Navigating the Cyber Risk Conundrum

How the Next Evolution of MDR – Managed Cyber Risk Reduction (MCRR) – Helps Organizations Achieve Measurable Risk Reduction

CRITICALSTART®

Don't Fear Risk. Manage It.

Table Of Contents

Executive Summary

The cost of cybercrime is rising and subsequent mandates for cybersecurity are increasing without adequate understanding of security posture to make informed cybersecurity risk decisions. Security and risk management leaders are struggling to confidently align cyber protection measures to the risk appetite of the organization. Even where risk is known, organizations wrestle with under-resourced teams already over capacity, broad multi-domain security expertise requirements, and limited budgets to take an optimal full stack risk-based approach to security that monitors, manages, and measures risk reduction. As a result, organizations are playing security investment roulette and are guessing where to place their security bets.

If you really care about reducing cyber risk, you need a proven, cost-effective, guided, and measurable approach to cyber risk reduction that goes *beyond* traditional manual, non-evidence based, limited scope assessments and management of risks (aka cybersecurity risk management). You need an ***evidenced, actionable, risk prioritized view across a broad array of risks*** to evaluate potential financial investments to identify, protect, detect, respond, and recover to a wide range of threats.

Managed Cyber Risk Reduction (**MCRR**), the next evolution of Managed Detection and Response (**MDR**), brings together cyber risk monitoring technology with a human-led risk and security operations team to deliver continuous security posture improvement and the strongest possible protection against threats.

With managed cyber risk reduction, an organization gains a holistic and continuous view of its cyber risk landscape that is prioritized and actioned. An organization can gain a third-party endorsed, framework aligned, risk assessment benchmarked to peers. On an ongoing basis an organization can:

- Identify critical assets requiring protection.
- Ensure key security controls are operating and effective.
- Evaluate events for untrusted behavior.
- Quickly action and contain potential incidents.
- Ensure restore capabilities are in place to recover systems and business operations.

MCRR empowers security and risk management leaders with the ability to analyze the potential impact of different security measures and helps prioritize investments to achieve the greatest reduction in breach and business disruption risk for the dollars spent.

Introduction

The Cyber Risk Conundrum

Mandates for cybersecurity are increasing without adequate understanding of protection levels to make informed cybersecurity risk decisions.

Security leaders are under constant pressure to demonstrate effective management of cyber risk, with increasing concerns from stakeholders including boards, regulators, and customers. It's understandable considering the cost of cybercrime is predicted to hit $8 trillion in 2023 and will grow to $10.5 trillion by 2025.[1] Making the struggle worse, security leaders are plagued by a shortage of talent and a wide assortment of threats, vulnerabilities, and risks to respond to quickly. It's incredibly difficult to confidently align cyber protection measures to the risk appetite of the organization.

Furthermore, according to research conducted by Critical Start in partnership with Censuswide,[2] 66% of organizations have limited visibility and insight into their cyber risk profiles, hindering their ability to prioritize investments and allocate resources effectively.

Security and risk management leaders struggle with answering questions like:

- How much security risk does the organization have?
- How can I know how our cyber risk level changes over time?
- How do my cyber risk and security maturity levels compare with peer organizations?
- How do I access and analyze data to communicate cyber risk in a way that drives action?
- What security metrics do I use to drive action that reduces risk?

Data from the Critical Start research cited above shows that security leaders are looking for a proven, cost-effective, guided, and measurable approach to manage their cyber risk that goes beyond traditional cybersecurity approaches.

66% of organizations have limited visibility and insight into their cyber risk profiles, hindering their ability to prioritize investments and allocate resources effectively.[2]

[1]Brooks, C. (2023, March 6). Cybersecurity Trends & Statistics For 2023; What You Need To Know. https://www.forbes.com/sites/chuckbrooks/2023/03/05/cybersecurity-trends--statistics-for-2023-more-treachery-and-risk-ahead-as-attack-surface-and-hacker-capabilities-grow/?sh=66cddfd019db

[2]Critical Start in partnership with Censuswide.

Traditional Approaches to Cybersecurity Risk Management Fall Flat – *Here's Why*

The struggle to align cyber protection measures to risk appetite

Business stakeholders and cybersecurity teams often have different perspectives and priorities. Cybersecurity teams are primarily concerned with risk mitigation and protection, while business leaders focus on growth, innovation, and operational efficiency. Balancing these perspectives and aligning them to the risk appetite of the organization requires communication, collaboration, and common understanding.

