing, Automobile, Shipping, Energy & Power

Professional Services

17%

Consulting, Business Services, Legal (Law), General Services

Healthcare & Life Sciences

17%

Healthcare, Medical, Pharmaceuticals, Research

Consumer & Retail

17%

Retail, Food & Beverage, Event & Retail, Consumer Goods

Technology & Media

14%

IT, Data, Communications, Telecom/Media

Financial Services

14%

Banking, Insurance, Finance

Government & Education

3%

Education

Major Threats and Statistics (Cont.)

2025 Data Events by Industry

The Americas

In 2025, the Americas region experienced a notably diverse impact from cyber incidents, with threat activity spanning a wide array of industries and critical functions. **Professional Services** accounted for the highest proportion of reported incidents at **22%,** underscoring the sector's vulnerability due to its extensive handling of sensitive client data, reliance on digital platforms, and frequent third-party interactions.

Government and Education organizations comprised **15%** of incidents, highlighting the ongoing risk to national and public sector bodies, including educational institutions. These often face resource constraints and are responsible for safeguarding large volumes of personal and operational data.

Industrial and Manufacturing, Fast Moving Consumer Goods, and Retail sectors, each represented **18%** of reported events, reflecting the persistent targeting of both operational environments and customer-facing domains. These sectors are particularly exposed to supply chain disruptions, ransomware, and attacks aimed at operational systems.

Technology & Media organizations, at **(13%),** continue to be targeted for intellectual property theft, service disruption, and reputational risk, while **Healthcare & Life Sciences (9%)** remain attractive to threat actors seeking access to confidential patient information and research assets. **Financial Services**, though representing a smaller share **at 5%,** are persistently targeted due to the high value of financial data and the potential for fraud.

Key Takeaway

In the Americas, the narrative is driven by the sheer scale and complexity of incidents, particularly within the mature U.S. and Canadian markets. Engagements frequently involve deeply embedded threat actors within large, multinational corporations, making the response a massive program of work. This complexity moving from simple containment to painstakingly hunting an adversary across a vast network inherently creates a longer and more costly incident response cycle. Consequently, our approach has evolved to include deep, transformative requirements and enterprise-wide resilience-building, turning what was once a short-term IR event into a prolonged and necessarily expensive strategic recovery effort.

Percentage of events reported in the Americas (generalized)

Professional Services

22%

Consulting, Business Services

Industrial & Manufacturing

18%

Manufacturing, Construction, Heavy Industry

Consumer & Retail

18%

Retail, Food & Beverage, Hospitality

Government & Education

15%

Public Sector, Education

Technology & Media

13%

IT, Communications

Healthcare & Life Sciences

9%

Healthcare, Pharmaceuticals

Financial Services

5%

Banking, Insurance

Major Threats and Statistics (Cont.)

2025 Data Events by Industry

Oceania

In 2025, Oceania exhibited a balanced distribution of cyber incidents across both core service and operational sectors, highlighting the region's broad exposure to evolving threat activity. **Professional Services** represented the most frequent target, **accounting** for **33%** of reported incidents. This reflects the sector's significant reliance on digital platforms, sensitive client data, and complex third-party relationships, which collectively increase its vulnerability to cyber-attacks.

Government & Education, Financial Services, and **Industrial & Manufacturing sectors** each reported comparable levels of impact, with **17%** of incidents attributed to each category. This parity indicates that both public and private entities in Oceania face similar risks, regardless of their operational focus. The persistent targeting of government and educational institutions underscores the importance of safeguarding critical public services and personal data, while the exposure of financial and industrial organizations highlights ongoing risks to economic stability and the integrity of supply chains.

Technology & Media organizations, comprising **16%** of reported incidents, continue to be targeted for intellectual property theft, service disruption, and reputational risk. The consistent presence of these sectors within the incident dataset demonstrates that threat activity in Oceania is not confined to any single vertical but rather affects a spectrum of essential services and operational domains.

Overall, the data reinforces the imperative for organizations in Oceania to maintain incident response frameworks, foster cross-sector collaboration, and invest continuously in cyber resilience. This approach is essential for addressing the complex and evolving risk landscape that affects both public and private entities across the region.

Key Takeaway

The Oceania landscape is defined by its position as a high-value target for sophisticated, globally operating cybercrime syndicates. A ransomware attack on a major Australian retailer, for instance, is rarely a simple encryption event; it is often a multi-faceted crisis involving 'double extortion,' where sensitive customer data is also stolen and threatened to be leaked. This tactic drives response costs well over $750K, as engagements must expand beyond technical recovery to include crisis communications, potential extortion negotiations, and managing intense public and regulatory scrutiny. Our approach is therefore a comprehensive transformation aimed at hardening defenses against these persistent, globally orchestrated criminal campaigns.

Percentage of events reported in Oceania (generalized)

