RICHMOND ADVISORY GROUP

RichmondAdvisoryGroup.com

Sponsored by LevelBlue

Why Organizations Are Prioritizing Incident Readiness and Response in the Face of Regulatory Scrutiny

Abstract

The Richmond Advisory Group, LLC conducted a survey in December 2023, involving 500 US-based private sector cybersecurity decision-makers from mid-market to small/medium enterprises (500 to 5,000 employees, SMEs). The study aimed to explore the motivations and goals behind purchasing incident readiness and response services. It found that over a third of respondents dedicated more than 50% of their time to cybersecurity, emphasizing the significance of cybersecurity leadership within their organizations. The document aims to educate buyers on the incident readiness and response market, highlighting the services deemed most valuable for 2024. It also discusses the impact of recent SEC regulatory changes on cybersecurity risk management and strategy, emphasizing the increased emphasis on effective cybersecurity measures for SMEs. The importance of proactive incident readiness is underscored, detailing steps for SMEs to improve their readiness, such as conducting risk assessments and implementing vulnerability management programs. Additionally, it outlines the benefits of a proactive approach, including reduced impact of security incidents, regulatory compliance, and cost savings. The study further reveals SMEs' purchasing preferences, emphasizing a preference for subscription, retainer, or fixed-fee pricing models, and highlights the top service providers in the market. Overall, the white paper advocates for a proactive and strategic approach to cybersecurity resilience, essential for protecting assets, maintaining business continuity, and adhering to regulatory requirements.

Table of Contents

A Proactive and Strategic Approach to Cybersecurity Resilience

In December 2023, Richmond Advisory Group, LLC surveyed 500 US-based private sector cybersecurity decision-makers and influencers, including IT leaders, incident responders, CISOs, and other security leaders in the mid-market to small/medium enterprises (500 to 5,000 employees), to uncover motivations and goals for purchasing incident readiness and response services. More than a third of the respondents spend more than 50% of their time on cybersecurity and all are cybersecurity leaders for their organization. This document will seek to educate the buyer on the incident readiness and response market and provide insight into the key takeaways of this recent study. The bulk of the discussion will highlight the specific incident readiness and response services buyers believe are the most valuable and are planning on purchasing in 2024. Additionally, the discussion will focus on the motivation for buying these services, the specific drivers and goals that pushed them to purchase, the service providers on their A-list and their preferred pricing models for these services.

> Respondents spend more than 50% of their day working in cybersecurity.

It is first imperative to understand that incident readiness market dynamics shifted in 2023 with regulatory changes announced by the Securities and Exchange Commission (SEC) to risk management over the last 12 months, particularly in cybersecurity risk management, strategy, governance, and incident disclosure. On July 26, 2023, the SEC adopted rules requiring registrants to disclose their cybersecurity risk management strategy and governance, as well as the material impact of cybersecurity incidents on the registrant. These recent SEC regulatory changes are expected to have a significant impact on the mid-market. For small to mid-market enterprises (SMEs), this means an increased emphasis on implementing effective cybersecurity measures, as they are often targeted by cybercriminals due to perceived vulnerabilities in their security posture. Failure to comply with these regulations could lead to legal consequences and fines, as many industries have regulations governing the protection of customer data. Indeed, this recent survey highlights that SMEs received the message and are prioritizing cybersecurity risk awareness.

The Importance of Proactive Incident Readiness

Incident readiness and incident response are related concepts within the broader field of cybersecurity, but they refer to different stages and aspects of managing security incidents. Incident readiness refers to the state of being prepared for potential security incidents. It involves proactive measures taken by an organization to anticipate, prevent, and mitigate the impact of security incidents. The primary focus of incident readiness is on preparation and prevention. It encompasses activities such as risk assessments, vulnerability management, security awareness training for employees, and the development of incident response plans.

Incident preparedness is a proactive and strategic approach that enables organizations to respond effectively to security incidents, protect their assets, maintain business continuity, and demonstrate a commitment to cybersecurity best practices. It is a critical component of a comprehensive cybersecurity strategy.

