White Paper

Cybersecurity Readiness in the Age of Digital Transformation

Sponsored by: BDO

Yogesh Shivhare
July 2025

SITUATION OVERVIEW

The disconnect between digital transformation (DX) ambitions and cybersecurity execution is widening. While organizations invest in AI/ML, cloud, and analytics to drive growth, only 40% integrate cybersecurity during the planning stage. As a result, cyberincidents frequently delay or derail key IT and business projects, undermining time to value, eroding stakeholder confidence, and jeopardizing future competitiveness in an increasingly digital world.

According to the survey, the average time to respond to a cyberincident exceeds four days, and full recovery takes over seven days. In today's threat landscape, these delays can significantly disrupt operations, impact customer trust, and stall digital momentum. However, organizations with mature processes and modern capabilities, such as AI-driven threat detection, 24 x 7 response teams, and predefined recovery playbooks, often achieve containment and recovery significantly faster than others. The data reinforces a key shift: budgets are no longer the primary barrier. Instead, organizations must focus on how effectively those budgets are applied, aligning investments with modern methods, operational readiness, and proven practices that limit damage and accelerate recovery.

Priorities are shifting toward automation, endpoint protection, and employee awareness. Generative AI (GenAI) introduces new risks like phishing, data leakage, and governance gaps, and while some mitigation efforts are underway, most lack a cohesive risk management framework in the age of AI.

Ultimately, security must move upstream, embedded early and supported by experienced teams, automation, and orchestration. When aligned with strategy and investment, these capabilities enable near-real-time threat detection and response, turning cybersecurity into a decisive driver of resilience and innovation.

July 2025, IDC #US53615525

METHODOLOGY

This IDC white paper presents findings from a cybersecurity market survey, sponsored by BDO, of 411 qualified respondents conducted across 7 countries: United States (25%), Australia, Canada, United Kingdom, Germany, Netherlands, and Belgium (each ~12.5%).

Respondents were screened for their role and knowledge of cybersecurity practices within their organizations. The survey covered 15 industries, with no single industry comprising more than 15% of the sample.

For analysis, respondents were segmented into 5 business size categories based on number of employees:

- 100–499 employees: 106 respondents
- 500–999 employees: 77 respondents
- 1,000–2,499 employees: 98 respondents
- 2,500–4,999 employees: 67 respondents
- 5,000+ employees: 63 respondents

All respondents had cybersecurity responsibilities or influence within their organizations.

DIGITAL TRANSFORMATION AND THE CYBERSECURITY DISCONNECT

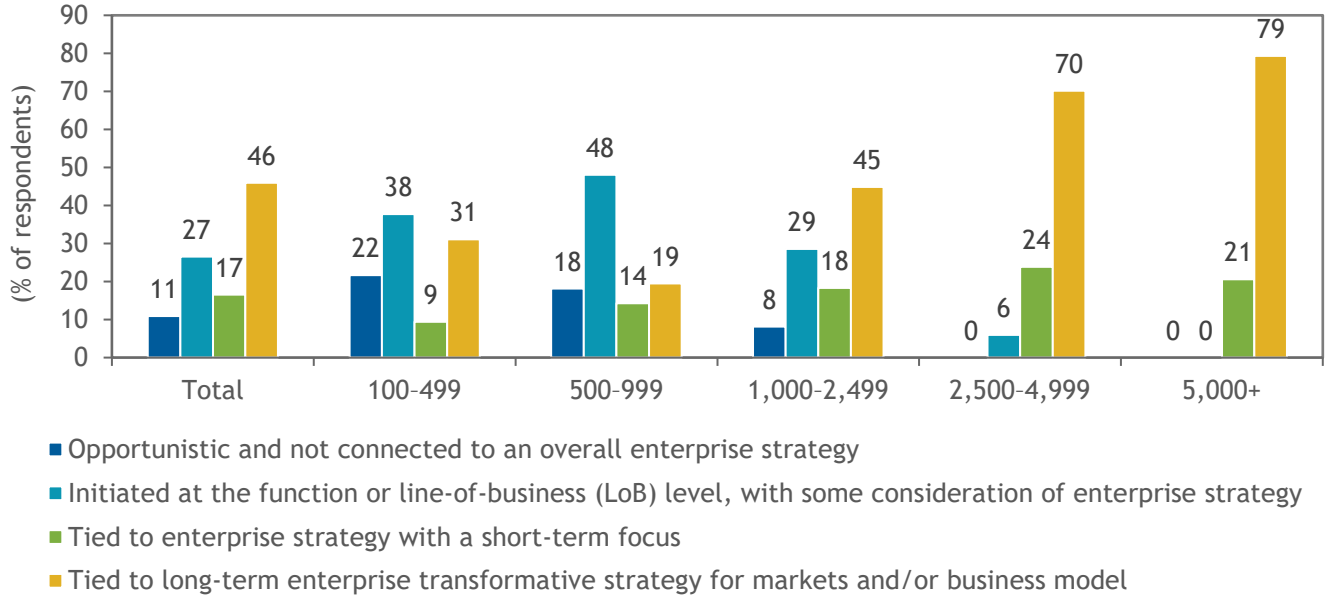
Digital transformation is now a cornerstone of competitiveness, efficiency, and innovation. However, organizations are progressing along this path at vastly different speeds and with very different levels of security maturity.