Professional Services

33%

Consulting, Business Services

Government & Education

17%

Public Sector, Education

Financial Services

17%

Banking, Insurance

Industrial & Manufacturing

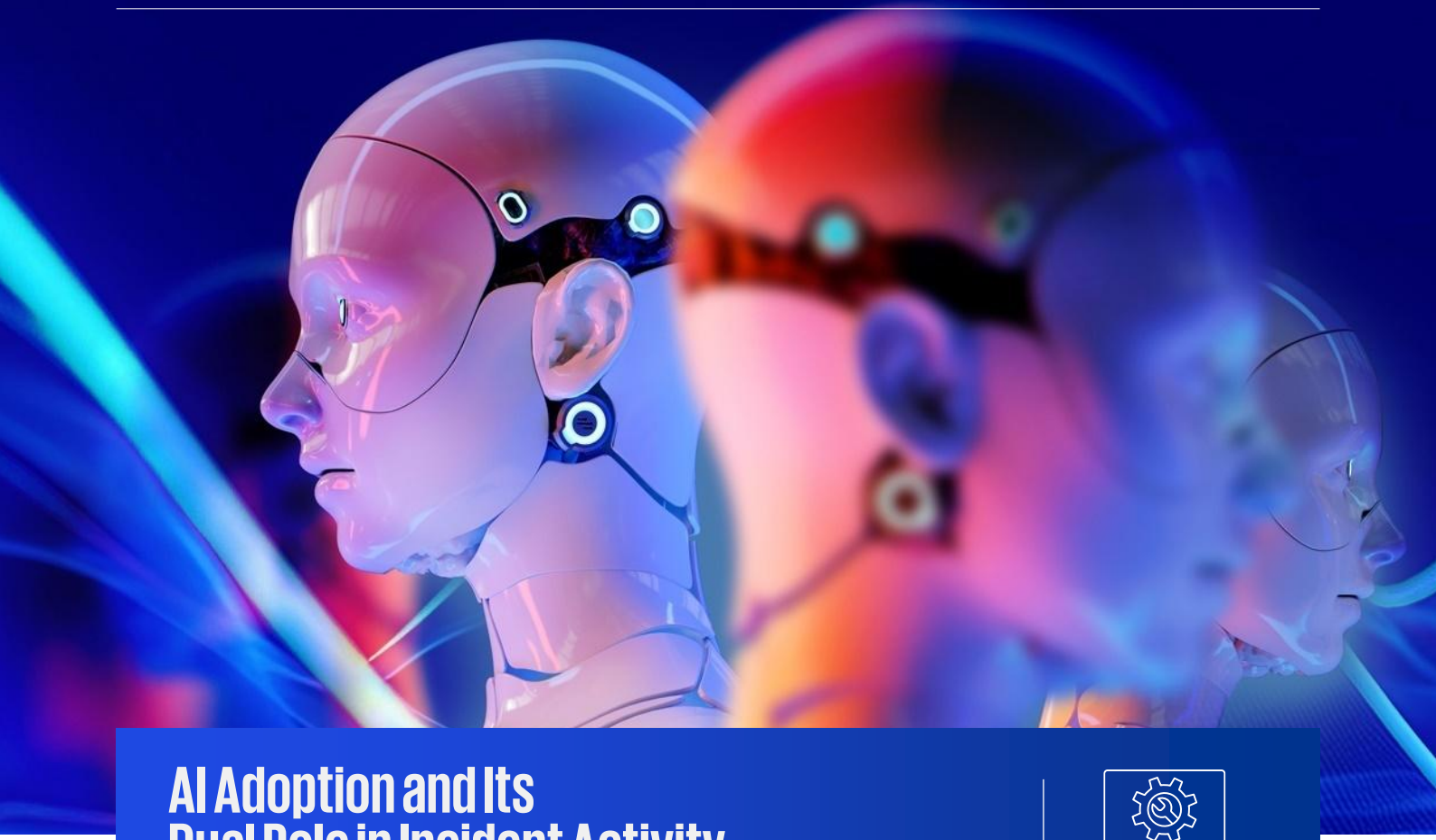
17%

Manufacturing, Heavy Industry

Technology & Media

16%

IT, Communications



AI Adoption and Its Dual Role in Incident Activity

AI usage in Threat Vector Enhancement

While truly autonomous Artificial Intelligence (AI)-driven malware has not yet been observed in the wild, 2025 marked a notable rise in threat actors using Large Language Models (LLMs), such as ChatGPT, Gemini, and other publicly available tools, to enhance their operations during active breaches. Threat actors increasingly rely on AI to troubleshoot exploitation errors, refine attack paths, and adjust tactics at runtime, similar to how early career developers use LLMs to solve technical challenges. For example, comments and icons can make scripts appear more structured and AI-generated. In several investigations this year, AI was also used by adversaries to draft extortion communications and improve negotiation strategies, resulting in more polished and targeted interactions with victims.

AI usage in Incident Response

At the same time, incident responders are harnessing AI to accelerate forensic and analytical activities, which has reshaped response timelines. Tasks that previously required manual reverse engineering, such as de-obfuscating scripts, interpreting encoded payloads, or identifying malicious logic embedded in offensive tools, can now be completed within seconds using AI-assisted analysis. These capabilities reduce investigative cycle times, improve accuracy, and allow responders to redirect their effort toward higher-value activities such as adversary attribution, containment strategy, and risk quantification. The growing integration of AI across both threat activity and defensive operations reflects a significant shift in how incidents unfold and how organizations prepare for response.

Key Takeaway

In 2026, our global incident response teams anticipate that threat actors will heavily use AI to develop and deploy malware, while incident responders will leverage AI-based tools to create strategies and capabilities to quickly detect and respond to these threats.

2025 Regulatory Trends

Across global jurisdictions, regulatory authorities are intensifying their focus on cybersecurity incident reporting, driving a shift from flexible, organization-defined notification practices to more prescriptive, regulator-mandated requirements. This evolving landscape is characterized by shorter reporting windows, standardized reporting templates, and explicit obligations to disclose incidents involving third-party or outsourced services. Recent regulatory changes in the United States, Canada, the European Union, the United Kingdom and China reflect a collective move toward greater transparency, accountability, and harmonization in incident response processes. These developments underscore the need for organizations to proactively adapt their compliance strategies, enhance reporting capabilities, and ensure readiness to meet increasingly stringent regulatory expectations.

Note

1. https://www.nist.gov/news-events/news/2025/04/nist-revises-sp-800-61-incident-response-recommendations-and-considerations
2. https://www.osfi-bsif.gc.ca/en/guidance/guidance-library/osfi-technology-cyber-incident-report-detailed-instructions
3. CP24/28: Operational Incident and Third Party Reporting | FCA
4. CP17/24 – Operational resilience: Operational incident and outsourcing and third-party reporting | Bank of England
5. https://www.lw.com/en/insights/china-cac-announces-new-cybersecurity-incident-reporting-measures

The Americas (USA & Canada):

In the United States, the National Institute of Standards and Technology (NIST)[1] updated their incident response guidance to align with the CSF 2.0 framework. The new recommendations organize incident response activities according to standardized functions, categories, and subcategories, supporting more efficient and effective detection, response, and recovery. This guidance aims to reduce the number and impact of incidents, while promoting leading practices for structured and timely reporting across the sector.

In Canada, regulators have reinforced a more structured approach to cybersecurity incident reporting. The Office of the Superintendent of Financial Institutions (OSFI)[2] in January 2025, published updated instructions and a refreshed incident reporting form, introducing clearer requirements and implementation timelines for regulated entities. This shift emphasizes the need for timely, standardized, and transparent reporting, aligning with global trends toward regulator-defined timetables and explicit declarations regarding third-party involvement in incidents.

