TECHNOLOGY ASSESSMENT GUIDE

Sponsored by: Trend Micro

Cyber-risk equates to business risk; risky exposures extend beyond traditional vulnerabilities to include misconfigurations, outdated software, and overlooked assets. Addressing these issues is not merely a technical challenge but a fundamental component of organizational resilience and agility that necessitates a platform to solve.

Across the Entire Attack Surface: Risk Requires a Platform

August 2024

Written by: Frank Dickson, Group Vice President, Security and Trust, and Michelle Abraham, Senior Research Director, Security and Trust

AT A GLANCE

KEY TAKEAWAYS

- Cyber-risk is equal to business risk.
- AI and GenAI introduce potential net-new risks such as data or model poisoning, model exfiltration, and prompt injection.
- Organizations should focus on preventing malicious or unintended access, preferably at the early initial access stage.
- Platforms consolidate point products to provide a reality weighted view of risk.

Introduction

Our modern reality has fundamentally changed the approach to security, as IT has evolved from a cost center to a profit center. Even traditional organizations are driving revenue from their digital products and services. This IT profit center movement is accelerating as AI is injected at all levels of the IT stack. Regrettably, many large organizations find themselves battling the adoption of AI technologies in a piecemeal manner, with individual business units making their own determinations about where and how AI and GenAI technologies should be embedded into their department.

As a result, an organization's management at all levels also needs to view cybersecurity not as a cost center but as a way to quickly and confidently move the business forward rather than slowing it down. Companies need to view risk exposure management as a step toward managing their overall enterprise risk and becoming more cyber-resilient. Cyber-risk is equal to business risk. Managing risk exposure with a proactive cybersecurity platform and tools is a required mindset, not a single "magic bullet" technology.

The use of the word "exposure" instead of "vulnerability" is purposeful. Exposures are not solely vulnerabilities that are found through scans that receive a number from a common vulnerabilities and exposures (CVEs) numbering authority. It is necessary to think about all risk factors that present traditional cybersecurity risk. These include misconfigurations and certificate expirations, data controls, identity activity, cloud app behavior, attack intensity, or pressure on the organization, as well as vulnerabilities in physical, open source, and cloud assets. AI and GenAI introduce potential new risks such as data or model poisoning, model exfiltration, and prompt injection. Whether the organization develops its own GenAI large language models (LLMs), licenses LLMs from third parties, or uses GenAI applications developed by others, adversaries may attack the unique risks of each approach.

IDC's expanded view of exposures includes the following:

- Open ports that attackers from outside the organization can access
- End-of-life software because discovered issues are no longer being fixed
- Unsupported/antiquated devices that lack innate protections such as printers or IoT/OT assets
- Forgotten/unused/unauthorized applications, including SaaS applications, because the security team is not paying attention to vulnerability issues in that software, the data that is being stored in and transferred to or shared through that application, or misconfigurations in user access or password policies
- Remote desktop protocol (RDP) open to the internet
- Misconfigurations in cloud access policies
- Unknown domains/subdomains and forgotten subsidiaries
- Data in the cloud that is inadvertently exposed to cloud administrators through improper cryptographic key management
- Sensitive or confidential data that is stored improperly with a "trusted" third party
- Expired certificates because the browser cannot tell whether the website is authentic (When users connect, they cannot be assured that their communications with the website are secure and not through someone in the middle rerouting their traffic.)
- Unknown application programming interfaces (APIs) since APIs are being used to share information between applications (The organization or a third party may create APIs to share information or integrate with partner applications.)
- Insufficiently protected APIs are often the gateway into AI applications (Traditional API protections may not be appropriate for attacks on GenAI applications.)
- Vulnerabilities in the code and applications the organization writes or assembles from open source
- Data exposed through lazy backup practices such as storing information in public folders during routine backup maintenance
- Hardcoded credentials/secrets such as storing API keys where they are accessible to attackers
- External-facing assets and unmanaged devices

Implementation Recommendations

When thinking about risk exposures, organizations should focus on preventing malicious or unintended access, preferably at the early initial access stage. The leveraged impact neuters all subsequent potentially malicious actions that follow, such as the malware incursion or malicious lateral movement using living-off-the-land techniques. During the search and discovery of risk exposures, continuous real-time scanning enables constant discovery and monitoring for the assessment and analysis of the asset and data.

