Enterprise Strategy Group | Getting to the bigger truth.™

Increasing Cyber-risk is Driving the Need for Attack Path Management

Jon Oltsik, Senior Principal Analyst & ESG Fellow

CONTENTS

Executive Summary

Cyber-risk is on the rise. Most organizations believe that cyber-risk is increasing, driven by sophisticated threats, a growing attack surface, greater business use of IT, and even poor security hygiene. With this growth, cyber-risk management is also becoming more complex, especially as organizations take advantage of digital transformation opportunities and burgeoning services used for cloud-native applications.

Cyber-risk leads directly to cyber-attacks. While organizations use multiple siloed tools and manual processes to address cyber-risk management, adversaries use automated tools to continually scan the attack surface for pedestrian and business-critical vulnerabilities. The result can be classified as a mismatch—two-thirds of organizations have experienced a cyber-attack resulting from an unknown, mismanaged, or poorly managed internet-facing asset. And once cyber-adversaries compromise a system, it's easy for them to move laterally across networks. These incidents include ransomware attacks, data breaches, and regulatory compliance violations.

Organizations need a threat-informed defense. Rather than monitor and measure cyber-risk through siloed/fragmented data or layering on more disconnected defenses, organizations should build their defenses as countermeasures to the tactics, techniques, and procedures (TTPs) used by cyber-adversaries. This includes a deep understanding of all assets, network connections, and business-critical systems, as well as a perspective on how an adversary might proceed through a cyber-kill chain. Attack path management can help organizations gain this perspective as it brings together an attacker's perspective with context about the existing security infrastructure, security controls, and existing defenses. In this way, attack path management can help security teams identify risks, develop strategies for risk mitigation, and improve cyber-risk management programs.

Back to Contents

Compared to Two Years Ago, Cyber-risks Are Increasing

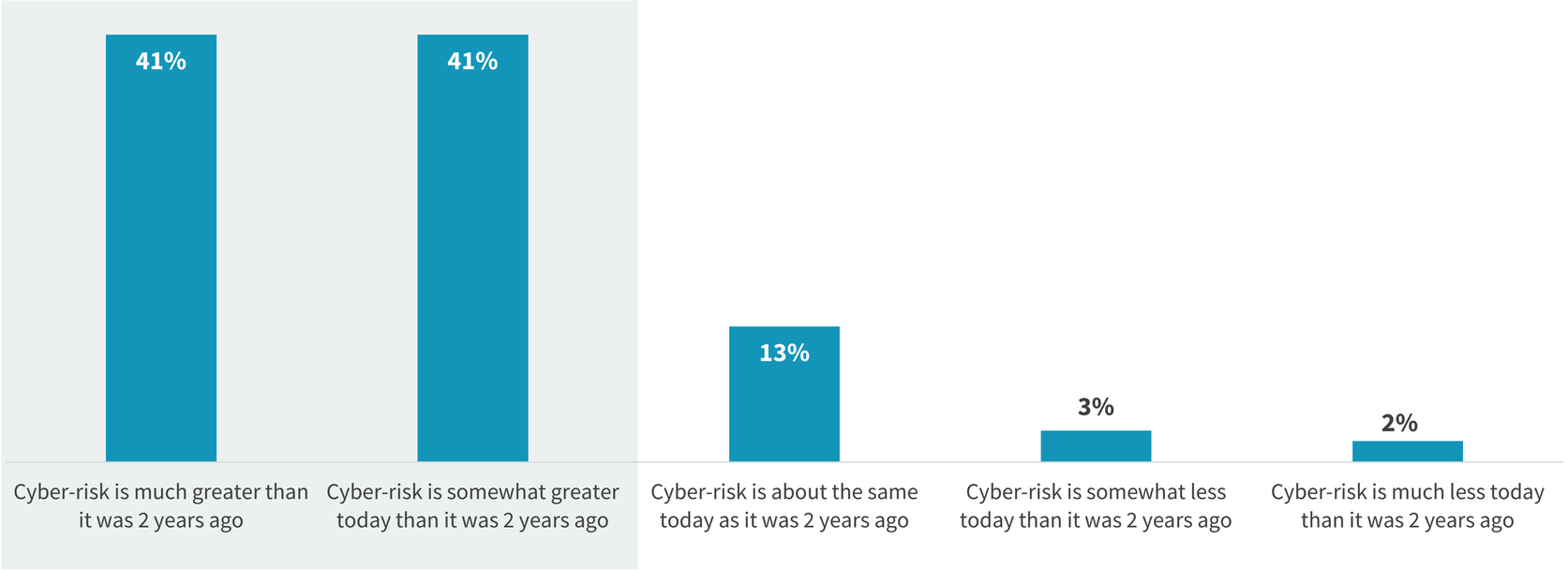
According to ESG research, 82% of organizations believe that cyber-risk has increased over the past two years. This increase is due to factors such as an increase in cyber-threats, greater dependence on IT to fulfill its business mission, and an increase in the number of assets on the attack surface.

