2024

CRITICALSTART® CYBER RISK LANDSCAPE PEER REPORT

83% of cybersecurity professionals reported experiencing a cyber breach requiring attention despite having traditional threat-based detect and respond security measures in place.

CRITICALSTART®

TABLE OF CONTENTS

Introduction

As digital transformation drives business innovation and growth, cyber risk remains a critical challenge for organizations worldwide. Businesses must stay ahead by understanding the current landscape and implementing robust security measures. To stay ahead, organizations must understand the current landscape and implement robust security measures.

Purpose and Scope

The second annual CRITICAL**START**® Cyber Risk Landscape Peer Report, based on a survey of over 1,000 VP+ cybersecurity professionals, provides a comprehensive overview of the state of cyber risk today. For many organizations, detection and response form the foundation of their security program and cyber risk capabilities. Through data-driven insights, this report explores market trends in cyber risk, where organizations of various sizes see their risks, and how those organizations are working to mitigate risks.

Section 1:

The Evolution of Threat Detection & Response

Since the 1980s, Detect and Respond cybersecurity solutions have evolved in response to emerging cyber threats and technological innovation. These tools progressed from basic intrusion detection to sophisticated, integrated solutions capable of real-time threat detection and response, highlighting continuous cybersecurity innovation.

Early Intrusion Detection Systems (IDS) 1980s to 1990s

Emergence: The concept of intrusion detection began to take shape in the 1980s. One of the earliest systems, the Intrusion Detection Expert System (**IDES**), was developed at SRI International.

Functionality: Early IDS focused on detecting unauthorized access and misuse by monitoring network traffic and system logs.

Limitations: These systems were largely passive, generating alerts without any capability to respond to or mitigate threats.

Network Intrusion Detection Systems (NIDS) 1990s

Development: As network-based attacks became more prevalent, NIDS were developed to monitor and analyze network traffic for signs of intrusion.

Examples: Notable early NIDS include Snort and Cisco's NetRanger.

Challenges: High false-positive rates and the inability to respond to threats in real-time were significant limitations.

Intrusion Prevention Systems (IPS) Early 2000s

Advancement: To address the reactive nature of IDS, Intrusion Prevention Systems (**IPS**) were introduced. These systems could take automated actions to block or mitigate threats in real time.

Integration: IPS integrated both detection and prevention capabilities, enhancing the ability to stop attacks before they could cause harm.

Adoption: Adoption was driven by the increasing complexity and frequency of cyberattacks.

Security Information and Event Management (SIEM) Mid-2000s

Innovation: SIEM solutions emerged to aggregate, correlate, and analyze security data from various sources, providing a more comprehensive view of security events.

Capabilities: SIEMs enabled better detection through event correlation and centralized logging and alerting.

Evolution: Over time, SIEMs incorporated advanced analytics and machine learning to improve threat detection.

Endpoint Detection and Response (EDR) 2010s

Focus: EDR solutions emerged to address the need for advanced threat detection and response at the endpoint level.

Features: These solutions provided continuous monitoring and response capabilities, allowing for the detection of sophisticated threats such as zero-day exploits and advanced persistent threats (**APT**s).

Examples: Notable EDR solutions include Carbon Black, CrowdStrike, and Cylance.

Managed Detection and Response (MDR) Late 2010s to Present

Service Model: Combines technology and human expertise to provide 24x7x365 threat monitoring, detection, and response.

Benefits: MDR services offer organizations access to advanced threat detection capabilities and skilled security analysts without the need for in-house resources.

Evolution: MDR providers continuously evolve their offerings, integrating capabilities like threat hunting, incident response, and proactive security measures.

Extended Detection and Response (XDR) 2020s

Integration: XDR solutions provide a holistic approach by integrating multiple security products into a unified platform, improving detection and response across various security layers (network, endpoint, cloud, etc.).

Advancement: By leveraging AI and machine learning, XDR enhances threat detection accuracy and response efficiency.

Adoption: XDR is becoming increasingly popular as organizations seek comprehensive and streamlined security solutions.

Future Innovations

Trends: Future detect and respond solutions will further integrate with AI, machine learning, and automation to enhance threat detection and response capabilities.

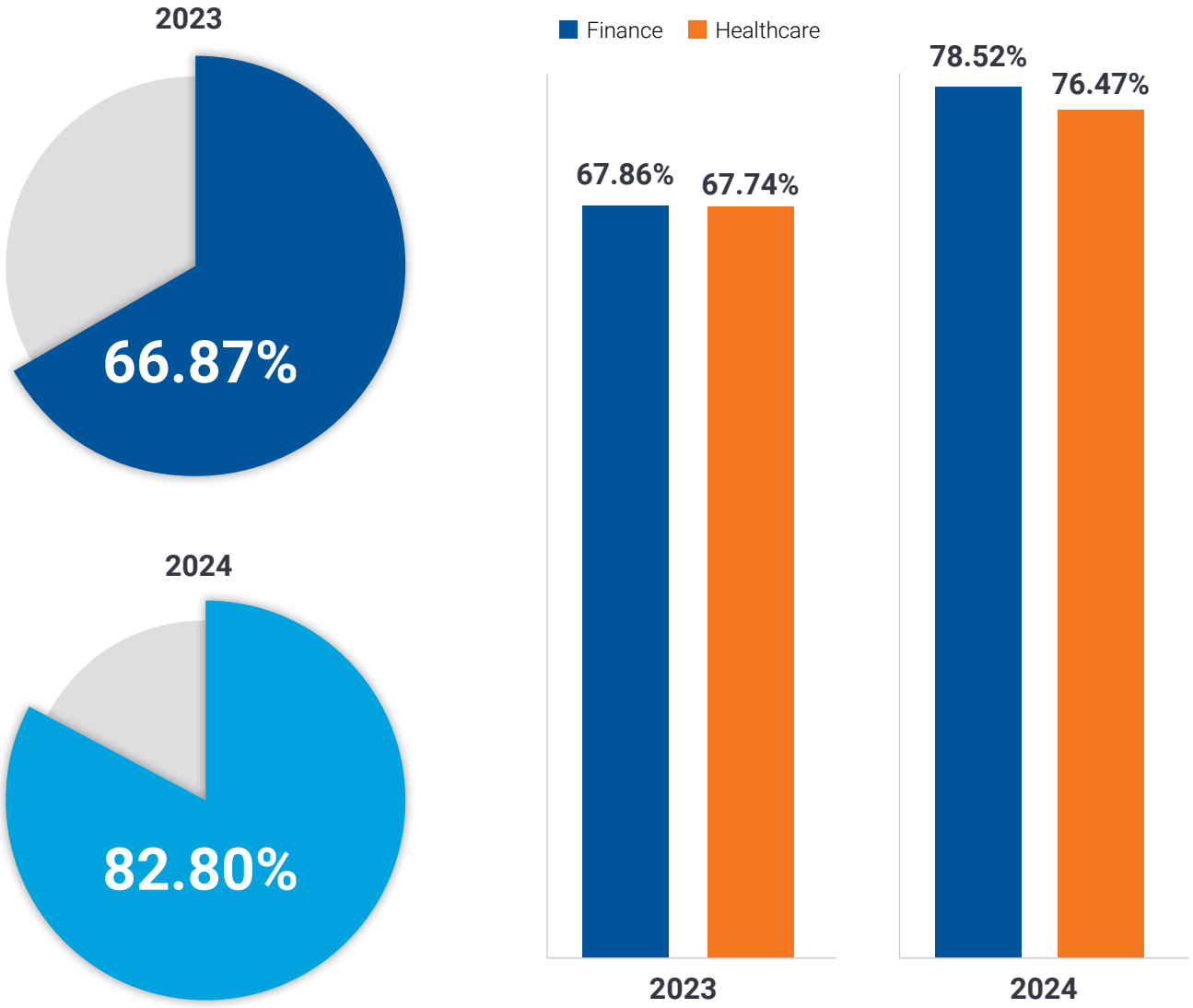
Focus: There will be a continued emphasis on reducing false positives, improving response times, and providing more proactive security measures.

