SYGNIA

CISO SURVEY 2026

THE STATE OF INCIDENT RESPONSE READINESS

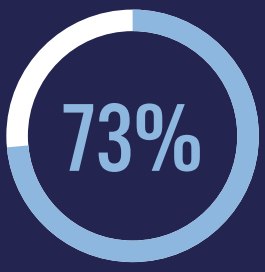
INTRODUCTION AND KEY FINDINGS

Today, cyberattacks are an accepted reality of operating in an increasingly complex, AI-driven world. Regulators expect preparedness. Customers assume resilience. Whether your organization's Incident Response can withstand the next attack may determine whether disruption is contained swiftly or if it escalates into lasting operational, financial, and reputational damage. As threat actors get better at evading defenses, every minute counts.

Incident Response should include executive and technical crisis management, enterprise-wide investigation, regulatory and stakeholder alignment, co-ordinate remediation and recovery efforts, and post-incident monitoring to ensure the attacker does not return. Yet, for many organizations, that level of preparedness is out of reach. While IR plans and tools are in place, confidence in their ability to deliver under pressure is limited. Nearly three quarters (73%) report that their organization would not be fully ready if a serious cybersecurity attack occurred tomorrow.

Drawing on insights from 600 senior IT security decision makers, Sygnia explores how ready organizations truly are to manage a significant cyberattack, where structural weaknesses emerge, and why limited executive alignment and visibility gaps undermine response.

The sections that follow outline what organizations must address to ensure IR readiness holds when it is tested under pressure.



do not feel 'fully ready' to withstand a significant cyberattack without disruption

89%

cite limited executive or board involvement in incident response readiness and decision-making.

90%

say they would experience difficulty in coordinating stakeholders in the event of a significant incident.

75%

agree delays and uncertainty around legal and communications team involvement slow down decision making during cyber incidents.

78%

agree blind spots in their environment risks persistent attacker access and increases the risk of repeat incidents.

84%

are concerned about attackers crossing from corporate IT systems into OT/ICS environments.

of organizations have experienced at least one cyberattack in the last 12 months.

GAPS IN INCIDENT RESPONSE LEAVE ORGANIZATIONS EXPOSED

RISKING IT ALL

Incident Response (IR) readiness is continuous preparedness that holds under pressure, with documented plans kept current, coordination rehearsed, and visibility proven across environments. Yet when IT security decision makers were asked to rate their organization's IR readiness if a significant cyberattack were to occur, almost three quarters (73%) say they would not be fully ready [Figure 1].

73%

do not feel 'fully ready' to withstand a significant cyberattack without disruption

Figure 1. How would you rate your organization's IR readiness if a significant cybersecurity attack were to occur tomorrow?

STRENGTH IN COORDINATED EXECUTION

That lack of confidence is reflected in how organizations rate their IR capabilities, with fewer than 40% describing their organization's various IR components as 'highly effective' [Figure 2]. This demonstrates how IR capabilities alone do not generate confidence in response. Instead, strength of performance is determined by comprehensive and coordinated execution, where these elements work together as an integrated whole.

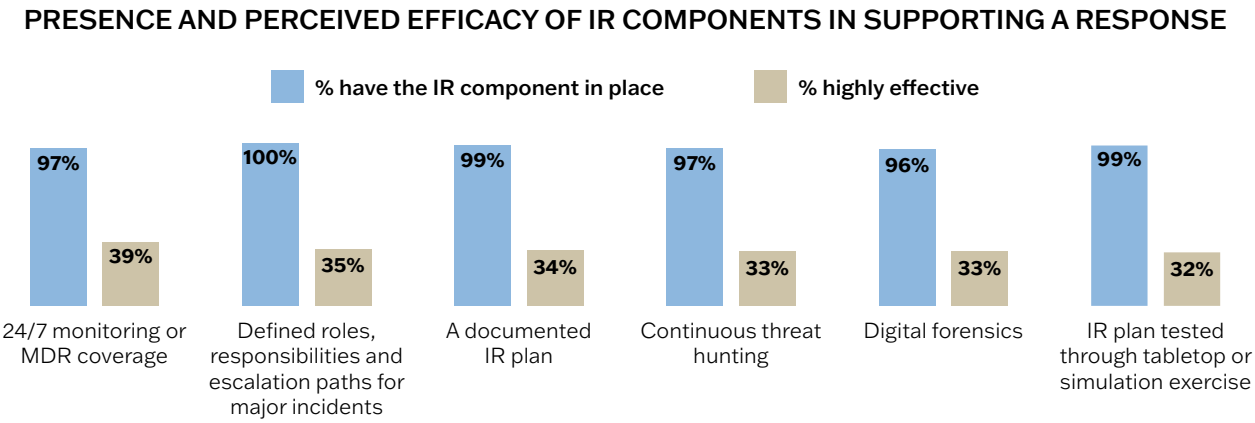


Figure 2. If your organization were to experience a significant cyberattack tomorrow, how effective are each of the following elements in supporting a response?

SECTOR AND REGION DIFFERENCES

SECTOR

Retail is the most likely sector to say they are not fully ready if a significant cyberattack were to occur, followed closely by Crypto/ decentralized finance [Figure 3]. Tabletop testing (29%), digital forensics (31%) and documented plans (32%) are all the least likely to be considered 'highly effective' in Retail, while Crypto/decentralized finance points to under-institutionalized IR, with efficacy lagging at every IR component compared to more established sectors (only 17%-28% 'highly effective').

REGION

APAC is the most likely region to say they are not fully ready if a significant cyberattack were to occur [Figure 3], while also being the least likely to rate their documented IR plan (26%), tabletop testing (27%), threat hunting (29%), and digital forensics (29%) as 'highly effective'. Meanwhile, North America is the most likely to rate the foundations of their IR response as highly effective (~34%-39%).