Recognizing this trend, executives and corporate boards are pressuring CISOs to improve cyber-risk mitigation—but there's a problem. Many organizations lack the right level of risk context. In other words, they don't understand whether increasing exposures places their critical assets at risk. This situation poses a real conundrum for CISOs since they can't communicate an accurate cyber-risk status to business managers, and they aren't sure how to prioritize investments for risk mitigation.

82%

of organizations believe that cyber-risk **has increased over the past two years.**

How organizations characterize cyber-risk today

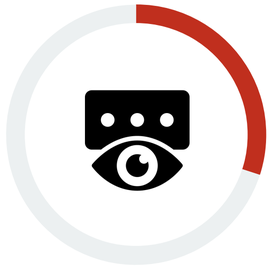


Source: ESG Research Report, *Cybersecurity in the C-Suite and Boardroom,* February 2021.

Back to Contents

> **Innocent cloud management mistakes can easily turn into major cyber-attacks and data breaches.”**

Issues associated with misconfiguration of a cloud application or service



Default or no password for access to management consoles

30%

Externally facing **server workloads**

27%

Overly permissive service accounts

25%

Overly permissive user accounts

25%

Organizations Have Detected Multiple Types of Cloud Application Misconfigurations

The global pandemic accelerated cloud workload proliferation and cloud-native applications. While cloud computing has introduced a degree of business and software development flexibility, it also greatly expanded the attack surface and associated cyber-risks. In fact, cloud misconfigurations are common, including default or no passwords for management console access, externally facing workloads, and overly permissive service and user accounts.

Attackers recognize and take advantage of these growing trends, using automated scanning tools to look for vulnerable accounts and administrator credentials. And once attackers gain access, they seek to exploit not just one, but a series of misconfigurations, making understanding how a chain of misconfigurations represents an attack path critical to reducing cyber risk. Innocent cloud management mistakes can easily turn into major cyber-attacks and data breaches.

Source: ESG Research Report, *Maturation of Cloud Native Security*, May 2021.

Back to Contents

Organizations Admit that Attack Surface Vulnerabilities Lead Directly to Cyber-attacks

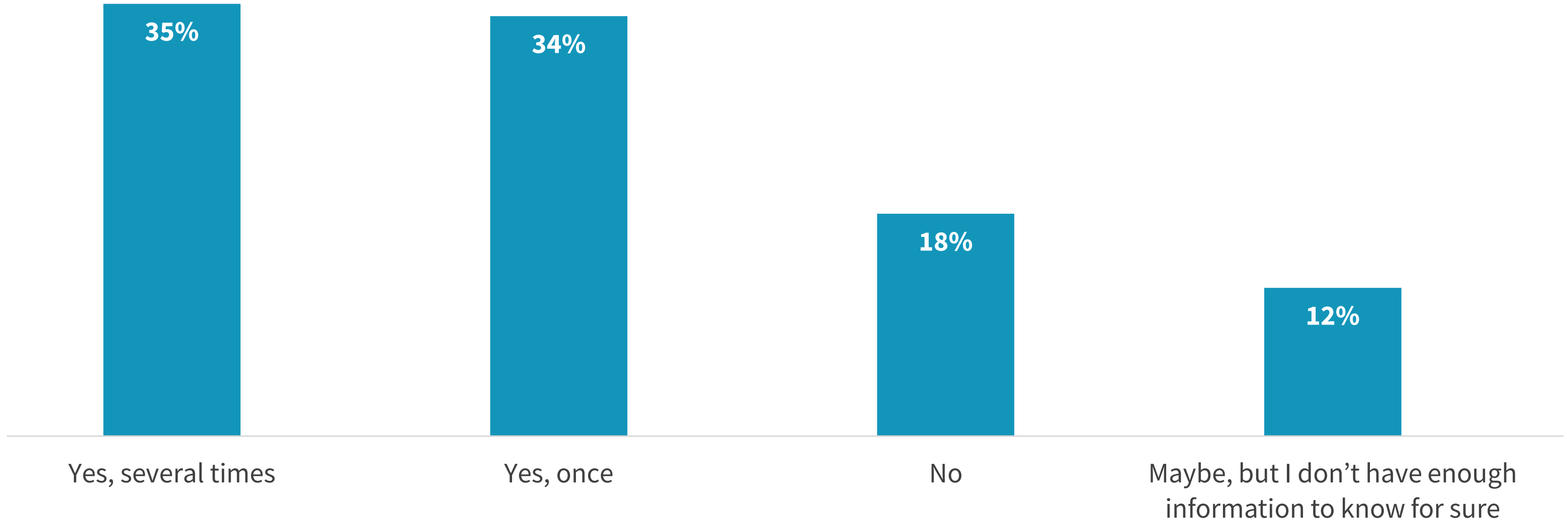
Growing cyber-risks should be setting off alarms in executive suites, corporate boardrooms, and CISO offices for one simple reason—increasing cyber-risk is a gateway to damaging cyber-attacks. For example, ESG research indicates that 67% of organizations claim that their attack surface has grown over the past two years. At the same time, 69% of firms have experienced one or several cyber-attacks, which started through the exploit of an unknown, unmanaged, or poorly managed internet-facing asset.

