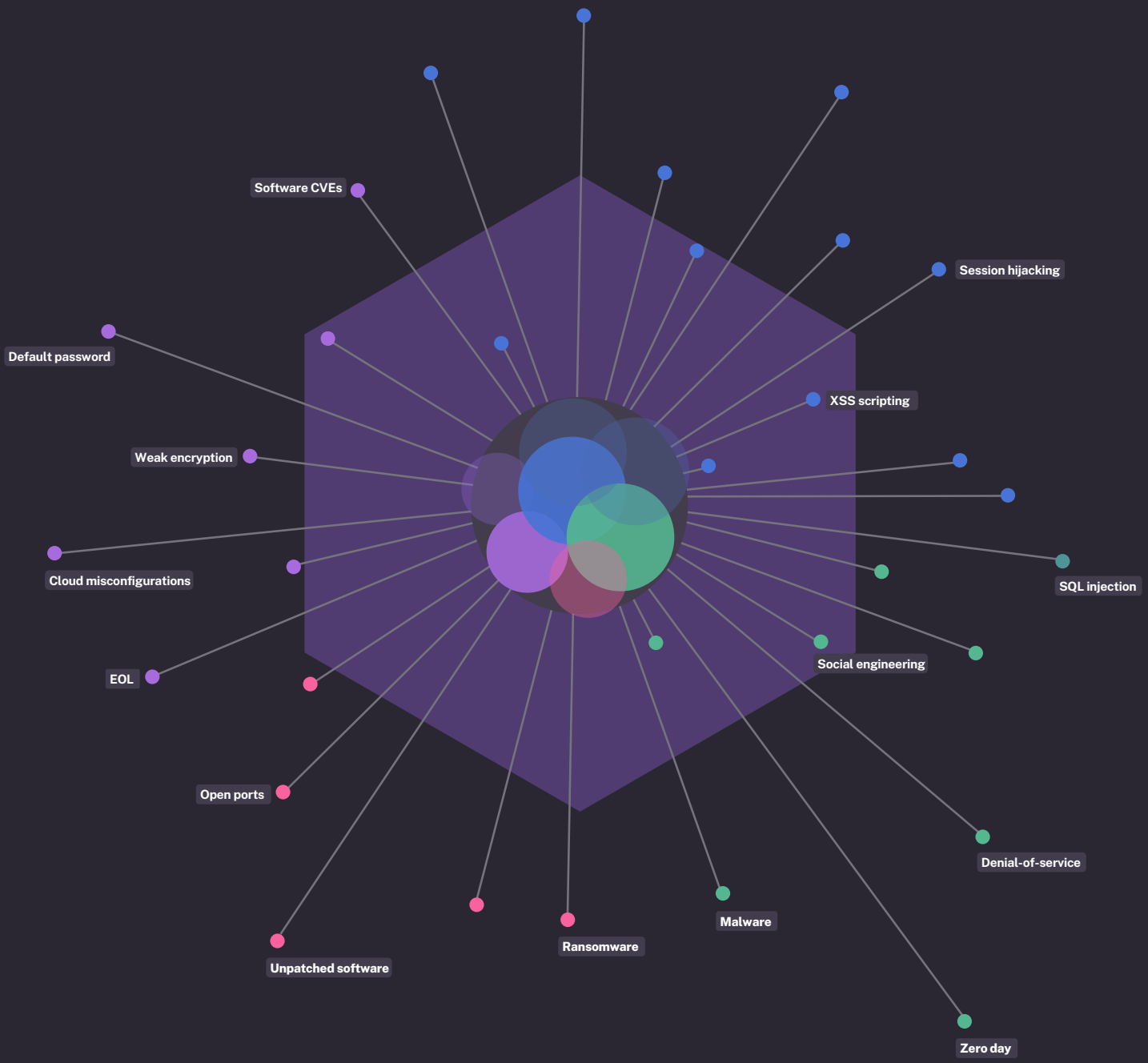
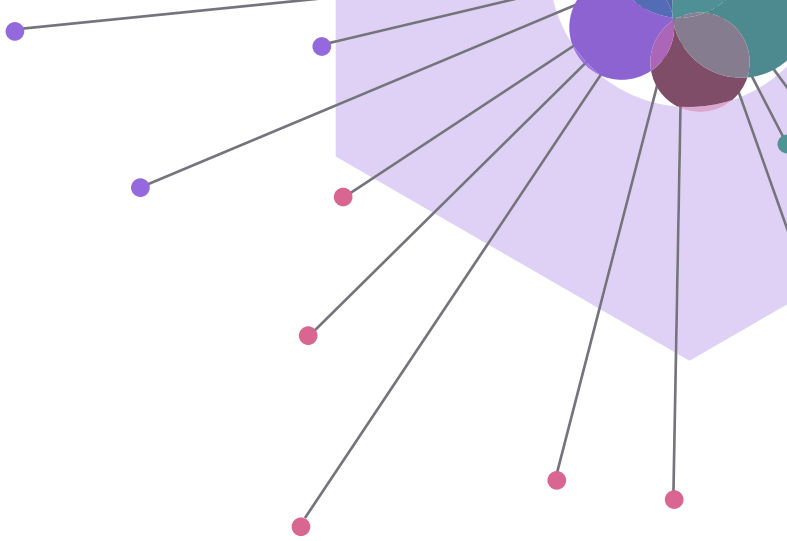
Ponemon INSTITUTE

State of Enterprise Cyber Risk in the Age of AI



Sponsored by Balbix®

2024



contents

Executive Summary

In our State of Enterprise Cyber Risk in the Age of AI, we identified several trends that demonstrated most organizations still lack basic cyber hygiene.

Consider the following alarming statistics from the research: a concerning **10%** of U.S. organizations admitting to never scanning for vulnerabilities and more than half only scanning for vulnerabilities only once a week or less.

Additionally, **65%** of respondents rely on an organizational security plan designed for two or more years. Since new security risks and attack vectors evolve much faster, most processes, plans, and tools must be reviewed and revised often. However, it isn't all doom and gloom. AI is revolutionizing business and has the potential to significantly improve cybersecurity outcomes. Many already have plans to use integrated AI in cyber tools, especially for inferencing, data analysis, and GenAI conversational systems.

Like two sides to a coin, organizations must also prepare for vulnerabilities, errors, and biases AI can introduce through generative AI code, but right now, the pros outweigh the cons.

This report provides insights into the current state of enterprise cyber risk and the role of AI in it. We hope you find them useful in shaping your cyber risk plans for the rest of the year.

About the Ponemon Institute research sponsored by Balbix
This report, independently conducted by Ponemon Institute and sponsored by Balbix, examines how organizations identify the state of cyber risk amidst the rapid proliferation of AI-powered cyber attacks and the rising adoption of AI. Ponemon Institute surveyed 632 U.S. cybersecurity professionals involved in their organization's cyber risk management.