Section 2:

Understanding the Current Cyber Risk Landscape

Survey Findings on Cybersecurity Incidents

In our latest Landscape Peer survey, 83% of cybersecurity professionals reported experiencing a cyber breach requiring attention despite having traditional threat-based detect and respond security measures in place. That's a 21% increase over our inaugural survey in 2023 (67%). For organizations in heavily regulated industries such as healthcare and finance, which reported increased breaches in our 2024 survey, these costs can be significantly higher due to fines and compliance requirements.



Within the last 2 years have you experienced a cyber breach requiring attention despite having traditional threat-based detect and respond security measures in place?

Section 2:

Understanding the Current Cyber Risk Landscape (continued)

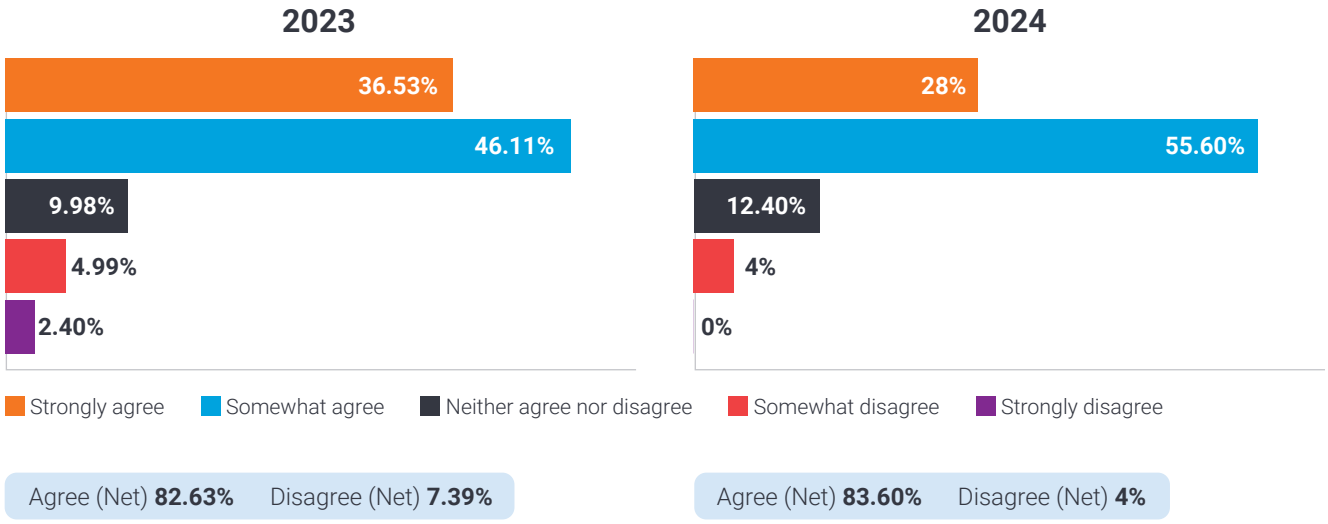
Financial and Operational Implications of Cyber Breaches

The financial implications of data breaches are significant. The average cost of a data breach reached an all-time high of $4.45 million in 2023, representing a 15% increase over the past three years. Additionally, organizations with fewer than 500 employees reported an average breach impact increase from $2.92 million to $3.31 million, a 13.4% rise. These costs encompass various aspects, such as detection and escalation, which alone increased from $1.44 million in 2022 to $1.58 million in 2023.[1]

Beyond financial losses, cyber incidents can severely damage customer trust and corporate reputation and lead to substantial fines and regulatory penalties. Given the substantial economic and reputational impacts, it's crucial for organizations to understand and stay ahead of the evolving cyber risk landscape. Proactive risk management, strategic decision-making, and regulatory compliance are essential components of a robust cybersecurity strategy. Understanding the current cyber risk landscape enables organizations to adopt measures that effectively mitigate risks, ensuring both operational resilience and regulatory adherence.

The Current State of Cyber Risk: Costs Over Security

Despite an observed increase in costs associated with breaches, our survey reveals a troubling trend: **most respondents continue to prioritize budget over security.** This year, 84% of survey respondents reported that their organization prioritizes the cost of security over the risk of a security breach, a slight increase from 83% last year. This indicates a persistent tendency to prioritize reduced spending over increased security, regardless of the escalating threat landscape.



Agree (Net) **82.63%** Disagree (Net) **7.39%**

Agree (Net) **83.60%** Disagree (Net) **4%**

To what extent do you agree or disagree with the following statement: My organization prioritizes the cost of security over the risk of a security breach?

While the data between 2023 and 2024 trends toward an increased prioritization of breach protection, organizations that continue focusing on cost must shift their strategies. Holding onto that zero-risk mindset is not sustainable in the face of growing cyber threats.