On the other hand, incident response refers to the reactive measures taken by an organization to address and mitigate the impact of a security incident that has occurred. It involves a coordinated and structured approach to managing and resolving the incident. The primary focus of incident response is on reacting to and resolving an ongoing security incident. The goal is to minimize the impact, contain and eradicate the threat, recover affected systems, and learn from the incident to improve future security posture.

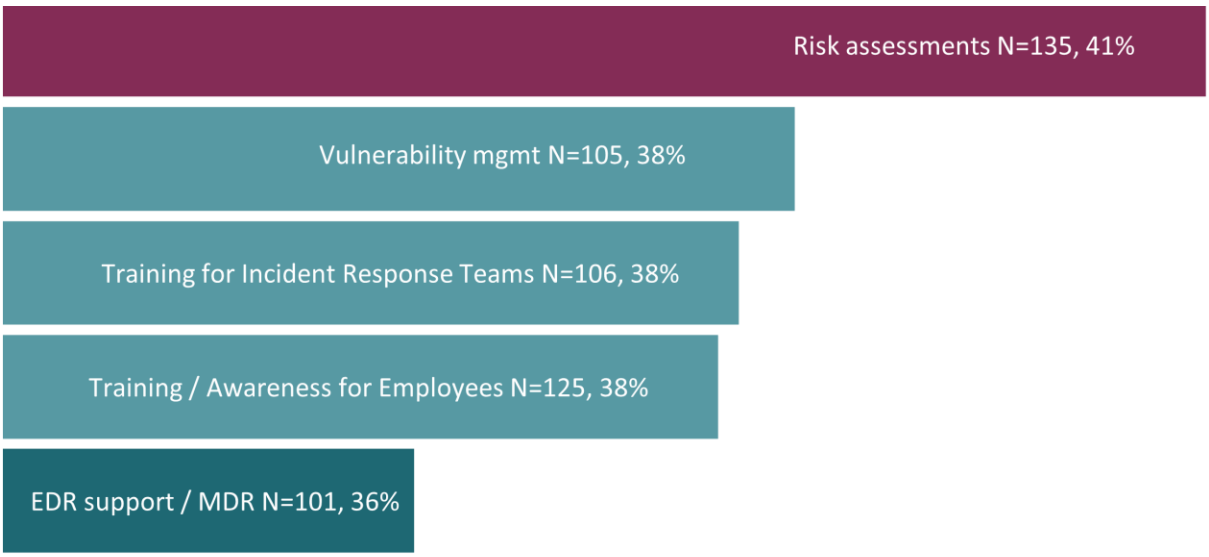
How SMEs Can Benefit from a Proactive Approach

There are many benefits to taking a proactive and strategic approach to incident readiness. By being prepared, organizations can:

- Reduce the impact of security incidents
- Improve their ability to recover from security incidents
- Minimize downtime and disruption
- Protect their reputation
- Comply with regulations
- Save money
- Learn from incidents to improve future response

In fact, the proactive incident readiness services that SMEs are purchasing in 2024 are risk assessments, vulnerability management, training for incident response teams, and employee cybersecurity training and awareness. The key

Top Incident Readiness Services Prioritized Next 12 Months



Source: Richmond Advisory Group, 2024.

benefits of readiness services according to this same study are increased security, protecting assets, enhancing safety, reduced liability, quick recovery and improving operational efficiency.

Taking the First Step

If you are an SME that is looking to improve its incident readiness, there are several first steps you can take, beginning with:

- Conduct a risk assessment to identify your vulnerabilities and create a risk management plan.
- Implement a vulnerability management program that prioritizes mitigation based on risk.

Many SMEs lack resources and budget to improve readiness by themselves and seek third-party service providers for support to additionally:

- Develop an incident response plan.
- Train incident responders.
- Provide security awareness training for employees.

In the context of incident readiness, risk assessments involve identifying, analyzing, and evaluating potential risks that could impact an organization's ability to respond effectively. The goal is to proactively identify vulnerabilities and assess the likelihood and potential impact of various scenarios, enabling organizations to prioritize resources for risk mitigation.