At a Glance

2 out of 3

organizations want to use AI to prioritize threats and vulnerabilities

Operational vs. Communication Challenges

OPERATIONAL

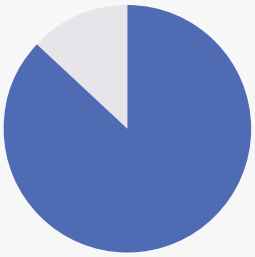
54%

of respondents say unpatched vulnerabilities are the most significant concern

49%

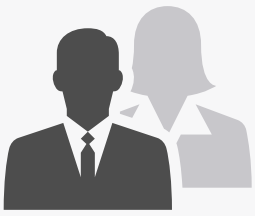
of respondents say they scan for vulnerabilities once a week or less frequently

COMMUNICATION



87%

of CISOs or CSOs have not defined cyber risk metrics



>50%

of senior management is uninterested in cybersecurity or finds metrics unengaging

INSIGHT 1

Vulnerabilities, Misconfigurations, and User Errors Are Top Concerns

Unpatched systems and software are leading the race of top cyber risk concerns. **54%** of survey respondents are grappling with the persistent issue of unpatched vulnerabilities.

Despite recognizing the criticality of addressing these exposures, many lack the resources or desire to conduct frequent scans. The National Vulnerability Database (NVD) receives hundreds of vulnerabilities daily. This gap in proactive security measures leaves enterprises exposed to potential exploits, underscoring a fundamental weakness in current cyber risk management practices.

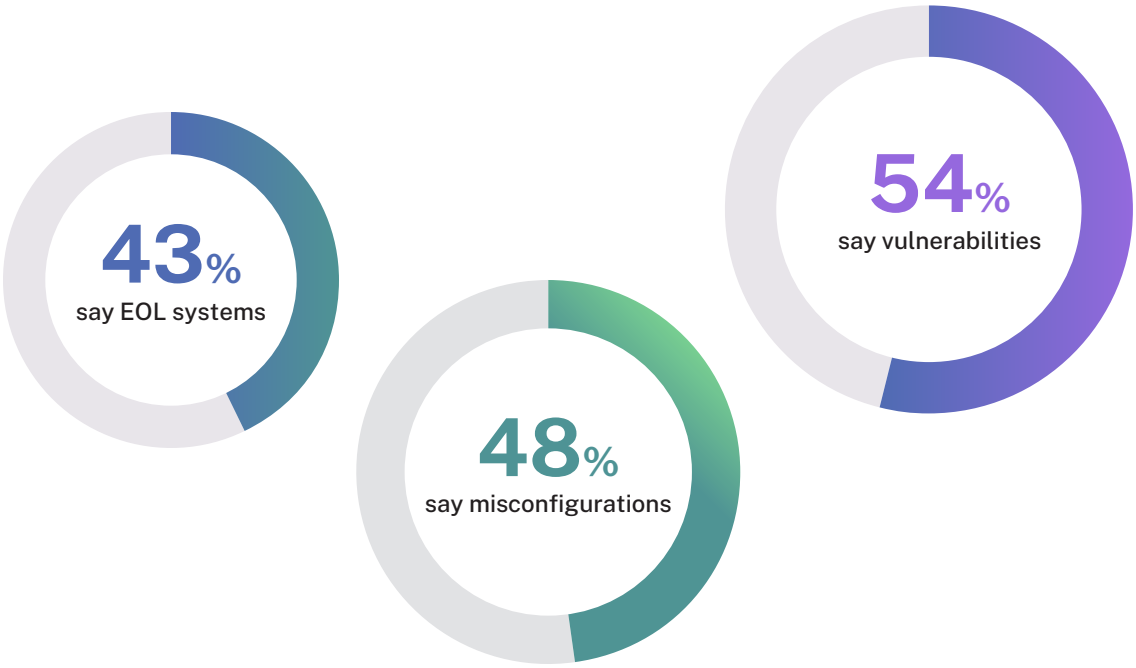
Furthermore, **48%** of respondents are concerned about misconfigurations, and **43%** are worried about End-of-Life (EOL) systems. In 2024, if defenders have to worry about EOL systems, we are far from ready to tackle AI-powered attacks.

Startlingly, **49%** of respondents claim to scan for vulnerabilities once a week or less frequently.

Based on many industry reports, certain vulnerabilities can be exploited within days.

The lack of adequate resources and frequent scanning practices highlights a critical vulnerability in many organizations' cybersecurity strategies.

Top Cyber Risk Concerns: Unpatched Vulnerabilities and EOL Systems



49%
of respondents say they scan for vulnerabilities once a week or less frequently

Recommended Next Steps

Organizations must invest in better tools and frameworks to reduce these low-hanging fruit, such as EOL. Scan-based approaches are outdated, and enterprises should look for continuous monitoring and patch management. Other techniques, such as risk-based prioritization, can help.

Dedicated staff should focus on managing vulnerabilities and receive continuous training. These efforts, along with regular testing and intelligence on threats, are crucial to a comprehensive cybersecurity strategy.

Also, raising employee awareness through regular training can mitigate human-error risks. These different methods quickly find and fix vulnerabilities, protecting against possible attacks.