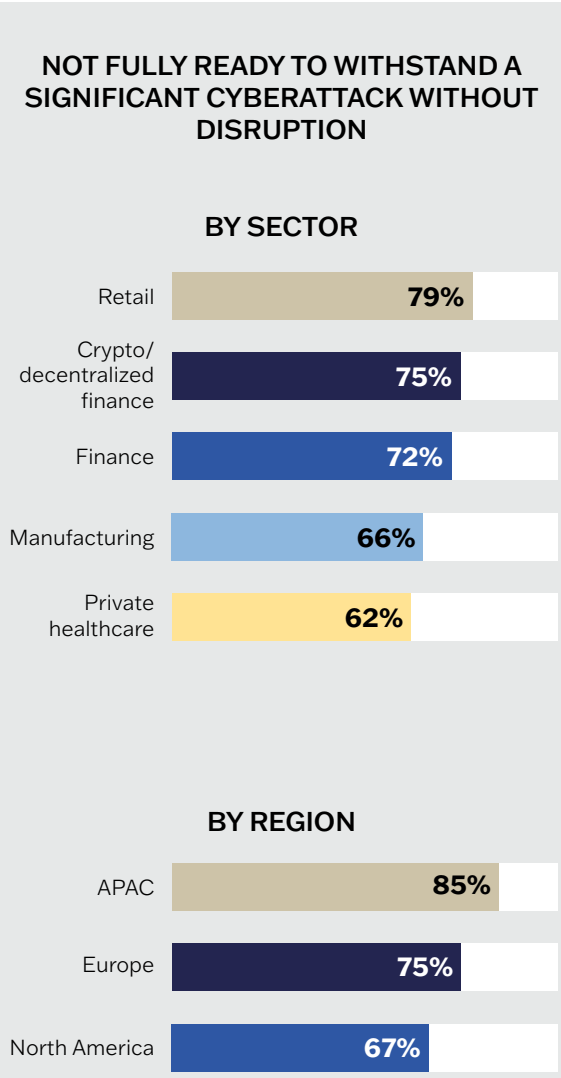


Figure 3. How would you rate your organization's IR readiness if a significant cybersecurity attack were to occur tomorrow?

INTERNAL FRICTION POINTS IN INCIDENT RESPONSE

WHERE COORDINATION STALLS

Roles, responsibilities, and escalation paths are foundational to IR, yet most organizations lack coordination with cross-functional key stakeholders and are uncertain about the involvement of legal and communications teams during incidents [Figure 4].

90%

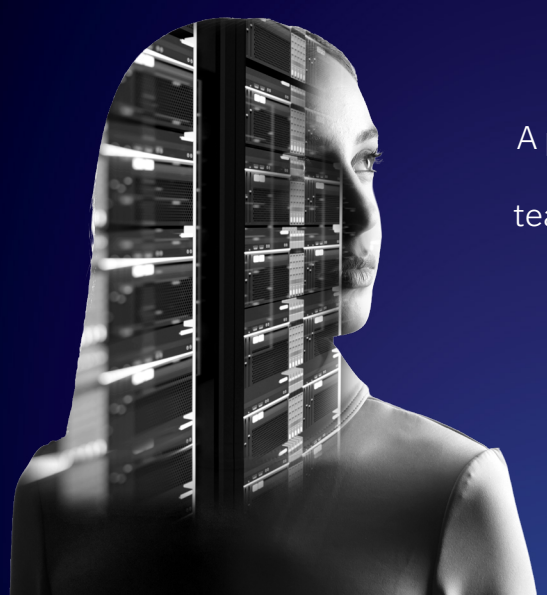
say they would experience difficulty in coordinating stakeholders in the event of a significant incident

75%

agree delays and uncertainty around legal and communications involvement slow down decision making during cyber incidents

Figure 4. To what extent are the following a challenge when it comes to managing IR in your organization? / To what extent do you agree or disagree with the following statements?

When ownership and decision rights are unclear, technical progress and executive decision-making fall out of sync. As evidence accumulates, approvals and disclosures lag, turning response into a reactive cycle where escalation slows, communications are delayed, and disruption compounds.



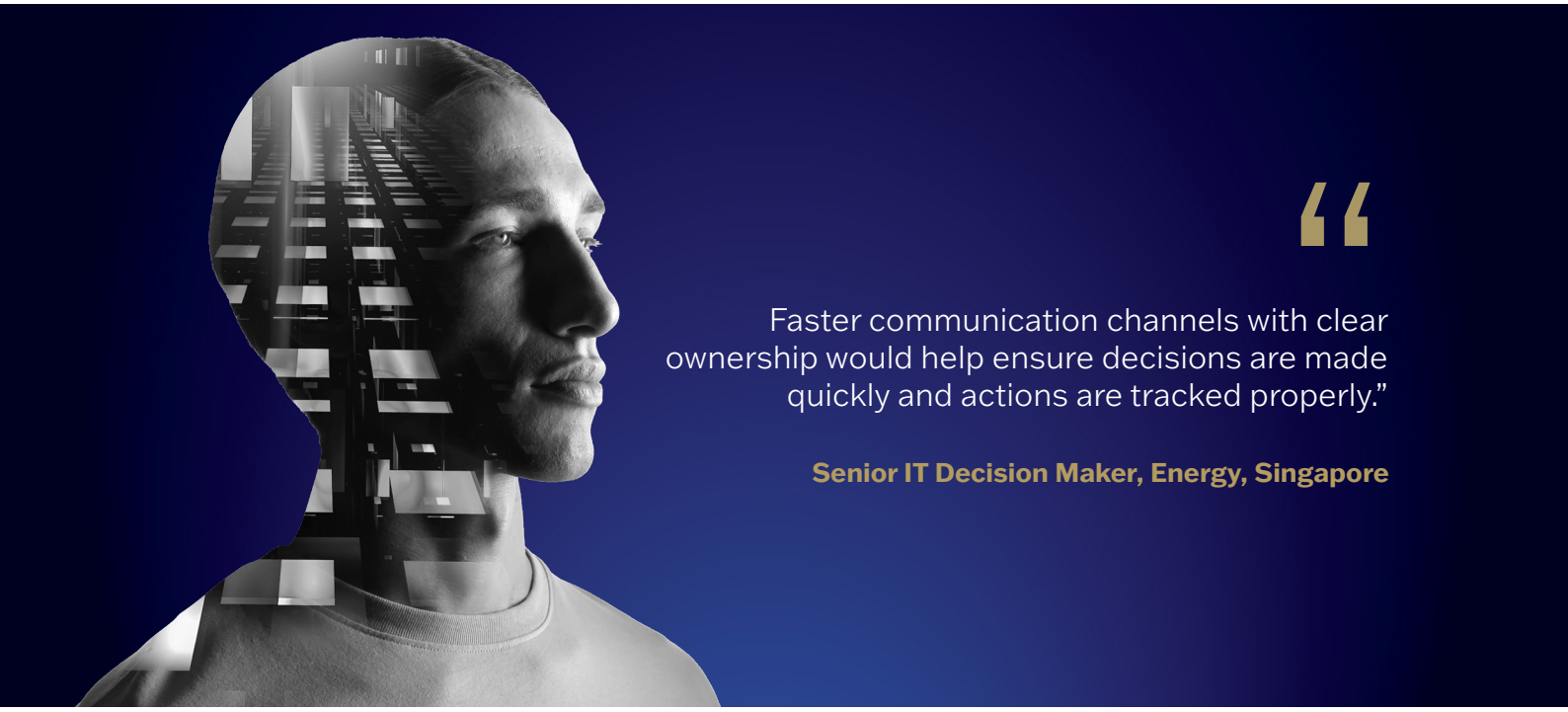
> A priority for us is to establish clearer integration and communication protocols between our IR team and non-technical business units, ensuring a swift, coordinated response that minimizes operational disruption
>
> **Senior IT Decision Maker, Insurance, UK**