The survey reveals a sharp divide based on company size. Among very large organizations (5,000+ employees), nearly 79% say their digital transformation efforts are tied to a long-term, enterprisewide strategy. This figure drops significantly for small organizations (100–499 employees), where only 31% report a similar strategic orientation. In fact, nearly 60% of small firms pursue either opportunistic projects or transformation initiatives driven by line-of-business (LoB) leaders with limited enterprise integration. Midsize firms (1,000–4,999 employees) reflect a transitional posture: 45–70% report strategic alignment, though many remain focused on shorter-term goals (see Figure 1).

FIGURE 1

DX Strategy by Organization Size

Q. Based on what you have read, which of the following best describes your organization's approach to digital transformation (DX) initiatives?



n = 411

Source: IDC's *BDO Security Survey,* March 2025

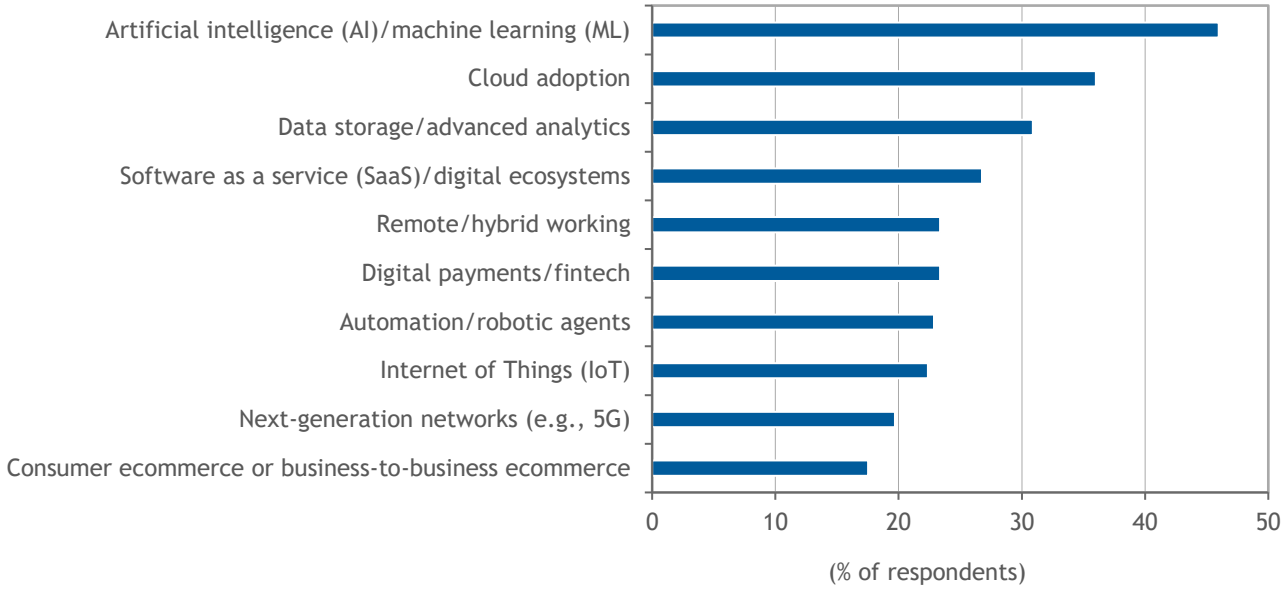
Despite these structural differences, the motivating factors behind transformation are broadly shared. Survey responses indicate that operational efficiency is the most cited driver of DX (52%), followed by scaling and growth (45%) and managing business risk (40%). These results underscore a consistent desire to make organizations more agile and resilient in the face of economic and competitive pressure.

In pursuit of these goals, organizations are investing in a range of technologies, with artificial intelligence and machine learning (AI/ML) leading the way. AI/ML, cloud platforms, and advanced analytics are among the top tools cited as enabling transformation. But while these technologies accelerate innovation, they also expand the digital attack surface, posing new risks that many organizations are not yet prepared to manage (see Figure 2).

FIGURE 2

Technologies Fueling DX

Q. *What are the top key digital initiatives you are currently adopting that will have the most notable impact on your organization's cyber-risk?*



n = 411

Source: IDC's *BDO Security Survey,* March 2025

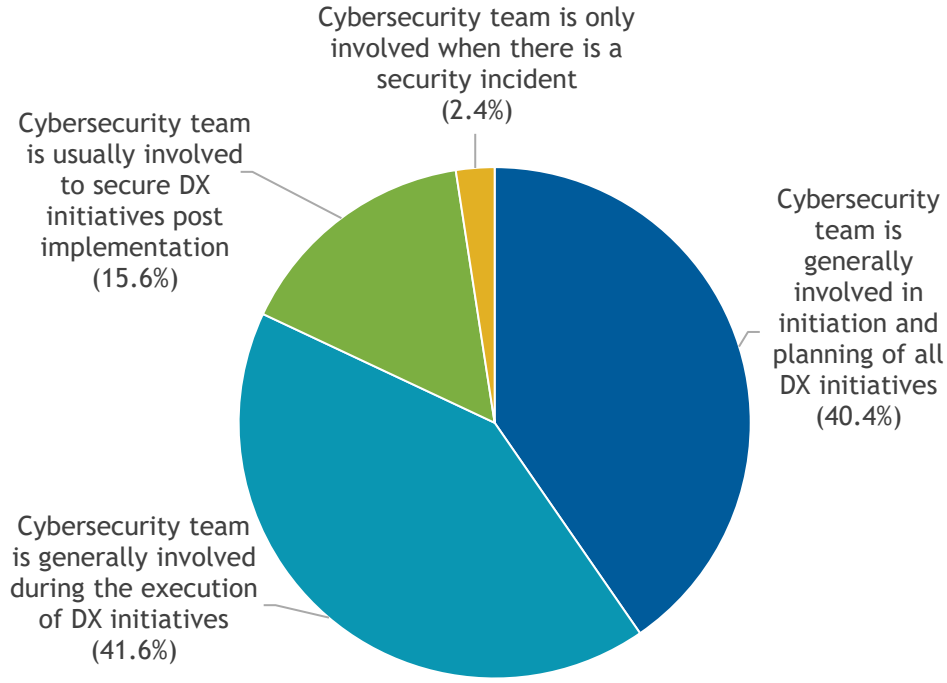
Cybersecurity remains an afterthought in many transformation journeys.