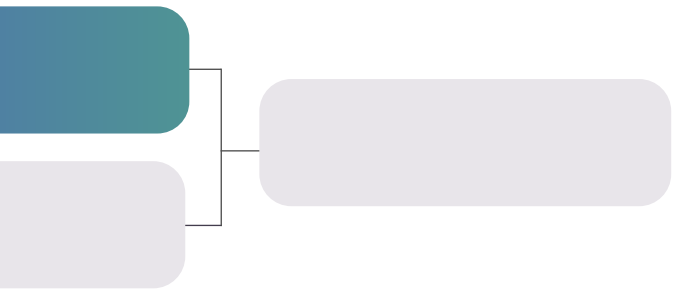
INSIGHT 2

Most Organizations Use Inadequate Prioritization Strategies for VM

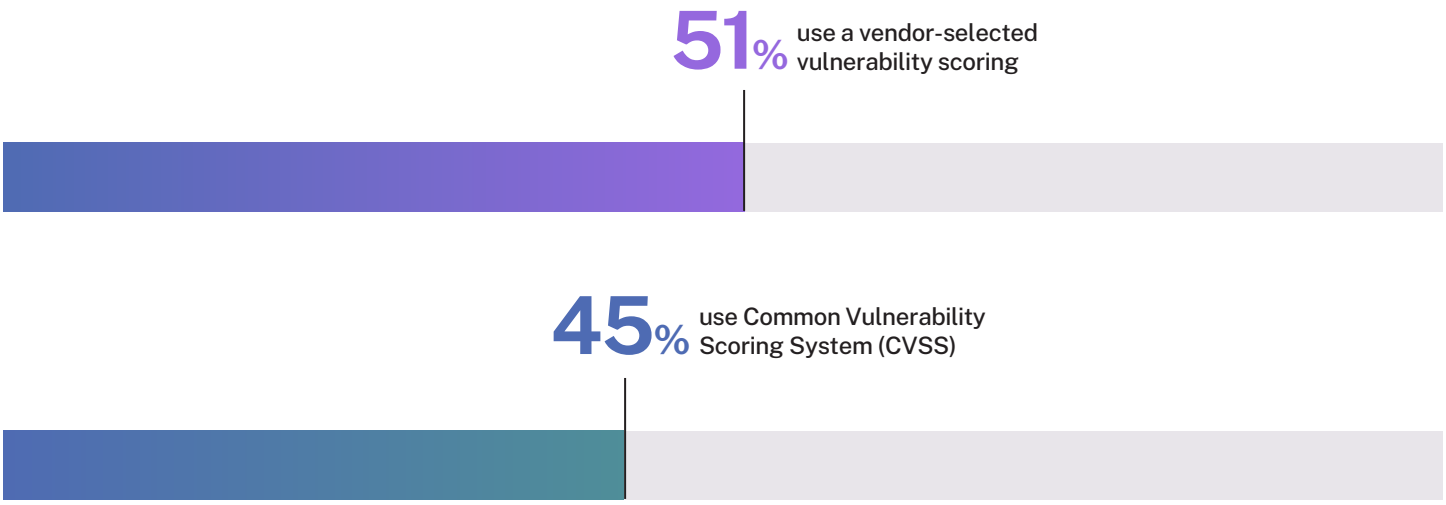
Many organizations prioritize vulnerabilities based on severity or criticality without considering the asset context. **51%** of respondents say their organizations rely on the on vendor-selected vulnerability scoring, and **45%** say Common Vulnerability Scoring System (CVSS) is used.

These frameworks overlook asset exposure and fail to account for adequate security controls. For effective risk management, organizations need to develop better ways to prioritize what needs attention. This involves assessing the severity and potential impact on specific assets, the likelihood of exploitation, and existing controls. By integrating factors like business criticality, asset value, and threat intelligence, organizations can better align their efforts with their actual risk exposure.

Incorporating contextual factors into vulnerability management enhances the ability to address unique risks, ultimately improving overall cybersecurity posture.



Inadequate Vulnerability Prioritization Strategies: Reliance on Vendor Scores and CVSS



Recommended Next Steps

Organizations should move beyond generic scoring systems to improve prioritization by incorporating environmental context into vulnerability assessments. This involves evaluating the potential impact, likelihood of exploitation, and existing controls specific to their assets and operations. By adopting risk-based prioritization that considers business criticality, asset value, and threat intelligence, organizations can ensure the most significant risks are addressed first.

INSIGHT 3

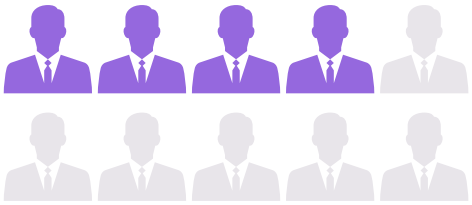
Lack of Senior Executive Engagement De-emphasizes Cyber Risk

A significant area of improvement in current cyber risk programs is the need for greater engagement from senior executives and management outside the security function. The technical nature of reporting and a general lack of understanding of the impact of cybersecurity metrics contribute to this disengagement. Survey findings reveal that **40%** of executives are not briefed regularly on cybersecurity. **54%** of senior management is uninterested in cybersecurity or finds metrics unengaging.

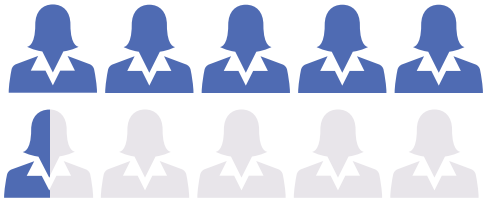
Furthermore, only **13%** of respondents say the CISO or CSO has overall responsibility for defining metrics in its cybersecurity risk management strategy. A challenge to communicating cybersecurity metrics is that preparing reports to communicate cybersecurity metrics to senior management takes too much time (**29%**). Bridging this gap requires simplifying communication and demonstrating the business relevance of cybersecurity efforts.

By making metrics more accessible and relevant to business outcomes and streamlining the reporting process, organizations can foster greater interest and proactive involvement from senior management, ultimately enhancing their overall cyber resilience.

Challenges in Reporting Cyber Risk Metrics to Senior Management



40% of execs not briefed on cybersecurity



54% of senior management is uninterested in cybersecurity or finds metrics unengaging.

13% of respondents say CISOs are overall responsible for defining metrics

29% 29% of respondents say it takes too much time to prepare reports

Recommended Next Steps

To improve communications and reporting to executive staff, organizations should simplify cybersecurity metrics and align them with business outcomes. This can be achieved by translating technical data into clear, impactful insights highlighting potential business implications for security risks.

Regular, concise briefings should be scheduled to keep executives informed and engaged.

A CISO should use KPIs that translate cyber risk into concrete financial terms. This allows senior executives to clearly understand the potential cost of cyber risks and impact on the business.

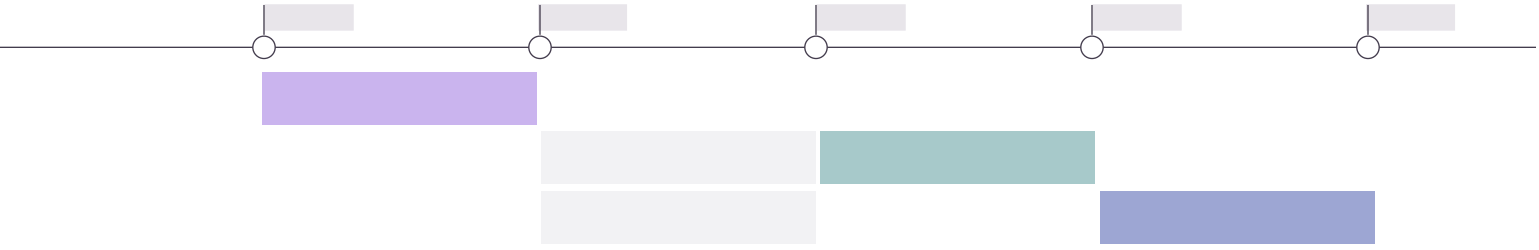
INSIGHT 4

Most Security Teams Use Impact-Related Metrics to Determine theCost of a Cyberattack or Other Security Incident