Key elements of risk assessments include:

- Evaluating and identifying critical assets, information, and resources to prioritize protection efforts during incidents.
- Identifying potential incidents, hazards, or vulnerabilities by analyzing historical incident data, threat intelligence, and organizational context.
- Assessing vulnerabilities in infrastructure, systems, and processes to understand their likelihood of exploitation by threats.
- Combining visibility of business-critical assets, data, and workloads with the likelihood of exploitation to evaluate overall risk and determine priorities for attention and resources.
- Developing and implementing strategies based on identified risks to effectively mitigate or manage them, including security measures, policy updates, and technology investments.
- Aligning risk management and incident readiness strategies with relevant regulatory requirements and data protection laws.
- Regularly reviewing and updating risk assessments ensures ongoing relevance and effectiveness in response to changes in the threat landscape and organizational context.

Conducting risk assessments enhances overall preparedness, improves incident response capabilities, and minimizes the impact of disruptions. Integrating compliance efforts with risk management not only protects against legal and financial repercussions but also guides the establishment of a robust security framework.

Vulnerability management services, which complement risk management services, play a crucial role in incident readiness by proactively managing weaknesses in an organization's systems and infrastructure. Key elements include continuous scanning, automated tools, and manual assessments to identify vulnerabilities, as well as monitoring threat intelligence for emerging threats. Integrating real-time cyber threat intelligence into both the risk assessment and vulnerability management processes can help more accurately identify and prioritize threats based on the latest threat landscape, and to assist with alignment of the organization's defenses with current trends and attack vectors. Vulnerability mitigation should be prioritized based on known exploits in the wild and criticality of business assets, applications, and data. Continuous management includes patch and configuration management, incident response integration, and may lead to employee training to foster a culture of security awareness. Beyond general security awareness training for all employees, consider developing role-specific training programs. Different roles may have varying levels of access and control over sensitive information and systems, and as such, tailored training can better prepare individuals for the specific risks associated with their roles.

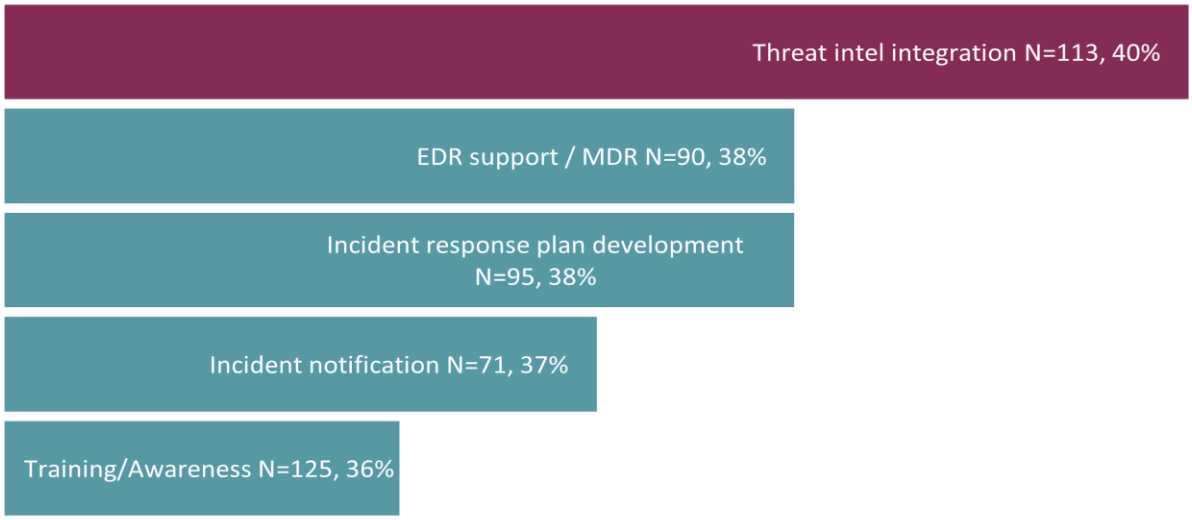
Vulnerability mitigation should be prioritized based on known exploits in the wild and criticality of business assets, applications, and data.