FRAGMENTATION IN AUTHORITY

This breakdown doesn't just impact operations, it escalates upwards, with the large majority citing limited executive or board involvement in IR readiness and decision-making [Figure 5]. When there is a lack of executive engagement, teams spend time re-briefing for approvals instead of taking action. This risks longer response times and greater operational disruption when clarity and authority are needed most.

89%
cite limited executive or board involvement in IR readiness and decision-making

Figure 5. To what extent are the following a challenge when it comes to managing IR in your organization?



"Faster communication channels with clear ownership would help ensure decisions are made quickly and actions are tracked properly."

Senior IT Decision Maker, Energy, Singapore

Fundamentally, IR must be owned at both the security and executive levels, with defined decision rights, pre-agreed escalation pathways, and regular board-level rehearsal. Organizations that formalize cross-functional governance, align IR planning with crisis management structures, and ensure leadership is actively engaged can act faster on containment and escalation decisions when the minutes matter.

SECTOR AND REGION DIFFERENCES

SECTOR

Stakeholder coordination is a universal challenge, with only marginal differences by sector [Figure 6]. For Private Healthcare, where incidents often carry higher regulatory and reputational stakes, 86% agree that delays or uncertainty around legal and communications slow decision-making, the highest agreement of all sectors. Conversely, Crypto/decentralized finance is the least likely to agree, implying fewer formal legal/comms gates, or simply that these functions are less embedded in incident response.

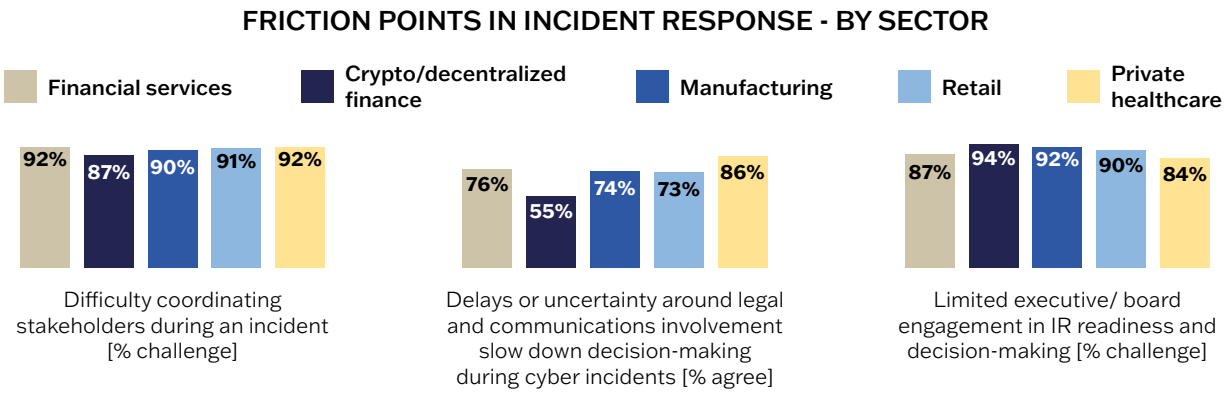


Figure 6. To what extent are the following a challenge when it comes to managing IR in your organization? / To what extent do you agree or disagree with the following statements?

REGION

Lack of stakeholder coordination during an incident is a universal problem, with minimal regional variation [Figure 7]. There is also broad agreement that uncertainty around legal and communications slows decisions, with APAC marginally higher than North America and Europe. The clearest regional gap is leadership, where North America and APAC are significantly more likely than Europe to see limited executive/ board engagement as a challenge.