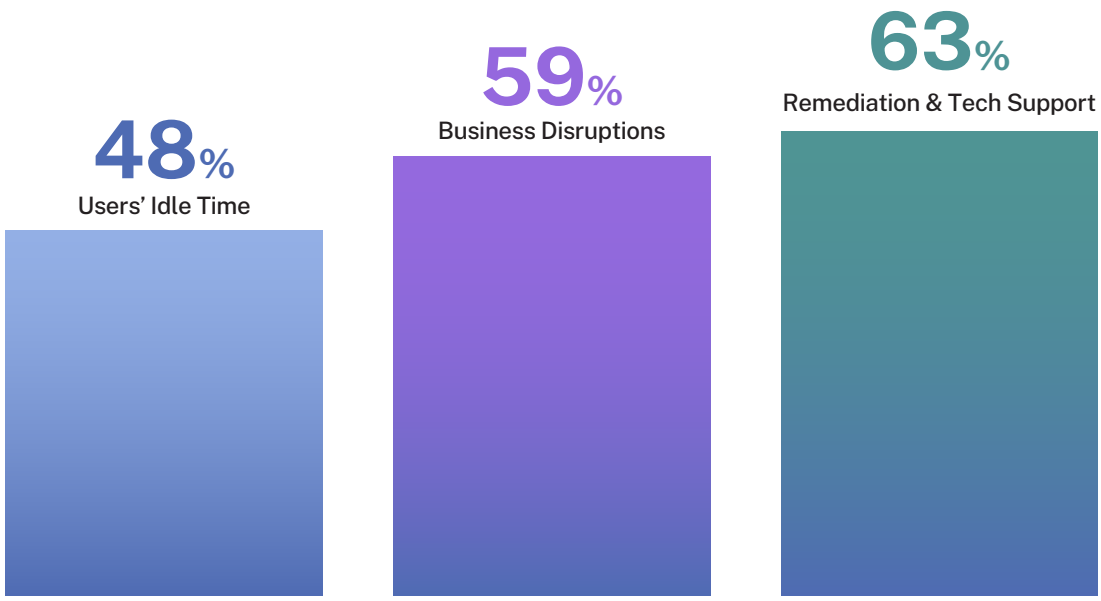
Organizations are shifting focus from traditional metrics like Mean Time to Repair (MTTR) and Mean Time to Detect (MTTD) to impact-related metrics. This provides an opportunity to align cyber risk with business goals by emphasizing the impact of disruptions on users and operations, however, many companies find such measurements difficult.

59% of respondents measure users' idle time and lost productivity because of downtime or system performance delays to determine the cost of a cyberattack or other security incident. **48%** measure disruptions to normal business operations because of system availability and **63%** measure remediation and technical support activities including forensic investigations, incident response activities, help desk responses, and delivery of services to customers.

Of these respondents, only **35%** have adopted a way to quantify risk in financial terms, indicating that more work is needed to realize its full potential.



Top Focuses When Measuring the Cost of Cyber Incidents



Recommended Next Steps

To advance the shift towards impact-related metrics, organizations should adopt Cyber Risk Quantification (CRQ) methods to quantify and effectively communicate the financial impact of cyber risks. By integrating these metrics into executive reporting, organizations can better prioritize security investments, justify expenditures, and enhance overall resilience by making informed business decisions. This approach ensures that cybersecurity efforts are aligned with business goals, ultimately improving the organization's ability to manage and mitigate risks.

INSIGHT 5

ChatGPT and Copilot Adoption Outpaces Security Team Ability to Manage Their Usage

The rapid adoption of AI tools like ChatGPT and Copilot is outstripping the ability of security teams to effectively monitor and manage their use, posing a significant threat.

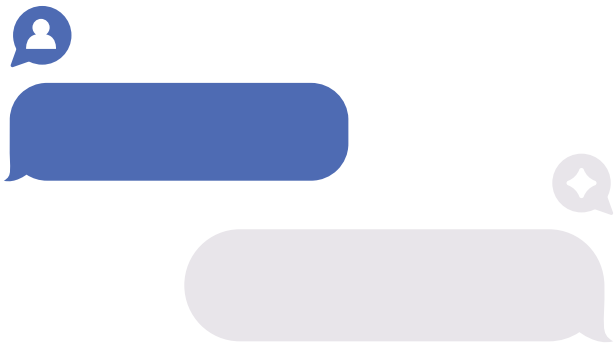
This disparity arises from the lack of established best practices and oversight mechanisms, which can lead to unintentional data breaches or misuse of these powerful AI tools.

Security teams increasingly see AI as a source of new risks, with **47%** of survey respondents expressing concerns about vulnerabilities due to AI-generated code.

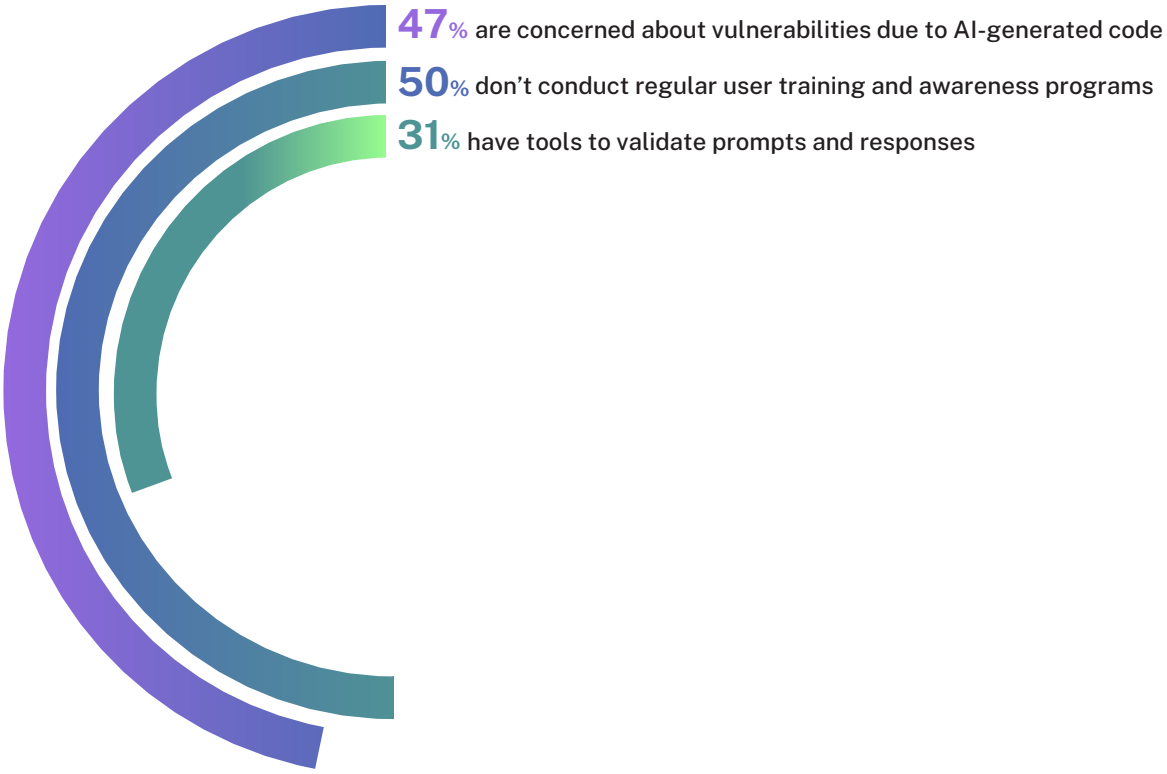
54% of respondents say their organizations have adopted AI either fully or partially.

Despite these concerns, only **50%** of survey respondents conduct regular user training and awareness programs about the security implications of AI.

Furthermore, only **31%** of organizations use tools to validate AI prompts and their responses, leaving a substantial gap in security.