In 2024, SME organizations prioritize these services, recognizing their interconnected nature and the collective impact on overall security readiness.

Enhancing Incident Readiness with Threat Intelligence, EDR/MDR Services, and Incident Response Planning

When considering crucial incident readiness services beyond what they have prioritized to purchase in 2024, SMEs emphasize the importance of threat intelligence integration, Endpoint Detection and Response (EDR) or Managed Detection and Response (MDR) services, and incident response plan development. These services collectively expand an organization's ability to detect, respond to, and mitigate security incidents effectively across the attack surface. When considering technology, look for a platform with integrated threat intelligence which enhances visibility, provides deeper context, and improves forensic evidence gathering when an incident occurs.

Most Important Incident Readiness Services



Source: Richmond Advisory Group, 2024.

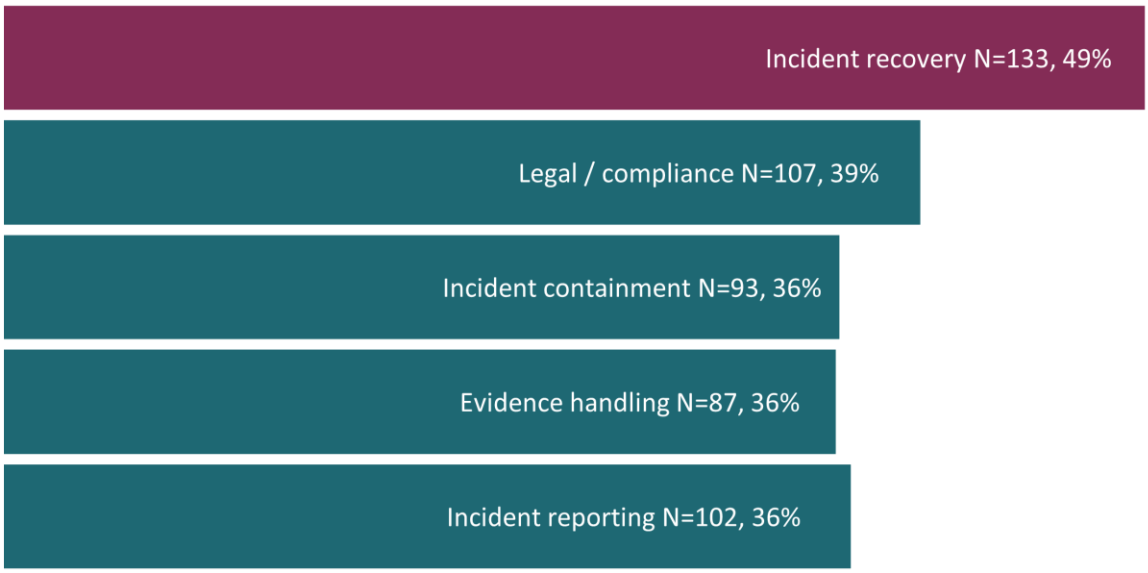
Proactive threat intelligence informs EDR and MDR solutions, enabling organizations to detect and respond to potential incidents before they escalate. These services leverage threat intelligence to respond to security incidents swiftly and effectively, minimizing the impact of a breach. Threat intelligence feeds offer insights into emerging threats, aiding continuous improvement of EDR, MDR, and incident response capabilities.

The integration of threat intelligence, EDR, and MDR into incident response plans creates a cohesive and well-coordinated approach to handling security incidents. This comprehensive strategy ensures organizations are prepared not only to respond to known threats but also to adapt to evolving and unknown threats. In essence, the integration of these components results in a more holistic incident readiness strategy, equipping organizations to navigate a range of security challenges effectively.