Like other criminals, cyber-adversaries are opportunistic and look for direct, easy, and unguarded entry points and paths to accomplish their goals. Therefore, security teams must better understand their attack surface and its relationship to network connections and business-critical assets. In fact, the prevalence of vulnerable externally facing assets is such that organizations should assume they will be exploited with an objective of business-critical assets, highlighting the need for attack path management.

67%

of organizations claim that their attack surface **has grown over the past two years.**

Organizations have experienced a cyber-attack where the attack itself started through an exploit of an unknown, unmanaged, or poorly managed internet-facing asset



Source: ESG Research Report, *Security Hygiene and Posture Management,* January 2022.

Back to Contents

Organizations are Attempting to Monitor and Measure Cyber-risk Through Siloed Data with 73% Still Relying on Spreadsheets

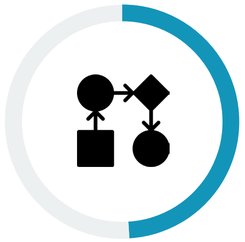
Organizations are relying on siloed fragmented data to monitor and measure cyber-risk

61%

agree that their organization finds it difficult to **prioritize the right actions that can have the biggest impact on risk reduction.**

57%

of organizations struggle **to know which assets are business-critical.**



49%

admit that it is **difficult to understand how individual assets relate to each other** and how an attacker might use assets in attacks.

49%

claim it is difficult to keep up with security hygiene and posture management **due to the dynamic and growing attack surface.**

CISOs recognize that they need to do more to support effective cyber-risk management—but they face several security hygiene and posture management challenges. More than six out of 10 respondents (61%) agree that their organization finds it difficult to prioritize the right actions that can have the biggest impact on risk reduction. Furthermore, 57% of organizations struggle to know which assets are business-critical, 49% admit that it Is difficult to understand how individual assets relate to each other and how an attacker might use assets in attacks. Moreover, 49% claim it is difficult to keep up with security hygiene and posture management due to the dynamic and growing attack surface.

There's a common theme within this data: Organizations are attempting to monitor and measure cyber-risk through siloed/fragmented data that doesn't chain together how attackers could use exposures in the environment to move across hybrid networks to reach and compromise critical assets. What's particularly alarming is that 73% of organizations still rely on spreadsheets to analyze all of this disparate data.

Back to Contents

Security Professionals Firmly Believe Security Testing and Attack Modeling Can Be Extremely Valuable

With the growing attack surface and given limited resources, how can CISOs improve cyber-risk management? By operationalizing a “think like the enemy” methodology. This requires an outside-in understanding of attack paths—how an adversary would exploit an asset, move laterally through the network, and then find business-critical systems and data.