Environments have grown complex with hybrid work, hybrid cloud, ephemeral workloads, and a lack of a traditional perimeter that a firewall can protect, meaning point-in-time data is not good enough. The days of monolithic software applications that undergo biyearly updates on a planned cadence have passed, replaced with CI/CD-fueled microservices software architecture that experiences up to thousands of code drops daily. The code coming from open source as opposed to all internal development only adds to this challenge.

In addition to new types of exposures, the sheer number of CVEs and zero-day vulnerabilities is growing, as they are becoming increasingly identified and weaponized more quickly. Security teams need help to make sense of what is important.

Vulnerability management, attack surface management (ASM), and breach and attack simulation are all components of proactive cybersecurity, but there is a need to think more broadly. Tools are necessary to find assets where agents are not deployed and therefore not protected with vulnerability management, network traffic controls such as CASBs or gateways, or an endpoint protection system. It is impossible to assess the risk to the business of unknown assets, and it is exponentially harder to protect unknown assets that are no longer behind the firewall and open to the internet.

Therefore, cybersecurity asset management, which provides visibility into the internal and internet-facing physical and virtual assets in an organization's environment, is another necessary part of proactive cybersecurity. Visibility into assets is paramount because security, developer, and IT teams cannot manage what they do not know. Part of this is assessing asset criticality from role, applications, and data perspectives. Assets include internal and third-party hardware, software, SaaS, APIs, IP/domain, identities, and cloud. The scope of understanding what assets exist and where they are located is incredibly challenging. Many organizations IDC has spoken to feel they have a handle on observability — the ability to see data and assets as they move throughout the organization or are in use. However, uncovering and managing all data and assets seem like insurmountable tasks.

The cybersecurity asset management system should be synced with the configuration management database for the business context and asset ownership and to ensure both are up to date. The information helps with prioritization and knowing who is responsible for remediation. As the attack surface expands with technological evolution and innovation, other potential risk exposures are left behind, forgotten in assets that may not be widely used or of which the security team is unaware.

Optimization Strategies

Today, many point security products identify and report on these exposures, including ASM, cloud workload protection, application security orchestration and correlation, SaaS security, API security, certificate management, and vulnerability management. The data may come from various types of sensors: passive sensors, network scanners, internet scanners, agents, virtual scanners, secrets scanners, cloud connectors, APIs, and SaaS connectors. Each point product has its own reporting system, assessment process, risk factor weighting, and possible integrations with other products, making it harder, if not impossible, to correlate the data effectively. For operational and commercial reasons, it's become untenable to attempt to manage, report, and mitigate risk in silos. Homogenizing data from a collection of point products further complicates data analysis and analyst workflows.

Ideally, all risk exposures should flow into a singular platform to ensure they can be comprehensively prioritized so the security team can direct their efforts accordingly and ensure it is maximizing cyber-risk reduction across the organization. With a platform approach, the team can assess, measure, and weigh risk exposures based on a singular, homogeneous scoring criteria instead of individual security tools each measuring risk using its own unique and inconsistent method. The risk score is then a comprehensive measure of cyber-risk that can be integrated into the ultimate assessment for executive and board-level reporting — business risk.

Consolidating point products provides a view of risk that when combined with contextual threat intelligence, enables a reality weighted view. For example, a vulnerability that has a known rootkit that is leveraged within a market vertical and geography has a higher risk, all things being equal, than one that does not. Other benefits may include a reduction of agents, simplicity in implementation, volume-based pricing available from a single vendor, and potential tool consolidation because fewer vendors require less time to manage and greater experience outcomes for security analysts.

Worksheet Section

Exposure risk management is within the security team's control, while third-party behaviors are not, though teams can anticipate what might happen. Until an organization understands its active risk exposures, mitigates those it can, and has technology in place to monitor its environment for new risks, it is not controlling the controllables.

With proactive cybersecurity in mind, organizations must consider the suggestions described in Table 1.