In many organizations, there is a communication gap between the cybersecurity function and other business units. Limited communication and collaboration make it challenging to understand and address the specific risk appetite of the organization. Without clear understanding of the organization's risk tolerance, cybersecurity measures may not be appropriately aligned with the organization's overall objectives and priorities.

Determining the risk posture of an organization requires a comprehensive risk assessment process. However, the constantly evolving threat landscape, the shortage of skilled security professionals, and the proliferation of technology make accurately assessing cyber risk incredibly complex.

Evolving cyber threat landscape

The cyber threat landscape is constantly evolving, with new attack techniques, vulnerabilities, and risks emerging regularly. ***This rapid pace of change makes it challenging for organizations to keep up and effectively align protection measures with the evolving risks.***

Growing variety of attack vectors: Attackers have a wide range of attack vectors at their disposal, including social engineering, phishing, malware, ransomware, and insider threats, among others. The diversity of these attacks increases the potential risks organizations face and requires comprehensive risk management strategies to address each vector effectively.

Expanded surface area: The explosion of connected devices, cloud services, and the Internet of Things (**IoT**) has expanded the attack surface for potential breaches. Organizations now need to manage risks associated with a larger number and variety of device types, networks, applications, and third parties, making it more challenging to implement effective security controls with a holistic view across the entire infrastructure.

Traditional Approaches to Cybersecurity Risk Management Fall Flat – *Here's Why* (continued)

Proliferation of security tools

According to Venture Security and the IT Harvest Dashboard[3], the largest cybersecurity vendor database counts 3,231 companies across seventeen security categories. Acquiring a multitude of security tools without proper planning or coordination results in a fragmented and disjointed security infrastructure where tools operate in isolation, leading to inefficiencies, redundancies, and difficulty in managing and integrating these tools effectively.

Lack of integration and incompatibility: Accumulating tools without a strategy introduces the risk of selecting tools that are not compatible or do not integrate well with existing systems and processes. The result is data silos, manual workarounds, and challenges in sharing information and insights between different tools. The organization's ability to gain a holistic view of security posture is hampered and can lead to missed opportunities for comprehensive risk management.

Increased complexity: Each security tool can introduce unnecessary complexity with different management interfaces and reporting mechanisms. Complexity overwhelms security teams, increases the risk of misconfigurations, and hinders effective monitoring and response efforts.

Resource drain: Implementing and maintaining security tools requires resources – people, finances, and infrastructure. Without a strategy in place, organizations may allocate resources to tools which are not aligned with their specific security needs or lack proper return on investment (**ROI**) analysis.

Lack of focus and prioritization: Without a clear understanding of the organization's risk profile and security objectives, it becomes challenging to identify the most critical areas that require immediate attention. Resources may end up spread thin across a wide variety of tools, neglecting the essential areas requiring stronger safeguards.

False sense of security: Having numerous tools in place does not guarantee effective protection against cyber threats. Relying solely on tool accumulation without a strategic approach leads to vulnerabilities and blind spots, leaving the organization exposed to potential threats. According to Critical Start 2023 Cyber Risk Confidence Report[2], 67% of organizations experienced a cyber breach in the last two years, despite having traditional threat-based security measures in place.

Ultimately, unless carefully evaluated, additional tools may not be delivering the expected risk reduction impacts.

[2]Critical Start 2023 Cyber Risk Confidence Index. https://www.criticalstart.com/resources/cyber-risk-confidence-index-report/

[3]Haleliuk, Ross. (2023, January 16). Why there are so many cybersecurity vendors, what it leads to and where do we go from here. Venture in Security. https://ventureinsecurity.net/p/why-there-are-so-many-cybersecurity#:~:text=The%20number%20of%20security%20providers,3231%20companies%20across%2017%20categories.

Traditional Approaches to Cybersecurity Risk Management Fall Flat – *Here's Why* (continued)

Under-resourced cybersecurity teams

According to the (ISC) 2 Cybersecurity Workforce Study[4], at the end of 2022, there was a security workforce gap of 436,080 jobs in the U.S. and 3.4 million globally. *A shortage of skilled professionals with the expertise and knowledge required to defend against evolving cyber threats prevents organizations from effectively managing cyber risk.*

Lack of expertise and specialized skills: Cybersecurity is complex and a rapidly evolving field. Specialized skills and knowledge are required to not only navigate the intricacies of emerging threats, but also implement, monitor, and maintain security controls, and respond effectively to incidents. Without the right individuals, it's challenging to develop, prioritize, and execute risk management strategies.