Navigating Incident Recovery

When examining incident response services for 2024, SMEs are prominently prioritizing the acquisition of incident recovery services, with legal and compliance assistance following closely. Incident recovery, a pivotal

Incident Response Services Prioritized Next 12 Months



Source: Richmond Advisory Group, 2024.

phase in the overall incident response lifecycle, is dedicated to restoring affected systems, services, and data after a security incident or disruptive event. The essential goals of incident recovery encompass restoring normal operations, conducting risk analysis, minimizing downtime and impact, ensuring data integrity and availability, preventing recurrence, learning, and improving, and managing communication and reputation.

The essential goals of incident recovery encompass restoring normal operations, conducting risk analysis, minimizing downtime and impact, ensuring data integrity and availability, preventing recurrence, learning and improving, and managing communication and reputation.

The key elements of incident recovery are:

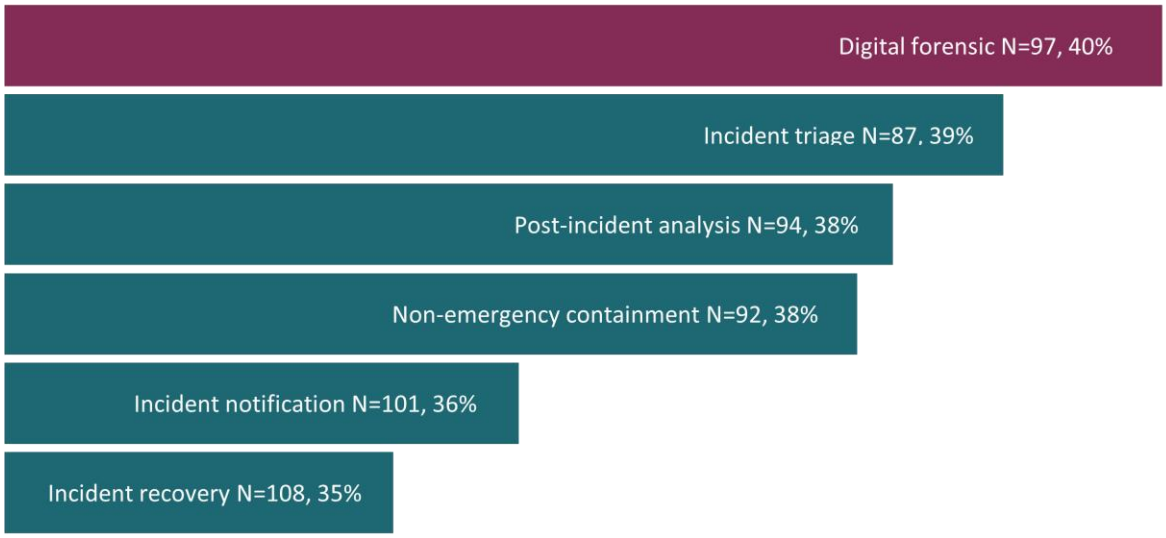
- To swiftly bring affected systems and services back to their normal state, addressing and remedying the incident's impact for seamless business operations.
- To further identify potential risks, their likelihood and potential impact, prioritizing risks based on severity and occurrence likelihood.
- To minimize organizational downtime, limiting impact on business operations, customer service, and overall productivity.

- To ensure the integrity and availability of critical data with tasks such as restoring data from backups, validating data integrity, and safeguarding sensitive information.
- To prevent the incident's recurrence, including patching vulnerabilities, updating security configurations, and implementing safeguards.
- To learn and improve by conducting post-incident analysis, understanding what happened, and refining incident response processes.
- To create and disseminate transparent communication with stakeholders, such as employees, customers, partners, and the public, to manage the organization's reputation.

Incident recovery services are essential for maintaining business continuity. Swift recovery minimizes disruptions, ensures the prompt resumption of critical business functions, and demonstrates a commitment to protecting customer data. Rapid recovery also helps prevent incident escalation, containing and eradicating the incident promptly. Learning from incidents during recovery allows organizations to refine incident response plans, update security measures, and enhance staff training. Considering the regulatory landscape, legal and compliance services naturally complement incident recovery, providing a comprehensive approach to compliance and incident response. Incident recovery is crucial in demonstrating to the C-Suite, board, and regulators tangible improvements to the security posture based on lessons learned.