Only 40% of respondents say cybersecurity is included during the planning stage of digital initiatives. Another 42% report that security is brought in only during execution, while the remaining 16% admit it is considered only at the end of the project life cycle. This late-stage involvement introduces systemic risks, as security is often seen as a compliance checkbox or technical add-on rather than a strategic enabler (see Figure 3).

FIGURE 3

When Cyber Is Brought into DX Planning

Q. Which of the following best describes the role of cybersecurity within digital transformation (DX) initiatives?



n = 411

Source: IDC's *BDO Security Survey,* March 2025

This disconnect has measurable consequences.

Among the many impacts of cyberincidents, the most frequently reported is the delay or cancellation of critical IT and business projects. This finding illustrates the operational cost of sidelining cybersecurity during transformation: organizations invest heavily in becoming digital first, only to have their momentum stalled by preventable disruptions. In a world where the future is increasingly digital, such delays directly erode competitive advantage (see Figure 4).

FIGURE 4

Impact of Cyberincidents on IT/Business Projects

Q. Which of the following areas were notably impacted because of cyberincidents in the past 12 months?

n = 411

Source: IDC's *BDO Security Survey,* March 2025

The contrast between long-term strategic intent and short-term security thinking highlights a persistent disconnect in how organizations approach transformation and risk management. While technology adoption and transformation planning are becoming more sophisticated, many organizations, particularly smaller ones, have yet to embed cybersecurity as a foundational component of that journey. Until cybersecurity is treated as a strategic partner rather than a downstream control, the full value of digital transformation will remain out of reach for much of the market.

SECURITY GAPS UNDERMINE DIGITAL ADVANTAGE

A closer look at attack patterns highlights persistent weaknesses in foundational cyberpractices. Phishing, social engineering, supply chain attacks, and malware via removable media remain among the most common attack vectors. These findings align with technical impacts as per the survey. Email systems, endpoints, and file storage systems are frequently encrypted, exfiltrated, or locked during incidents.

Recovery timelines add further context. According to the survey, the average time to respond to an incident is over four days, while the average recovery time exceeds

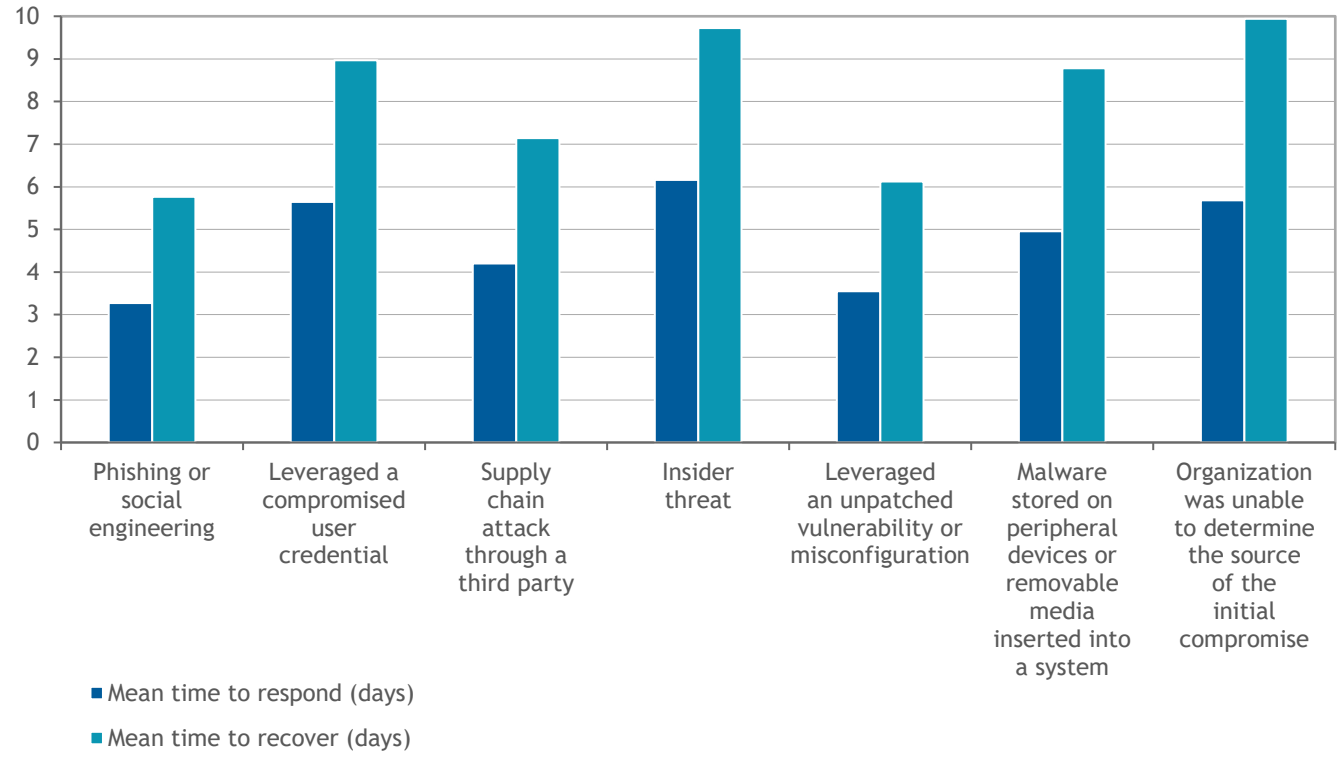
seven days. Attacks originating from insider threats or unknown sources tend to take the longest to detect and recover from, reflecting the challenges in attribution, access visibility, and internal monitoring (see Figure 5).

