Modern Enterprise Cybersecurity

Cultivating Resilience with Reduced Detection and Response Times

WHITE PAPER

ISG Research™

Sponsored by:

BT

Table of Contents

The Complexities of Enterprise Security

In recent years, enterprise cybersecurity has undergone a profound transformation. Historically, organizations relied on well-defined security perimeters. They built robust defenses around their internal networks, treating them like castles surrounded by protective moats. This approach assumed that threats would come from outside, and the primary goal was to keep adversaries at bay. However, the rise of cloud computing, internet of things devices and remote workforces has disrupted this approach, and enterprises now face a delicate balancing act: they must protect their workforce, sensitive data and critical endpoints while also embracing digital transformation. Enterprises cannot turn back the clock to the days of impenetrable castles. Instead, they must embrace resilience.

Better detection, response and recovery does more to change an enterprise's cybersecurity risk profile than prevention of incremental attacks. The better an enterprise's detection, response and recovery, the more resilient it is and the incremental value of preventing attacks with more security measures becomes much lower. Prevention, detection, response and recovery all work together, and resilience does not require an all-or-nothing approach within each category. But an enterprise cannot be way out of balance on any of those four facets. Our ISG cybersecurity research shows that spending is often skewed toward protect and detect at the expense of efforts on response and recovery.

In the past 12 months, 95% of enterprises report at least one security incident—and that only accounts for incidents that were discovered.

In today's threat environment, the goal for enterprise security teams should be to improve their performance on those two metrics: the amount of time it takes to identify or detect, and the mean time to remediation or response. Ultimately, it is not about reducing successful attacks to zero, but rather it is about minimizing damage. If an enterprise can bring those numbers down, there is a direct correlation with lower damage from attacks.

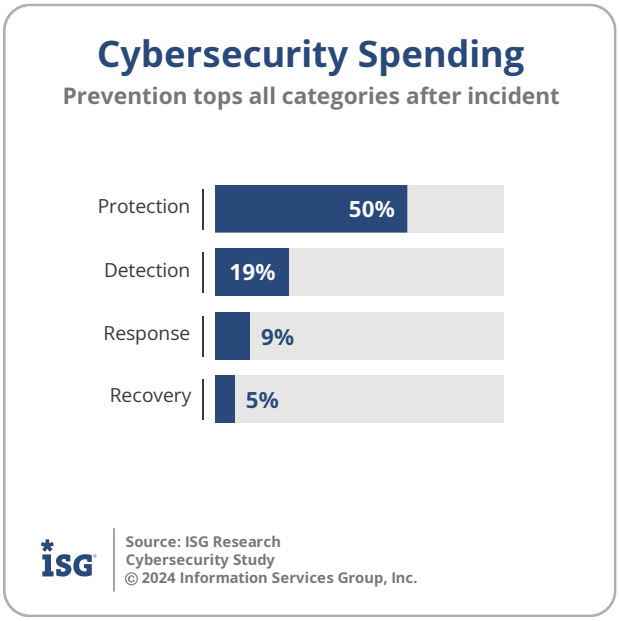
By determining an acceptable level of cyber risk, digital security tools can be applied to monitor, mitigate and respond to enterprise threats. Conversely, without understanding risk tolerance, an enterprise will constantly be a step behind in "fix" mode. In the past 12 months, 95% of enterprises report at least one security incident—and that only accounts for incidents that were discovered. Security incidents have the attention of executives, board members and regulators, and Chief Information Security Officers (CISOs) are looking to change their approach.

With the proliferation of cloud computing services, the enterprise security perimeter has all but disappeared. The adoption of remote and hybrid work environments reinforced the change in boundaries of what security teams are responsible to protect. As a result of the on-

going expenditures in security software, the incidents of more concern are those that made it through when a security measure was already in place.

No single blueprint exists for what security software consists of in the enterprise. Platforms and point products do exist, but the full stack is often a patchwork of software from multiple providers that evolves over time to accommodate a changing attack surface. Because every enterprise is at a different point in their security posture, single-source suppliers are unrealistic because of variance in the enterprise and needs. However, multiple point solutions do not necessarily get an enterprise closer to having good security. They simply represent that enterprise's attempts trying to prevent certain things. By setting fundamental security posture goals, an enterprise positions itself to be able to deal with incidents that happen and recover from them while minimizing loss.

Interoperability of security products is hard to achieve. Low success rates of integration and collaboration among software providers do not instill confidence that full interoperability is even possible. Because there is no guarantee of achieving this approach, enterprises often opt for an integrated software platform strategy.