European Union & United Kingdom:

In the EU, the Digital Operational Resilience Act (DORA) became applicable in January 2025, mandating in-scope financial entities to report major ICT-related incidents and, in some cases, significant cyber threats, using harmonized criteria and supervisory processes. Additional amendments, such as the Cyber Solidarity Act and updates to the EU Cybersecurity Act, are establishing EU-level mechanisms for coordinated response. The UK has also advanced its regulatory framework, with the FCA[3] and Bank of England[4] consulting on operational incident and third-party reporting requirements. The proposed Cyber Security and Resilience Bill[5] will require managed service providers to comply with mandatory security standards and report significant incidents within strict timeframes, further tightening the regulatory landscape.

Asia Pacific (China):

China has long required organizations to maintain incident response capabilities and report significant cybersecurity incidents. This framework was materially strengthened in 2025 with the issuance of the National Cybersecurity Incident Reporting Management Measures, which introduced a centralized, standardized incident reporting regime with clear incident classification and strict, tiered reporting timelines, including one-to-four-hour notification requirements depending on incident severity and the involvement of Critical Information Infrastructure (CII).

In parallel, amendments to China's Cybersecurity Law, adopted in 2025 and effective from January 2026, further reinforce mandatory incident response and reporting obligations and expand regulatory enforcement authority, increasing accountability for delayed, omitted, or inadequate incident disclosure.

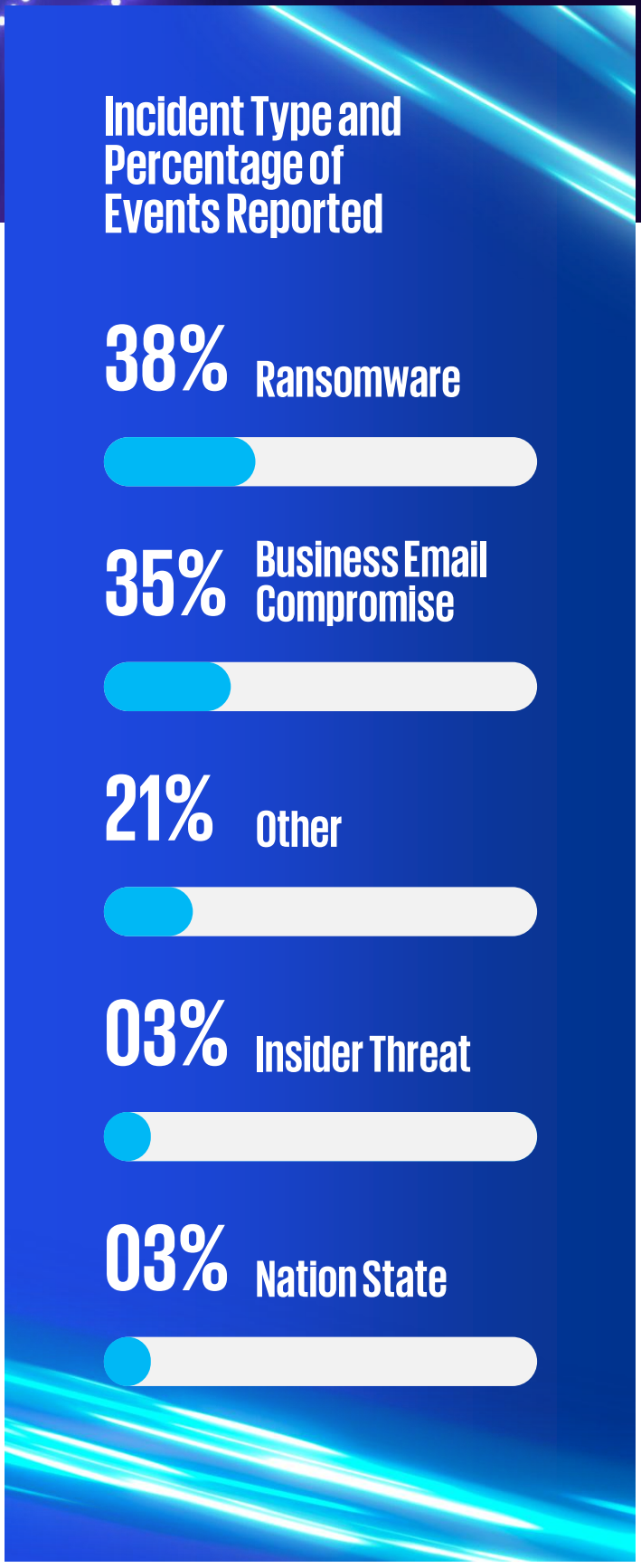
Incident Classification Metrics

In 2025, **ransomware** and **Business Email Compromise (BEC)** continued to dominate the cyber threat landscape, together accounting for most reported incidents. **Ransomware** attacks comprised **38%** of all cases, underscoring the persistent risk posed by adversaries seeking to disrupt operational systems and extort organizations through data encryption and ransom demands. **BEC** followed closely at **35%,** reflecting ongoing pressure on corporate email environments and the increasing sophistication of social engineering tactics used to facilitate unauthorized fund transfers, data theft, and reputational harm.

While these two incident types remain at the forefront, a notable proportion of events fell into other categories, including insider-related threats and nation-state activity. **Insider threats**, though representing a smaller share at **3%,** highlight the ongoing challenge of managing privileged access and detecting malicious activity within the organization. The proportion of **Nation-state sponsored** incidents at **3%** emphasize the continued presence of highly motivated and well-resourced actors targeting critical infrastructure, intellectual property, and sensitive data for strategic advantage. Even with a low volume of these incidents, it is critical to continue investing in security programs to enhance organizational security posture against these persistent threats.

The remaining 21% of incidents were classified as "Other," encompassing a diverse array of attack vectors and threat actor motivations. This distribution illustrates the multifaceted nature of the threat environment, where organizations must contend with a broad spectrum of risks beyond the most prevalent attack types.

Incident Type and Percentage of Events Reported



Unmasking Modern Ransom: Cyber Extortion and Negotiation Trends for 2025

KPMG collaborated with CyberSteward Inc. to bring forward 2025 insights into the evolving landscape of ransomware negotiations and attack tactics, informed behind the scenes experience. Leveraging CyberSteward's extensive experience in handling high-stakes cyber extortion cases, these perspectives inform and enhance KPMG's own incident response strategies, equipping CISOs and IT leaders to better understand adversary tactics and refine their defensive posture.

