BITSIGHT

EBOOK

Creating Trust in an Insecure World

Strategies for Cybersecurity Leaders in the Age of Increasing Vulnerabilities

Introduction

It's not easy being a cybersecurity leader these days.

Organizational attack surfaces are expanding as a result of dramatic shifts to leverage cloud infrastructure, internet connected devices, and third-party vendors.

Security vulnerabilities in software, hardware, and devices are rising in number and severity, bringing with them risk of ransomware, breach, and other dangerous cybersecurity incidents.

Critical stakeholders — including corporate executiveations on security leaders to successfully protect their organization.

How can cybersecurity leaders address these challenges and increase trust in their organization's cybersecurity program? This report describes the key issues shaping the cybersecurity landscape and explains how leaders can:

Improve awareness of their organization's digital assets and risks internally and across the supply chain and partner ecosystem.

Strengthen vulnerability and exposure management programs.

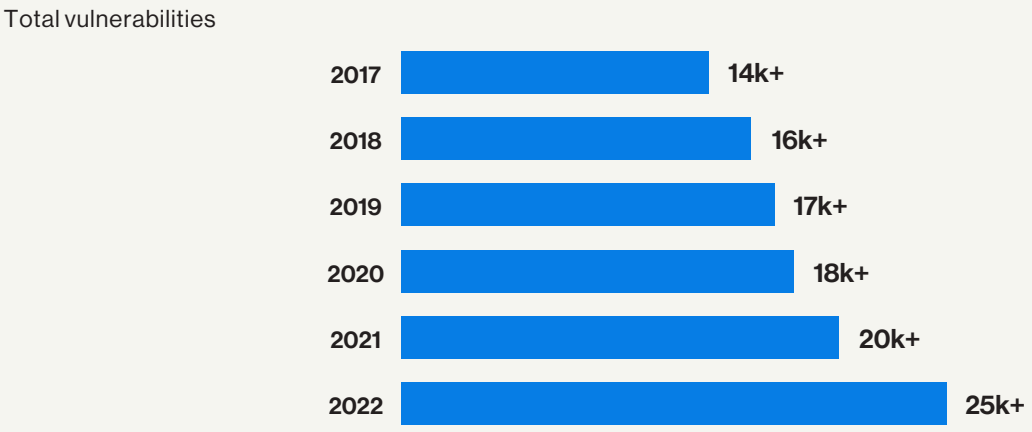
Create trust in their organizations by communicating the effectiveness of their cybersecurity program to critical internal and external stakeholders.

The challenge: An expanding, insecure ecosystem

The modern organizational attack surface is expanding rapidly as a result of enterprise investments in cloud infrastructure; deployment of shadow IT and new internet-connected devices; increased dependencies on third-party vendors and business partners; and the explosion of the remote workforce.

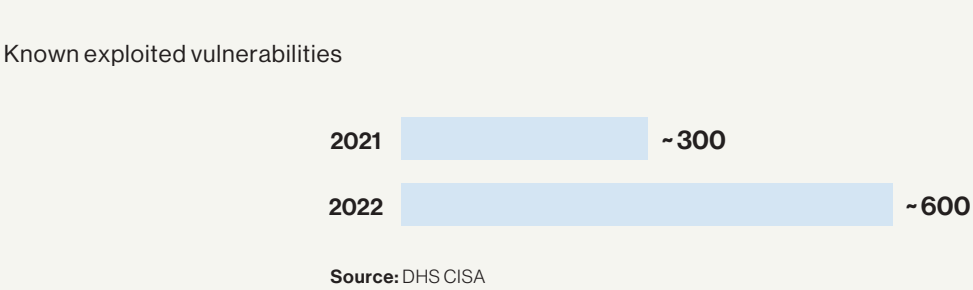
This is creating significant challenges for cybersecurity leaders to discover and understand their attack surface, including identifying enterprise assets and systems.