FIGURE 5

Mean Time to Respond/Recover by Attack Type

Q. What was the most successful attack method used by adversaries that impacted your organization in the past 12 months?

Q. How much time in number of days does your organization take to respond to and recover from cyberincidents?



n = 411

Source: IDC's *BDO Security Survey,* March 2025

While insider and unknown-source threats require specialized detection and response capabilities, the survey also highlights broader control deficiencies, particularly in vulnerability management and third-party risk management. These remain two of the most frequently cited organizational weaknesses and contribute significantly to exposure via preventable, externally driven threats. Together, these issues reflect a broader maturity gap across both internal and external threat surfaces (see Figure 6).

FIGURE 6

Top Cybersecurity Weaknesses

Q. When it comes to efficiently managing cyber-risk, which of the following areas is your organization's biggest weakness? Please select up to 3 responses.

n = 411

Source: IDC's *BDO Security Survey,* March 2025

There is a clear disconnect between awareness and execution. For instance, while supply chain attacks are a top 3 attack vector, supply chain risk ranks surprisingly low as a concern when survey respondents are asked about top cyberthreats in near term. This gap reflects a broader issue: the absence of strong governance structures and proactive risk modeling, particularly in midmarket organizations.

REALIGNING INVESTMENT, OVERSIGHT, AND PROCESS DISCIPLINE TO BUILD CYBER-RESILIENCE

Across industries and organization sizes, cybersecurity maturity is not solely a function of budgets or technology adoption. Instead, it is the product of how organizations structure accountability, deploy resources, and operationalize security processes. Despite growing awareness and formal oversight structures, many firms struggle to translate investment into consistent performance.

As per the survey, while larger organizations are more likely to appoint formal cybersecurity leaders, such as CISOs or CROs, and establish oversight through risk or technology committees, this structure does not guarantee maturity in execution. The survey revealed that 97% of organizations report some form of board or committee-level oversight, yet rising incident volumes and prolonged recovery times suggest that governance alone is insufficient without effective implementation and sustainment.

Cybersecurity budgets, for the most part, are no longer the primary constraint. Most organizations describe their budgets as at least "adequate," with a meaningful proportion classifying them as "flexible" or "readily available." However, as the data reveals, having budget is not the same as using it effectively.

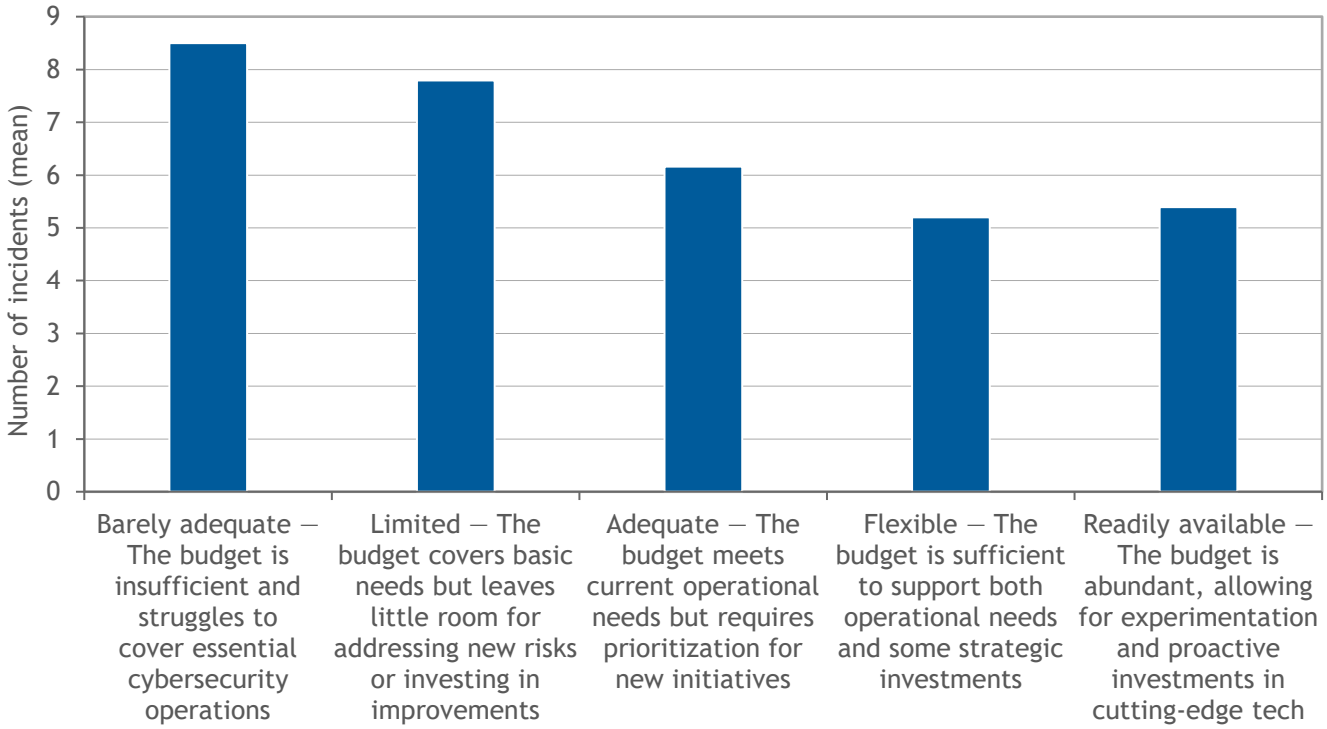
Organizations with higher security budgets generally report fewer incidents, but the reduction is not linear. While those with "barely adequate" or "limited" budgets experience the highest average number of incidents, even organizations with "readily available" or "flexible" budgets report a mean of over five incidents annually. This indicates that while budget is a foundational enabler, its effectiveness depends on how well it is allocated and operationalized. Without a deliberate focus on program maturity, process optimization, and disciplined execution, the returns on increased investment diminish. To achieve stronger outcomes, organizations must not only fund cybersecurity but also ensure those resources are strategically directed toward the capabilities, processes, and controls that most effectively reduce risk (see Figure 7).