To gain an outside-in perspective, many organizations are increasing security testing and attack modeling frequency. Security professionals firmly believe that security testing and attack modeling can be extremely valuable. Nearly half (47%) believe that security testing and attack modeling are a best practice for risk assessment and reduction, 39% conduct tests and attack modeling after experiencing some type of security incident, and 38% say that they conduct security testing and attack modeling based on mandates from executives and corporate boards.

By taking the perspective of an adversary, security testing and attack modeling can expose the vulnerable resources most likely to be used as part of a cyber-attack campaign. Armed with this information, CISOs can harden their environment, pinpoint investments, and communicate risk mitigation plans to business executives. And unlike periodic penetration testing, security testing and attack modeling should be continuous to maintain currency with ever changing environments.

Top five reasons organizations are increasing security testing and attack modeling

47%

We believe that penetration testing/red team exercises are a best practice for risk assessment and reduction.

39%

We conduct penetration testing **after experiencing some type of security incident** in order to assess risk.

38%

Executive managers/board of directors **mandate that we do so.**

37%

We are required to do so for **regulatory compliance.**

35%

We conduct penetration testing **after another firm in our industry has experienced a data breach.**

Back to Contents

What can organizations do to address the growing attack surface and institute a ‘think like the enemy’ defensive strategy?

Strategies organizations can take to address a growing attack surface

29%

Deploying attack surface management technology that can discover and test internet-exposed assets and can alert/ prioritize associated cyber-risks.

29%

Taking a more adversarial/offensive approach to cybersecurity so we can adjust our defenses as counter measures to modern attack TTPs.

29%

Increasing integration of the MITRE ATT&CK framework into our cybersecurity strategy.

19%

Establishing better KPIs, metrics, and reports that could help communicate the importance of security hygiene and posture management to the business.

35%

Establishing one or several risk scoring systems to help us prioritize remediation actions.

Cybersecurity Professionals’ Security Hygiene and Posture Management Improvement Suggestions

What can organizations do to address the growing attack surface and institute a “think like the enemy” defensive strategy? Hybrid coverage is especially critical as 46% of production applications/workloads run on public cloud services today, and this is expected to rise to 53% in 24 months.[1]

Security professionals have several suggestions, such as deploying attack surface management technology (29%), taking an adversarial/ offensive approach to cybersecurity (29%), increasing integration with the MITRE ATT&CK framework (29%), and establishing formal KPIs and metrics for security hygiene and posture management (19%). This is extremely important as 85% of corporate boards are more engaged in cybersecurity status, decisions, and strategy than they were two years ago.[2]

[1] Source: ESG Research Report, *Security Hygiene and Posture Management,* January 2022.
[2] Source: ESG Research Report, *Application Infrastructure Modernization Trends Across Distributed Cloud Environments*, March 2022.

Back to Contents

CISOs Can Identify their Critical Exposures with Attack Path Management Technology

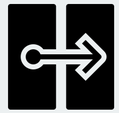
CISOs may also want to look at technologies for attack path management, as they combine many of these functions in a single toolset. Rather than learn about all assets, attack path management takes an adversary perspective to answer questions such as: “How can I be attacked?” “Which of my critical assets are at risk?” “How can I mitigate these risks with minimal effort?”

Armed with this knowledge, CISOs can identify their most critical exposures like misconfigurations, risky users, and software vulnerabilities across hybrid IT. CISOs can also apply cost-effective remediation actions by directing resources to fix choke points—those junctures where many attacks paths traverse through. These actions can help CISOs to detect and communicate business risks, identify risk mitigation strategies, and track success over time.

ESSENTIAL ATTACK PATH MANAGEMENT USE CASES

Connections between misconfigurations, vulnerabilities, and overly permissive identities

Single view of on-prem and cloud networks for universal security posture management



Detection of lateral movement opportunities

Choke point identification for prioritization and cost-effective remediation

Visualization of an attacker’s approach

Back to Contents

XM Cyber

XM Cyber is the hybrid cloud security company that's changing the way innovative organizations approach cyber-risk. Its Attack Path Management platform continuously uncovers hidden attack paths to businesses' critical assets across cloud and on-premises environments, enabling security teams to cut them off at key junctures, and eradicate risk with a fraction of the effort. Many of the world's largest, most complex organizations choose XM Cyber to help eradicate risk. XM Cyber has offices in North America, Europe, and Israel.

REQUEST A DEMO

Back to Contents

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm providing market intelligence, actionable insight, and go-to-market content services to the global technology community.