The number of cyber vulnerabilities and risks is growing and it is getting worse. The number of new disclosed cyber vulnerabilities jumped 25 percent in 2022.



Source: CVE Details

Alongside a sharp rise in the total number of vulnerabilities, the number of "Known Exploited Vulnerabilities"—those vulnerabilities observed to be exploited by malicious actors in the wild—is growing significantly faster, nearly doubling from 2021 to 2022.



Source: DHS CISA

Unfortunately, vulnerability management programs struggle to keep up. Quantitative research from the Marsh McLennan Cyber Risk Analytics Center suggests that vulnerability management may be the single most important thing a cybersecurity leader can implement to effectively and measurably reduce the risk of experiencing a cybersecurity incident.[1] However, many organizations struggle to implement an effective vulnerability management program. After analyzing 140 medium, high, and critical software vulnerabilities across over 100,000 organizations around the world with varying rates of remediation at the time of observation, Bitsight found that the average vulnerability remediation rate across organizations is about five percent per month.[2] The statistics are startling, considering how critical vulnerability remediation is to reduce the likelihood of a cyber incident.

Organizations are facing significant challenges in understanding and managing vulnerabilities in their extended third-party ecosystem, especially during major security incidents such as Log4j, SolarWinds, and other zero-day events where it is crucial to comprehend and mitigate the impact from third parties. Most security leaders lack the essential tools to address these emerging threats, leaving organizations with a major hurdle when trying to rapidly and comprehensively notify affected third parties. Without a tool to assess the level of potential exposure, organizations often rely on manual methods, such as disseminating mass emails and spreadsheets with questionnaires, which may lack prioritization and result in inefficiencies.

Sources: Bitsight, CISA

[1] The Marsh McLennan Cyber Risk Analytics Center analyzed thousands of cyber incidents across their vast, proprietary claims database to identify which security program initiatives might objectively reduce the likelihood of experiencing an incident. The research pro duced a ranked list of analytics most correlated with incidents, revealing patching cadence — the rate at which an organization remediates vulnerabilities — as the analytic most correlated with experiencing a cyber incident.

[2] Bitsight's analysis aimed to identify a typical rate of remediation and to better understand why some vulnerabilities are remediated faster or slower. Software vulnerabilities studied span those present in firmware, operating systems, applications, programming languages, frameworks and more. For example, we studied firmware vulnerabilities in Zyxel USG firewalls, operating systems exploits like BlueKeep in Windows, and application issues like the Grafana zero-day. Bitsight's research uncovered that organizations tend to remediate vulnerabilities at a compound rate of 5 percent every month. This means if 1000 organizations are affected by a vulnerability at the beginning of month one, then 951 will remain affected by the end of that month; and by the end of month two, roughly 905 will remain affected, and so on. In our example with 1000 affected organizations, after an entire year more than half of the originally affected organizations would remain affected.

Stakeholders are concerned about cybersecurity

While cybersecurity leaders confront these new risk dynamics for their organizations, they must also engage with a growing number of stakeholders who are concerned about cybersecurity and have high expectations for effective management. These stakeholders include:

- **Executives**, including the CEO, CFO, and General Counsel, who are legally responsible for ensuring the funding and effective execution of the organization's cybersecurity program. According to Gartner, by 2026 at least 50 percent of C-level executives will have performance requirements related to cybersecurity risk built into their employment contracts.[3]

- **Board members**, who are responsible for overseeing cyber risk across the organization and holding executives accountable and may be legally liable for cybersecurity incidents.

- **Customers and business partners**, who want to work with secure, trustworthy businesses.

- **The capital marketplace – including investors, insurers, and credit rating agencies**, who desire information and assurance that their investments will not be negatively impacted by a cybersecurity incident.

- **Government regulators**, who set cybersecurity requirements and expect adequate implementation of those laws and policies.