Learning from Incidents and Operational Response are Critical Functions

Most Important Incident Response Services



Source: Richmond Advisory Group, 2024.

When considering important incident response services beyond what they have prioritized to purchase in 2024, SMEs emphasize digital forensics, incident triage, post-incident analysis and non-emergency containment services. Digital forensics services are focused on detailed investigation and evidence collection for legal or disciplinary purposes, while incident response is centered around the immediate actions taken to manage and recover from security incidents.

Incident triage involves quickly assessing and prioritizing incidents based on severity and impact. This rapid response helps minimize the damage and potential disruption to business operations. These services also identify incidents that pose immediate threats, providing insights into the nature and scope of the incident which is vital for refining incident response plans.

Post-incident analysis involves a detailed examination of the incident to identify its root causes. This is essential for implementing corrective measures to prevent similar incidents in the future. By analyzing the incident response process, organizations can identify areas for improvement, evaluate the effectiveness of security controls, and enhance overall cybersecurity posture.

Non-emergency containment services involve controlled measures to prevent the escalation of potential security incidents. This provides operational continuity and helps to avoid disruptions. Non-emergency containment services also allow organizations to proactively manage risks by addressing potential threats before they become major incidents. This proactive approach contributes to a more robust security posture.

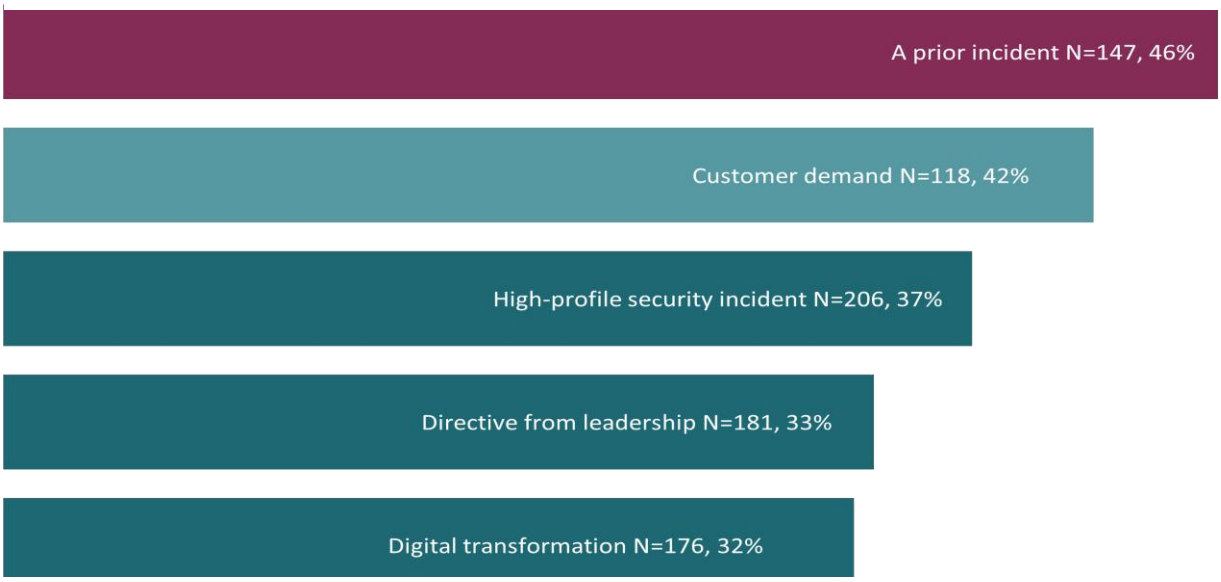
Digital forensics services contribute significantly to both the operational aspects of incident response and the learning process. They enable organizations to respond promptly to incidents, mitigate risks, and, through careful analysis, continually improve their cybersecurity resilience. The insights gained from incident triage, post-incident analysis, and non-emergency containment collectively contribute to an organization's ability to adapt and enhance its security measures over time.