Based on CyberSteward Inc.'s (www.CyberSteward.com) experience in 2025, business services (general), retail, and manufacturing were the most heavily impacted sectors. Professional services and education also remained key targets due to the nature of data residing within their systems, including PII, PHI and IP. While CyberSteward continued to see demand for its global services increase, most cases originated from the USA, Canada, and the UK, with a notable increase in incidents from Asia and LATAM compared to previous years. Incident volumes were similar to last year, with the September-November period being the busiest, while the January-March period was the least active. Throughout the year, CyberSteward frequently engaged with several well-known and established Threat Actor groups, including **Akira, Qilin, INC Ransom, RansomHub,** and **Cl0p.** We observed that Threat Actors treated their attacks as a crime of opportunity and focused on the revenues of the organization and nature of the data they had obtained to inform their demands and guide negotiations. CyberSteward supported organizations ranging from small, family-owned businesses to multi-billion-dollar companies.

In 2025, CyberSteward observed initial ransom demands averaged USD ~$1.75M, with a median demand of USD ~$500K. In cases where negotiations were warranted, ~50% of organizations negotiated a settlement for decryptors and/or the deletion and suppression of stolen data.

AI use by Threat Actors is growing immensely in various layers of the attack kill-chain, including negotiations. CyberSteward has noted an increase in the trend of receiving threat actor communications that are clearly structured by LLMs. CyberSteward has undertaken internal research on LLM understanding of ransomware negotiations and identified that prevalent negotiation methods used by the industry are well understood by such models, and hence, it is clear that the risk of following scripted negotiation approaches will be rebuffed by adversaries using LLMs to oppose such discussions.

Data exfiltration capabilities are growing exponentially, with Threat Actors using improved tooling, growing experience in data candidate selection and even AI-built tools to select sensitive data elements and improve the rate of exfiltration speed. These capabilities were observed in numerous incidents, where data exfiltration is quickly moving from the Gigabyte realm and quickly into the Terabyte realm. **Cl0p's** recent campaign demonstrates an average of over a Terabyte of exfiltrated data per victim organization. Similar levels of exfiltration have been observed in **Qilin** and some **Akira** incidents.

Unmasking Modern Ransom: Cyber Extortion and Negotiation Trends for 2025 (cont.)

CyberSteward noticed Threat Actors were generally unwilling to offer meaningful reductions until a counteroffer was presented, unlike previous years when they were more willing to provide initial **10%-20%** discounts to kick-start negotiations. This change may have been driven by the perception that the demand was reasonably priced and within the organization's ability to pay. CyberSteward found that threat actors often expected victims to make the first offer, applying time pressure and threatening data publication, with reductions typically granted only after an offer was made that they considered credible or serious. Across all matters, CyberSteward successfully negotiated demands down to an average of approximately **68%** across all aggregate matters by applying a unique modified approach to its standard methodology, used in the market since 2020. Applying novel approaches to negotiations is a critical aspect to ensure that AI generated negotiation strategy from LLM models is not as effective, and that more experienced adversaries are pushed into unknown territories.

Overall, throughout 2025, CyberSteward observed an increase in data extortion cases compared to double extortion events, with more organizations opting to pay for data deletion and suppression, particularly in incidents involving sensitive, regulated, or high-value information. Approximately **34%** of matters were for data only, an increase of **35%** over the previous year. It appeared that Threat Actors focused on identifying data with extortion value rather than relying on traditional ransomware and encryption. Companies not relying on outdated human-centric recovery methods have fared most favorably as they can return to a trusted model of operations, minimizing business interruption costs and taking additional risk operating on non-vetted, possibly compromised systems.

Additionally, CyberSteward observed a rise in unaffiliated or **"lone wolf"** Threat Actors operating without established brand names or reputations in 2025. These Threat Actors often operated independently, without leveraging formal ransomware-as-a-service platforms or sharing proceeds with operators, resulting in greater unpredictability in the engagement and increasing risk. CyberSteward also observed fragmentation within the Threat Actor landscape, including the emergence of new groups and the splintering of existing ones. Across all matters, the average negotiation duration prior to resolution or publication was 1-3 weeks, with some negotiations extending 4+ weeks depending on the client's objectives, highlighting the variability of engagement timelines.

Notable Observations

This section highlights key observations from our global network of incident responders regarding the common control failures that have directly led to security incidents.

Inconsistent MFA and Deficiencies in Password Security Controls

Deficiencies in password security, encompassing weak credential policies, ineffective rotation practices, and inconsistent MFA enforcement represented the most frequently observed control gap. MFA was often only partially deployed, misconfigured, or bypassed through legacy authentication methods, increasing exposure to credential theft, BEC, and unauthorized access. These combined weaknesses indicate that identity-centric controls remain a persistent challenge across sectors.

Insufficient Security Training and Awareness

Security training and awareness continue to be a significant challenge for organizations, with many employees unable to effectively identify phishing attempts, malicious attachments, or social engineering tactics. These gaps frequently enable initial access for threat actors, particularly in BEC and credential-harvesting incidents. The data highlights that human-centric controls remain a critical component of an organization's security posture and are a common point of failure.

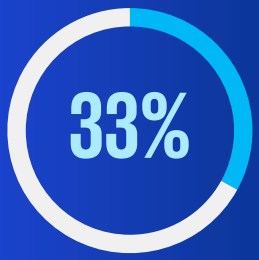
Persistent Gaps in Patch Management

Patch management failures were widely reported, with organizations citing outdated software, delayed remediation cycles, and incomplete asset visibility as key barriers to effective patching. Notably, several intrusions highlighted missed or delayed firewall patching, which left critical perimeter defences vulnerable to exploitation through known vulnerabilities. These gaps directly contributed to ransomware execution, unauthorized access, and lateral movement, underscoring ongoing difficulties in maintaining secure baselines in hybrid and distributed environments.

Weakness in Detection Controls

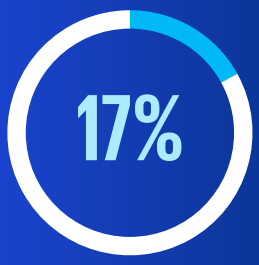
The observations underscore that successful compromises are most often driven not by novel attack techniques, but by systemic weaknesses in foundational controls or failure to detect anomalous behavior. Addressing these gaps, particularly in identity and access management, user education, detection capabilities and asset hygiene, represents one of the most effective opportunities to materially reduce risk, improve detection timelines, and strengthen organizational resilience against both financially motivated and state-aligned threat activity.