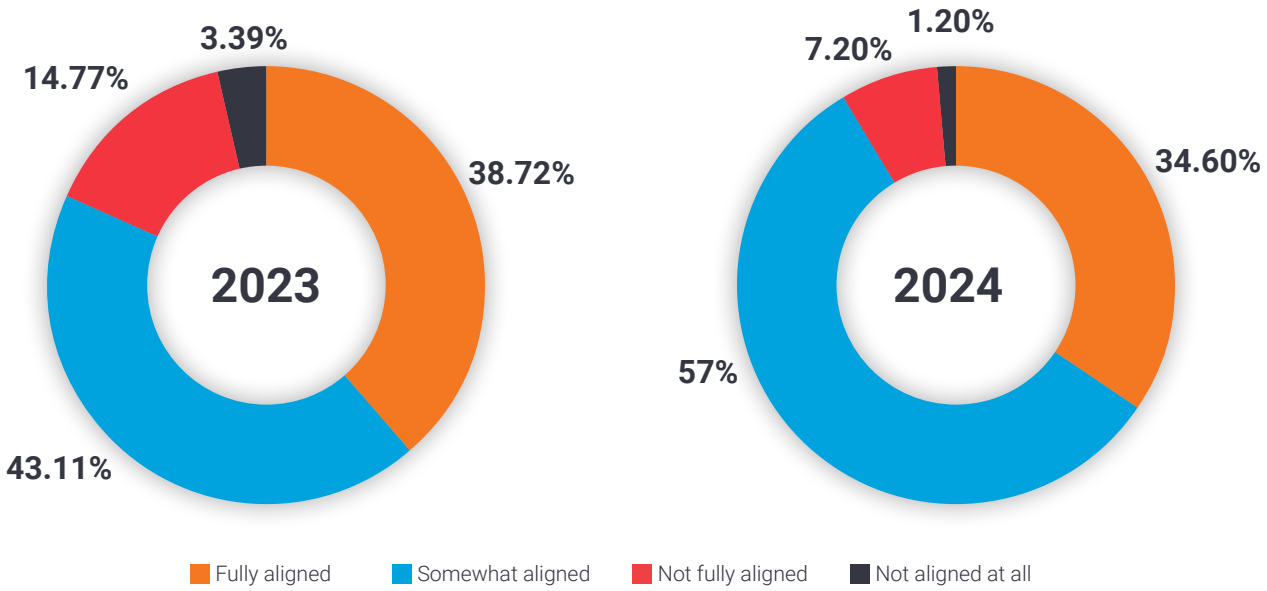
Section 2:

Understanding the Current Cyber Risk Landscape (continued)

Aligning Security Investments with Impact Tolerance

Organizations must shift from a cost-centric approach to one that aligns with impact tolerance. Impact tolerance, a concept supported by focuses on the ability to withstand and recover from adverse cyber events. Instead of aiming for zero risk, which is unrealistic, organizations should invest in cybersecurity measures that balance cost with the ability to manage and mitigate the impact of breaches.

Our survey also found that the number of respondents who feel their company's cybersecurity investments are fully aligned with quantifiable risk reduction priorities remains alarmingly low and has decreased year-over-year. This misalignment indicates a pressing need for organizations to reassess their cybersecurity strategies and ensure that investments directly contribute to measurable risk reduction.



How aligned, if at all, are your cybersecurity investments and your organization's quantifiable risk reduction priorities?

Organizations must recognize that prioritizing cost over security can lead to significant risks and higher long-term costs due to breaches and their financial, operational, and reputational impacts. By aligning cybersecurity investments with impact tolerance, companies can develop more resilient security postures that protect against threats and ensure quicker recovery and minimal operational disruption when incidents occur.

Cost considerations are important but should not overshadow the need for robust cybersecurity measures. A strategy that emphasizes impact tolerance will better equip organizations to handle the complexities of the current cyber threat landscape.

Section 3:

MDR: The Foundation of Modern Defense

Threat Detection and Response: The Final Defense

Threat detection and response mechanisms are crucial in identifying and mitigating cyber threats before they escalate into significant breaches. These capabilities are particularly vital as the final layer of defense against sophisticated attacks that have bypassed initial preventative measures. When properly implemented, threat detection and response can prevent what might otherwise become a catastrophic compromise.

Internal SOCs vs. MDR Services

Large enterprises with extensive resources can often manage their cybersecurity needs through internal Security Operations Center (**SOC**s). These SOCs are equipped with advanced technologies and staffed by experienced security professionals who can provide continuous monitoring and rapid response to threats. A well-staffed and fully operational SOC knows the organization's environment and understands what is at risk. They can prioritize efforts to align with organizational risk reduction priorities and keep their organizations ahead of emerging threats. However, building and maintaining such an infrastructure is prohibitively expensive and resource-intensive for many organizations.

For these organizations, MDR services offer a practical alternative. MDR providers work with the tools that organizations already own, bringing specialized knowledge and expertise to deliver continuous monitoring with some also providing rapid incident response services. Typically, MDR services cost a fraction of what organizations would spend maintaining a fully staffed internal SOC.

With MDR services, organizations realize a full return on their security tools investments by putting them in the hands of experts who specialize in their use. Additionally, MDR teams stay ahead of the evolving threat landscape, providing a critical eye and deep insights to catch signals and suspicious behaviors that might otherwise go unnoticed. MDR services not only reduce the financial impact of breaches, but also significantly improve detection and response times. Both outcomes directly reduce cyber risk, lowering the likelihood of a breach and the potential impact if a threat actor gets past their defenses, and it's the people behind the MDR services that make these outcomes a reality.

Section 4:

Challenges Driving the Evolution of MDR to Shift Left

Lack of Time and Resources

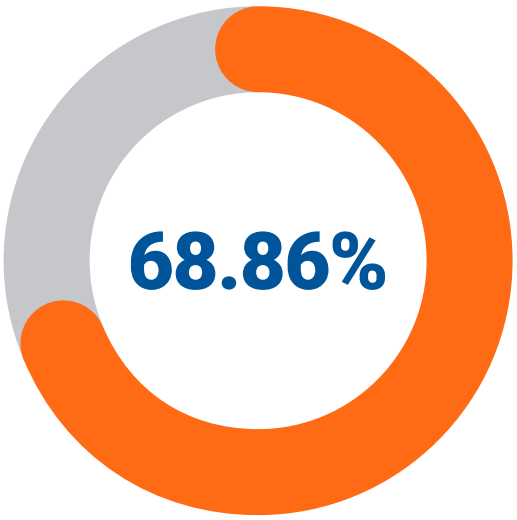
A significant challenge highlighted by the survey is the lack of time and resources available to adequately address cyber risks. About 97% of respondents indicated that they either somewhat or completely lack the time to continuously monitor their security posture and identify potential areas of control failure. This lack of resources hampers their ability to implement comprehensive security measures and respond promptly to threats.