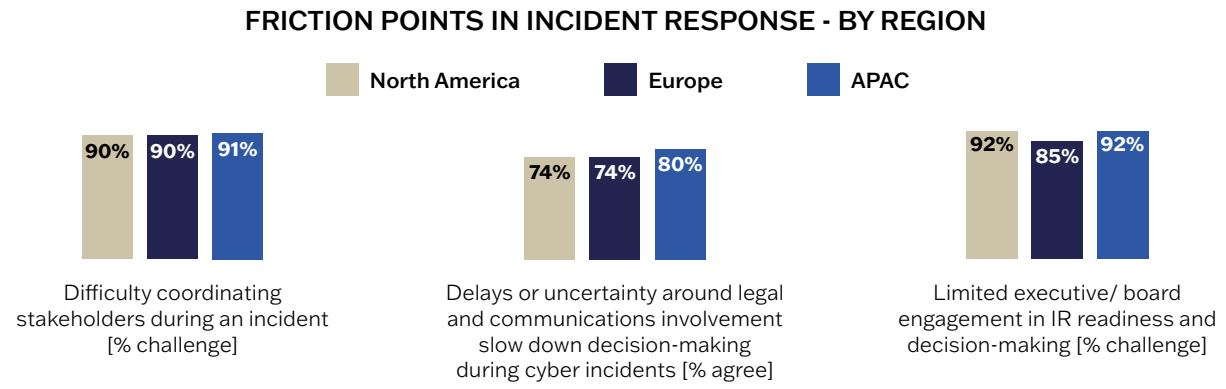


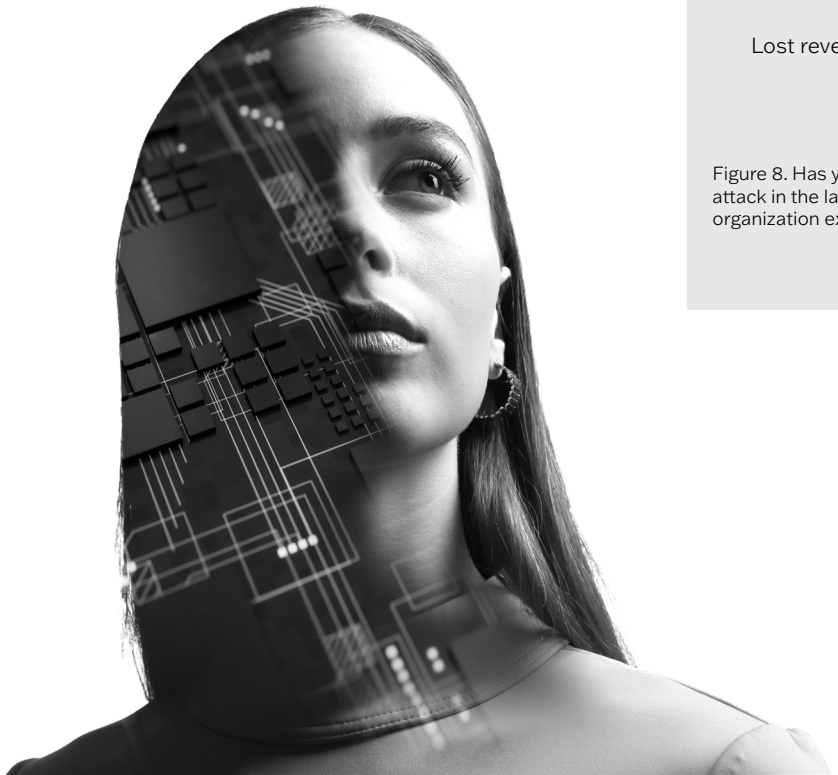
Figure 7. To what extent are the following a challenge when it comes to managing IR in your organization? / To what extent do you agree or disagree with the following statements?

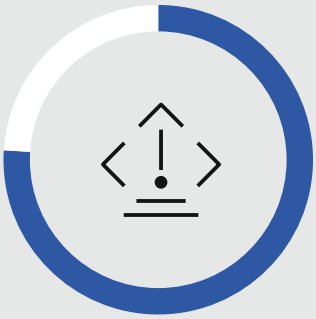
CYBERATTACKS EXPOSE THE TRUE COST OF IR GAPS

THE DEFAULT IS DISRUPTION

For most organizations, a cyberattack is no longer a question of 'if', but when and how. Our research shows that over three quarters (76%) experienced at least one cyberattack in the last 12 months, with almost a third (32%) experiencing more than one.

This has had serious consequences, from operational shutdowns to reputational damage and lost revenue [Figure 8]. The differentiator is not whether an organization is attacked, but how effectively it responds. The effectiveness and co-ordination of IR capabilities determine whether disruption is contained or escalated, yet as per our findings in section 3, many organizations lack the cross-functional alignment and operational clarity required to achieve this in practice.





76%
experienced at least one cyberattack in the last 12 months

IMPACTS OF CYBERATTACK(S):

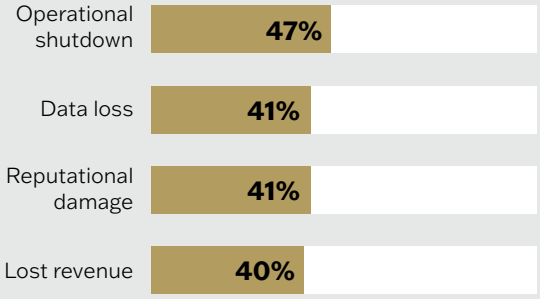


Figure 8. Has your organization been the victim of a cybersecurity attack in the last 12 months? / What impact(s) did your organization experience from the cybersecurity attack?

YOU CANNOT CONTAIN WHAT YOU CANNOT SEE

Many organizations lack cross-environment visibility required to respond with confidence when a cyberattack hits. Visibility gaps exist across on-premises infrastructure through to public cloud environments and endpoints. This risks security teams operating with partial insight into where an attack has moved and what has been affected.

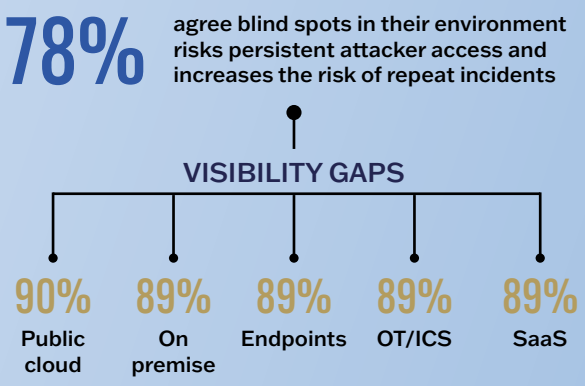


Figure 9. To what extent do you agree or disagree with the following statements? / During a significant cyber-attack, in which of the following areas do you think your organization would face visibility gaps that could slow detection or investigation of malicious activity?

IT security decision makers recognize this, with 78% admitting that blind spots in their organization's environment risks persistent attacker access and increases the risk of repeat incidents [Figure 9]. Closing these gaps requires unified visibility across all environments and regular validation through threat hunting and attack simulation to test whether visibility translates into proof of containment. Without this, blind spots will remain and the potential impact will only continue to increase.

OT AT RISK

The stakes are particularly high if an incident reaches operational (OT/ICS) environments. When activity cannot be reliably and quickly detected and validated, threats can pivot from IT into operational systems before teams can isolate them. Escalation to OT can magnify disruption by increasing the likelihood of operational downtime and extending recovery time. Those delays compound financial cost and elevate reputational damage when customers or stakeholders experience disruption. IT security decision-makers' high concern underscores that this is a material, recognized exposure [Figure 10].

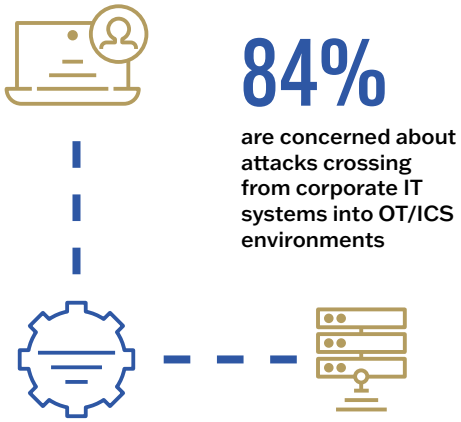


Figure 10. How concerned are you about your organization's OT/ ICS environment being compromised via your IT environment (e.g. corporate network, cloud, user endpoints)?