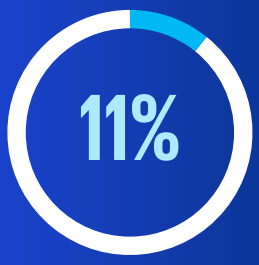
Control Failure Category and Percentage of Events Reported

1 Rank
Strong Authentication (MFA) Failures


2 Rank
Password Security Failures


3 Rank
Security Training and Awareness Gaps


4 Rank
Patch Management Failures


5 Rank
Anomalous Behavior Detection Failures


03 | Notable IR Incidents

Key Case Studies (for illustrative purposes only)

Case Study #1 – Education Sector – Insider Threat

Overview

KPMG supported an organization responding to an internally driven security incident involving an employee who executed malicious tools, attempted credential theft, and conducted unauthorized security testing within the corporate IT environment. The incident was first identified when the organization deployed a new EDR solution within its IT environment, which alerted to malware detections on the user's assigned workstation. Subsequent interviews and technical analysis confirmed intentional misuse of privileged access and wide spread possession of offensive tooling.

Threat Actor Profile

- **Attribution:** Known insider (employee)
- **Motivation:** Unauthorized security experimentation, privilege escalation, and attempted credential compromise
- **Access Level:** Standard employee account with access expanded through misuse of offensive tools
- **Behaviors:** Persistent credential harvesting, reconnaissance, unauthorized data aggregation, removable-media exfiltration

Threat Actor Activity (TTPs Observed)

Initial access

- Employee with access into the IT environment
- Executed offensive security tools undetected prior to EDR alerts
- Insufficient restrictions around PowerShell, credential stores, and removable media
- Capability to access sensitive directories and authentication systems (Active Directory, KeePass stores, ERP reference

Reconnaissance

- Internal network scan results
- System information exports
- Tools and scripts used to probe and test internal systems

Privilege Escalation

- Mimikatz for credential extraction
- PowerSploit for exploitation and post-exploitation activity
- Impacket modules for lateral movement and credential operations

Exfiltration

- Removable media used for exfiltration
- KeePass password database files
- ERP-related references
- File names suggesting organized data staging
- Credential sets and other sensitive exports copied to USB

Business Impact

- Unauthorized disclosure and theft risk involving credentials, Active Directory stores, and sensitive business files
- Compromise of identity integrity requiring extensive remediation
- Insider threat escalation requiring HR, legal, and cyber coordination
- Potential exposure of confidential operational and password-management information
- Disruption due to investigation, workstation seizure, and account suspension

What Went Wrong

- Controls governing the use of PowerShell, offensive tooling, and access to credential repositories were insufficiently restrictive, allowing high risk activity to occur without prevention
- Detection mechanisms for insider misuse were limited, with inadequate visibility into Active Directory data access, internal reconnaissance activity, and unauthorized changes to privileged group memberships
- Removable media usage was not appropriately restricted or monitored, increasing exposure through unmanaged data transfer pathways
- Behavioral detection capabilities were immature, limiting the organization's ability to identify anomalous credential access and harvesting activity
- Identity governance processes were not consistently enforced, particularly for privileged access management and Active Directory access paths, resulting in elevated access persisting without timely oversight

Notable IR Incidents (Cont.)

Key Case Studies (for illustrative purposes only)

Case Study #2 – Technology – Data Disclosure

Overview

KPMG supported an organization to respond to a security incident in which the client identified a post on the social media platform "X" related to a potential data leak of source code from 820 GitLab repositories. On further analysis, the client team assessed the incident, examined their servers on Google Cloud Platform (GCP) and confirmed that data had been leaked. KPMG conducted a comprehensive cyber incident analysis and initiated response procedures, WAF Logs, Load Balancer Logs, Linux Server Logs, Message Tracer Logs, Azure AD User Sign-In and Audit logs, etc., to detect potential events related to data leakage activity.

Threat Actor Profile

- **Motivation:** Data exfiltration
- **Access Level:** Access of confidential data
- **Behaviors:** Phishing emails, malware execution, payload delivery and exfiltration

Threat Actor Activity (TTPs Observed)

Reconnaissance

- Multiple GET/POST requests from external IP addresses to probe client's endpoints
- Targeting of public subdomains suggests discovery/use of publicly exposed services

Initial Access

- SQL Injection and RCE attempts against an internet facing web server.
- Use of internal email address to send email with foreign IP addresses

Execution

- Suspicious CMD/HTTP-based command to download executable PHP scripts
- Use of content management systems to execute SQL commands

Persistence

- Attempts to write/deploy a backdoor on the content management system for remote command execution

Exfiltration

- Multiple zip files of approximately 57.33 GB have been exfiltrated via Gitlab

What Went Wrong

Based on the investigation of the cyber incident, the following key root causes were identified:

- GitLab was not protected by Web Application Firewall (WAF), which led to large-scale data exfiltration without inspection
- A feature of the content management system was publicly exposed, providing SQL Injection and Remote Code Execution (RCE) ability which was used to deploy a backdoor
- Content Management System lacked proper input validation and WAF shielding, leading successful SQLi exploitation
- Email accounts were misused from public IP addresses, and anomalous traffic (probes and data transfers) went undetected for weeks

Notable IR Incidents (Cont.)

Key Case Studies (for illustrative purposes only)

Case Study #3 – Legal Sector – Ransomware

Overview

An organization in the legal sector was breached by a MetaEncrypter (also known as MetaEncryptor), a lesser-known ransomware group that uses the MetaPowder ransomware and has been active since at least 2023. The incident was detected when ransom notes and encrypted files were discovered in the morning, following the encryption of the environment overnight. In this incident, the threat actor managed to stay under the radar for close to a month, from initial access to impact (encryption). KPMG observed that they moved from a single compromised workstation, escalating to a legacy account which was part of the Domain Admins group, and moved laterally to two servers, holding their position in the network. Most of their attack was then orchestrated from these systems, by leveraging built-in Windows tools and protocols such as PowerShell, PowerShell Remoting, WinRM, WMI and Scheduled Tasks to execute their attack. They identified servers of interest to exfiltrate data from and once complete, proceeded with the encryption.