But on-going security spending is not the answer. It is easy to slip into a reactive mode of spending to patch issues as they arise. Our research shows that security spending after an incident is significantly more for protection (50%) than detection (19%), response (9%) and recovery (5%) combined, as enterprises look to "solve" security concerns, and yet, 95% of enterprises still experience a cyberattack. And the cost to recover from damages to data and damages to reputation outweigh the cost to provide a proactive and holistic security software strategy in the first place.

Cybersecurity as Risk Management

Ultimately, cybersecurity must be thought of as a risk management discipline. Enterprises need to understand the level of vulnerability and exposure across assets, processes and people in order to develop an effective security strategy. Tracking and measuring security posture enables an enterprise to identify gaps and weaknesses in security measures, prioritize remediation actions, evaluate the effectiveness of digital security investments and demonstrate compliance with regulatory standards. This is important because an enterprise's security posture is related to its cybersecurity risk.

Many enterprises today lack a clear understanding of their risk tolerance. Without this clarity, enterprises may allocate excessive resources to risks that are already below the appetite threshold, while neglecting critical risks. This is the result of security functions lacking awareness of broader organizational risk factors. Digital security best practices vary by enterprise but generally map to existing business activities, such as governance, risk management, compliance, awareness and technology. The CIO or IT leader can take steps to ensure all stakeholders communicate effectively about digital security.

Today's leaders face significant challenges in maturity, regulation and risk management. Cybersecurity awareness within enterprises has grown as the threat landscape intensifies:

- Tools and attack methods are becoming more sophisticated.
- The dark web and other networks like it encourage and enable the distribution of cybercrime profits, and there are more resources in terms of skills, personnel and funding to drive the attacks.
- The scale and scope of nation-sponsored cyber-attacks are increasing.
- Cloud security and the accelerated development of digitization are weak spots that, when left unmanaged, can lead to increased risk for the enterprise.
- Remote work environments may also pose a security risk through the use of unapproved devices.

Risk management is maturing as a practice, acting as an enabler for digitalization through a greater business focus on security. Cyber risk quantification (CRQ) offers enterprises a quantitative look at the probability of cyber loss events and their impacts by utilizing quantitative values as inputs. Enterprises should prioritize risks based on the financial exposure to the enterprise and ensure that investments made are specific and sufficient to that particular enterprise. They should allocate limited resources in the most efficient manner, ensure that security insurance coverage is sufficient and measure the ROI for any given security investment based on risk reduction. An enterprise's amount of spend should be proportional to the amount of risk that the enterprise is willing to tolerate, but enterprises lack clarity around risk appetite, treatment through avoiding, reducing, transferring or accepting risk and reduction.

> **Resilience should be a key goal, rather than the complete elimination of security events.**

Resilience should be a key goal, rather than the complete elimination of security events. An enterprise's capacity to maintain its operation under challenging circumstances requires a level of agility and readiness to tackle any disruptions that could hinder operational effectiveness. To improve its security posture, an organization must adopt and implement best practices that enhance visibility, protection and resilience against cyber threats.

Security controls are perceived by some as an overhead because they may require adding resources and additional planning. However, controls reduce the risk of security incidents, data breaches and unauthorized access. They also contribute to business continuity by safeguarding critical systems and data. Security controls streamline incident detection, response and recovery, which leads to operational resilience.

Ensuring operational resilience involves establishing appropriate programs and processes for business continuity, which must be supported by the right technology investments. Business continuity has long been a cornerstone for enterprises. For instance, whether facing natural disasters, supply chain disruptions or cyber threats, organizations must ensure uninterrupted operations. But the digital age has introduced new complexities, with cyber risk looming large.

> **While cyber security remains critical, a myopic focus on perfection can hinder progress.**

A "zero-tolerance" approach to cyber security is not viable or reasonable. While cyber security remains critical, a myopic focus on perfection can hinder progress. Instead, enterprises should adopt a holistic approach to cyber risk management that aligns with broader business strategies. A proper risk management approach includes development of these three factors:

- Risk prioritization. Not all risks are equal. Prioritize cyber risks based on their potential impact on business operations.
- Resilience strategies. Rather than chasing an elusive state of perfect security, invest in resilience.
- Business impact assessment. Quantify the impact of cyber incidents on revenue, reputation and customer trust. This informs decision-making and resource allocation.