FIGURE 7

Budget Adequacy Versus Incident Volume

Q. How would you describe your organization's current cybersecurity budget in relation to its needs and goals?

Q. To the best of your knowledge, estimate how many cybersecurity incidents occurred in the past 12 months?



n = 411

Source: IDC's *BDO Security Survey,* March 2025

A more reliable predictor of cybermaturity is operational readiness, particularly the level of monitoring coverage.

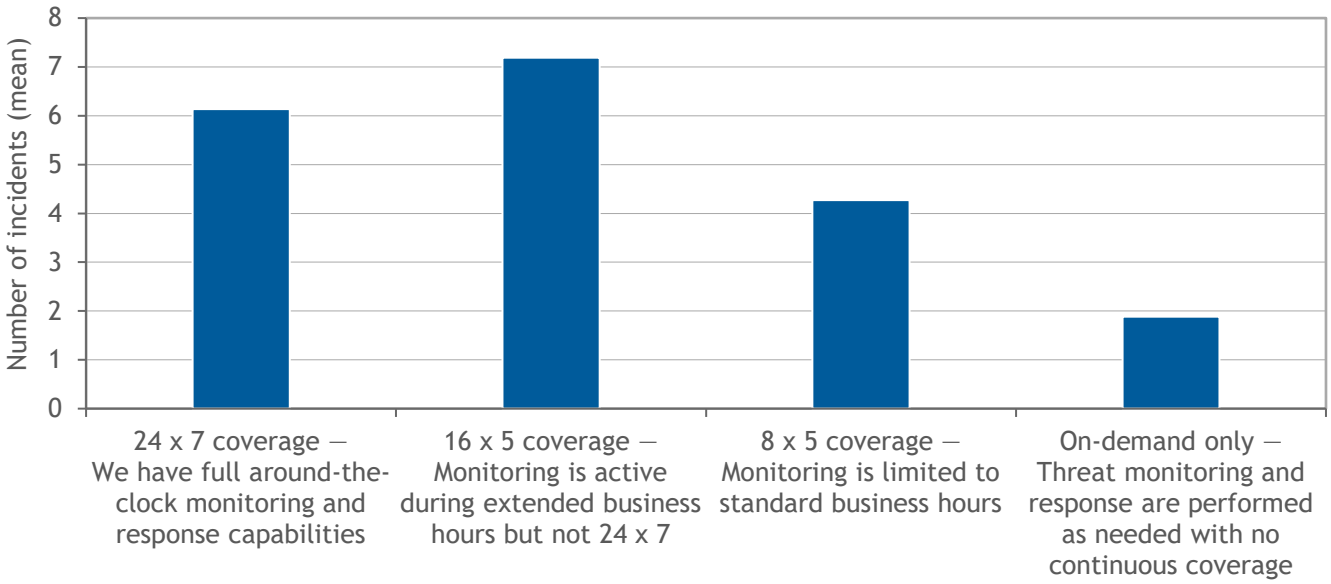
Organizations with 24 x 7 threat monitoring and response capabilities tend to detect more incidents than those with limited or on-demand coverage. This higher detection rate indicates that continuous operations offer improved visibility and faster identification of threats. Around-the-clock monitoring enables earlier detection and response, reducing dwell time and limiting the potential impact of attacks (see Figure 8).

FIGURE 8

24 x 7 Coverage and Incident Volume

Q. What is the current state of your organization's threat monitoring and response coverage (internal + outsourced)?

Q. To the best of your knowledge, estimate how many cybersecurity incidents occurred in the past 12 months?



n = 411

Source: IDC's *BDO Security Survey,* March 2025

Process maturity further differentiates organizations that manage risk proactively from those that remain reactive.