Tools and Techniques to Manage AI Internally



Recommended Next Steps

Rather than taking heavy-handed approaches to ChatGPT and Copilot usage, organizations should start by educating their users on the business risks of using ChatGPT and best practices for preventing sensitive information from entering these tools.

Tools that validate AI prompts and responses can be deployed, but as we have seen with other management tools, such as mobile device management (MDM), users will find other ways to bypass such controls.

Ensure that continuous training, education, and assessment of AI tools are more effective.

INSIGHT 6

Most Cyber Professionals Feel Unprepared for AI-Powered Attacks

Many organizations feel unprepared for potential AI-powered attacks, highlighting a significant threat in the evolving cyber landscape. Only **37%** of respondents rate the ability to protect assets from a breach against AI-powered attacks as high or very high, underscoring the urgency of this issue.

AI-powered attacks can adapt and evolve rapidly, making detection and mitigation difficult for unprepared security teams. Additionally, coupled with a number of open and outstanding vulnerabilities, many security teams may not have all the resources to tackle fast changing threats.

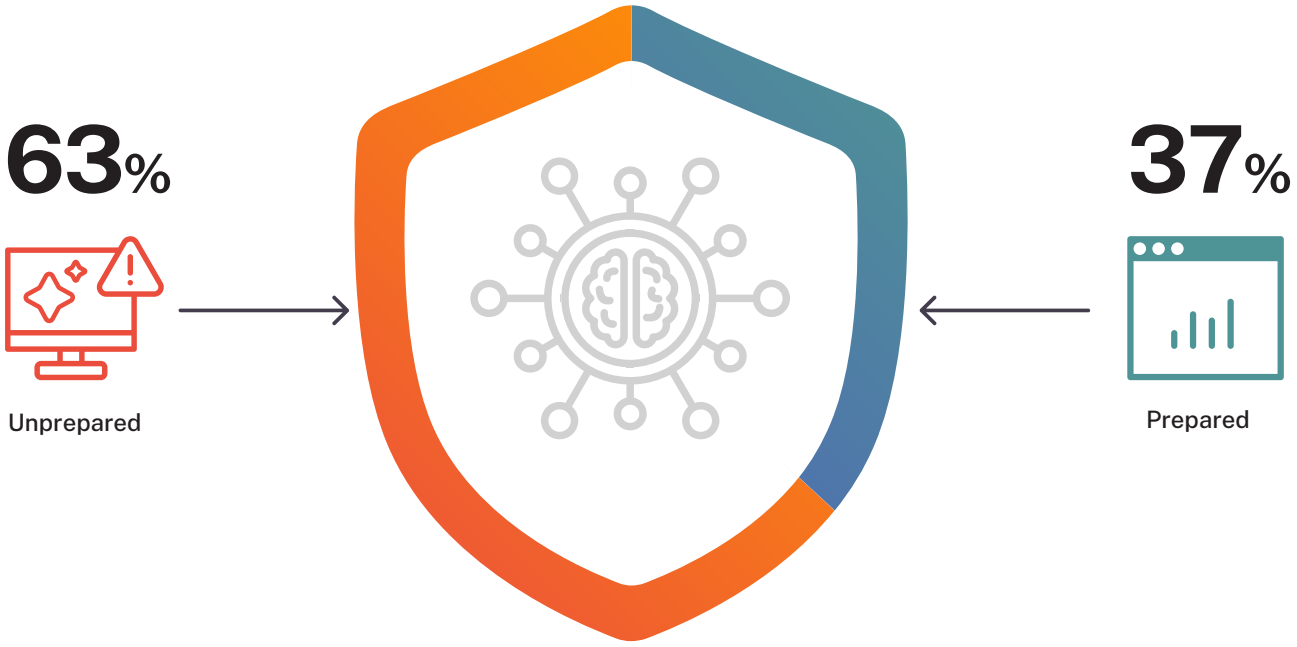
This preparedness gap increases the risk of successful breaches and heightens the potential impact for organizations.

Recent Breach Examples

An AI-powered phishing attack in 2023 targeted a large financial services firm during its annual benefits enrollment period. The attacker posed as the Benefits Administration department, sending polished, error-free emails with malware-laden attachments. The attacker exploited the urgency of the enrollment process to steal employee credentials and sensitive information.

In January 2023, hackers used AI to launch a ransomware attack on Yum! Brands, compromising corporate and employee data. The AI automated decisions on which data to target, forcing Yum! to close nearly 300 UK branches for weeks, highlighting the increased damage potential of AI-powered cyberattacks.

Readiness for AI-powered Cyber Attacks



Recommended Next Steps

Enterprises must invest in AI-powered defenses and training to better prepare for AI-powered attacks. Security teams should receive specialized training to enhance their understanding and capabilities in handling AI-powered threats.

Additionally, organizations should focus on regularly updating their threat intelligence to stay ahead of malicious actors. This proactive approach involves continuously monitoring the threat landscape for new AI techniques and adapting defenses accordingly.

By prioritizing these investments, training and updates, organizations can significantly improve their preparedness and resilience against the growing menace of AI-powered cyberattacks.

INSIGHT 7

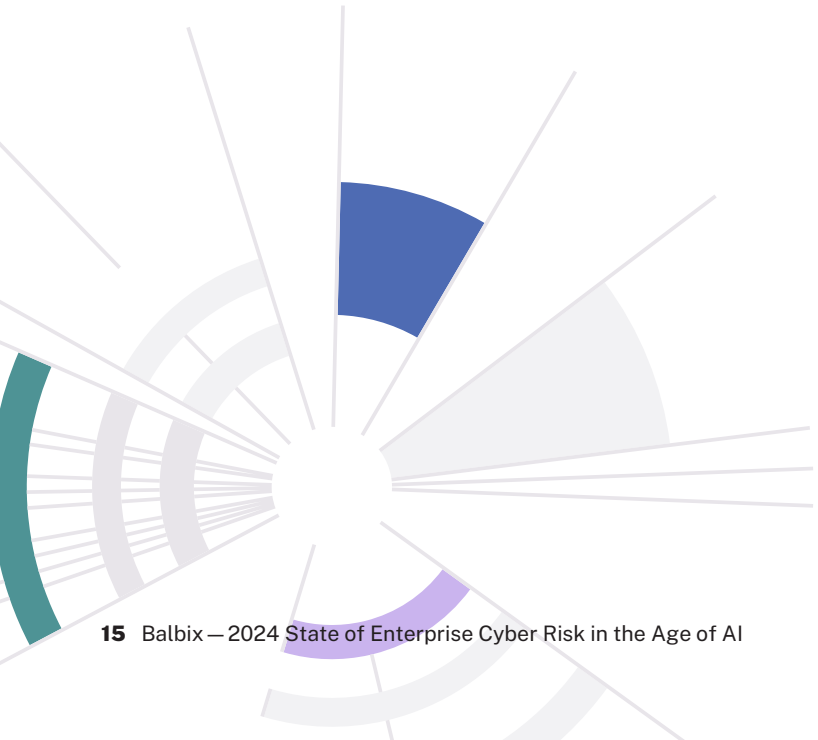
AI Is a Tool That Can Help Bridge The Cybersecurity Skills Gap

AI offers significant potential as a tool to address the cybersecurity skills gap. Embracing AI could be a game-changer in enhancing enterprise cybersecurity.