Increased workload and stress on existing staff: Existing staff members may be stretched thin and burdened with additional responsibilities. A study of mental health in cybersecurity by Tines shows 66% of the over 1,000 respondents report significant stress at work with 64% claiming the stress is rising.[5] If staff is required to manage a larger workload, cover multiple areas of cybersecurity, or oversee complex risk management tasks without adequate support, the result is reduced effectiveness in managing cyber risk.

Slower response to incidents: The workforce gaps results in delayed incident response times, leaving organizations vulnerable for longer, increasing attacker dwell-time, and potentially amplifying the impact of an incident.

Incomplete implementation of security protection measures: Effective cybersecurity risk management involves implementing a range of protection measures, but without sufficient resources to maintain and measure these controls, potential vulnerabilities can be exploited by attackers, increasing overall cyber risk exposure.

> **A cybersecurity workforce gap jeopardizes the most foundational functions of the profession like risk assessment, oversight, and critical system patching. More than half of employees at organizations with workforce shortages feel that staff deficits put their organization at a 'moderate' or 'extreme' risk of cyberattack. And that risk increases substantially when organizations have a significant shortage.[4]**

[4](ISC)2 Cybersecurity Work force Study. (2022). ISC2-Cybersecurity-Workforce-Study.ashx

[5]Hinchy, Eoin. (2022). State of Mental Health in Cybersecurity. Tines. https://www.tines.com/reports/state-of-mental-health-in-cybersecurity#key-findings

Traditional Approaches to Cybersecurity Risk Management Fall Flat – *Here's Why* (continued)

The security assessment challenge

Security leaders are continually evolving their assessment practices to keep up with digital transformation and evolving work practices. Security teams must now factor in risk-exposure of human error, SaaS platform and third-party application dependencies, and/or misconfigurations of their security controls.

These factors have led to an increased adoption of assessment and risk-discovery tools and processes, to attempt to quantify risk. However, ***the proliferation of assessment tools has amplified the need for an ability to prioritize the most relevant remediation actions.***

Here's why:

Data overload: Assessment and discovery tools can lead to an overwhelming amount of data and findings. Organizations may now have multiple tools that each have its own set of risks, vulnerabilities, threats, and recommendations. The flood of information is difficult to consolidate and analyze effectively. Overwhelming amounts of data can make it challenging to identify the most critical issues and prioritize the necessary remediation actions.

Lack of consistency and standardization: Different assessment tools often use varying methodologies, metrics, and scoring systems, which can lead to inconsistent results and recommendations. Without standardization, organizations struggle to compare and prioritize remediation actions across different tools. It becomes challenging to assess the severity and potential impact of identified vulnerabilities consistently, making it difficult to make informed decisions about remediation priorities.

Limited contextual understanding: Discovery tools may provide vulnerability scan results or technical findings, but they often lack the context and understanding of the organization's specific environment and risk landscape. They may not consider factors such as business criticality, data sensitivity, implementation effort, or the potential impact on operations. As a result, organizations have difficulty prioritizing remediation actions based on their unique risk profile and priorities.

Lack of integration and automation: When multiple assessment tools are used in isolation, integrating and correlating the findings becomes a manual and time-consuming process. Organizations may need to consolidate data from various tools manually, leading to delays and inconsistencies in identifying and prioritizing remediation actions. The lack of automation and integration hinders the organization's ability to streamline the prioritization process and respond promptly to critical risks and threats.

Complexity in decision making: With numerous assessment tools providing different findings and recommendations, decision-making becomes complex. Organizations may find it challenging to weigh the severity of risks, consider potential dependencies and cascading effects, and balance the need for remediation with other business priorities. This complexity can lead to analysis paralysis and delays in taking necessary actions.

Outsourced assessments: Facing the challenges previously laid out, many organizations focus on implementing the controls, and leveraging third parties to perform security assessments only when necessary. While the outsourcing model seems like a solution, the provider will likely experience many of the same challenges, rely on the internal team to provide all data and evidence, and will provide only a point-in-time snapshot of security posture, preventing the measurement of security maturity improvements over time.

The Next Evolution in Cybersecurity

From the early inception of cybersecurity, groundbreaking innovations have often cycled between detection (**reactive**) and prevention (**proactive**) in focus. Here is a quick look at the evolution in the industry throughout the years, from Antivirus through MDR.