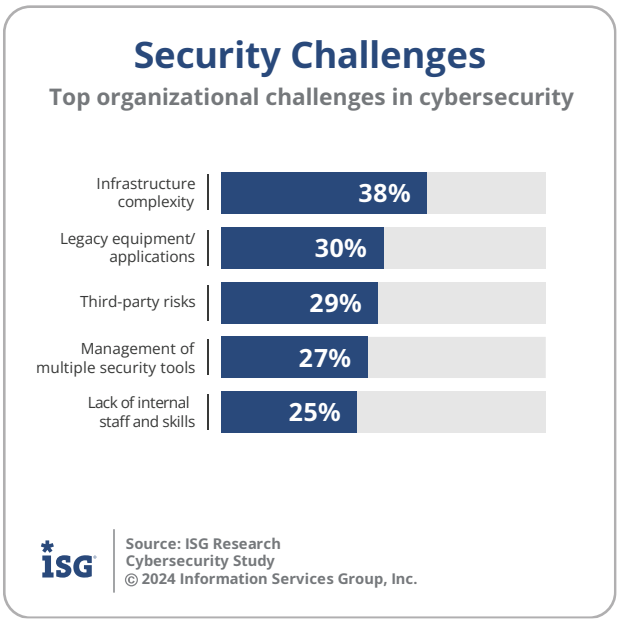
Cyber risk management shares similarities with other complex domains. Enterprises can draw insights from fields such as financial risk management, supply chain optimization and regulatory compliance. By identifying analogous challenges, businesses can apply proven strategies to enhance operational resilience.

Protection vs. Detection and Response

Evolving from protection approaches to proactive detection and response is key to minimizing damage to the enterprise. Threat actors have access to the same emerging technologies found in the enterprise, including generative AI (GenAI), machine learning (ML) and large language models (LLMs). Highly personalized phishing attacks occur at scale facilitated by ransomware-as-a-service and turnkey phishing kits. Traditional security approaches catch most attacks, but they are not foolproof. Despite protection measures, security breaches are

inevitable due to expanding threat surfaces, multi-cloud infrastructures and sophisticated attackers. Organizations must accept that some attacks will get through their defenses.

Managed detection and response (MDR) services take a holistic approach to traditional endpoint detection and response strategies. Combined with human security analysts, this approach helps address threats that have already infiltrated the network. Moving to MDR enables enterprises to reduce the legacy software tech debt of continuing to spend on protection software and instead focus security team resources on threat hunting and other issues that are not easily automated. This can be a key step forward as nearly 2 in 5 (38%) organizations in our research cited infrastructure complexity as one of the top three challenges in maintaining security performance for the enterprise. The second-most cited challenge was legacy equipment or applications, and these two factors—infrastructure complexity and legacy software—are key contributing factors to a ballooning legacy software tech debt.



Strengthening Enterprise Security

Detection and response play an important role in safeguarding enterprises against security breaches. Enterprises face an array of risks, from sophisticated cyberattacks to insider threats, and their ability to detect and respond effectively can significantly impact their resilience and overall security posture.

Detection is the first line of defense against security threats, and resilient organizations prioritize early threat detection. By identifying malicious activity promptly, they can minimize the impact of security incidents and prevent them from escalating. Unfortunately, many enterprises still struggle with slow detection times. Delays in identifying threats allow attackers to gain a foothold and move laterally within the network. There are tools and technologies available that enhance detection capabilities, including behavior-based anomaly detection, threat intelligence feeds and machine learning algorithms.

Threat actors have become increasingly sophisticated, leveraging emerging technologies to their advantage. Tools like GenAI and LLMs enable them to craft highly personalized attacks, making it harder to distinguish malicious activity from legitimate user behavior. Prebuilt and proven attacks exploit human vulnerabilities and can bypass traditional security measures. While traditional security approaches catch most attacks, they are not foolproof. Zero-day exploits, malware and social engineering tactics continue to challenge even the most robust defenses.

Despite enterprises' best efforts, security breaches are inevitable. Several factors contribute to this reality.

- As enterprises adopt cloud services, IoT devices and remote work environments, their attack surface widens. Each new entry point represents a potential vulnerability.
- Organizations increasingly rely on multi-cloud architectures. While this offers flexibility, it also introduces complexity and potential blind spots.
- Adversaries continuously evolve their tactics.
- Advanced persistent threats (APTs) and nation-state actors pose significant challenges.

MDR services go beyond traditional endpoint detection and response. Providers continuously monitor network traffic, endpoints and logs to detect anomalies, suspicious behavior and indicators of compromise. MDR combines automated tools with skilled security analysts who investigate alerts and validate threats to respond swiftly. When threats infiltrate the network, MDR teams are prepared to respond. Their goal is containment, eradication and recovery.

Building a Cyber Incident Recovery Practice

Effective cyber incident recovery is a cornerstone of organizational resilience, but enterprises often neglect recovery practices. Despite the growing threat landscape, many organizations prioritize prevention and detection over recovery. This bias stems from the misconception that investing in recovery is unnecessary if robust preventative measures are in place. Organizations may underestimate the likelihood of a successful cyberattack or assume that their defenses are impenetrable.