Threat Actor Profile

- **Attribution:** MetaEncrypter/ MetaEncryptor
- **Motivation:** Financial (extortion)
- **Access Level:** Standard user account on a domain-joined PC that was then used for identity attacks against Active Directory

Threat Actor Activity (TTPs Observed)

Initial Access	• Compromised user workstation via NetSupport Remote Access tooling
Execution	• Microsoft Sysinternals tooling
Credential Access	• Identity-based attacks against Active Directory (e.g.: Kerberoasting)
Lateral Movement and Execution	• Built-in Windows tools and protocols (PowerShell, PowerShell Remoting, WinRM, WMI and Scheduled Tasks)
Collection	• WinRAR via the command-line
Exfiltration	• Exfiltration to a Cloud service using an open-source client (megacmd)
Impact	• Local encryption of physical servers, and encryption of virtualization hosts (Hyper-V)

Notable IR Incidents (Cont.)

Key Case Studies (for illustrative purposes only)

Case Study #4 – Services Sector – Advanced Persistent Threat

Overview

KPMG provided incident management and incident response support to a European-based services firm impacted by an Advanced Persistent Threat (APT) campaign attributed to a Chinese speaking APT group. The threat actor targeted network infrastructure devices to gain privileged access, perform reconnaissance, and harvest administrative credentials, resulting in operational disruption and service degradation.

Threat Actor Profile

- **Attribution:** High-confidence identification of a Chinese speaking APT
- **Motivation:** Sensitive data access
- **Access:** Administrative access following CVE exploitations
- **Behavior:** Data theft, long-term persistence mechanisms, and covert exfiltration techniques usage

Threat Actor Activity (TTPs Observed)

Initial Access

- Leveraged vulnerabilities in internet exposed edge network devices
- CVE-2023-20198: Exploited to create a local privilege accounts for persistent, legitimate-looking access
- Targeting of HTTP/HTTPS administrative portals accessible from the internet

Persistence

- Performed extensive edge device configuration extractions
- Modified configurations to add Telnet services enabling persistent remote access

Privilege escalation

- Added new servers for credential harvesting
- Leveraged captured credentials to escalate privileges on network
- Captured network traffic from administrative interfaces to intercept legitimate administrative credentials

Lateral Movement and Execution

- Used short-lived network addresses to facilitate lateral movement via VLAN hopping to expand network reconnaissance
- Traversed network by routing pathways into adjacent networks

Impact

- Contributed to widespread network disruption, degrading the organization's ability to support while incident response operations were ongoing
- Maintained access and data exfiltration via various protocols including SFTP, HTTPS, and HTTP
- Full extent of data loss unclear due to encrypted transfers

What Went Wrong

The incident was not the result of a single control failure but rather a highly sophisticated APT campaign leveraging advanced and previously unseen techniques to exploit vulnerabilities within the network and domain infrastructure.

The root cause lies in weaknesses within technology stacks shared between the provider and customers, where critical firmware patches and essential hardening activities were not applied across the entire estate, providing the threat actor with time and opportunity to gain privileged access and maintain persistence.

Key Learning: Enhancing Detection and Response Maturity

In 2025, incident response engagements continued to demonstrate that systemic weaknesses in identity controls, credential management, patching practices, and user awareness remain central drivers of successful compromise. These gaps are frequently compounded by limited detection and response capabilities, which allow threat actors to progress from initial access to material impact before containment measures are initiated. As attack paths become increasingly automated and opportunistic, traditional control implementations alone are often insufficient to meaningfully reduce disruption or dwell time.

For CISOs and IT leaders, these observations reinforce the importance of investing in advanced detection and response capabilities that enhance organizational resilience and enable faster, more effective containment. Solutions that leverage AI driven analytics and agentic response workflows can help prioritize high risk activity, support rapid investigation and containment actions, and reduce the operational burden on internal teams during incidents. Managed Detection and Response (MDR) services that incorporate these capabilities provide organizations with an opportunity to improve response consistency, accelerate decision making, and limit business disruption resulting from both financially motivated and state aligned threat activity. KPMG's incident responders have identified the top five focus areas that represent the industry's pivot from reactive to predictive and adaptive security. They align with the reality that attackers are leveraging automation and AI, making speed and intelligence the new differentiators in defense.

01 Strengthening identity controls: the center stage of cybersecurity

Leading organizations recognize that identity now serves as the new perimeter in cybersecurity. To address this shift, companies are actively implementing Identity Threat Detection and Response (ITDR) solutions, deploying robust Privileged Access Management (PAM) frameworks, and adopting Just-In-Time (JIT) access models. These initiatives are designed to enforce least privilege principles and facilitate continuous monitoring of identity behaviors for signs of anomalous activity. In response to the challenges presented by hybrid work environments and expanded cloud adoption, firms are prioritizing comprehensive identity governance strategies to effectively prevent lateral movement and privilege escalation attacks.

Additionally, companies are reinforcing Multi-Factor Authentication (MFA) across all critical systems, supported by stringent password policies and the adoption of enterprise-grade password management tools. These technical controls are complemented by ongoing user awareness initiatives, including targeted phishing simulations and training campaigns to ensure that employees are equipped to recognize and respond to social engineering attempts. This focus on human-centric defense remains essential for mitigating the risks associated with credential-based attacks, safeguarding organizational assets and maintaining operational resilience.