Increasing Trend Toward Outsourcing

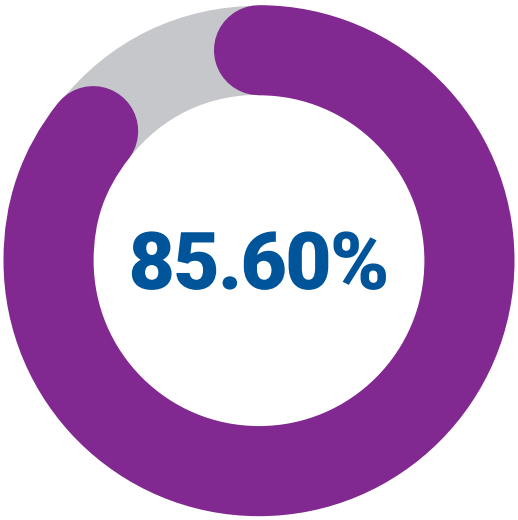
The survey also indicates a growing trend among cybersecurity professionals and executives to outsource specific segments of their cyber risk reduction efforts. About 99% of organizations plan to offload segments of cyber risk reduction workstreams or projects to security service providers within the next two years. Driving this trend is the recognition that unknown risks pose a serious concern, and outsourcing can provide the necessary expertise and resources to manage these risks effectively while enabling organizational resources to focus on implementing a broader security strategy.

Ineffectiveness of Traditional Detection and Response

Traditional security measures, such as firewalls and antivirus software, focus primarily on preventing known threats. While these tools are essential, they are often insufficient in dealing with sophisticated and evolving cyber threats. Of the cybersecurity professionals surveyed for this report, 86% told us that unknown organizational cyber risk is currently a top concern— up 22 % from our 2023 survey.



2023



2024

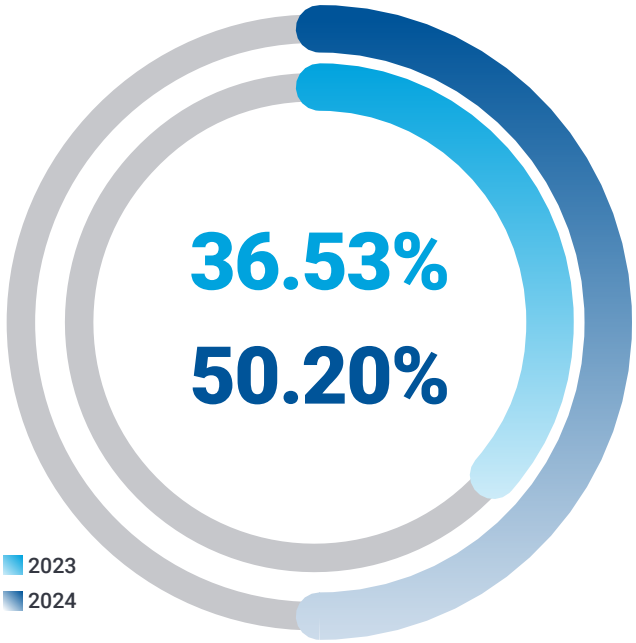
Is currently unknown organizational cyber risk a top concern?

Section 4:

Challenges Driving the Evolution of MDR to Shift Left (continued)

It's worth noting that in 2023, we reported that 37% of cybersecurity professionals cited a lack of expertise as a challenge faced in effective cyber risk management.

This year, that number increased to 50%. MDR is a clear solution for solving that staffing challenge without incurring significant costs.



Lack of Expertise

What challenges, if any, does your organization face in managing cyber risks effectively?

Now more than ever, organizations must adopt a comprehensive and proactive approach to cybersecurity. By tapping into trends, developing new and effective mitigation strategies, and benchmarking, businesses can significantly reduce their cyber risk and enhance their overall security posture. Continuous investment in cybersecurity and strategic outsourcing is essential for navigating the complex and dynamic cyber threat landscape.

Section 5:

The Need for a Proactive, Risk-Based Cybersecurity Approach

While there is a critical need for comprehensive, managed cybersecurity services as the foundation of any security program, traditional security measures are no longer sufficient. Organizations are increasingly recognizing the value of proactive, risk-based approaches and are looking to combine multiple elements of cybersecurity to enhance their overall effectiveness. Our 2024 survey found that:

83% **of organizations experienced a breach requiring attention within the last two years despite having traditional threat-based security measures in place,** indicating the need for a more robust and proactive approach to cyber risk management.

66% **of businesses reported limited visibility and insight into their cyber risk profiles,** hindering their ability to prioritize investments and allocate resources effectively.

99% **of organizations plan to offload specific segments of cyber risk reduction** workstreams or projects to security service providers within the next two years.

65% **of executives expressed concerns over the misalignment** between cybersecurity investments and the organization's risk reduction priorities.

84% **of organizations expressed the belief that a holistic, evidence-based approach to cyber risk management will yield a reduction in the likelihood of a significant cyber incident occurring.** This includes integrating risk assessment, protection, detection, response, and recovery into a cohesive strategy.

81% **of organizations are now planning to prioritize proactive risk reduction strategies to stay ahead of the evolving threat landscape.** This includes continuous risk monitoring, threat intelligence integration, and timely incident response.

86% **of organizations believe managed cyber risk reduction strategies will yield significant cyber protection value.**

99% **of organizations find it important to adopt a managed cyber risk reduction approach within the next two years,** signaling a shift in the cybersecurity landscape.

This data underscores the growing recognition of the limitations of traditional security measures and the importance of adopting a proactive, integrated approach to managing cyber risks.

Section 6:

MDR is the Foundation for Managed Cyber Risk Reduction

A Holistic View of Cyber Security

A Managed Cyber Risk Reduction (**MCRR**) approach offers organizations a holistic view of their cybersecurity posture and monitors real-time cyber threats, vulnerabilities, and risks across a broad range of security domains. This includes asset inventory, endpoint coverage gaps, risk assessments, vulnerability management, endpoint and network monitoring, threat intelligence, and incident response preparedness. With MCRR, you gain insights into your organization's cyber risk holistically, paving the way for effective risk management.

The Need for Symbiotic Security Strategies

MDR plays a critical role in the modern cybersecurity landscape and is **the foundation of a Managed Cyber risk Reduction strategy.** External MDR services provide essential capabilities, including expert analysis, 24x7x365 monitoring, and rapid response times that are both cost-effective and efficient.

However, while **MDR is crucial, it cannot operate in isolation.** The 2024 Cyber Risk Landscape Peer Report survey responses highlight the need for a symbiotic relationship between MDR and proactive security elements. This integrated approach involves:

- Regular evaluations to identify and prioritize potential threats.
- Maintaining a comprehensive inventory of all IT assets to detect vulnerabilities.
- Proactively identifying and mitigating vulnerabilities to prevent exploitation.
- Ensuring all endpoints are protected and monitored for suspicious activities.
- Event and threat analysis using cybersecurity frameworks for standardized threat identification and targeted mitigations.