SECTOR AND REGION DIFFERENCES

SECTOR

Cyberattacks are common across all sectors, but highest in Crypto/decentralized finance [Figure 11]. The level of impact felt differs across sectors. Retail's greatest weakness is in maintaining business continuity, being the most likely to report operational shutdown (60%) and lost revenue/profit (48%). Meanwhile, Manufacturing and Financial Services skew toward data loss (48% and 46% respectively), signaling deeper compromise before containment takes hold. Crypto/decentralized finance and Private Healthcare are more likely to report executive or board disruption (both 43%), which is likely because they were among the most likely to report lack of stakeholder alignment and board engagement during IR decision-making [Figure 6].

REGION

Cyberattacks are widespread across regions, but reported incidence is highest in North America [Figure 11], where attacks are most likely to drive operational shutdown (51%). Meanwhile, APAC is more likely to be impacted by data loss (45%), reputational damage (46%) and customer loss (33%). Europe reports fewer incidents overall, but when they happen, they are more likely to lead to lost revenue or profit (46%), particularly versus North America (36%).

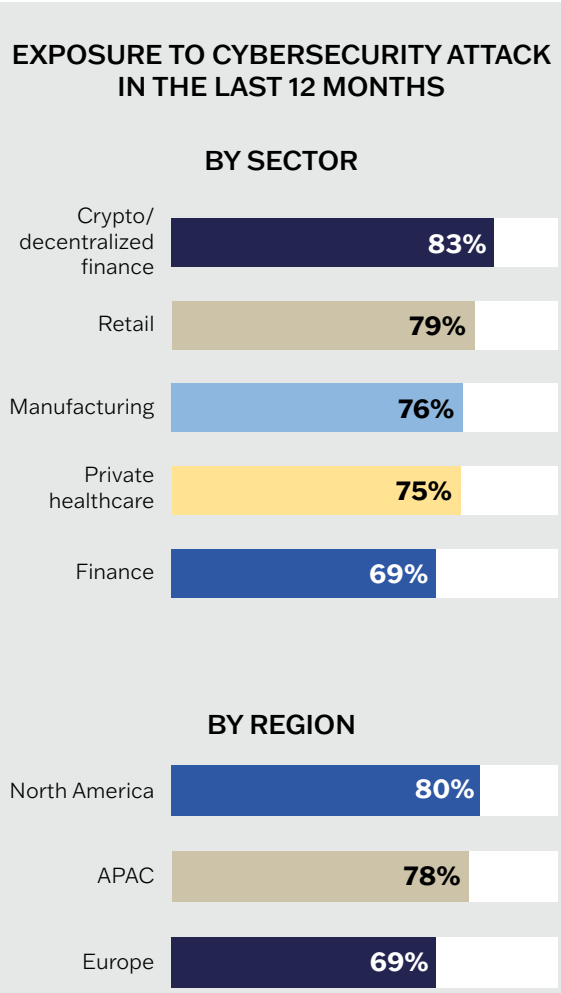


Figure 11. Has your organization been the victim of a cybersecurity attack in the last 12 months?

PREPARING INCIDENT RESPONSE FOR THE FUTURE

READINESS IS A MOVING TARGET

Incident Response must be treated as a continuous state of preparedness, evolving in line with the threat landscape. Over the next 12 months, IT security decision makers are concerned about a range of cybersecurity threats and their ability to seriously disrupt their organization financially, operationally, and reputationally.

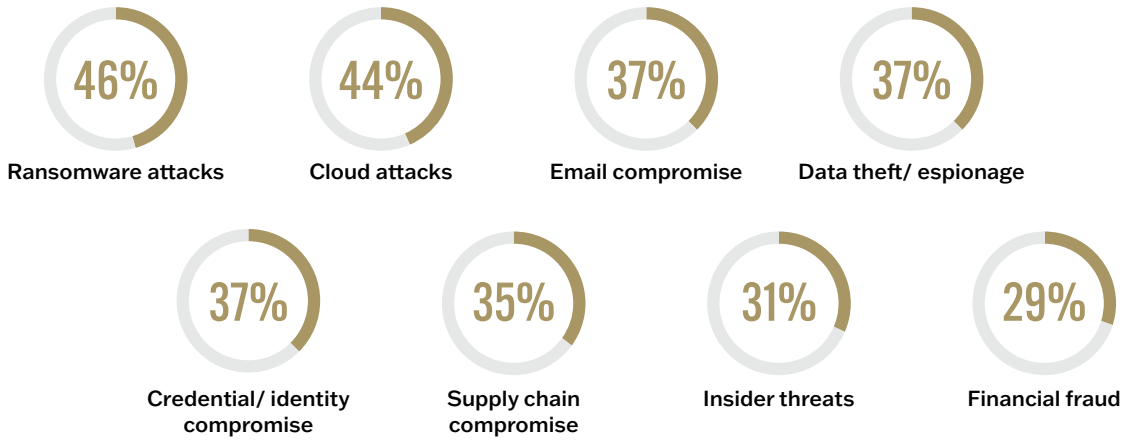


Figure 12. Thinking about the next 12 months, which cybersecurity threats most concern you because of the potential to seriously disrupt your organization (financially, operationally and/ or reputationally)?

Ransomware is the leading concern, closely followed by cloud environment attacks, but the wider picture presents a crowded threat landscape [Figure 12]. With no dominant threat, alongside gaps in visibility and friction across people, process, and tooling, organizations risk exposure at every angle.

> Attackers move quickly in many ways and are getting smarter. The landscape keeps changing. Our IR must always be on, know the threats, better integration and share intelligence.
>
> **Senior IT Decision maker, Crypto, US**

> Threat detection tools need improvement because I want them to identify emerging problems before they develop into complete operational incidents.
>
> **C-Suite IT Decision Maker, Healthcare, Singapore**

SCALING RESPONSE WITH AI

In this environment, speed and scale matter, which could be why many organizations are embedding AI into their threat detection and incident response. Today, almost a third of organizations report extensive AI use across most or all threat detection and IR activities, up from 25% last year. That rise likely reflects both increased adoption and the broader definition of what "AI" now includes, from embedded analytics and automation through to triage and investigation support.

By 2027, momentum is expected to accelerate further, with 63% anticipating AI to be embedded across their threat detection and IR activities. As adoption scales, AI is shifting from a bolt-on to a baseline capability in day-to-day security operations [Figure 13].