Year	Technology	Focus	Origin & Purpose
1987	Antivirus (**AV**)	Reactive	First antivirus software "Brain" released, designed to detect and remove malware from computer systems.
1992	Firewalls	Proactive	DEC SEAL, the first firewall, introduced as a barrier between internal networks and the internet to block unauthorized traffic and prevent cyber-attacks.
1998	Intrusion Detection System (**IDS**)	Reactive	Developed to monitor network traffic, detect potential threats, and send alerts when suspicious activity is identified.
1999	Security Information and Event Management (**SIEM**)	Reactive	Introduced to provide real-time analysis of security alerts generated by applications and network hardware, enabling efficient incident detection and response.
2000	Next-Generation Antivirus (**NGAV**)	Proactive	Combines traditional antivirus capabilities with machine learning, behavioral analysis, and exploit prevention to protect against more sophisticated threats.
2004	Intrusion Prevention System (**IPS**)	Proactive	Evolved from IDS technology to actively prevent and mitigate detected threats by blocking or quarantining malicious traffic.
2010	Next-Generation Firewall (**NGFW**)	Proactive	Integrates traditional firewall functions with advanced capabilities like deep packet inspection, application control, and user identity management.
2012	Network Packet Capture and Reconstruction	Reactive	Developed to record, store, and analyze network traffic in real-time or retrospectively, aiding in security incident identification and investigation.
2013	Endpoint Detection and Response (**EDR**)	Reactive	Developed to monitor endpoints for potential threats, collect data for analysis, and enable organizations to respond to security incidents more effectively.
2018	Managed Detection and Response (**MDR**)	Reactive	Combines advanced threat detection, incident response, and continuous monitoring capabilities with human expertise for a reactive approach to reduce cyber risk.

While many arguments can be made for the reasons behind this continuous shifting, three primary factors emerge:

1. **Under-resourced cybersecurity teams:** With a shortage in both headcount and expertise exacerbating a security function that lags innovation in networking and infrastructure, security teams often shift focus based on the priorities of the organization and the allocated resources.
2. **Technology advancements and vendor competition:** The integration of technology advancements, machine learning, and AI has empowered cybersecurity vendors to develop more sophisticated detection and protection solutions. Market demands for improved ROI on security investments, coupled with rising regulatory requirements, have driven vendors to continuously innovate and compete to maintain their market share.
3. **Cybercriminal innovation:** Cybercriminals continuously evolve their Tactics, Techniques, and Procedures (**TTPs**). Cybercrime has become a lucrative industry that incentivizes malicious actors to constantly find ways to circumvent prevention measures and avoid detection. These cybercriminals employ various tactics to steal, destroy, or extort from their victims, posing a significant threat to individuals, organizations, and economies worldwide.

The result of this shifting is a high-cost, high-stakes game of whack-a-mole detecting new TTPs and putting proactive controls in place, while the attacker develops newer TTPs less likely to be detected. ***This lag provides a window of opportunity to introduce new risk and potential business disruption.***

The Next Evolution in Cybersecurity

How MDR providers help manage risk and prove ROI

In this evolution of cybersecurity, MDR services have become a necessary reactive measure to help security operations teams respond after an attack has occurred. MDR, itself an evolution from Managed Security Service Providers (**MSSPs**), adds the value of expertise and action to reactively contain threats and lower attacker dwell time.

MDR is the cornerstone to improving security maturity and providing the greatest reduction in **threat detection and response risk** per dollar invested. With the right MDR service, an organization immediately reduces risk with:

- Contractual service level agreements for Median Time to Resolution (**MTTR**) for every alert, regardless of severity
- Every alert actioned across EDR, XDR, and SIEM (not just critical or highs)
- Operationalized threat intelligence that improves the effectiveness of detecting attacks
- Detection coverage aligned to the **MITRE ATT&CK® Framework** kill chain
- Full visibility and incident containment from a mobile application

74% 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.[2]

What's the next step?

Security leaders are recognizing the limitations of a reactive mindset and shifting their focus beyond thread-based detection and response measures to account for risk. Seventy-four percent 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.[2]

Relying solely on reactive measures leaves organizations vulnerable to sophisticated attacks that can cause substantial damage before they are detected. By the time an incident is detected, valuable data may already be compromised, leading to financial losses, reputation damage, and regulatory non-compliance. Attackers are pivoting to find the path of least resistance into an organization, while security teams are building defenses to combat existing threats.

Here's why proactive security is important:

Prevention over reaction: Proactive security emphasizes preventative measures that can significantly reduce the attack surface and minimize the likelihood of successful breaches. With the goal of preventing an incident from occurring, proactive controls include: vulnerability assessments, patch management, and robust access controls.

Compliance and regulatory requirements: Many industries are subject to stringent regulatory frameworks, such as General Data Protection Regulation (**GDPR**) and the Health Insurance Portability and Accountability Act (**HIPAA**), which necessitate proactive security measures. By proactively identifying and addressing risks and vulnerabilities, organizations ensure compliance and avoid costly penalties.