The insights gained from incident triage, post-incident analysis, and non-emergency containment collectively contribute to an organization's ability to adapt and enhance its security measures over time.

Decoding SME Incident Readiness and Response Purchasing Preferences

SME motivations for purchasing readiness and response services primarily stem from past incidents and customer demand, with a focus on achieving increased security and elevated brand reputation. Recovery and containment from incidents closely follow as key goals. Despite recognizing the benefits of cost savings, buyers acknowledge the cost-

Prior Incidents and Customer Demand Motivate Readiness Purchases



Source: Richmond Advisory Group, 2024.

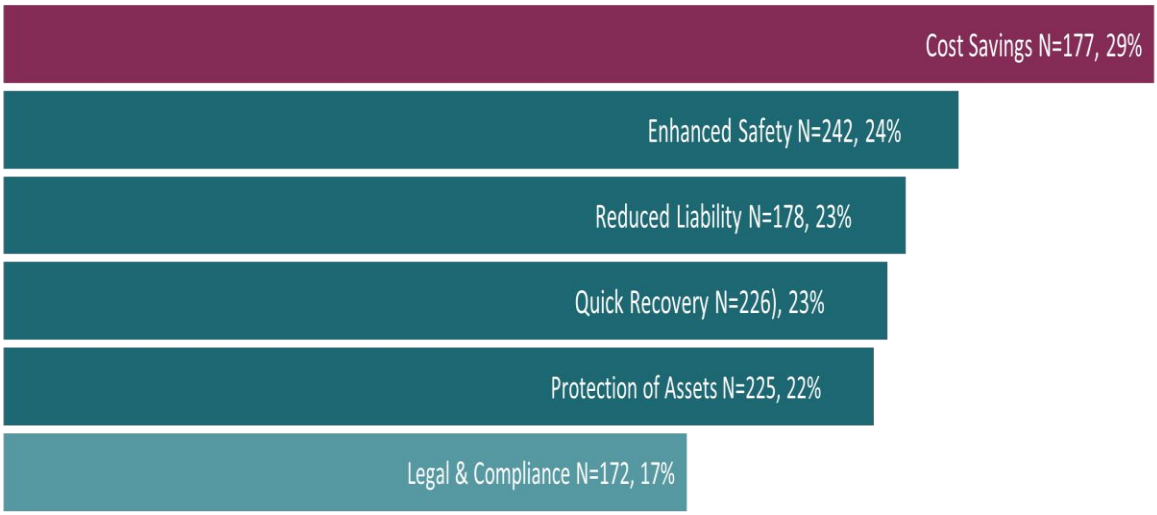
prohibitive challenge of readiness services. The understanding is that while preparedness incurs an initial cost, it results in long-term savings by reducing exposure, vulnerability, and enhancing detection and response capabilities.

Key benefits of incident preparedness identified by SMEs include cost savings, increased security, asset protection, safety enhancement, reduced liability, quick recovery, and improved operational efficiency. These benefits collectively

Key benefits of incident preparedness identified by SMEs include cost savings, increased security, asset protection, safety enhancement, reduced liability, quick recovery, and improved operational efficiency.

highlight the multifaceted value that incident readiness services bring to SMEs.

Key Benefits of Incident Readiness Services



Source: Richmond Advisory Group, 2024.

SMEs express a preference for subscription, retainer, or fixed-fee pricing structures, with tiered pricing as the least favored.

- Subscription models are particularly sought for policy and procedure reviews, business continuity/disaster recovery planning, and risk assessments.
- Retainer structures are preferred for incident response and vulnerability management assistance, while fixed-fee arrangements are commonly chosen for training and awareness initiatives.
- Subscription pricing finds prominence in EDR support or MDR services, as well as in non-emergency incident containment and mitigation. In the event of a ransomware attack, SMEs often lean towards retainer-based pricing.