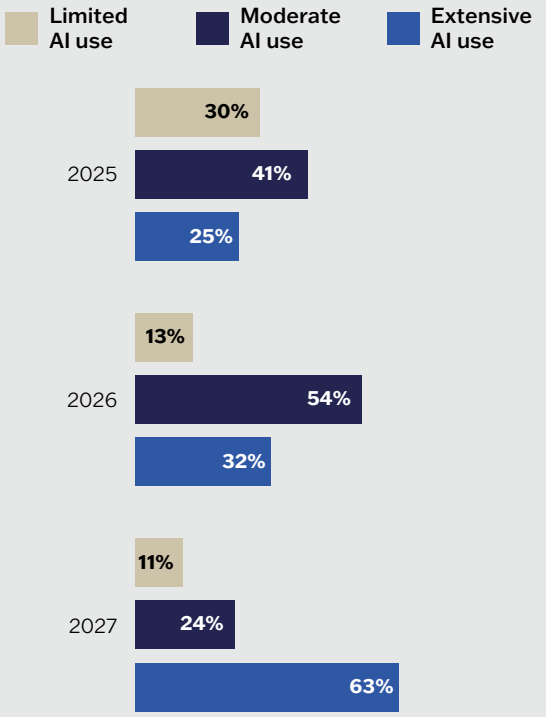


Figure 13. To what extent is your organization using AI or machine learning-driven capabilities to support threat detection and IR?

In practice, AI delivers most value when it strengthens IR foundations, rather than replaces it. Those with moderate or extensive AI use are more likely to rate their IR elements, including documented plans, 24/7 monitoring, and digital forensics, as effective, compared to those using AI in a limited way [Figure 14]. This suggests IR readiness improves when AI is embedded into workflows, not when teams default to automation as a substitute for judgement.

PERCEIVED EFFICACY OF IR COMPONENTS IN SUPPORTING A RESPONSE, BY AI USAGE TODAY (2026)

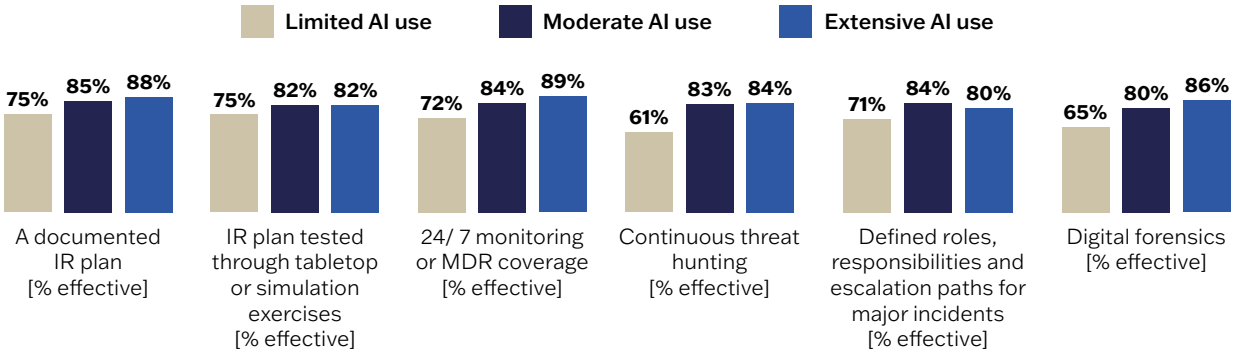


Figure 14. If your organization were to experience a significant cyberattack tomorrow, how effective are each of the following elements in supporting a response? / To what extent is your organization using, AI or machine learning–driven capabilities to support threat detection and IR? - This year (2026)

> So much of it goes back to our employees. We will improve our training so that they recognize threats, know how to respond and report them back to us. Technology, firewalls, MFA all play a role, but we are only as strong as our weakest human link.
>
> **Senior IT Decision Maker, Crypto, US**

SYGNIA'S PERSPECTIVE ON AI

Artificial intelligence (AI) is increasingly becoming a strategic priority for most organizations, driven by executive pressure to accelerate processes, increase productivity, and foster innovation. However, rapid adoption often outpaces consideration of the security implications, introducing AI as a new and expanding attack surface.

As AI models become embedded in core business operations and employees increasingly leverage external and internal AI tools, organizations must take a proactive approach to risk mitigation. AI security should be formally integrated into enterprise cybersecurity frameworks to balance innovation with resilience.

Effective AI risk management requires a structured approach spanning governance and regulatory compliance, security and risk oversight, secure adoption and integration, and ongoing tool lifecycle management.

INVESTING IN RESPONSE, RE-EVALUATING PROVIDERS

AI adoption is increasing, but organizations are not treating it as a standalone fix. Planned investment spans the IR stack, led by earlier threat discovery and continuous coverage [Figure 15]. Alongside forensics and rehearsal, this reflects a clear intent to reduce delay between detection and containment, and to keep decisions and escalation aligned with the pace of the investigation when pressure is highest.

INVESTMENTS PLANNED OVER THE NEXT 12 MONTHS

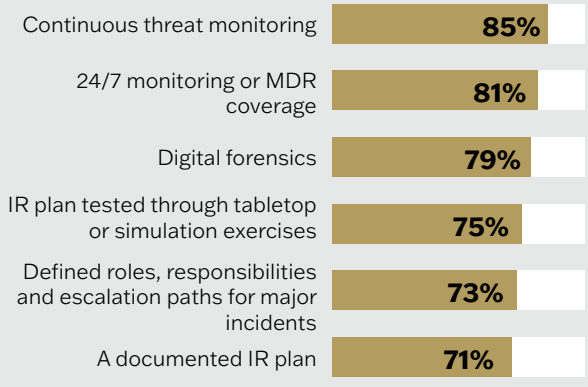


Figure 15. Thinking about your organization's IR capabilities, how much additional investment, if any, is planned for each of the following areas over the next 12 months?

Implement an automated collaborative response between departments and external organizations and establish threat attribution capabilities covering the entire attack chain.

Senior IT Decision Maker, Transport, Luxembourg

Focus on enhancing our IR capabilities by improving threat detection speed, integrating AI-driven analytics for faster incident response, and strengthening cross-team communication to ensure more proactive and coordinated handling of security incidents.

C-Suite IT Decision Maker, IT, UK

However, strengthening detection and response capabilities alone won't resolve the visibility and co-ordination breakdowns that we've seen can slow decision-making and containment. This is because execution still depends on what teams can actually see and how quickly the right stakeholders can act on that information.