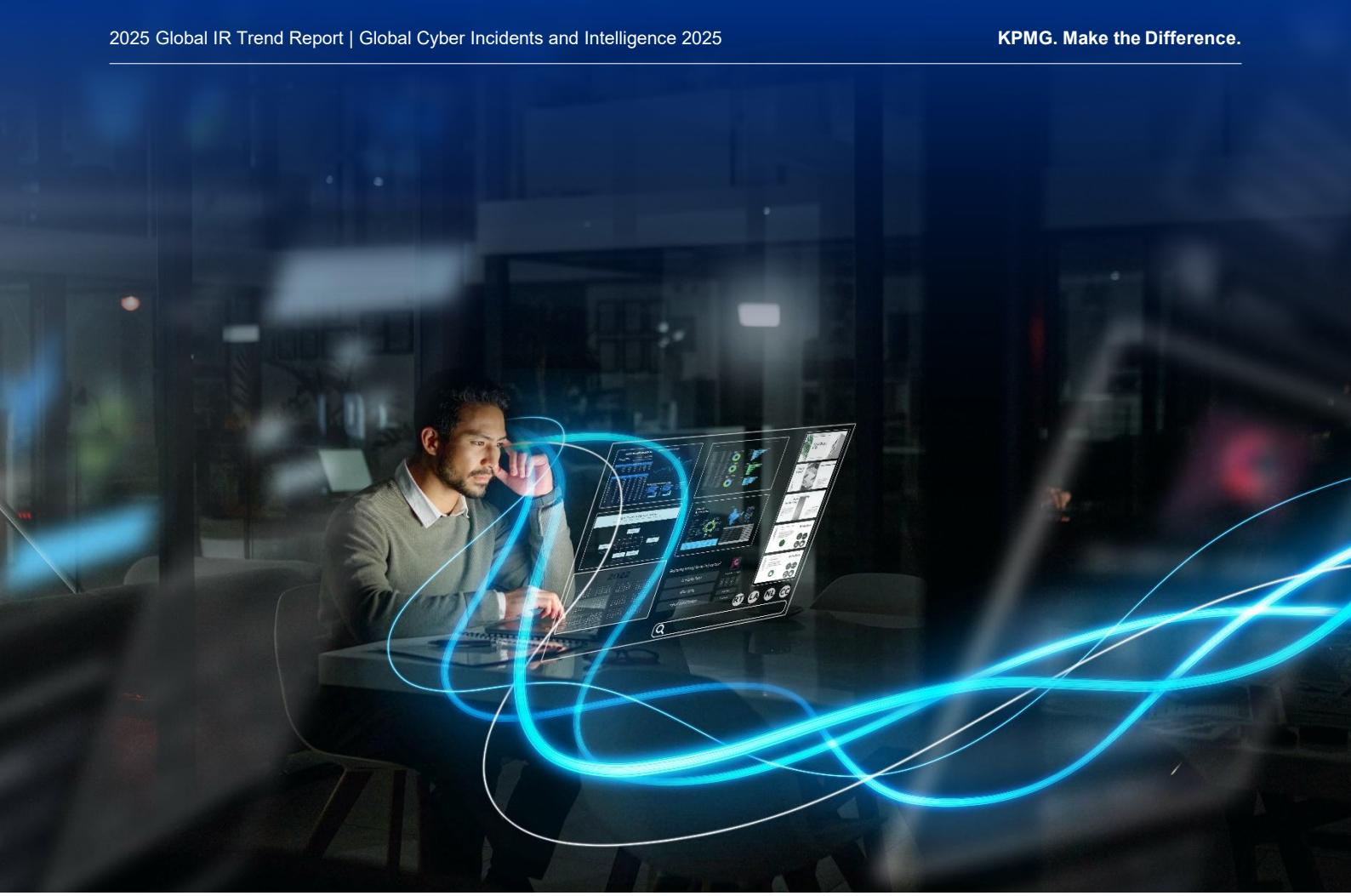
02 Cyber resilience and backups

Organizations are elevating their backup strategies to meet the demands of modern threats such as ransomware and destructive cyberattacks. Recognizing that backups are fundamental to cyber resilience, industry leaders are deploying immutable and air-gapped solutions that prevent unauthorized modification or access by threat actors. These robust backup architectures are strategically distributed across both on-premises and cloud environments, providing redundancy and enhancing recovery capabilities.

03 Drive towards agentic platforms and AI-based enablers

CISOs and IT Leaders are focused on learning and adopting sophisticated AI-driven security platforms that function as agentic systems, are autonomous, adaptive, and capable of orchestrating coordinated responses across endpoints, networks, and cloud environments. These advanced platforms harness machine learning to detect anomalies, utilize predictive analytics to anticipate emerging threats, and deploy automated response playbooks to enable rapid containment and mitigation.

It is anticipated that by 2030, the primary security investment driver for organizations will be AI. By embracing this technology, CISOs and IT leaders are positioning their organizations to effectively prepare against automated and AI leveraged attacks while scaling their security operations efficiently, without the need for exponential growth in human resources. This proactive approach reflects an industry-wide pivot toward resilient, intelligence-driven defense strategies that align with the realities of today's threat landscape.



04 Proactive defense: MDR, threat hunting, purple teaming, red teaming, and CTI

Today's leading organizations are adopting a proactive approach to cybersecurity, moving decisively beyond traditional reactive measures. Enterprises are investing in managed security services such as MDR to ensure continuous, 24/7 monitoring of their environments coupled with AI-based enablers, enabling early detection and rapid response to emerging threats.

Advanced Threat Hunting capabilities are being deployed to uncover stealthy adversaries and sophisticated attack techniques that may evade standard controls. In addition, Purple Teaming exercises integrating both offensive (red team) and defensive (blue team) tactics are routinely conducted to drive ongoing improvement and resilience across security operations.

Cyber Threat Intelligence (CTI) is now a cornerstone of modern defense strategies, empowering organizations to anticipate attacker behaviors and prioritize defensive investments based on actionable, real-world threat data. By embracing this proactive posture, CISOs and IT leaders are effectively reducing attackers' dwell time and reinforcing their organizations' resilience against advanced persistent threats, positioning themselves at the forefront of cybersecurity best practices.

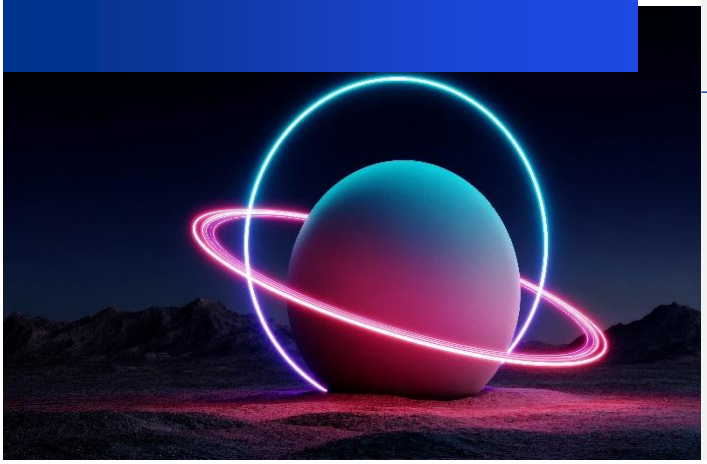
05 Prepare for the Worst: IR Readiness and tabletop exercises

Incident Response (IR) retainers and readiness has become a standard operating imperative for organizations at the forefront of cybersecurity. Today's CISOs and IT leaders are proactively orchestrating regular tabletop exercises and simulating ransomware attack scenarios to rigorously test and validate their business continuity and disaster recovery strategies. These organizations have established pre-negotiated agreements with forensic and legal experts, ensuring that decisive actions can be initiated without delay in the event of a breach. By embedding these practices into their operational fabric, industry leaders are minimizing operational disruption, reducing regulatory risk, and positioning their organizations to respond swiftly and effectively when, rather than if, a significant incident arises.