For MDR to function optimally, all assets must be accounted for to close security coverage gaps. Traditional methods such as manual audits, periodic scans, and relying on customers to self-report are insufficient, as they do not provide the real-time, continuous visibility needed to secure today's dynamic environments.

Section 7:

Integrating Proactive Security Intelligence into MDR

Utilizing an MDR platform to integrate proactive cybersecurity intelligence into the Security Operations Center (**SOC**) — such as comprehensive asset inventories, EDR coverage gaps, asset criticality, and MITRE ATT&CK® Mitigations — can significantly enhance effectiveness and provide a roadmap for organizational security maturity over time.

Asset Visibility is Essential to MDR Effectiveness

Asset visibility involves maintaining an up-to-date inventory of all IT assets, along with determining each asset's criticality in terms of organization impact in the case of a breach. Having this level of intelligence is essential for identifying gaps in security orchestration and tooling coverage, and for prioritizing the efforts to harden and secure assets. Asset visibility also ensures that SOC teams or MDR providers are receiving all expected signals so that threat actors cannot slip through gaps in coverage.

Without an effective asset visibility solution, the teams that work together to keep a business safe (Security, IT, etc.) may lack an understanding of which assets pose risks to the organization. Even with a full asset inventory as provided by CMDBs, vulnerability scanners, and similar tools, they may not have visibility into critical security gaps, including misconfigurations, improper access controls, a lack of security scanners (tooling), and more. Having the full, accurate account of an organization's assets provided by a dedicated asset visibility tool is the first critical step in finding and fixing security coverage gaps so that SOC teams and MDR providers reduce the chances of missed security signals.

Even though the potential negative consequences of not having comprehensive asset visibility are straightforward, only 29% of our survey respondents report having full visibility.

> **In First Steps to Overcoming a Lack of Asset Visibility[2], the Center for Internet Security (CIS) reports that "… lack of asset visibility is important to address, as it limits enterprises' ability to meet their security and operational objectives and increases the likelihood of data breaches and other security incidents."**

Asset Identification and Protection risks

How would you rate your organization's evidenced-based visibility into its cyber risk landscape for asset identification and protection risks?

Section 7:

Integrating Proactive Security Intelligence into MDR (continued)

Endpoint Coverage Gaps

In 2023, the Critical Start Cyber Incident Response Team (**CIRT**) found that 28% of the total network breaches worked were due to unmonitored/unmanaged devices with no/limited visibility. Furthermore, 75% of the network breaches investigated for existing Critical Start MDR customers were due to a lack of endpoint protection and visibility.

MDR effectiveness relies heavily on the threat signals it receives. Limited visibility into assets connected to the network leaves organizations exposed around the clock and security leaders unsure of their true level of risk exposure. Our survey indicates that 86% of security professionals are concerned about unknown organizational cyber risks.

SIEM Coverage Gaps

Security Information and Event Management (**SIEM**) systems are critical for logging and analyzing security events. However, SIEM systems can also suffer from coverage gaps. These gaps arise from incomplete data collection, misconfigurations, or a lack of integration with all relevant data sources. When SIEM systems fail to capture comprehensive data, it can lead to critical detection issues, leaving organizations blind to potential threats. Integrating SIEM with endpoint detection capabilities and ensuring that all data sources are accurately reported can help mitigate these gaps.

Impact of Coverage Gaps

Any gaps in inventory and coverage create significant threat detection issues. When security coverage gaps exist, they remain invisible, preventing threat signals from being accurately reported and received by the MDR system. This can result in breaches occurring via unprotected endpoints, user, cloud, and network infrastructures, leaving organizations vulnerable and often wondering how these threats went undetected.

To mitigate these risks, organizations must ensure comprehensive endpoint and SIEM coverage. This includes implementing real-time monitoring solutions that provide continuous visibility into all connected assets and logs being ingested across SIEM systems and endpoint detection tools. By addressing these issues, organizations can improve their overall security posture and ensure more effective threat detection and response.

Event and Threat Analysis

The MITRE ATT&CK® Framework is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. Utilizing this framework enhances threat intelligence and response strategies. By integrating MITRE ATT&CK® Mitigations, security professionals can respond more effectively to active threats. Additionally, when these mitigations are paired with prioritized recommendations for configuration and controls, they provide prescriptive steps to continually strengthen defenses.

A key benefit of this approach is the ability to identify recurring configuration and control issues. By analyzing events and threats using the MITRE ATT&CK® Framework, organizations can pinpoint patterns and repeat occurrences that highlight vulnerabilities in their security posture. This insight allows for targeted improvements to their security programs, addressing the root causes of issues rather than just the symptoms.

As noted above, 86% of survey respondents indicated that unknown organizational cyber risk is a top concern. The MITRE ATT&CK® Framework offers a structured methodology to better understand and address the evolving threat landscape. By leveraging this framework, organizations can gain a deeper insight into their security gaps and implement more effective controls, thereby reducing their overall risk exposure.

Section 8:

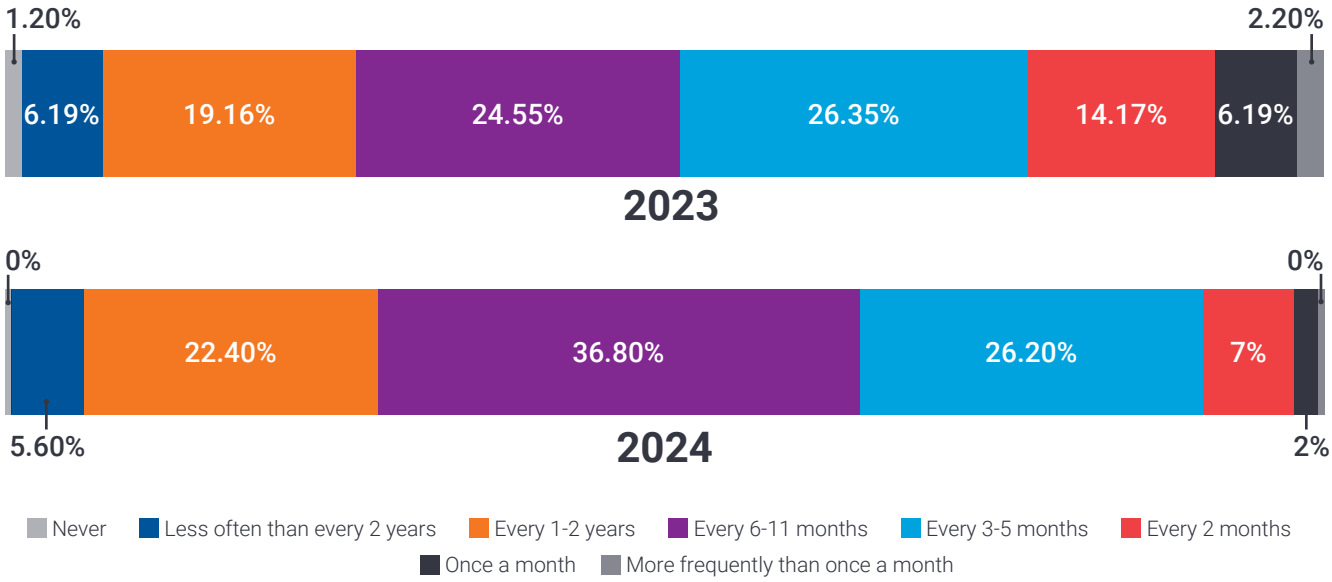
Enhance MDR with Proactive Security Measures