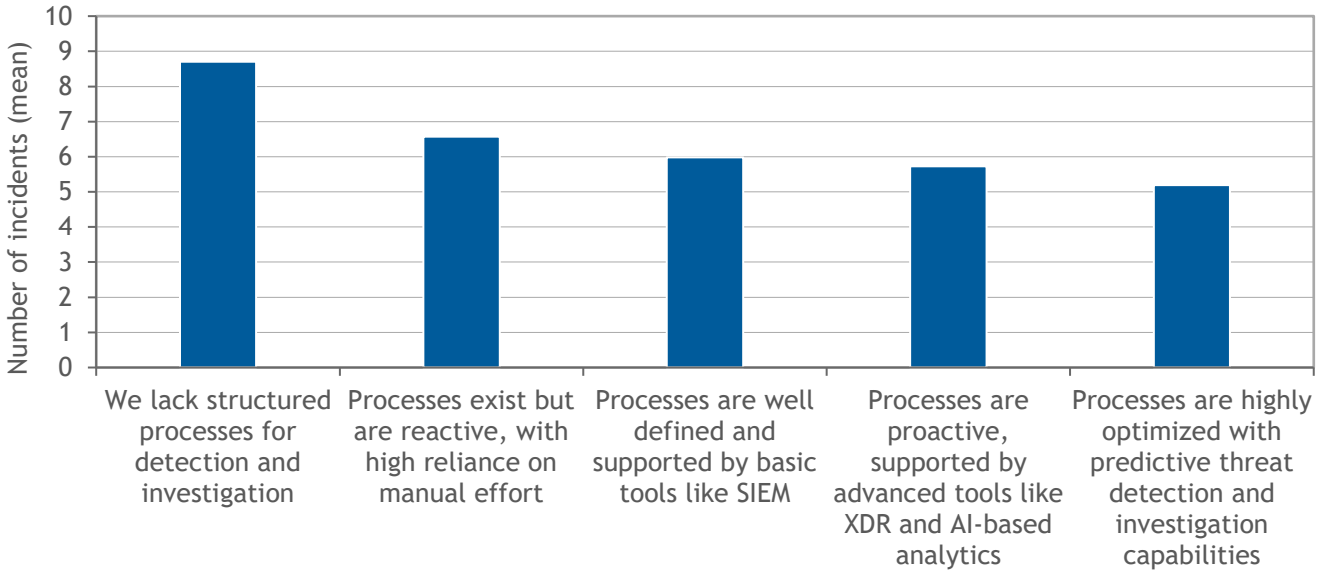
Respondents with well-defined or proactive detection and investigation processes, often supported by tools like XDR or AI analytics, reported fewer cyberincidents on average. In contrast, organizations relying on manual or reactive workflows were significantly more likely to experience repeated attacks (see Figure 9).

FIGURE 9

Process Maturity and Incident Volume

Q. How effective are your organization's processes for detecting and investigating threats?

Q. To the best of your knowledge, estimate how many cybersecurity incidents occurred in the past 12 months?



n = 411

Source: IDC's *BDO Security Survey,* March 2025

This process maturity also correlates strongly with faster recovery timelines.

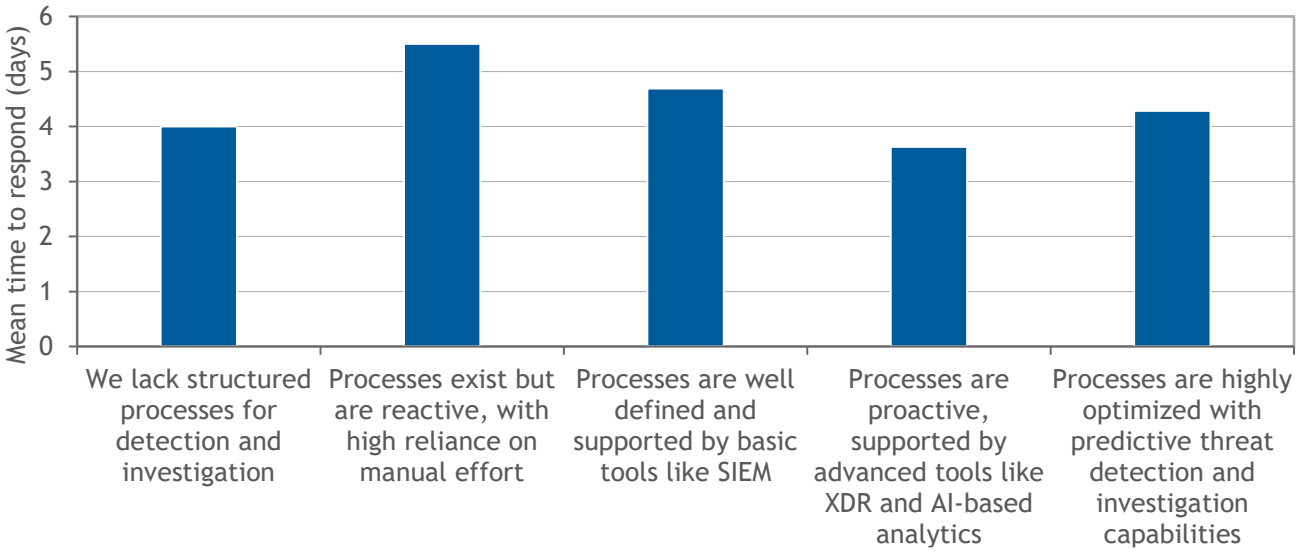
Organizations with predictive, optimized processes demonstrated faster response, often by several days compared with their peers. This reinforces the notion that maturity is not just about preventing attacks but about limiting their business impact when they do occur (see Figure 10).