Reputation and customer trust: Organizations that prioritize proactive security demonstrate their commitment to safeguarding customer data and protecting privacy. By implementing advanced security measures, organizations build trust with customers, partners, and stakeholders, enhancing their reputation and competitive advantage.

Increased effectiveness of reactive controls: With fewer inbound attacks, security teams can better detect and respond to threats that bypass proactive security controls. Providing some alleviation from alert fatigue, analysts have less "noise" to sift through to identify true positives from more advanced attacks.

[2]Critical Start 2023 Cyber Risk Confidence Index.
https://www.criticalstart.com/resources/criticalstart-research-reveals-66-of-cybersecurity-leaders-lack-a-high-degree-of-confidence-in-the-effectiveness-of-their-current-cyber-risk-mitigation-strategies/

The Next Evolution of MDR: Managed Cyber Risk Reduction

The future of MDR

With many information technology (**IT**) assets now living outside of traditional enterprise perimeters, security and IT leaders are rethinking how they approach extending security controls to distributed assets to ensure protection. The buying needs of organizations are shifting to rethinking about what to monitor and how to monitor it.

According to The Future of Managed Detection and Response[6] blog from Gartner, looking at exposure rather than just vulnerability will become more important. The future of MDR will go beyond reactive threat-based security, into proactive areas of security that include exposure awareness and cybersecurity validation.

Exposure awareness includes vulnerability prioritization, vulnerability management, managing and understanding your attack surface, and understanding digital risks. Cybersecurity validation includes understanding if your security controls are configured properly, continuous monitoring of these controls, and the ability to respond if a control is not working as expected.

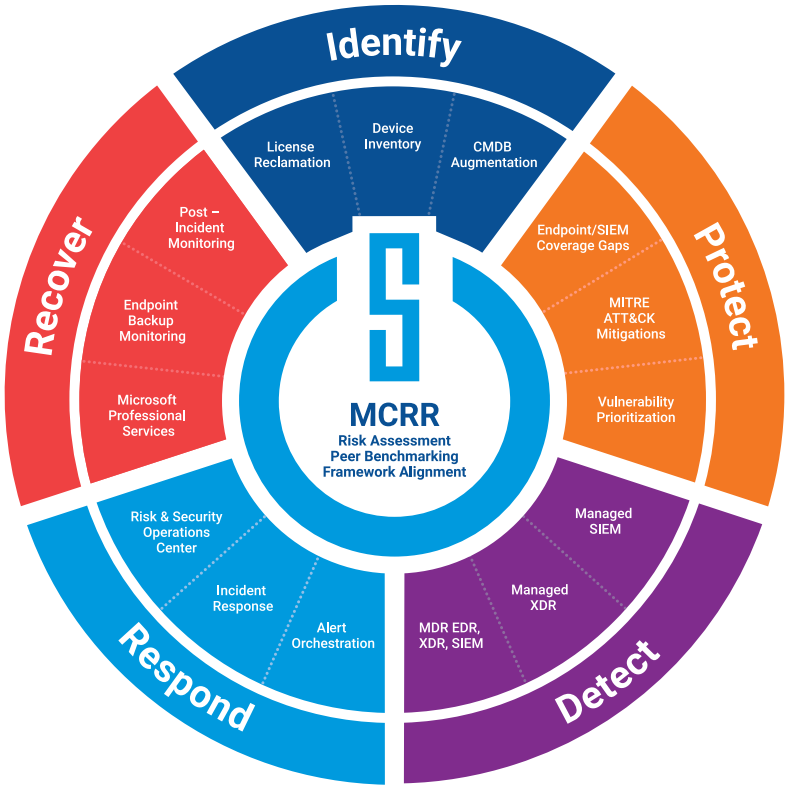
Exposure awareness includes vulnerability prioritization, vulnerability management, managing and understanding your attack surface, and understanding digital risks. Cybersecurity validation includes understanding if your security controls are configured properly, continuous monitoring of these controls, and the ability to respond if a control is not working as expected.

[6]Shoard, Pete. (2021, October 26). The Future of Managed Detection and Response. Gartner.

The Future of MDR is Now

MCRR, the next evolution of MDR, pioneered by Critical Start, brings together ***cyber risk monitoring technology with a human-led risk and security operations team***. The combined solution provides organizations with a comprehensive understanding of their cybersecurity posture along with real-time monitoring and response to cyber threats, vulnerabilities, and risks.

MCRR is designed to go beyond detection and response to support all five functions of the National Institute of Standards and Technology Cybersecurity Framework (**NIST CSF**).