Combining proactive cybersecurity measures — framework-aligned peer-benchmarked questionnaires, cyber asset management, and configuration and controls recommendations based on repeated events — with MDR enhances an organization's ability to prevent, detect, and respond to incidents. This comprehensive approach integrates multiple layers of defense, creating a robust security posture that addresses vulnerabilities and mitigates risks. Although 99.4% of 2024 survey respondents report that they plan to implement a managed cyber risk reduction solution that continuously monitors and mitigates cyber risks to proactively protect critical assets with a measurable ROI that aligns with the organization's risk appetite within the next six months to two years, a mere 0.40% currently have one in place.

Risk Assessments

A cyber risk assessment is a critical step in identifying and prioritizing potential risks to manage and mitigate their impacts. It involves evaluating potential threats, vulnerabilities, the value of assets at risk, and the likelihood and impact of potential incidents. A comprehensive risk management strategy entails conducting regular risk assessments based on industry-specific and regulatory frameworks (e.g., NIST CSF, ISO 27001) to pinpoint assets at risk, evaluating the efficacy of security controls, and anticipating the fallout from successful attacks. By understanding and mitigating cyber risk, your organization can proactively guard against potential threats.

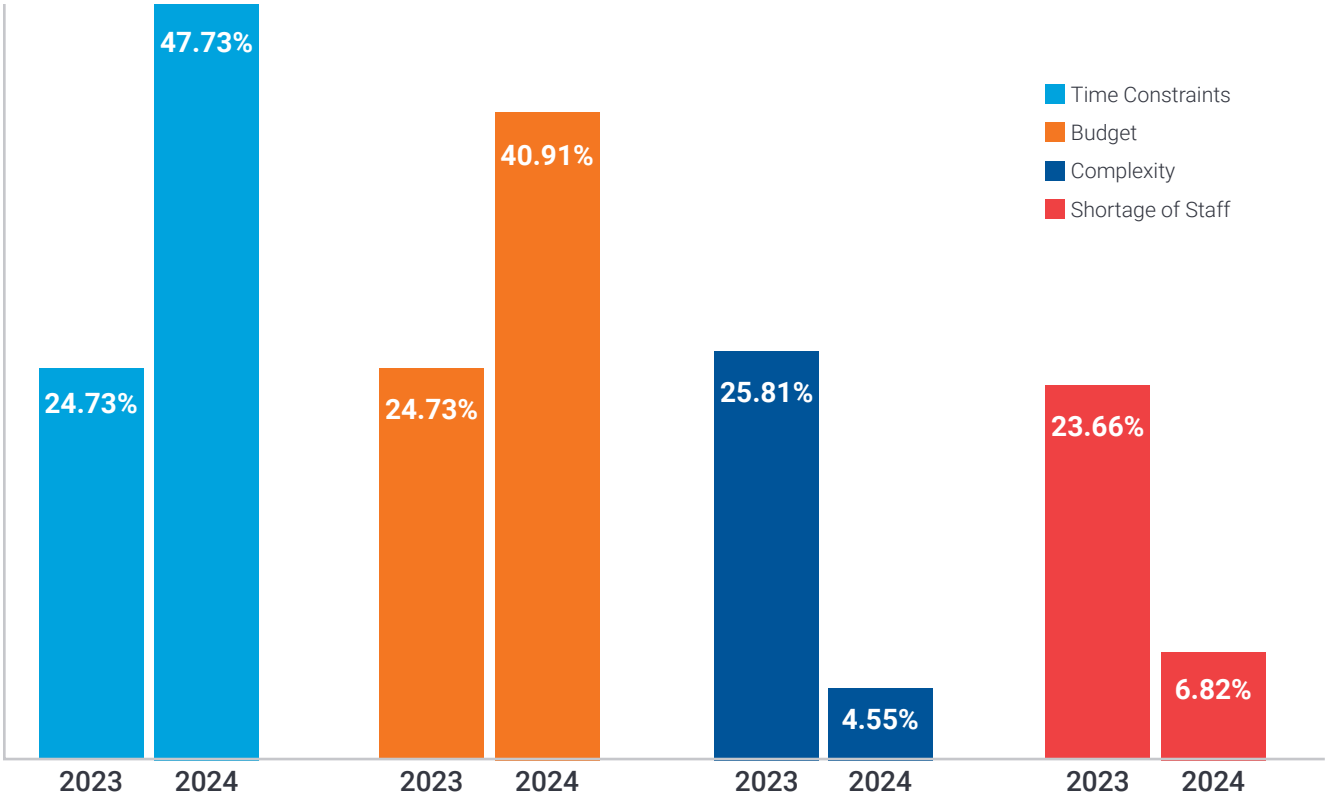
Unfortunately, our survey found that only 2% of respondents conduct risk assessments once per month, with most (36.8%) performing them every 6-11 months. Only 33% felt the frequency of their assessments was sufficient, attributing the inability to conduct them more frequently to time constraints (48%) and budget (41%).



How often, if ever, do you conduct full and comprehensive cybersecurity assessments and risk evaluations across your environment?

Section 8:

Enhance MDR with Proactive Security Measures (continued)



What, if anything, prevents you from conducting more frequent cybersecurity assessments and risk evaluations?

Risk-based decision-making often requires human insight to accurately assess the potential impact of threats and prioritize remediation efforts. Human-led teams excel at conducting thorough risk assessments, considering factors such as business context, regulatory requirements, and organizational risk appetite. They can also effectively communicate risk to stakeholders and guide the implementation of appropriate risk mitigation strategies.