FIGURE 10

Process Maturity and Mean Time to Respond

Q. How effective are your organization's processes for detecting and investigating threats?

Q. How much time in number of days does your organization take to respond to and recover from cyberincidents?



n = 411

Source: IDC's *BDO Security Survey,* March 2025

While boards increasingly demand proof of cyber-risk reduction, few organizations are tracking the effectiveness of their internal processes. Rather than focusing solely on outcome-based KPIs such as incident frequency or cost savings, organizations should also measure leading indicators of operational health, such as time to detect and contain threats, patching and vulnerability remediation rates, and the effectiveness of security awareness training. Without this process-level visibility, the gap between perceived performance and actual resilience is likely to persist, reinforcing the need to realign investment, oversight, and operational discipline.

FUTURE-PROOFING CYBERSECURITY

Organizations are increasingly aware of where their cybersecurity strengths lie and where they fall short. Foundational practices like IT asset management, basic risk assessments, and security testing are cited as current strengths. Yet external dependencies, such as third-party risk management, threat intelligence, and governance functions like GRC (governance, risk, and compliance), remain persistent

weaknesses. These gaps are well known, and in many cases, acknowledged by security leaders themselves.

What makes these shortcomings more concerning is the degree of misalignment between strategic intent and execution. Many organizations report having long-term digital transformation strategies and sufficient cybersecurity budgets. Yet a large portion still struggle with delayed threat detection, prolonged recovery times, and an inability to scale response processes. This disconnect between perceived readiness and actual capability continues to widen the resilience gap across the market.

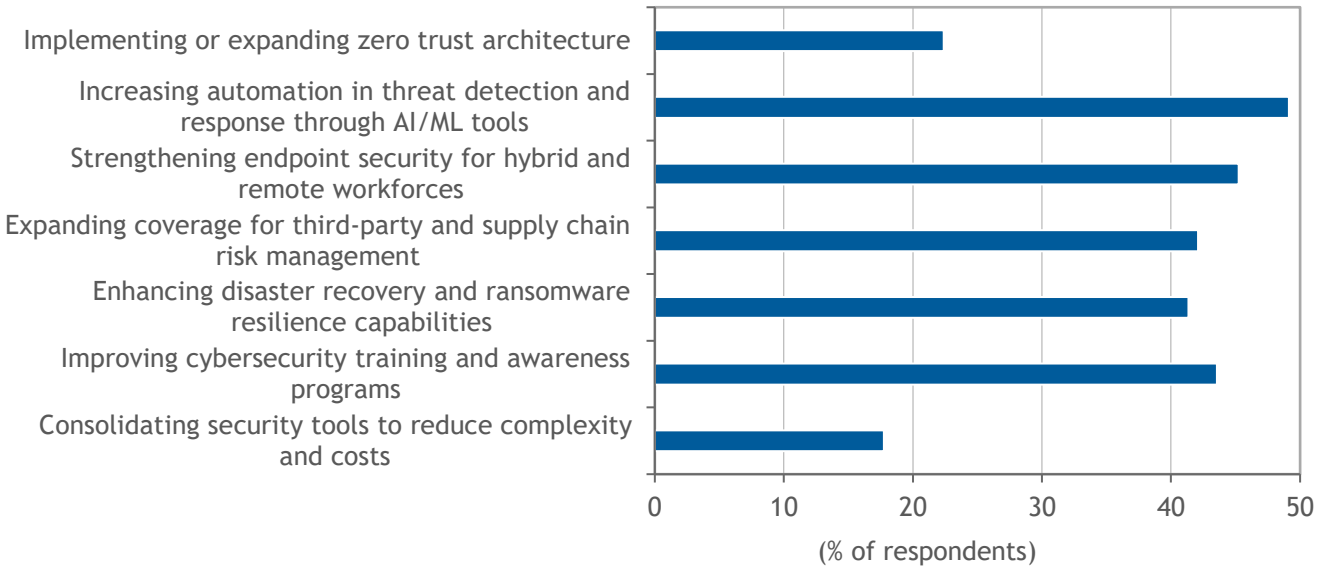
Encouragingly, organizations are beginning to shift their security priorities in ways that address these very issues. The top initiatives going forward reflect a strong emphasis on automation, advanced threat detection, and human-centric defenses.

Nearly half of all respondents say they are prioritizing increased automation in threat detection and response using AI/ML tools. Strengthening endpoint security and improving employee training and awareness programs also rank among the top 3 priorities, reflecting a balanced approach that combines advanced tooling with empowered workforces. Midsize enterprises in particular are focusing on disaster recovery and supply chain risk, suggesting an evolving understanding of the broader cyber ecosystem (see Figure 11).

FIGURE 11

Top Cybersecurity Priorities

Q. Which strategic initiatives is your organization focusing on to enhance its cybersecurity posture in the future?



n = 411

Source: IDC's *BDO Security Survey,* March 2025

Notably, GenAI has emerged as a pressing area of concern. As adoption accelerates across business functions, so too do the risks, from deepfake-driven phishing to unintentional data leakage through LLM prompts. Yet organizations are responding with tangible mitigation strategies.