This likely explains why many organizations are re-evaluating who they rely on when an incident hits. Many organizations expect to switch IR providers at the end of their current contract, driven by the need for more proactive readiness support, better coverage across IT/OT and cloud environments, and deeper expertise in complex incidents [Figure 16].

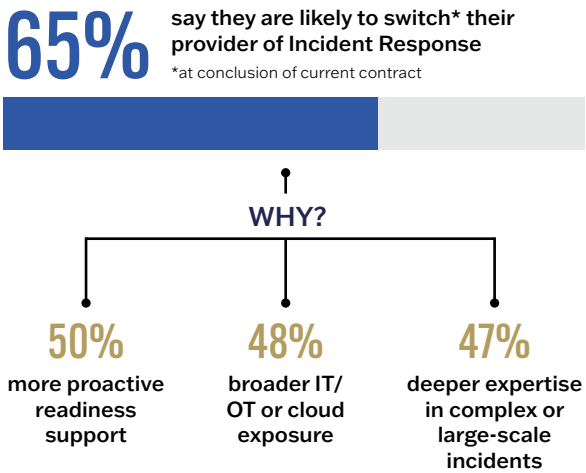


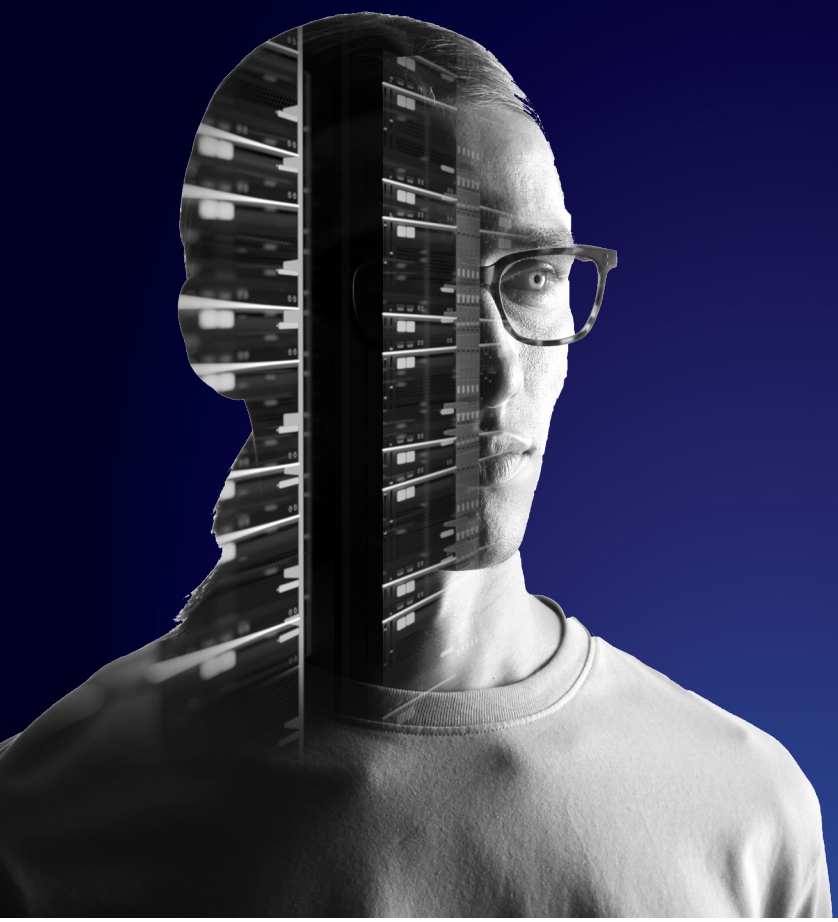
Figure 16. How likely are you to consider switching to a different MDR and/ or IR external provider at the conclusion of your current contract? / What is driving your likelihood to consider switching incident response providers?

This shift is also underpinned by a growing perception that vendor lock-in is a risk to incident response [Figure 17]. When providers are tied to a single ecosystem, scope and recommendations can be bound by what their tools can see and support, leaving gaps where certainty matters most. Vendor-agnostic partners widen the lens by operating across tooling to ensure incidents are scoped accurately and contained decisively.

79%

agree that relying on IR providers that aren't vendor-agnostic, could leave critical risks unaddressed

Figure 17. To what extent do you agree or disagree with the following statements?



> Improving visibility across cloud environments, endpoints, and third-party platforms would allow us to detect incidents and respond to them with greater accuracy.
>
> **C-Suite IT Decision Maker, Crypto, France**

> The IR team's integration with our internal systems was seamless, providing real-time data flow we never thought possible.
>
> **Senior IT Decision Maker, IT, US**

As organizations invest in speed detection and strengthen response execution, they must not mistake tools for readiness or overlook the value of vendor agnostic partners that can cut through complexity, broaden visibility across the stack, and drive decisive containment when it matters most.

SECTOR AND REGION DIFFERENCES

SECTOR

Retail and Private Healthcare are most likely to consider switching IR providers at contract end [Figure 18], indicating a larger perceived gap between current support and the level of execution assurance they need when incidents happen. Separately, concern about provider lock-in is strongest in Retail and Financial Services, highlighting vendor-agnostic capability as a key selection criterion even where switching intent may be lower.

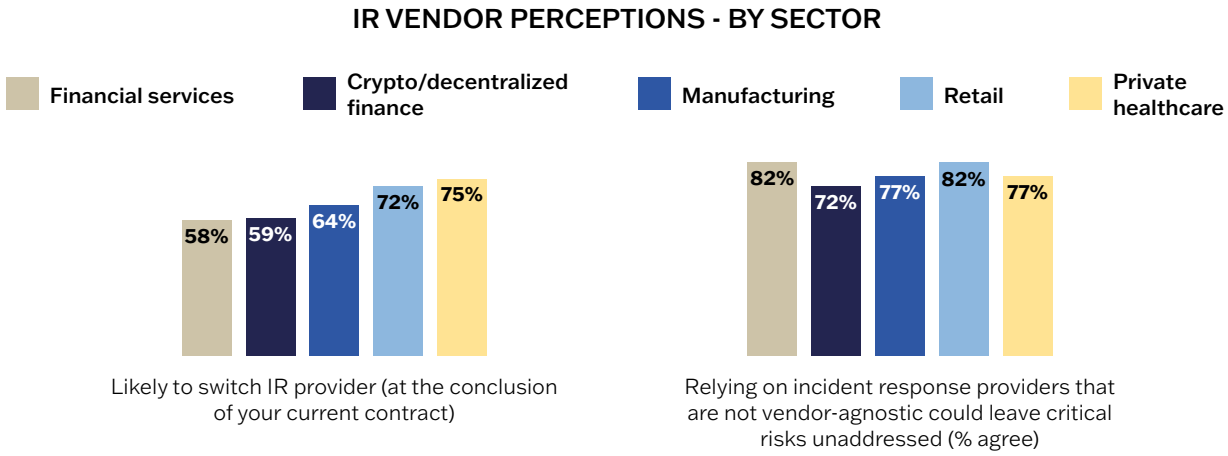


Figure 18. How likely are you to consider switching to a different MDR and/ or IR external provider at the conclusion of your current contract? / To what extent do you agree or disagree with the following statements?