> **Only 33% of respondents felt the frequency of their assessment was sufficient, attributing the inability to conduct them more frequently to time constraints and budget.**

Section 8:
Enhance MDR with Proactive Security Measures (continued)

Vulnerability Management

Cyber vulnerabilities are weaknesses or loopholes within system defenses that can be exploited by cyber threat actors or malicious code. These vulnerabilities stem from software flaws, outdated systems, misconfigurations, configuration drift, or subpar security practices, and can potentially result in unauthorized access or data breaches. Effective vulnerability management is a critical component of cybersecurity, requiring regular reviews and updates to system defenses to prevent exploitation by threat actors. Vulnerability management involves continuously identifying, assessing, and remediating vulnerabilities within an organization's IT environment.

While many organizations have vulnerability scanning tools in place, the complexities and demands of maintaining a fully functional vulnerability management program often requires expertise and time that the organization lacks. Vulnerability scanners can produce unmanageable amounts of data that largely lack risk-aware contextualization. While automated systems can identify vulnerabilities, the process to validate findings and assess real-world risks is critical to effective vulnerability management. Triaging and prioritizing vulnerabilities is a nontrivial effort that involves many moving parts, including vulnerability priority and severity, exploitability, exploit probability, weaponization, and the potential impact an exploit might have on the organization. Only with a prioritized list can organizations meaningfully reduce risk through patching and mitigation efforts.

Survey respondents have increasingly recognized the value of partnering with an expert vendor for vulnerability management services. Outsourcing not just detection and response but also the management, configuration, and continuous oversight of vulnerability management programs provides several advantages:

- **Comprehensive Management:** Providers offer end-to-end management of vulnerability programs, ensuring that all aspects, from detection to remediation, are handled efficiently.
- **Advanced Configuration:** Providers bring expertise in configuring security tools and systems to optimize vulnerability detection and response.
- **Resource Allocation:** Outsourcing allows organizations to allocate their internal resources more effectively, allowing them to focus on core business activities while leaving complex security tasks to specialists.
- **Continuous Improvement:** Providers stay updated with the latest threat intelligence and best practices, continuously refining their methods to protect against emerging threats.

Despite having internal vulnerability management programs, the growing complexity of cyber threats and the need for specialized expertise make these providers an invaluable partner. By outsourcing these critical functions, organizations can ensure a robust and proactive approach to cybersecurity, reducing the risk of breaches and enhancing their overall security posture.

Section 9:
The Critical Start Approach

In an era where cyber threats are evolving at an unprecedented pace, organizations need more than traditional security measures to safeguard their operations. Critical Start's Managed Detection and Response (**MDR**) is not just another cybersecurity solution; it's the cornerstone of a comprehensive Managed Cyber Risk Reduction (**MCRR**) strategy designed to deliver unparalleled risk mitigation and operational efficiency to mitigate business disruption. This strategy combines proactive security measures with comprehensive risk management, utilizing our Cyber Operations Risk & Response™ (**CORR**) platform. We integrate industry-leading tools and proactive cybersecurity intelligence into the Critical Start Security Operations Center (SOC) to provide comprehensive asset inventories, EDR/SIEM coverage gap analysis, asset criticality ratings, MITRE ATT&CK® Mitigations, and vulnerability management. This integrated approach ensures that we address threats proactively and manage vulnerabilities effectively, thereby minimizing business disruption and maximizing operational efficiency.

Unlike conventional security solutions that only detect and respond to threats, Critical Start's MDR integrates proactive security measures with comprehensive risk management capabilities. This holistic approach ensures:

Security Operations Signal Assurance: EDR gap and log source monitoring guarantee that your Security Operations Center (SOC) receives all necessary threat signals, leaving no blind spots in your defense.

Asset Visibility: Determine and maintain an accurate and persistent asset inventory of critical assets across your organization. Categorize risk impact based on business function, we help you prioritize security efforts where they matter most.

Human-Driven Investigation and True Response Mitigations: Our experts provide true response mitigations backed by contractual SLAs, ensuring swift and accurate threat resolution.

Flexible Deployment Models: Supporting all IT and OT threat types and log sources, our solutions are adaptable to your unique operational environment.

Maximizing Efficiency and Minimizing Disruption: Critical Start's MDR service is designed to minimize business disruption and maximize operational efficiency. Our human-driven approach, combined with advanced technology, ensures that every threat is addressed promptly and effectively. This integration of proactive measures with responsive action allows your organization to stay ahead of the curve, reducing the risk of breaches and enhancing overall security posture.

Comprehensive Vulnerability Management and Risk Assessments

In addition to our core MDR services, we offer robust vulnerability management and risk assessment programs. These include:

- **Vulnerability Management Service (VMS):** A tiered managed service that includes operational execution of vulnerability scanning, continuous monitoring, and detailed reporting. Customers benefit from expert analysis, contextualized scan reports, and actionable recommendations that reduce cyber risk.
- **Vulnerability Prioritization:** Enhances your existing vulnerability management tools by integrating multi-vector intelligence, including threat data, exploitability, and asset criticality. This solution provides dynamic risk scores for each vulnerability, accelerating patching efforts and improving vulnerability reporting.
- **Risk Assessments:** Guided risk assessments spotlight control deficiencies across frameworks, benchmarking your data against industry peers and your own improvements over time.
- **Cyber Risk Register:** An easy-to-use SaaS offering that allows security leaders to quickly record, track, and manage their organization's cyber risks in one centralized system.

Section 9:
The Critical Start Approach (continued)

The Indispensable Element in Cybersecurity: Humans

According to the 2024 Data Breach Investigations Report (DBIR), "… human element was a component of 68% of breaches … ."[3] The good news is that humans aren't just part of the problem; they're part of the solution, too. Even as cybersecurity technologies progress, human expertise remains a critical component of a holistic security approach.

Traditional automated defenses can fall short against increasingly complex cyber threats because they lack the nuanced understanding that human experts provide. MCRR integrates the latest technologies with human intelligence to provide a unified approach to managing cyber threats, risks, and vulnerabilities. Critical Start's SOC team includes security analysts, risk managers, compliance officers, and other cybersecurity professionals who provide:

- **24x7x365 Monitoring:** Round-the-clock surveillance of IT and OT environments to detect and respond to threats in real time.
- **Expert Analysis:** In-depth analysis of security events by experienced analysts, ensuring accurate threat identification and effective response.
- **Personalized Service:** Tailored services to meet each client's unique needs, providing personalized support and strategic guidance.
- **Advanced Detection Tools:** Utilizing state-of-the-art tools and technologies to quickly detect and respond to threats.
- **Collaboration and Coordination:** Working closely with customers to ensure seamless communication and coordination during incident response.
- **Continuous Learning:** Regular training and development for our analysts to stay ahead of emerging threats and techniques.