Building, maintaining, and communicating a strong cybersecurity program is critical to establishing trust with these stakeholders. Some forward- looking companies are going beyond the status quo by publishing reports with objective metrics and measurements regarding cybersecurity performance and outcomes. For example, Equifax publishes the Equifax Security Annual Report, a public document that includes key security metrics and performance indicators that describe the state of the Equifax cybersecurity program.[4] Beyond describing the initiatives undertaken by the organization, the Equifax Security Annual Report details metrics and key results in areas such as cloud security and supply chain assessments, security maturity benchmarking, and security performance benchmarking. These types of quantitative security indicators provide valuable validation for stakeholders.

Other leaders are taking steps to develop more secure products and a secure customer experience. For example, Schneider Electric is building a sophisticated, comprehensive cybersecurity program that focuses on internal protection and external product security. Given recent emphasis by national governments on the importance of secure coding and development practices, more organizations should consider joining their corporate and product security initiatives under one roof.

[3] Gartner, Predicts 2022: Cybersecurity Leaders Are Losing Control in a Distributed Ecosystem. Published Jan. 24, 2022.

[4] Equifax Security Annual Report, 2020 available at: https://assets.equifax.com/newsroom/2020-security- annual-report.pdf Equifax Security Annual Report, 2021 available at: https://assets.equifax.com/marketing/US/assets/2021- security-annual-report.pdf

Turning the tide

Cybersecurity leaders require innovative and comprehensive solutions that can assist them in identifying their attack surface, enhancing their vulnerability management programs, effectively handling zero-day vulnerabilities and other significant security incidents, and communicating their success to stakeholders. Prioritizing these initiatives can significantly reduce organizational risk and foster trust within the organization. Here are four crucial steps security leaders can implement:

1. Prioritize vulnerability management

From the board to the Chief Information Security Officer (CISO), vulnerability management should be considered critical to organizational security, because it is. This means putting adequate resources into your program, including human resources, technology solutions, and pillars that guide governance. Human resources alone are no panacea—vulnerability management professionals must be enabled, prioritized, and receive ample support from internal stakeholders if they are to successfully defend their organizations from the risks presented by vulnerabilities. The foundation of an effective vulnerability management program begins with strong governance and prioritization of key analytics to benchmark performance.

Bitsight is a trusted partner to help you improve your vulnerability management program. Our cybersecurity analytics set objective security performance standards, which promote sound cybersecurity governance and benchmarking.

The Bitsight Security Rating is the only security rating independently verified to have a significant correlation with cybersecurity incidents.

Additionally, Marsh McLennan found Bitsight's Patching Cadence risk vector—a measure of an organization's vulnerability management program—to be most correlated with incident likelihood.

Confidently leverage Bitsight's analytics to assess the effectiveness of your program, identify gaps, and take steps to improve your overall security posture.

2. Identify your attack surface

Organizations struggle to fully understand what makes up their attack surface, where the greatest risks are, and how to mitigate them.

Lacking visibility into the internal and external assets comprising your attack surface leaves you vulnerable to cyber attacks; and failing to effectively manage your attack surface leaves your organization vulnerable to breaches, ransomware, and other cybersecurity incidents resulting from successful exploitation. But visibility is only the start. Organizations then need to prioritize vulnerability management based on the risk of each asset and the criticality of the vulnerability itself.

Bitsight helps you see a complete view of your organization's attack surface — on-premise, in the cloud, and throughout the supply chain — and allows you to discover where your organization's cyber risk lies. This solution allows you to gain visibility into your digital assets, discover shadow IT, and visualize areas of disproportionate risk; ultimately arming you with what you need to identify and remediate cyber risks in your digital ecosystem.

3. Understand third-party cyber risks

A successful attack on your third-party vendors and relationships could potentially result in business disruption, financial loss, reputational harm, and even compromise your internal systems and data. But managing third-party cyber risk is anything but simple.