Managed Cyber Risk Reduction brings together cyber risk monitoring technology with a human-led risk and security operations team to deliver continuous security posture improvement and the strongest protection against threats possible.

Identify: Identify assets requiring protection.
By understanding what needs to be protected, appropriate security measures can be thoroughly implemented.

Protect: Ensure key security controls are operating and effective.
Continuous monitoring and assessing effectiveness helps verify that security measures and protocols are functioning as intended to mitigate risk.

Detect: Analyze events and activities within the organization to identify suspicious or unauthorized behavior.
With real-time monitoring and evaluation of events, potential threats or breaches can be quickly identified and appropriate action taken.

Respond: Quickly action and contain potential incidents.
When potential security incidents are identified, it is crucial to respond promptly and contain the situation to prevent further damage. This includes isolating affected systems, removing malicious code, or blocking unauthorized access.

Recover: Return to normal operations in the event of business disruption.
In the event of a cybersecurity incident or business disruption, organizations need to have plans and processes. This includes isolating affected systems, removing malicious code, or blocking unauthorized access.

The Power of MCRR

Traditional threat-based MDR services aren't enough to effectively manage cyber risk and build risk resilience. Critical Start MDR services, a foundational component of a successful MCRR strategy, are uniquely advanced with additional capabilities to include Identify, Protect and Recover capabilities. The power of MCRR provides many benefits and advantages to organizations who care about reducing cyber risk and are looking to move beyond threat-based MDR services to a proven, cost-effective, guided, and measurable risk-based approach to improve security posture.

Uncover gaps in endpoint, SIEM, and XDR controls coverage: MCRR addresses security controls gaps, including missing endpoint protection, additional log sources for SIEM ingestion, and log source health monitoring to ensure the Security Operations Center (**SOC**) is receiving expected signals.

Prevent attacks from happening again: Responding to the same attack repeatedly affects productivity. Implementing MITRE ATT&CK Mitigation recommendations based on live attacks in the environment provides the greatest risk reduction to prevent attacks from happening again versus buying more security technologies.

Understand what assets need to be protected: Determine and maintain an accurate and persistent asset inventory of critical assets across your organization.

Understand security investments that have the largest risk reduction impact: Intelligently align risk acceptance to the organization's risk appetite for risk-based decision making.

Know organization security maturity in comparison to peer organizations: Benchmark the security program to like companies.

Confidently demonstrate measurable security improvements: See how the security program is advancing and the impact of organizational investments.

Identify and respond to risk: Gain peace of mind with expert risk and security team members available to contain threats and respond to risk within contractual SLAs.

The Use Case for MCRR

MCRR allows organizations to understand their maturity and risk levels through risk assessments. Organizations start with a current state risk assessment of organization maturity across the five functions of NIST CSF. Organizations may want to start with deploying MDR services for their endpoints as an immediate measure to reduce risk, and follow-up with a risk assessment to understand other potential areas of cyber risk across the environment, benchmarked against peers. MCRR provides services that help advance security programs over time and mitigate risks in the most cost-effective ways possible.

The data below is a conceptual representation of what organizations with low security maturity might look like before MCRR.

*Figure 1 – Conceptual representation of what organizations look like **before** Managed Cyber Risk Reduction.*

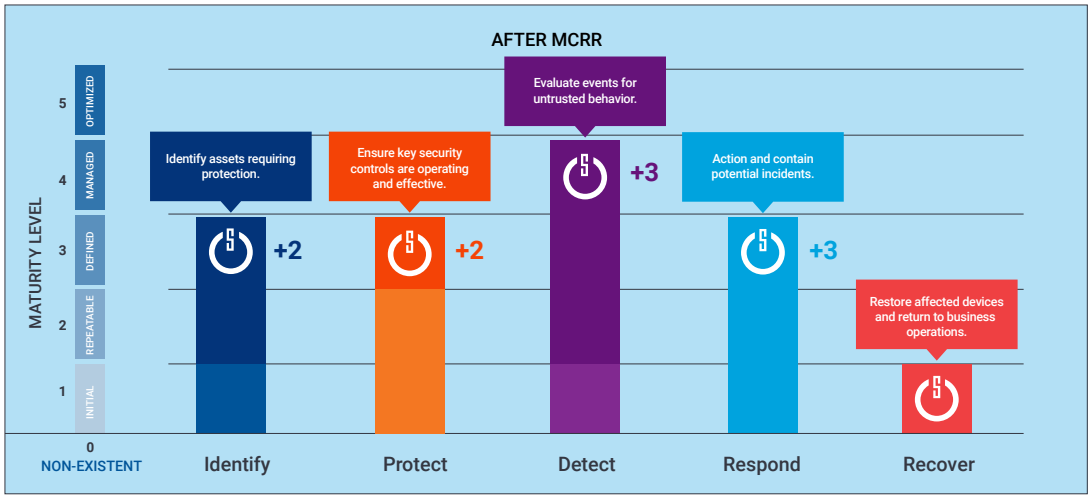


*Figure 2 - Conceptual representation of what organizations look like **after** Managed Cyber Risk Reduction.*

MCRR recommends the actions to improve an organization's security maturity and posture, and the impact it will have comparatively to like peer organizations.