REGION

Across regions, the likelihood of switching IR providers is high but fairly flat, with North America only marginally higher than Europe and APAC [Figure 19]. The sharper regional split is on vendor lock-in, where APAC is most likely to agree that non-vendor-agnostic providers could leave critical risks unaddressed.

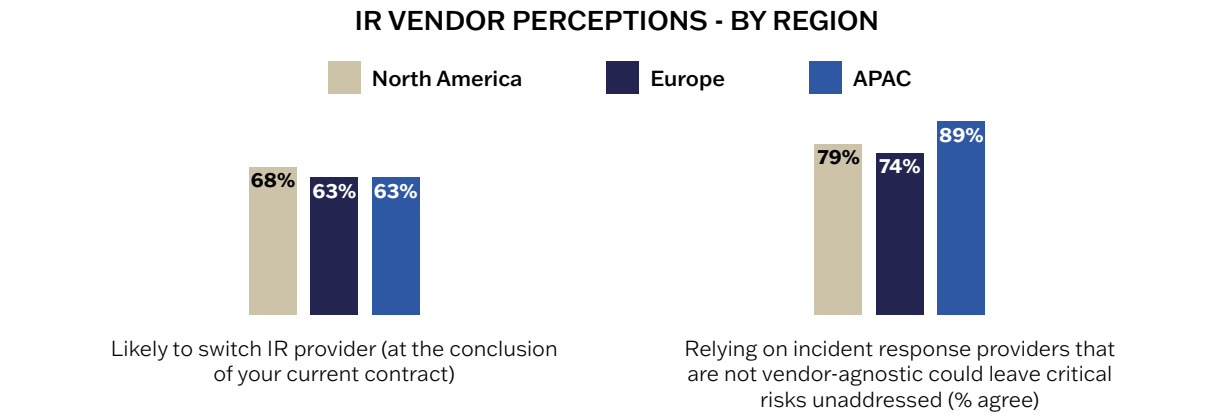


Figure 19. How likely are you to consider switching to a different MDR and/ or IR external provider at the conclusion of your current contract? / To what extent do you agree or disagree with the following statements?

SETTING YOUR ORGANIZATION UP FOR IR SUCCESS

Our findings demonstrate that while the foundational components of IR are in place for most organizations, they are not delivering as intended. Visibility gaps across cloud, IT and OT environments, combined with limited coordination and executive alignment prevent IR from functioning as a unified and resilient model.

Cyberattacks are no longer rare events; they are recurring business events. In this environment, organizations must be confident that their Incident Response capabilities can limit disruption decisively. When IR capabilities are not structured for coordinated execution, containment slows and recovery extends. The consequences are not contained to security teams – our research shows they are creating financial loss and lasting reputation damage.

Attackers are not slowing down, and neither can readiness efforts. Organizations that delay visibility and cross-functional improvements risk learning where their weaknesses lie during a live crisis. Incident response must be engineered to hold under pressure now, before the next attack puts it to the test.

WHAT DO WE RECOMMEND BASED ON THESE RESULTS?

Formalize cross-functional governance and executive ownership

Limited executive involvement and lack of coordination across legal, communications and security are key challenges when managing IR. We recommend establishing a structured Incident Response Retainer (IRR), running executive tabletop exercises, and defining clear escalation authority to ensure leadership is embedded before a crisis begins, not introduced during it.

Close visibility gaps across IT, cloud, SaaS and OT environments

78% state that blind spots increase the risk of persistent attacker access and repeat incidents. Unified investigative capability is essential. Cyber posture assessments, red and purple team engagements, and enterprise-scale investigation through a platform such as Velocity TDIR help identify exploitable gaps across hybrid environments and translate findings into prioritized remediation.

Choose a partner that you can both prepare with and call upon when you are in a real cyber incident

One of the most practical ways to offset the coordination, visibility, and execution gaps surfaced in this research is to choose a long-term partner with end-to-end capability. That partner should help you build readiness before an incident (governance, posture, exercises, visibility enhancements, and red/purple teaming) and deliver full-spectrum support during and after an incident, so you can make faster decisions, contain sooner, and recover with fewer surprises.

Treat AI as an accelerator, not a substitute for discipline

Organizations with moderate or extensive AI use are more likely to rate their IR elements as effective. AI should therefore be embedded into structured workflows, supporting threat hunting, triage, and investigation at scale, rather than positioned as a standalone maturity signal.

METHODOLOGY

Sygnia commissioned Vanson Bourne to survey 600 senior IT security decision makers in January and February 2026. Respondents represent organizations in the USA (200), Canada (50), Mexico (50), UK (50), France (50), Germany (50), BeNeLux (50), Australia (50) and Singapore (50). The organizations had 1,000+ employees (excluding Crypto) and $250 million+ global annual revenue and came from a range of public sectors, with a key focus on Retail, Finance, Crypto/decentralized finance, Manufacturing and Private Healthcare.

ABOUT SYGNIA:

Sygnia is the first call for organizations facing a cyber incident. Trusted by Fortune 500 and Global 2000 companies worldwide and bringing over a decade of frontline experience tackling the most complex breaches, Sygnia treats incidents as business crises—not just IT events—delivering fast, holistic, result-driven response across environments including IT, OT and blockchain. With global teams and boutique approach, Sygnia's responder-built technology and 100% vendor-agnostic model helps leaders contain attacks quickly, understand business impact clearly, and build lasting cyber resilience—while lowering costs and improving ROI. Learn more at www.sygnia.co

ABOUT VANSON BOURNE:

Vanson Bourne is an independent specialist in market research for the technology sector. Their reputation for robust and credible research-based analysis is founded upon rigorous research principles and their ability to seek the opinions of senior decision makers across technical and business functions, in all business sectors and all major markets. For more information, visit www.vansonbourne.com.