Many organizations rely on time-consuming processes to evaluate cyber risk in their third-party ecosystems, opting to send mass emails with spreadsheet questionnaires with little prioritization or way to track responses. This approach makes it difficult to swiftly and accurately assess and address cyber risks, particularly new, zero-day vulnerabilities that may arise.

A solution like Bitsight allows you to gain visibility into cyber risks impacting your entire third-party ecosystem. Bitsight empowers you to augment your annual assessment with continuous monitoring of risk in your thirdparty ecosystem, as well as detection and prioritization of vendor outreach for critical vulnerabilities in your portfolio that require remediation at scale.

Bitsight helps organizations streamline cyber risk detection, management, and mitigation within their third-party ecosystem, including critical, zero-day vulnerabilities. Through surfacing actionable vulnerability data based on severity and enabling scalable vendor outreach and remediation tracking through built-in questionnaire capabilities, organizations are empowered to efficiently remediate risk, especially for growing vendor ecosystems that are difficult to prioritize and respond to during major security events. Bitsight's solutions help organizations

- **Detect**, manage, and mitigate emerging zero-day events with speed.
- **Scale** and track vendor outreach efforts with precision.
- **Remediate** risk quickly with better prioritization of vendor outreach efforts.
- **Confidently** adhere to growing regulatory pressure with easy access to vulnerability data.

4. Communicate effectively with stakeholders

Organizations face a significant challenge in effectively communicating their cybersecurity posture to critical stakeholders such as the board, executives, and the capital marketplace. In today's digital landscape, a strong cybersecurity posture is becoming a crucial differentiator for businesses. Many executives are hesitant to onboard risky partners, while investors are increasingly cautious about investing in companies with high cyber risk. Transparency around cyber risk is already in motion; the U.S. Securities and Exchange Commission (SEC) has proposed mandatory cybersecurity disclosure rules aimed at strengthening investors' ability to evaluate public companies' cybersecurity practices and incident reporting. Insurers are taking notice – a weak cybersecurity posture will impact your ability to achieve a more competitive coverage and premium.

Bitsight provides independent, objective analytics that enable security leaders to have more effective conversations with internal and external stakeholders about their cybersecurity effectiveness. Bitsight lets you quickly pull universal metrics that reframe the conversation about cybersecurity towards business risk. For example, you can present information on how many vulnerabilities you have in your digital ecosystem and their severity — i.e., their likelihood of contributing to a breach — or the status of how many in your portfolio have been breached and made known of that breach. This enables executives and board members to make more informed decisions about where investments and resources are needed. Furthermore, because Bitsight's analytics are used and trusted by the world's leading investors, insurers, government agencies, and regulators, you can communicate your organization's security posture in a language that is recognized and understood by a broad, external audience.

Take action now

Being a cybersecurity leader in today's landscape is an immense responsibility that comes with many challenges. With the expansion of organizational attack surfaces and the increasing number of security vulnerabilities, it is critical for cybersecurity leaders to be proactive in addressing these issues. By improving their organization's awareness of digital assets and risks, strengthening their vulnerability and exposure management programs, and communicating the efectiveness of their cybersecurity program to critical stakeholders, leaders can increase trust in their organization's cybersecurity program. While the cybersecurity landscape will undoubtedly continue to evolve, leaders who are willing to adapt and implement best practices will be better equipped to protect their organizations from cybersecurity incidents and build trust with stakeholders.

Adopting the right tools and partners is critical.
Contact Bitsight to improve exposure management.

Bitsight is a cyber risk management leader transforming how companies manage exposure, performance, and risk for themselves and their third parties. Companies rely on Bitsight to prioritize their cybersecurity investments, build greater trust within their ecosystem, and reduce their chances of financial loss. Built on over a decade of technological innovation, its integrated solutions deliver value across enterprise security performance, digital supply chains, cyber insurance, and data analysis.

BOSTON (HQ) RALEIGH NEW YORK LISBON SINGAPORE BUENOS AIRES

BITSIGHT