Continuous risk monitoring then validates the measures are in place and functioning as intended to mitigate risk. Organizations are empowered with a strategic risk-based approach to security that provides quantifiable metrics and demonstrates security improvement over time. Through understanding risk across the security environment, security leaders understand return on investment (**ROI**) and risk reduction impact of actions.

The Use Case for MCRR

(continued)

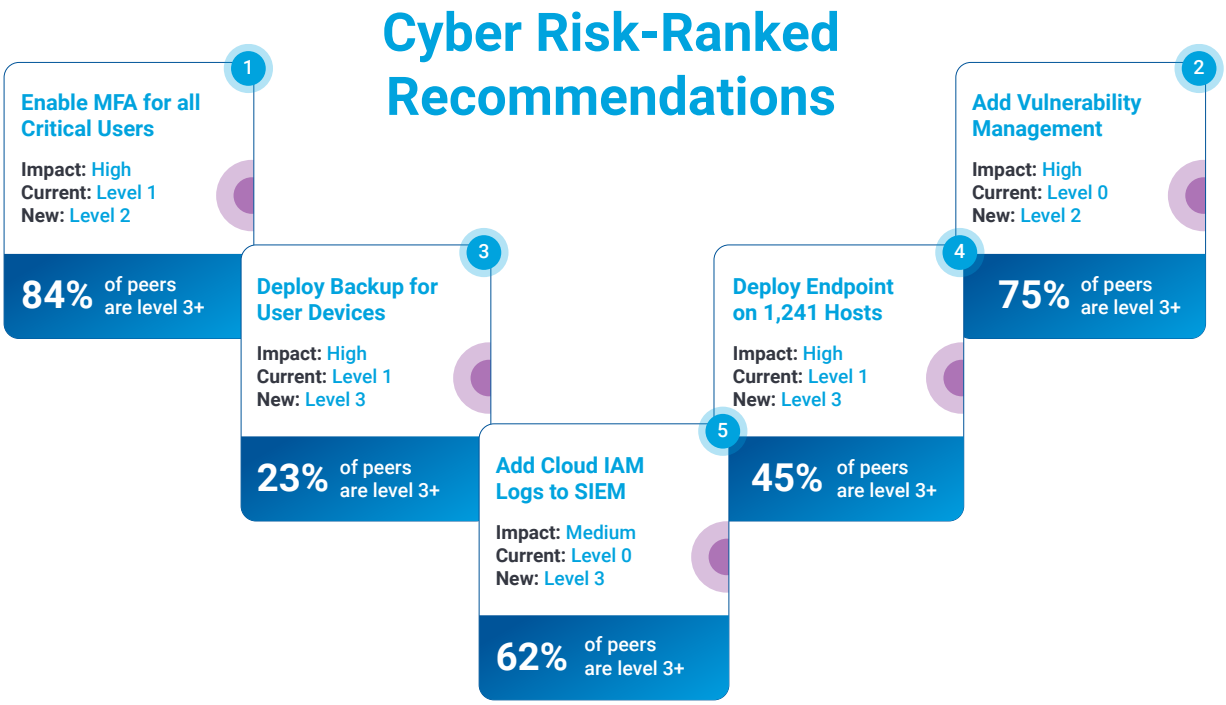


Figure 3: Conceptual representation of Cyber Risk-Ranked Recommendations

Leveraging a single platform, organizations gain a holistic understanding of risk across the environment with risk-ranked security recommendations. Added value comes from the ability to see how the organization compares to industry peers.

Key Components of MCRR

MCRR, as pioneered by Critical Start, a leading provider of MDR services, provides holistic cyber risk monitoring paired with a human-led risk and security operations team. With our platform, risk and security experts, and process, we uniquely provide organizations with the greatest cyber risk reduction per dollar spent.

The Risk Assessment

Critical Start offers both quick and comprehensive assessments, allowing you to choose between a high-level overview or a detailed analysis using the NIST CSF. Our questionnaires capture essential data efficiently, and the ability to attach evidence and add reviewers improves accuracy. You can also import existing assessments for a seamless transition.