Top concerns include increased susceptibility to phishing and social engineering, governance gaps in GenAI usage, and difficulty in securing sensitive IP used in model training. In response, nearly half of the organizations have implemented employee training on GenAI usage, while others are investing in AI-specific security solutions and access controls to limit exposure. However, broader actions like establishing risk assessment frameworks or embedding GenAI into data governance programs remain underdeveloped (see Table 1).

TABLE 1

GenAI Risks and Mitigation Strategies

Q. How is the adoption of generative AI (GenAI) impacting business risk in your organization?

Q. What steps is your organization taking to mitigate risks associated with generative AI adoption?

Top GenAI Risks (Ranked by Perceived Severity)	Mitigation Strategy Adopted and % of Organizations Implementing This Strategy
Greater susceptibility to phishing and social engineering attacks	Training employees on secure and ethical use of GenAI tools (49)
Challenges in governing GenAI use across employees and teams	Establishing usage policies or guidelines for internal teams (31)
Difficulty in securing intellectual property or proprietary data used in GenAI models	a. Investing in AI-specific security solutions to detect and mitigate risks (46) b. Implementing data access controls to limit exposure to sensitive information (41)
Limited understanding of how to assess and mitigate GenAI-related risks	Developing risk assessment methodologies for assessing risk (e.g., AI impact assessments) (34)
Increased risk of data leaks or accidental exposure through GenAI tools	Implementing data protection and data governance programs (20)
Regulatory considerations and ensuring our organization is compliant with regulations	Conducting regular audits of GenAI tools and outputs (40)
No significant impact on business risk due to GenAI adoption	No specific mitigation strategies are currently in place (7)

n = 411

Source: IDC's *BDO Security Survey,* March 2025

Ultimately, the path forward depends on a tighter alignment between strategy and execution. Many organizations recognize what needs to be done, from building automation and resilience into the environment to addressing emergent risks like GenAI, but execution lags behind awareness. Closing this gap will require not just more investment, but better integration of technology, people, and governance.

BDO OFFERINGS

Today, businesses across all industries are adopting advanced and emerging technologies at a much faster rate than ever before. Solutions driven by data and AI are

powerful assets to help you stay competitive in current markets; but they aren't without vulnerabilities.

Through BDO's end-to-end Perpetual Defence program, organizations benefit from the firm's experience in technology and in-depth industry knowledge to offer end-to-end cybersecurity solutions that help improve growth and profitability, maintain pace with technology change, and simplify and improve security operations.

The three-part Perpetual Defence program is made up of the following:

- **Active Insights** is a comprehensive approach for cyberplanning and strategy development that helps businesses understand their current posture and coverage and optimize their cyberprogram. Active Insights helps organizations ensure they are focusing their budgets in the most effective and efficient way to manage cyber-risks confidently.
- **Active Protect** provides 24 x 7 x 365 monitoring, detection, and response services, including automated and human-led actions to mitigate threats in near real time. It leverages automation and orchestration for rapid detection and immediate response, often stopping attacks before the adversary achieves their objectives.
- **Active Assure** provides incident preparedness to drive faster response and recovery and operational and offensive security testing services to test established controls to ensure they continue to function as intended as your technology environment continues to evolve.

CHALLENGES/OPPORTUNITIES

The survey reveals that organizations, particularly midsize and large enterprises, continue to grapple with foundational security challenges. Areas such as third-party risk management, vulnerability remediation, and the integration of security into broader transformation efforts remain weak spots. These gaps persist despite the presence of adequate budgets and formal board-level oversight in many cases, suggesting a disconnect between strategy and execution.

As cyberthreats grow more sophisticated, driven by trends such as GenAI misuse, rapid cloud expansion, and complex supply chain dependencies, organizations are under pressure to evolve from reactive controls to proactive, intelligence-led defenses. The challenge is not simply identifying risks, but translating that awareness into effective, scalable, and context-aware security practices.

This environment creates opportunities for organizations to reassess the support they need from external partners. Increasingly, buyers are looking beyond traditional

assessments and compliance checklists. They expect partners that can provide end-to-end advisory and execution support, from maturity diagnostics and control benchmarking to the design of integrated governance models and operational workflows.

To stay ahead, organizations should look for partners that bring deep sector knowledge, proven delivery frameworks, and the ability to align cybersecurity initiatives with enterprisewide transformation goals. The ability to address both emerging risks and day-to-day execution gaps, such as automation of security operations or governance of GenAI adoption, will be key differentiators.

Ultimately, as cybersecurity shifts from being a technical cost center to a strategic enabler, organizations have an opportunity to reframe their approach, choosing partners that help embed security into the core of resilience, innovation, and long-term competitiveness.

CONCLUSION

As organizations accelerate digital transformation, cybersecurity can no longer remain a reactive function. This study highlights that while investments are growing and awareness is high, gaps in execution, process maturity, and risk alignment persist, especially in the face of emerging threats like GenAI.

Closing these gaps requires more than funding. It demands a shift toward integrated security governance, continuous monitoring, and future-ready risk management frameworks. Organizations that succeed will treat cybersecurity not as a compliance task, but as a strategic enabler of operational resilience and long-term growth.

ABOUT IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology, IT benchmarking and sourcing, and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives. Founded in 1964, IDC is a wholly owned subsidiary of International Data Group (IDG, Inc.).

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com