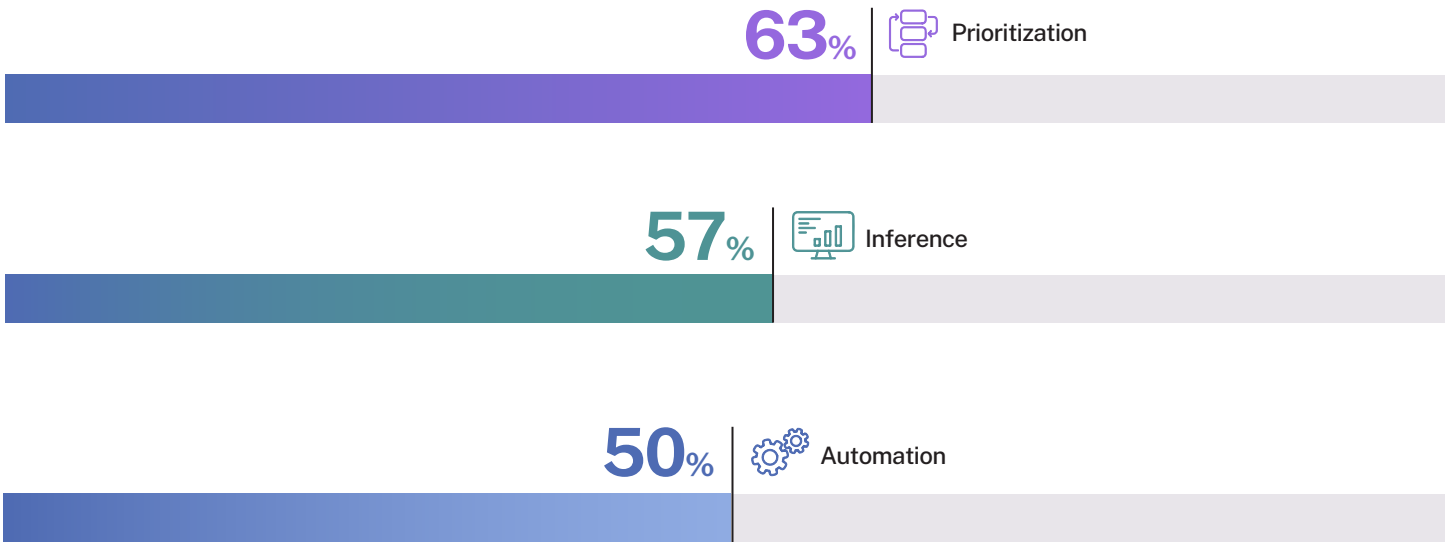
Survey findings for the **54%** percent of respondents that have fully or partially adopted AI highlight that **63%** of respondents want to use AI to prioritize threats and vulnerabilities. Additionally, **57%** of respondents consider inference to be the best functionality of AI.

This indicates a strong preference for AI's ability to analyze data and draw meaningful conclusions, enhancing decision-making processes.

50% of respondents say AI improves the ability to manage threats, alerts, and vulnerabilities, reflecting the technology's potential to streamline these crucial aspects of cybersecurity. The integration of AI in cybersecurity addresses the skills gap, optimizes threat management, and enhances training programs, making it an indispensable tool for modern enterprises.



AI's Role in Improving Threat Management and Alert Handling



Recommended Next Steps

Organizations should invest in advanced AI-powered tools that automate routine tasks and provide comprehensive threat analytics to bridge cybersecurity skills gaps. Integrating these tools into cybersecurity frameworks can streamline operations and free up security teams to focus on more complex threats. Regular training and upskilling security staff to use AI technologies are also crucial.

Additionally, organizations should implement AI for prioritizing threats and vulnerabilities, ensuring that critical issues are addressed promptly.

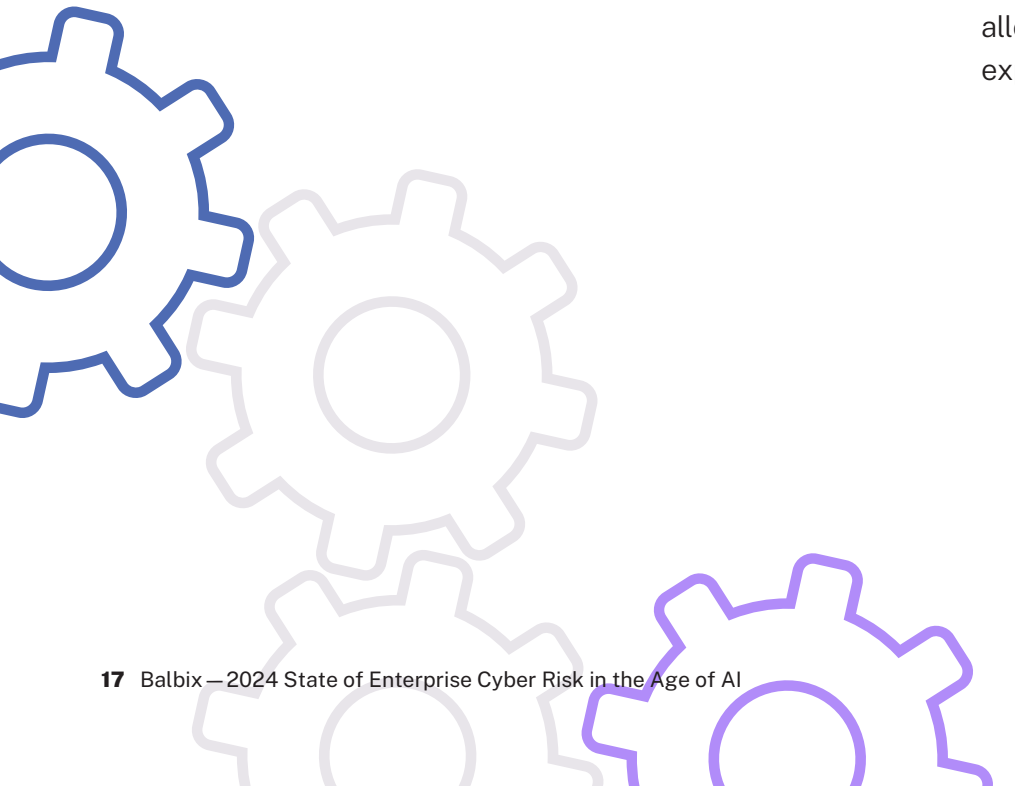
Finally, incorporating AI into employee training and awareness programs, especially for those with access to sensitive data, can further enhance the overall security posture.