Multiple benefits of prioritizing recovery exist. Swift recovery minimizes business disruption. Organizations can resume normal operations faster, preventing revenue loss and reputational damage. Effective recovery limits the extent of damage caused by security incidents. It prevents data loss, financial losses and customer dissatisfaction. Furthermore, regulatory bodies increasingly emphasize incident response and recovery as part of compliance requirements.

> **Just as individuals rely on muscle memory to perform repetitive tasks automatically, organizations need a well-practiced recovery process.**

Just as individuals rely on muscle memory to perform repetitive tasks automatically, organizations need a well-practiced recovery process. This "corporate muscle memory" is a good habit, and it improves the ability of security teams to respond effectively even under stress. Organizations should conduct regular incident response drills, tabletop exercises and simulations. These reinforce muscle memory and improve coordination among teams.

Involve the right people and roles in the recovery practice. Within IT, incident response teams lead the recovery efforts. They include security analysts, network administrators and system engineers. Technical specialists in key areas, such as forensics or malware analysis, contribute to identifying the root cause and restoring systems. Business stakeholders are also important to involve in the recovery practice. Business continuity managers ensure that critical business functions resume promptly. Legal and compliance teams address legal implications, regulatory reporting and contractual obligations. And the third component to a successful recovery practice is the executive leadership and board of directors. The board and executives play a crucial role in approving recovery budgets, policies and strategic decisions. They communicate with stakeholders, manage reputational risks and provide oversight.

The Role of Security Leaders

Government regulators worldwide are recognizing the severity of cyber threats and their potential impact on organizations. These entities have turned their attention to enterprise security incidents, emphasizing the need for timely response. The scope of incidents, the resulting damage and breach notifications are under scrutiny. In the United States, for example, financial reporting guidelines now explore security incident reporting as part of fiduciary responsibility for compliance reporting. Organizations must disclose security breaches transparently.

Enterprise security leaders, including the CISO, play a critical role in managing risk and the influence of security leaders in shaping risk management strategies is not always well understood. As CISOs gain a seat at the executive table alongside other leaders, they find themselves in the crosshairs of non-technical peers and board members. Communicating security incidents in business terms becomes essential.

A robust security strategy therefore requires more than just technology, and CISOs must align digital security strategies with broader business objectives.

Digital security extends beyond acquiring and deploying the latest technology. While cutting-edge tools and approaches enhance an enterprise's security posture, they are not a panacea. A robust security strategy therefore requires more than just technology, and CISOs must align digital security strategies with broader business objectives. Demonstrating how investments in security contribute to positive business outcomes is crucial.

Work must also continue to shift the enterprise's overall mindset from cybersecurity to IT resilience. Rather than framing incidents solely as cybersecurity problems, enterprises should view them as IT recovery challenges. This perspective emphasizes the need for swift response and getting back to business as usual.

Key Takeaways

- Security is an outcome, not an action.
- The goal for organization security teams is to reduce the amount of time it takes to identify or detect while also reducing the mean time to remediation or response.
- Enterprises must assess risk tolerance to effectively allocate budgets and resources. The cost to recover from damages to data and damages to reputation outweigh the cost to provide a proactive and holistic security software strategy.
- Detection and response are key to minimizing damage, and a better response and recovery process does more to change an enterprise's risk exposure than the prevention of incremental attacks.
- Enterprises with a high focus on resilience achieve excellent results.

About ISG Research

ISG Research™ provides subscription research, advisory consulting and executive event services focused on market trends and disruptive technologies driving change in business computing. ISG Research™ delivers guidance that helps businesses accelerate growth and create more value. For more information about ISG Research™ subscriptions, please email contact@isg-one.com.

About ISG

ISG (Information Services Group) (Nasdaq: III) is a leading global technology research and advisory firm. A trusted business partner to more than 900 clients, including more than 75 of the world's top 100 enterprises, ISG is committed to helping corporations, public sector organizations, and service and technology providers achieve operational excellence and faster growth. The firm specializes in digital transformation services, including AI and automation, cloud and data analytics; sourcing advisory; managed governance and risk services; network carrier services; strategy and operations design; change management; market intelligence and technology research and analysis. Founded in 2006, and based in Stamford, Conn., ISG employs 1,600 digital-ready professionals operating in more than 20 countries—a global team known for its innovative thinking, market influence, deep industry and technology expertise, and world-class research and analytical capabilities based on the industry's most comprehensive marketplace data. For more information, visit isg-one.com.