Mighty Guides

CHANGING VULNERABILITY MANAGEMENT TO MORE EFFECTIVELY CONTROL CYBER-RISK

Sponsored by RISKSENSE

INTRODUCTION

Vulnerability management can be a powerful tool for reducing cyber risk, but in many organizations, vulnerability management is like a neglected step-child in their cyber security program.

This eBook reviews steps companies can take to reduce cyber risk. These include treating the entire workforce as part of the security function, and holding people accountable. It also requires access to quality threat data so organizations can weigh their raw risk ratings and more effectively prioritize their defensive actions.

Regards,
David Rogelberg
Publisher, Mighty Guides, Inc.

Mighty Guides

Mighty Guides make you stronger.

These authoritative and diverse guides provide a full view of a topic. They help you explore, compare, and contrast a variety of viewpoints so that you can determine what will work best for you. Reading a Mighty Guide is kind of like having your own team of experts. Each heartfelt and sincere piece of advice in this guide sits right next to the contributor's name, biography, and links so that you can learn more about their work. This background information gives you the proper context for each expert's independent perspective.

MEET THE EXPERTS

JOSH BAILEY
Senior Information Security Engineer, DocuSign

KIM MAURER
Chief Information Security Officer, Prince William County

Josh Bailey, Senior Information Security Engineer, DocuSign

Josh Bailey is the Lead Information Security Engineer in the Vulnerability Management team at DocuSign. He has over 19 years of experience in IT, ranging from server administration, to network security, and in more recent years, tool development and automation. These days, he spends most of his time working with departments across the company to understand and secure their cloud workloads.

"The difficulty is tracking vulnerabilities month over month and ensuring things are remediated in a timely manner."

It is clear that cyber-risk is becoming a core business risk. Major breaches in recent years have cost businesses hundreds of millions of dollars in brand damage, lost revenue, and recovery costs, not to mention a newfound enthusiasm within the Securities and Exchange Commission (SEC) for levying big fines on companies that fail to promptly report breaches.

Vulnerability management can be a powerful tool for reducing cyber-risk, but in many organizations, vulnerability management is like a neglected stepchild in their cybersecurity program. How can companies change their vulnerability management practices in ways that reduce their exposure to cyber-risk?

There are steps companies can take, such as having distinct cyber-risk profiles for different parts of an organization, having third-party assessments validating security controls, and having more frequent scans and tests. These can be highly effective at reducing cyber-risk. For many organizations, finding the right balance of risk intelligence and risk prioritization is a challenge. Josh Bailey, senior information security engineer at DocuSign, says, "It's easy to generate the data; scanning, analysis, and even CVE prioritization can be done with relatively minimal setup.

Kim Maurer, Chief Information Security Officer, Prince William County

Kim Mauer is a highly competent, results-driven cybersecurity risk manager, and enthusiastic business leader with experience managing large teams, complex projects, contracts, task orders and personnel, with outstanding results. A Cybersecurity policy and compliance thought leader with 17 years specialized experience in the development of IT security programs and risk management strategies.

"Threat data is key to reporting meaningful cyber-risk, especially given the increased weaponization of vulnerabilities."

The difficulty is tracking vulnerabilities month over month and ensuring things are remediated in a timely manner. Even if you have the time and resources to do that, adding in the context of critical systems and services, and business risk, compounds the issues, especially when teams aren't aligned from the top down."

Kim Maurer, chief information security officer at Prince William County, Virginia, believes there is danger in creating a security silo within the organization. "To truly minimize risk, cybersecurity must be made a team sport," she says. "The more I've seen organizations try to centralize the security function, the less effective they have been at managing the complex collection of security activities, much less the risk. The complex ecosystem of cybersecurity spans far beyond the IT department, tools, or patching. It is imperative that organizations treat the entire workforce as part of the security function, distribute individual security control activities as widely as possible, hold people accountable for their part, and then take a step back and let the team play the game. There are a host of governance, risk, and compliance (GRC) tools available on the market to facilitate this approach."

Bailey would agree, believing that risk reduction needs to almost become an aspect of the organization's culture. He advises approaching business with security in mind and treating everyone as a partner in maintaining security. "Bake it into the DNA," he says. "When security is approached this way, there is room to have discussions about what business risks the company faces, what compliance requirements there are, what controls need to be put in place, what processes and policies need to be developed, and how it all can be done without disrupting the culture (or as little as possible). It's no longer seen as red tape, "extra work," or a hassle when it's understood and openly discussed."

However, even with these organizational approaches, it still comes back to threat intelligence and being able to prioritize risk. Maurer explains, saying, "Threat data is key to reporting meaningful cyber-risk, especially given the increased weaponization of vulnerabilities. With access to quality threat information, there is no reason organizations cannot do a better job at applying weights to their otherwise raw risk ratings and more effectively prioritize their defensive actions. Whether the threat data offers insight into affected devices, impacted technology, or behaviors (for example, methods of access), we have an opportunity to use this data to inform risk decisions and refine our defensive operations in a meaningful way." ■

CLOSING THOUGHTS

Without a doubt, you struggle with prioritizing the plethora of threats and vulnerabilities that hit your organization. Penetration testing findings add to the problem. There are never enough hours in the day, nor enough staff to remediate all of the possible exposure on both your internal and external IT infrastructure.

Shift your thinking. Narrow down the threats and vulnerabilities to the ones that have active exploits, are dangerous with remote code execution capabilities, and are trending with active threats in the wild. This is impossible if you don't have a platform that takes in all of your vulnerability scanner data, across your dynamic attack surface: network, endpoints, database, applications, cloud, and IoT devices. Leverage human intel, combined with AI and machine learning to achieve prescriptive prioritization in minutes. Security and IT teams can focus on what matters the most with a new efficiency to manage cyber risk.

This article illustrates the value of risk-based vulnerability management to predict, prioritize, and take control of your most dangerous vulnerability and risk findings.

Regards,
Srinivas Mukkamala
CEO and Co-Founder, RiskSense

RISKSENSE

RiskSense®, Inc. provides vulnerability management and prioritization to measure and control cybersecurity risk. The cloud-based RiskSense platform uses a foundation of risk-based scoring, analytics, and technology-accelerated pen testing to identify critical security weaknesses with corresponding remediation action plans, dramatically improving security and IT team efficiency and effectiveness.

The company delivers a fully-informed picture of group, department, and organizational cybersecurity risk with our credit-like RiskSense Security Score (RS3). The RiskSense platform continuously correlates customer infrastructure with comprehensive internal and external vulnerability data, threat intelligence, human pen test findings, and business asset criticality to measure risk, provide early warning of weaponization, predict attacks, and prioritize remediation activities to achieve security risk goals.

By leveraging RiskSense threat and vulnerability management solutions, organizations significantly shorten time-to-remediation, increase operational efficiency, strengthen their security programs, heighten response readiness, lower costs, and ultimately reduce attack surface and minimize cyber risks. For more information, visit www.risksense.com or follow us on Twitter at @RiskSense.