04 | Looking Forward to 2026

2026 is likely to be a year of flux in the threat landscape. While some classic threats like ransomware and hacktivism will persist, the introduction of new technology will have a greater impact than in 2025. As the hype around AI begins to simmer, the realities of what it can and cannot do in a defensive role are becoming clearer, while the ability for threat actors to leverage it for social and phishing attacks grows. Though there are concerns about autonomous ransomware and AI-enabled ransomware attacks, the greater risk is likely in highly convincing social engineering attacks leveraging the human vulnerabilities in every organization.

Additionally, the geopolitical environment is likely to become less stable, leading to a potential increase in state-sponsored cyber-espionage and the establishment of beachheads in critical infrastructure. With tensions rising, cyber threat activity designed to disrupt energy, communications and other critical operational technology may increase, alongside threat actors leveraging cyber assets and AI in disinformation campaigns. These efforts may have a knock-on effect on the recruitment of insiders by both criminal and state actors as they prepare new attacks.



The battleground of 2026 is being defined today. As technology accelerates, the nature of cyber risk is coalescing around five critical developments that will dictate the future of digital conflict:

1 AI-Powered Attack Automation:

Threat actors will routinely use AI to develop adaptive malware, automate reconnaissance, and launch sophisticated, high-speed attacks, overwhelming traditional human-led defensive measures.

2 The Hyper-Targeting of Digital Identities:

With remote work and cloud infrastructure being standard, identity will be the primary battleground. Expect a surge in advanced attacks aimed at compromising multi-factor authentication, exploiting privileged access, and using deepfakes for social engineering.

3 Weaponization of OT and Critical Infrastructure:

Attacks will increasingly move beyond data theft to cause real-world disruption by targeting Operational Technology (OT) in sectors like manufacturing, energy, and transportation.

4 Systemic Supply Chain Compromise:

Attackers will increasingly bypass the defenses of large organizations by infiltrating their smaller, less secure software vendors and service providers, turning trusted updates and tools into weapons.

5 Defensive AI Becomes a Target:

As more companies adopt AI-driven security platforms for autonomous threat detection and response, attackers will focus on new techniques to evade, poison, or manipulate these defensive AI systems, creating a new layer of conflict.

The cybersecurity battlefield has fundamentally shifted. As threat actors weaponize automation and AI, our response must be faster, smarter, and more resilient than ever. The era of passive, reactive defense is over. By treating identity as the new perimeter, building for resilient recovery, embracing agentic AI platforms, proactively hunting threats, and rigorously preparing for the inevitable, CISOs can transform their security posture from a cost center into a strategic enabler. In this new landscape, speed and intelligence are not just advantages, they are the very core of survival and success.

05 About KPMG

KPMG's global network of cyber security professionals and incident responders supports organizations worldwide in detecting, responding to and recovering from cyber incidents.

Member firms combine cross-jurisdictional experience in digital forensics, incident response, threat intelligence, and remediation to help clients understand the nature of an incident, preserve evidence, mitigate business risks, and meet regulatory and legal obligations across diverse regions. KPMG approaches cyber security as a dynamic, enterprise-wide capability that adapts to emerging threats and aligns with organizational strategy. Our focus is on enabling long-term resilience and providing clarity in a rapidly evolving threat environment, helping clients safeguard their operations and pursue growth with confidence.

350+
Dedicated cyber partners

30+
Industry leading alliances

6000+
Global clients

45,000+
Global technology and risk consultants

9300+
Cyber professionals

145+
Countries provided cyber, digital transformation. IT, regulatory and forensic services

Incident Response Readiness and Planning

Strengthens preparedness with globally informed response frameworks, simulations, and strategic planning to support consistent, high-quality incident response across regions.

Digital Investigations and Remediation

Provides forensic analysis and coordinated global response capabilities to determine incident scope, identify root causes, support recovery efforts, and enable secure restoration of operations.

Cyber Global Threat Intelligence

Offers intelligence-driven insights into global threat actors, regional trends, and industry exposures, enabling organizations to anticipate evolving risks and prioritize defensive investments.

Data Identification and Remediation

Supports organizations in reducing exposure by identifying sensitive data, eliminating redundant or high-risk information, and establishing secure data governance practices across jurisdictions.

Managed Detection and Response (MDR) Services

Delivers continuous global monitoring, advanced threat detection, and guided response to help organizations quickly identify and contain cyber threats before they escalate. MDR services integrate automation, analytics, and expert investigation to support efficient remediation and recovery worldwide.

Contact Us

Incident Response

Oisin Fouere

Partner, KPMG UK
Global Incident Response Leader
Email: Oisin.Fouere@kpmg.co.uk

Alexander Rau

Partner, KPMG Canada
Deputy Global Incident Response Leader
Email: alexanderrau@kpmg.ca

Americas	**Jason Haward-Grau** KPMG US jhawardgrau@kpmg.com		
APAC	**Eddie Toh** APAC Leader eddietoh@kpmg.com.sg	**Dakai Liu** KPMG China & Hong Kong dakai.liu@kpmg.com	**Manish Tembhurkar** KPMG India mtembhurkar@kpmg.com
Europe	**Seosamh Gowran** EMA Leader seosamh.gowran@kpmg.ie	**Ronald Heil** KPMG Netherlands heil.ronald@kpmg.nl	**Michal Kurek** KPMG Poland michalkurek@kpmg.pl
	Michael Sauermann KPMG Germany msauermann@kpmg.com	**Sergi Gil Lopez** KPMG Spain sergigll@kpmg.es	**Stefan Prinz** KPMG Austria stefanprinz@kpmg.at
Oceania	**Paul Black** KPMG Australia paulblack1@kpmg.com.au	**Philip Whitmore** KPMG New Zealand PWhitmore@kpmg.co.nz	

KPMG

kpmg.com/uk

Document Classification: KPMG Public