TABLE 1: ***Questions to Ask When Assessing Your Risk Posture***

Question	Comment
Can you comprehensively identify and define your IT environment?	Determine what the team needs to protect in assets, data, applications, people, and so forth. Complete visibility is critical to protect the environment. Visibility is binary, you either have it or you do not.
Do you understand the criticality of assets?	Understand what is critical/sensitive and where the organization is willing to accept risk. Know the fallout of being open to attack. Discovery and asset classification are the foundation of a zero trust architecture because security needs information about the asset to apply a trusted access policy. Ensure you have proper context around the assets, including what it does, what is running on it, who can access it, what is connected to it, and what is externally exposed.
What is the timeliness of your scans?	Continuous scanning is required since attackers are not just operating on a quarterly basis, and the organization needs to find and fix exposures before attackers discover them.
How many exposure scoring systems do you have?	Use a centralized risk console to get a holistic view of risk exposures. This gives an organization a better understanding of risk with data in one place, all scored the same way. Performing manual correlation slows down the flow of information. Part of any good solution will be the deduplication of the data from the many tools being used. Look across assets to understand the normal configuration and identity for the asset so that items that are outside of the norm bubble are noticeable.

Can you prioritize based on risk?	Organizations must know: • What is the current posture? • How did the organization assess and score the posture, including the meaning of the score? • How does the organization's cyber-risk compare with its peers? • What does the organization need to accomplish to improve the score? • What impact will there be to the score if they take an action?
Is risk information shared throughout the organization?	Make sure thinking about risk is everyone's job, not just one department's. Business units may compete to have the lowest risk score. A platform needs dynamic, not static, assessments with unified reporting that can go to the board as well as benchmarks against its own KPIs and those of its peers so the organization can set goals and show improvement over time.
Are your risk metrics clear and transparent?	Boards are not cyberexperts, so present any progress in a defined framework that uses the same metrics and references each reporting cycle. The board will want to know about potential losses that stem from risks. Vulnerability remediation that is incomplete is a risk that should be part of the metrics.
What role does your current solutions play in compliance?	Ensure selected solutions demonstrate compliance with industry standards, regulations, or best practices. Reports and audits of platforms for compliance have to show independence from internal calculations. Identify ways to share risk findings with partners/vendors to make everyone stronger.
What is the "people" impact?	Solutions need to assist in quick remediation, automating whenever possible. Look for security tools that provide guidance on how to fix it, who is responsible for fixing it, and who has ownership of the asset, application, or program to reduce the amount of time an exposure is open. Consider ways to automate the remediation workflow with no-code workflows and playbooks that are part of the security tools.

Source: IDC, 2024

About the Analysts

***Frank Dickson,** Group Vice President, Security and Trust*

Frank Dickson is the group vice president for IDC's Security and Trust research practice. In this role, he leads the team that delivers compelling research in the areas of security services; information and data security; endpoint security; trust; governance, risk, and compliance; identity and digital trust; IoT security; network security; privacy and legal tech; security analytics; and application security and fraud. Topically, he provides thought leadership and guidance for clients on a wide range of security topics, including ransomware and emerging products designed to protect transforming architectures and business models.

***Michelle Abraham,** Senior Research Director, Security and Trust*

Michelle Abraham is research director in IDC's Security and Trust Group responsible for the security information and event management (SIEM) and vulnerability management practice. Ms. Abraham's core research coverage includes SIEM platforms, attack surface management, breach and attack simulation, cybersecurity asset management, and device and application vulnerability management.

MESSAGE FROM THE SPONSOR

About Trend Micro

Stopping adversaries faster and taking control of cyber risk starts with a single platform. With Trend Micro, teams can manage security holistically with comprehensive prevention, detection, and response capabilities powered by AI, leading threat research and global intelligence. The expanding attack surface makes exploitation easier and protection harder, requiring full visibility for effective risk assessment and communication. Security teams need proactive cyber risk discovery and continuous monitoring to reduce vulnerabilities and eliminate breach potential.

Own your attack surface with Trend Vision One. Full lifecycle cyber risk management enables you to proactively fortify your security posture through comprehensive risk assessment, real-time prioritization, and automated mitigation across all asset types while streamlining workflows from start to finish.

Proactive security starts here.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.