INSIGHT 8

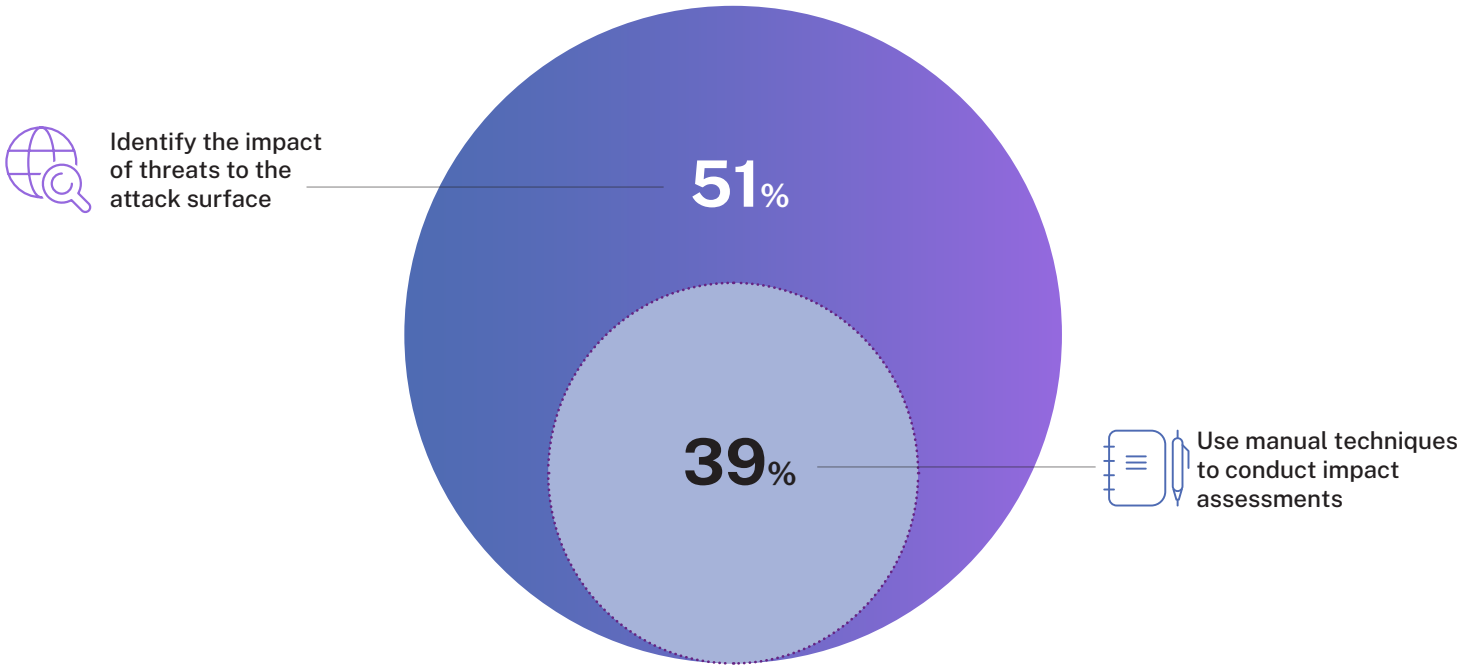
Many Organizations Have Not Embraced Automation to Address Resource Constraints

51% of respondents say their organizations identify the impact of threats to the attack surface. Of these respondents, **39%** say their organizations continue to rely on manual techniques for cyber hygiene, an apparent weakness that significantly undermines their cybersecurity posture. Manual processes are inherently labor-intensive, requiring substantial human effort and time to identify, assess, and mitigate potential security threats. This reliance on manual labor increases overhead costs and diverts valuable resources that could be utilized more effectively elsewhere.

Moreover, manual processes are prone to human error, which can result in overlooked vulnerabilities or misconfigured systems. These errors create gaps in the security framework, making the organization more susceptible to cyberattacks. The inefficiency of manual techniques also means that responses to threats are often delayed, allowing malicious actors more time to exploit vulnerabilities.



Manual vs. Automated Techniques in Cybersecurity Operations



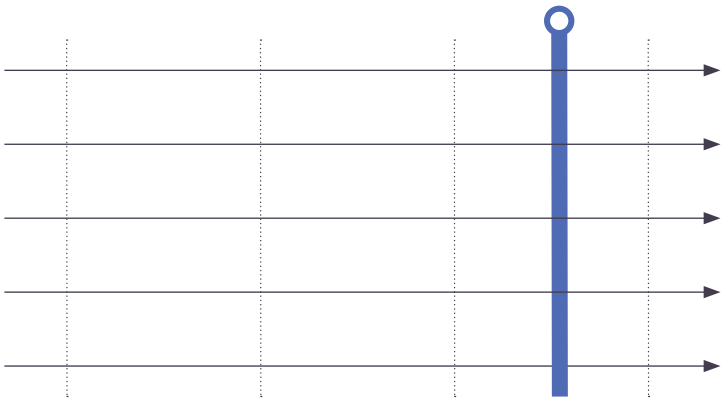
Recommended Next Steps

Organizations should implement automated tools and methods to mitigate risks associated with relying on manual cyber hygiene to enhance accuracy and efficiency. Automated solutions can systematically identify and address vulnerabilities faster than manual processes, reducing the risk of human error. Additionally, organizations should embrace risk-based prioritization of vulnerabilities for remediation. This approach ensures that the most critical and impactful vulnerabilities are addressed first, reducing the time and resources needed for remediation. Organizations can improve their cybersecurity posture by focusing on the most significant threats, ensuring a more robust and resilient defense against potential cyberattacks.

INSIGHT 9

A Majority of Organizations Trust Established Cybersecurity Frameworks

The good news is that organizations rely on established cybersecurity frameworks such as NIST and MITRE ATT&CK to guide their security programs. This trust in well-respected frameworks is a significant strength, providing a solid foundation for building robust cybersecurity practices. These frameworks offer comprehensive guidelines and best practices that help organizations structure their defense strategies effectively, ensuring a systematic and thorough approach to managing cyber risks.

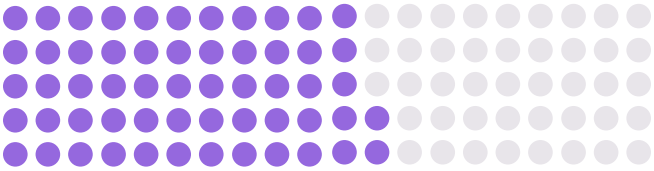


Survey data indicates that **57%** of survey respondents base their cyber risk management on the NIST Cybersecurity Framework (CSF) to prioritize cyber risk. NIST CSF is highly regarded for its comprehensive approach, covering all aspects of cybersecurity, from identifying and protecting against threats to detecting, responding to, and recovering from incidents. By following NIST CSF, organizations ensure they adhere to best practices recognized and recommended by industry experts.

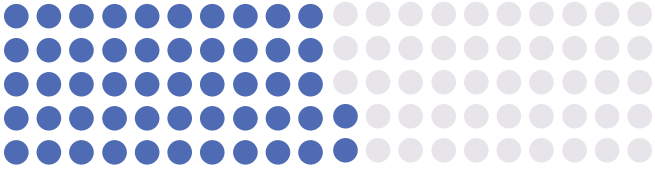
Additionally, **52%** of respondents use the MITRE ATT&CK framework to prioritize risks and vulnerabilities. MITRE ATT&CK provides a detailed matrix of tactics and techniques used by adversaries, enabling organizations to better understand potential threats and how to defend against them. By leveraging this framework, organizations can prioritize their cybersecurity efforts based on the most relevant and pressing threats, ensuring their resources are used efficiently and effectively.