When it comes to Service Providers, managed service providers (MSPs), managed security service providers (MSSPs), and managed detection and response (MDR) providers stand out as the top choices for incident readiness and response service engagements. Telecom cybersecurity providers closely follow, preferred ahead of vendors, specialty incident response providers, cloud providers, consultancies, and systems integrators. This underscores the inclination of SMEs towards comprehensive, managed solutions for their incident readiness needs.

Addressing Challenges and Prioritizing Solutions

Incident preparedness holds paramount importance for organizations across the spectrum, with SMEs facing distinctive challenges. The specialized expertise required for comprehensive cybersecurity planning, incident detection, and response is often a hurdle, particularly when considering the budget constraints of smaller companies.

Incident response planning may pose additional challenges for SMEs, ranging from the absence of formalized plans to irregular updates and testing, resulting in confusion and delays during security incidents. Like larger enterprises, SMEs rely on third-party vendors for numerous services, and a security incident within a vendor can create a cascading impact

on SME operations. Compliance with industry-specific regulations adds another layer of complexity for SMEs, consuming valuable resources.

Operationally, SMEs may lack the necessary tools and resources for continuous network monitoring, hampering timely incident detection. This delay can lead to the discovery of security incidents only after they have caused considerable damage.

To overcome these challenges, SMEs should prioritize cost-effective security measures, invest in employee training, collaborate with managed security service providers (MSSPs), and managed detection and response (MDR) providers, and adopt a risk-based approach to prioritize security efforts based on critical assets and potential threats.

For MSSPs to cater effectively to this customer segment, services must align with the topmost priorities of SMEs, focusing on critical risk assessment, planning, and recovery services. These services should be bundled sensibly, offering the guidance expected from a reputable managed security service provider.

Cybersecurity Resilience in the Face of SEC Scrutiny

In the landscape of incident readiness, the motivations, and priorities of SMEs are reshaping with a keen focus on cybersecurity resilience. The insights derived from the study conducted by Richmond Advisory Group, LLC provide a valuable window into the minds of SME cybersecurity decision makers. The shift in dynamics, especially with the regulatory changes introduced by the SEC in 2023, has heightened the significance of incident readiness for SMEs.

Proactive incident readiness emerges as a strategic approach crucial for SMEs to identify and mitigate risks, respond effectively to security incidents, protect assets, maintain business continuity, and adhere to regulatory requirements. In fact, SMEs are prioritizing the purchase of services such as risk assessments, vulnerability management, training for incident response teams, and employee cybersecurity training and awareness in 2024. The benefits identified by SMEs of these services span cost savings, increased security, asset protection, safety enhancement, reduced liability, quick recovery, and improved operational efficiency. These collectively underscore the comprehensive value that incident readiness services bring to SMEs, positioning them not only as a compliance necessity but also as a strategic investment in long-term resilience.

In conclusion, the future landscape for incident readiness in SMEs is intertwined with the adoption of a strategic, proactive, and resilient approach. The journey toward cybersecurity resilience is a shared endeavor, and this white paper serves as a guide for SMEs to fortify their defenses and thrive in an increasingly digitized and regulated business environment.

Sponsored By: LevelBlue

We simplify securing valuable business assets by providing broad cybersecurity experience and award-winning services for network security, extended detection and response, and endpoints. From traditional computing to edge computing, we're focused on business innovation. We help make complexity easy to understand and navigate.

By providing affordable, strategic services, our clients rely on us as trusted advisors. Our cybersecurity consulting is product neutral, so you get unbiased answers for your business. Our managed security services, threat awareness, and ground-breaking research are dedicated to help keep you protected today and prepared for tomorrow.

LevelBlue manages the risk. You reap the reward.

Take the first step towards improving cybersecurity resilience today and click here to learn more about *LevelBlue*'s comprehensive suite of incident readiness and response services that range from risk assessments, vulnerability management, threat intelligence, incident response planning, breach investigations, and employee training. These services are customized to each organization's distinct requirements, aiming at proactive prevention and mitigation of cyber incidents.


Read LevelBlue's Cyber Aware Blogs


Contact LevelBlue Consulting


Learn more about LevelBlue


Download whitepaper