With in-depth analysis, you receive prioritized risk rankings, helping you focus efforts and budget effectively. You can track risk trends over-time for long-term strategic planning. Mitigation reports offer a prioritized action plan and specific steps to minimize risks, guiding you in enhancing your organization's cybersecurity.

The Platform

Leveraging advanced technology is a critical component of implementing MCRR. The Critical Start **Cyber Operations Risk & Response™ platform** provides a single platform that offers continuous cyber risk monitoring with posture and event analytics, response orchestration capabilities, and threat intelligence. By utilizing advanced tools, organizations can proactively identify risks, threats, and vulnerabilities, prioritize them based on their potential impact, and allocate cybersecurity resources effectively for maximum risk reduction.

The Experts

Expanding beyond traditional security operations, the Critical Start **Risk and Security Operations Center** (**RSOC**) combines both security and risk expertise. We have skilled professionals who possess a deep understanding of security and can address cyber risks and implement essential mitigation strategies. Regardless of whether a threat or risk is identified, the RSOC is at your side ready to act.

The Proven Service Model

Our MCRR model encompasses services such as managed detection and response (**MDR**), incident response readiness, NIST CSF risk assessment to peer benchmarks, vulnerability prioritization, controls monitoring and gap identification, and asset inventory discovery. By leveraging this structured service model, organizations can establish clear processes and procedures for actioning risks, threats, and vulnerabilities. This systematic approach enables efficient and effective management of organizational cyber risks, minimizing potential disruptions to business operations.

By incorporating MCRR, organizations achieve the highest level of cyber risk reduction for every dollar invested. MCRR provides organizations with the necessary tools and expertise to proactively address cyber risks and safeguard their digital assets in an ever-evolving threat landscape.

Embracing Managed Cyber Risk Reduction:

Securing a Proactive Future

In today's ever-changing cybersecurity landscape, the cost of cybercrime continues to soar, driving organizations to seek effective protection measures. However, the lack of a clear understanding of security posture leaves security and risk management leaders struggling to align cybersecurity measures with the organization's risk appetite.

Many cybersecurity programs today focus on threat-based detection and response, which are proving inadequate in the face of evolving cyber threats. Recognizing the need for a proactive risk reduction strategy, MCRR emerges as the next evolution of MDR, offering a comprehensive and actionable risk-based approach to a comprehensive cybersecurity strategy.

MCRR empowers organizations with a third-party endorsed, framework-aligned risk assessment, providing a prioritized and quantifiable view of cyber risks. With this strategic insight, security leaders can confidently analyze the potential impact of various security measures, making informed decisions on risk reduction investments.

MCRR combines cyber risk monitoring technology with a human-led risk and security operations team. This holistic approach enables organizations to identify critical assets requiring protection, ensure the effectiveness of key security controls, evaluate events for suspicious behavior, and respond swiftly to potential incidents.

The benefits of MCRR are manifold, enabling organizations to uncover gaps in security controls coverage, benchmark their security maturity against peers, and demonstrate measurable security improvements. By adopting MCRR, organizations can take a proactive stance against cyber threats, reducing their attack surface, and minimizing potential disruptions to business operations.

As security leaders, embracing MCRR helps build resilience and confidence that critical assets are safeguarded. MCRR offers a data driven, outcome focused, and cost-effective solution to manage cyber risk effectively.

Embrace Managed Cyber Risk Reduction today and embark on a journey towards a comprehensive, strategic, and risk-based approach to security.

CRITICALSTART®

Don't Fear Risk. Manage It.

About Critical Start

Organizations today face the challenge of aligning their cyber protection measures with their risk appetite. CRITICAL**START**®, a pioneer of the industry's first Managed Cyber Risk Reduction solutions, provides holistic cyber risk monitoring via its **Cyber Operations Risk & Response™ platform**, paired with a human-led risk and security operations team, combined with over 12 years of award-winning Managed Detection and Response (**MDR**) services. By continuously monitoring and mitigating cyber risks, Critical Start enables businesses to proactively protect their critical assets with a measurable ROI. The company's platform provides maturity assessments, peer benchmarking, posture and event analytics, and response capabilities. Its risk and security operations team evaluates and actions threats, risks, vulnerabilities, and performs comprehensive threat intelligence research. Critical Start enables organizations to achieve the highest level of cyber risk reduction for every dollar invested, allowing them to confidently reach their desired levels of risk tolerance.

READY TO LEARN MORE?

https://www.criticalstart.com