The Most Trusted Cybersecurity Frameworks

57% NIST



52% MITRE | ATT&CK®



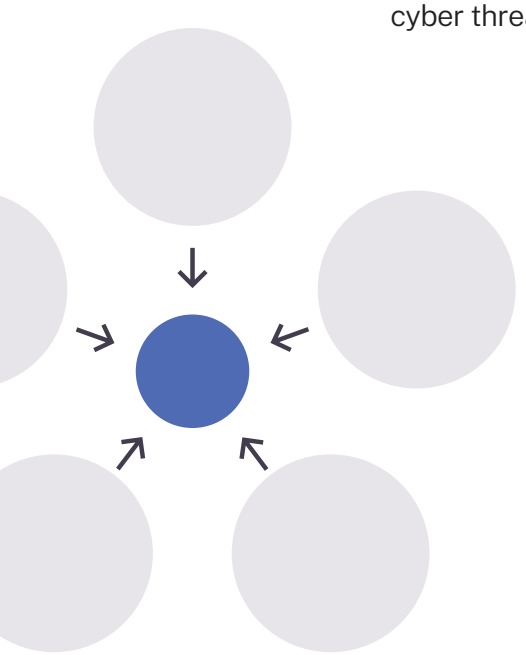
Recommended Next Steps

Organizations should continue to use and expand the usage of NIST and MITRE ATT&CK frameworks. Regular training sessions will ensure that all security team members understand how to effectively implement and leverage these frameworks. Additionally, integrating these frameworks into the organization's cybersecurity policies, procedures, and tools will ensure consistent application.

INSIGHT 10

Many Organizations Have Obsolete Cyber Risk Strategies

Organizations often plan their cyber risk strategies too far in advance, which can significantly threaten their overall security posture. In a rapidly evolving environment where cyber threats and exposures are constantly changing, long-term plans can quickly become obsolete, exposing organizations to new types of attacks that were not anticipated. Survey findings indicate that **65%** of organizations develop cyber strategies for two or more years. While this approach might appear thorough and proactive, it frequently fails to account for the dynamic nature of the cyber threat landscape.



The primary issue with long-term planning is its need for more flexibility. As new vulnerabilities and attack vectors emerge, a rigid strategy may not swiftly accommodate these changes, resulting in security gaps. The static nature of long-term plans can lead to a false sense of security, where organizations believe they are protected but are vulnerable to the latest threats. This disconnect can be particularly dangerous as it may delay the implementation of necessary security measures until the following scheduled review or strategy update.

Furthermore, focusing on long-term strategies can divert attention from immediate threats and critical vulnerabilities that need urgent remediation. This misalignment can cause organizations to overlook or deprioritize currently exploitable risks, increasing the likelihood of successful attacks. The cybersecurity landscape demands a more dynamic and responsive approach that adapts to cyber adversaries' ever-changing tactics.

The Prevalence of Outdated Cyber Risk Strategies Among Organizations

Cyber strategy is for two or more years

65%

Recommended Next Steps

Organizations should adopt more agile and adaptive planning processes for timely adjustments as new threats emerge. The Cybersecurity and Infrastructure Security Agency (CISA) recommends focusing on immediate threats to maintain a more resilient security posture. This involves prioritizing critical and exploitable vulnerabilities ensuring that the most pressing risks are addressed promptly.

Organizations can better respond to the ever-changing threat landscape by implementing a flexible, adaptive approach. This involves continuously monitoring the environment, updating risk assessments, and revising strategies as necessary to address new vulnerabilities and threats. Adopting this mindset helps mitigate immediate risks and ensures the organization remains prepared for future challenges. Organizations can enhance their cybersecurity resilience by focusing on critical and exploitable vulnerabilities and staying agile.

Conclusion

Two-thirds of organizations are interested in using AI to prevent vulnerabilities, presenting significant opportunities and challenges for enterprises. The data report sheds light on the critical state of enterprise cyber risk, providing important insights that need immediate attention and action.

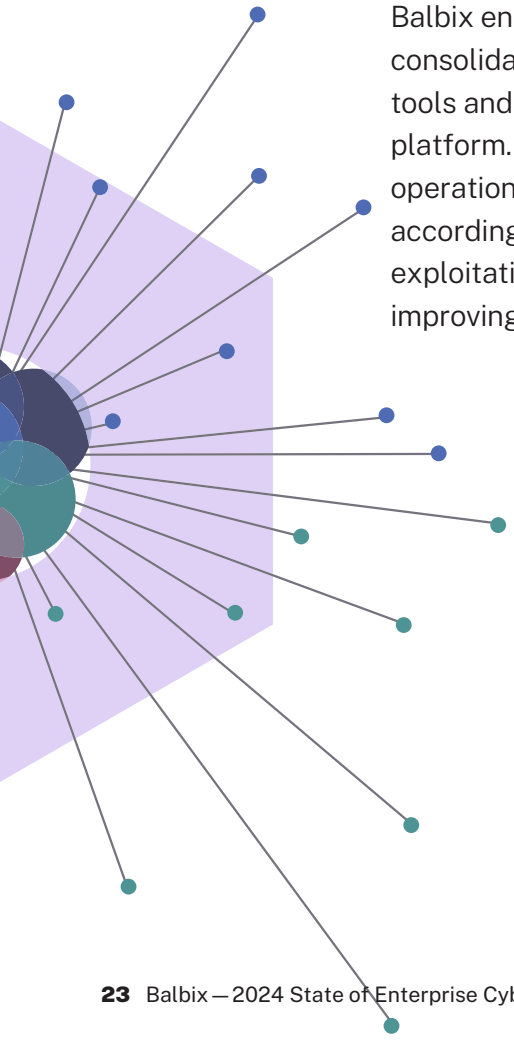
Let's discuss two crucial actions Balbix can help organizations take:

1

Risk and Exposure Management
Balbix enables security teams to consolidate vulnerabilities from various tools and environments into a single platform. Additionally, security operations can prioritize vulnerabilities according to their likelihood of exploitation and business impact, improving cyber hygiene.

2

Cyber Risk Quantification
Balbix provides security leaders and executives with a quantified view of risk in monetary terms. Furthermore, CRQ enables them to understand the ROI of security tools and programs, improving executive engagement and decision-making.



Final Thoughts

The state of enterprise cyber risk in the age of AI is complex and multifaceted, characterized by an interplay of strengths, weaknesses, opportunities, and threats. By strategically addressing these elements, organizations can enhance their cyber resilience and better prepare for the dynamic challenges of AI-powered technologies. Proactive measures, continuous improvement, and robust engagement across all levels of the organization are essential for navigating this challenging landscape and securing a safer digital future.

Request a demo to learn more about how Balbix can help you improve your security.