The Critical Start Critical Response Unit (**CRU**) works as an extension of your team, providing proactive threat intelligence and comprehensive cyber defense. The CRU assists security professionals in establishing robust Cyber Threat Intelligence (**CTI**) capabilities. By offering contextual, evidence-based guidance, including actionable advice tailored to your environment, vertical, and operational scope, it equips your organization with the necessary tools to fortify defenses, mitigate risks, proactively stay ahead of emerging cyber threats, and prevent breaches. Your organization is provided with a straightforward view of what's happening across the threat landscape, including assessments of newly exploited vulnerabilities, industries, organizations, or specific technologies targeted, and new and trending malware.

The CRU is composed of specialists in cyber threat intelligence, threat research, malware analysis, reverse engineering, detection development, and more. It builds and enriches detections and Indicators of Compromise (**IOC**s) with up-to-the-minute threat intelligence. Their research supports product enrichment, continuously updating and refining detection strategies for EDR, XDR, and SIEM security tools based on the latest threat intelligence to respond to evolving cyber threats. Their work supports our MDR services and expanded MCRR offerings delivered 24x7x365 by our U.S.-based Risk & Security Operations Center (SOC) analysts, helping them augment defenses with continuous identification, analysis, and mitigation of emerging threats tailored to each organization's environment.

Cost-Effective Security

By outsourcing detection and response capabilities to an MDR provider, organizations can achieve a high level of security without the need for extensive in-house resources. This makes MDR a cost-effective solution for businesses of all sizes. Our survey found that this trend is increasing: A significant majority (98.6%) of respondents plan to offload specific segments of cyber risk reduction workstreams or projects to security service providers within the next two years. Of these, 67.8% are planning to do so for the first time, a 14% increase over 2023. While the number of respondents with one-person in-house cyber risk personnel increased to 67%, those with more than a single-person team decreased, highlighting the value security service providers can bring.

MDR services continuously update and adapt based on new threat intelligence and incident learnings. This ensures organizations remain protected against evolving threats and maintain a proactive security stance. Most survey respondents (84%) agree that continuous risk monitoring will reduce the likelihood of a breach. At the same time, 97% report that they either completely (61%) or somewhat (36%) lack the time to continuously monitor areas of potential failure.

By leveraging MDR as the foundation of MCRR, organizations can ensure comprehensive cyber risk lifecycle management, exposure management, and continuous improvement in their security posture. This integrated approach provides a resilient and adaptive defense mechanism, crucial for mitigating the cyber risks organizations face today.

Conclusion and Key Takeaways

The 2024 Critical Start Cyber Risk Landscape Peer Report underscores the increasingly complex and pervasive nature of cyber threats that businesses face today. With digital transformation continuing to drive innovation and growth, the cyber risk landscape evolves correspondingly, demanding more robust and proactive cybersecurity measures.

Key Takeaways

1. Combining MDR with proactive cybersecurity elements such as risk assessments, asset visibility, vulnerability management, and endpoint security significantly enhances an organization's defense capabilities. These measures ensure comprehensive visibility, timely remediation of vulnerabilities, and robust protection against potential threats.
2. Cyber threats are more sophisticated and frequent than ever. Our survey revealed that 83% of cybersecurity professionals experienced a breach requiring attention within the last two years, a significant increase from previous years. This highlights the inadequacy of traditional security measures and the growing need for advanced threat detection and response capabilities.
3. The financial consequences of cyber incidents are substantial, with the average cost of a data breach reaching $4.45 million in 2023. Beyond financial losses, breaches severely damage company reputations, erode customer trust, and result in regulatory penalties. Organizations must prioritize cybersecurity investments to mitigate these risks effectively.
4. Managed Detection and Response (MDR) services are essential in modern cybersecurity strategies. MDR provides continuous monitoring, advanced threat detection, and rapid response to incidents. By integrating technologies such as machine learning and threat intelligence with human expertise, MDR enhances the ability to identify and mitigate sophisticated threats in real time.
5. Human expertise remains indispensable in cybersecurity. While technology is crucial, the nuanced understanding and strategic insights provided by skilled security professionals are vital for effective threat detection and incident response. Security Operation Centers (SOCs) staffed with experienced analysts are key to maintaining a resilient cybersecurity posture.
6. Cybersecurity is not a one-time effort but a continuous process. Organizations must regularly update and adapt their security measures based on new threat intelligence and learnings from past incidents. This proactive approach ensures ongoing protection against evolving threats and helps maintain a proactive security stance.

This report highlights the urgent need for businesses to adopt comprehensive, proactive cybersecurity strategies. By leveraging MDR services and integrating proactive security measures, organizations can significantly reduce cyber risk and enhance overall security posture. Continuous investment in cybersecurity, coupled with the invaluable expertise of human analysts, is essential for navigating the complex, dynamic cyber threat landscape.

Survey Methodology

The survey included responses from 1001 VP+ cybersecurity professionals, conducted over a specified period. The participant demographics covered a diverse range of industries, ensuring a comprehensive view of the cybersecurity landscape.

Data Collection Period and Process

Data was collected between June 27, 2023, and July 3, 2023, with a follow-up period from June 11, 2024 to June 25, 2024. The survey design included a mix of qualitative and quantitative questions to capture detailed insights.

About Critical Start

Organizations today face the challenge of optimally aligning their cyber protection measures to reduce the risk of breaches and business disruptions. CRITICAL**START**® Managed Detection and Response (MDR) is the foundation to Managed Cyber Risk Reduction, which improves security operations outcomes and minimizes the probability and impact of breaches. Utilizing their Cyber Operations Risk & Response™ platform, they integrate industry-leading tools and proactive cybersecurity intelligence into the Security Operations Center (SOC) — such as comprehensive asset inventories, EDR coverage gaps, asset criticality, MITRE ATT&CK® Mitigations, and vulnerability management. Their security operations team evaluates and responds to threats, vulnerabilities, and risks, while conducting extensive threat intelligence research. Supported by a human-led risk and security operations team with over 10 years of MDR experience, Critical Start empowers businesses to protect their critical assets, demonstrating a measurable return on investment.

The platform offers maturity assessments, peer benchmarking, posture and event analytics, and robust response capabilities. This approach ensures that organizations achieve optimal cyber risk reduction for every dollar spent, enabling them to confidently reach their desired risk tolerance levels.

For more information, visit *criticalstart.com*. Follow Critical Start on *LinkedIn*, @CRITICALSTART, or on *Twitter*, @CRITICALSTART.

READY TO LEARN MORE?
https://www.criticalstart.com