Mighty Guides

VULNERABILITY MANAGEMENT IS NOT HOPELESS, BUT IT NEEDS TO MATURE

Sponsored by

RISKSENSE

INTRODUCTION

Organizations fall short in their vulnerability management practices in many ways, including not having a comprehensive and accurate asset inventory, and failing to prioritize vulnerability remediation efforts based on contextualized business risk.

This eBook looks at ways to address shortcomings and build a mature vulnerability management practice. Efficiency and coverage need to be opposing forces in vulnerability management. Balance can be found by prioritizing risks. Let risk drive the rate and level of coverage needed to be effective.

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

BRADLEY SCHAUFENBUEL
Vice President and Chief Information Security Officer, Paylocity

PETER RIEDMAN
Information Security Architect, Proskauer Rose LLP

Bradley Schaufenbuel, Vice President and Chief Information Security Officer, Paylocity

Bradley J. Schaufenbuel is currently Vice President and Chief Information Security Officer at Paylocity in Chicago. He has over 23 years of experience in the information security field, has written numerous books and journal articles, possesses an MBA, a JD, and an LLM, maintains two dozen professional certifications, and regularly keynotes industry conferences. Bradley was recognized as the Chicagoland CISO of the Year in 2018.

"Organizations often fail to prioritize vulnerability remediation efforts based on contextualized business risk."

Although sophisticated new exploits get lots of publicity, the most common causes of intrusion and data breaches are, by far, unpatched software vulnerabilities and human errors that inadvertently expose data. It is an old story repeated over and over. While one recent breach resulting from a known vulnerability that went unpatched exposed the personal data of 143 million people, smaller occurrences happen every day. The growing complexity and dynamic nature of IT environments is making vulnerability management more critical than ever. The challenge for many organizations, however, is developing a mature approach to vulnerability management.

There are many ways organizations fall short in their vulnerability management practices. Bradley Schaufenbuel, VP and chief information security officer at Paylocity, sees two common failings in the way many companies approach vulnerability management. He explains, "First, organizations fail to maintain a comprehensive and accurate asset inventory. You cannot address vulnerabilities in assets you don't know you have, and asset management is difficult for many organizations. Second, organizations often fail to prioritize vulnerability remediation efforts based on contextualized business risk.

Peter Riedman, Information Security Architect, Proskauer Rose LLP

Peter Riedman, CISSP, GCFE, has over 18 years of experience in the field of information technology. He currently works as an information security architect for an international law firm after having held a number of positions in network security, network engineering, and system administration in a variety of industries such as manufacturing, retail, distribution, and market research.

"There is very often a tangible communication gap between information security staff and sysadmins/ application development staff tasked with fixing discovered vulnerabilities."

The sheer volume of vulnerabilities in most environments and the pace in which new vulnerabilities are discovered makes it very difficult for organizations—even those that devote substantial resources to vulnerability management—to keep up. If an organization tries to eradicate all vulnerabilities regardless of risk, it will fall hopelessly behind. If an organization makes a concerted effort to determine the contextualized business risk of all vulnerabilities and focuses on eradicating the highest risk items first, returning to lower risk items as time and resources allow, it will at least minimize the risk of exploitation."

Peter Riedman, information security architect at Proskauer Rose LLP, sees additional challenges that many organizations face. "I think there is too much emphasis on the tools themselves and not enough emphasis on analysis of the findings that come from the tools," he says. "Purchasing and installing tools to scan for vulnerabilities is the easy part. The difficult part is maintaining an effective level of care and feeding for the tools so that they remain effective as the environment evolves. The real value of those tools comes from analysis of what the tools are showing. If done properly, you will be able to identify issues such as use of insecure protocols, default device credentials, ineffective patching processes, inventory blind spots, and much more."

Riedman points out that many organizations also struggle with effectively communicating remediation deliverables. “I find there is often a very tangible communication gap that exists between information security staff and sysadmins/application development staff who are tasked with fixing discovered vulnerabilities. We in information security need to make sure we are effectively putting vulnerabilities into relatable terms for these other teams so they can clearly understand the risks, vulnerabilities, and impacts.”

One does not create a mature vulnerability management practice overnight. There are stages to maturity. Bradley Schaufenbuel says that an important step toward mature vulnerability management is the ability to perform vulnerability scans in a consistent way. “A moderately mature vulnerability management program is one in which vulnerability scans are performed regularly and there is a repeatable process in place to remediate the vulnerabilities that are found,” he explains. “After getting the vulnerability management basics right, the next step would be to prioritize vulnerability remediation efforts based on contextualized business risk and report vulnerability metrics over time to drive continuous improvement.”

He also equates greater efficiency in vulnerability management to working smarter. He says that’s better than trying to eliminate every vulnerability, which often means working harder while accomplishing less actual risk reduction. “Eradicating every single vulnerability (i.e., achieving complete coverage) in an environment in which new vulnerabilities are constantly being found, assets are being added and changed, and the threat landscape is continuously shifting, is a fool’s errand,” he says. “Few organizations have the resources required to achieve high levels of coverage. In the world of limited resources that most organizations live in, efficiency—or eliminating vulnerabilities in the order of severity based on contextualized business risk—is a more effective and achievable strategy.”

Peter Riedman agrees that risk prioritization is a key factor in the maturity of a vulnerability management practice. “I don’t think that efficiency and coverage need to be opposing forces in the universe for vulnerability management. A balance can be found by prioritizing risks. Let risk drive the rate and level of coverage needed to be effective. Like many other information security topics, it comes down to a mixture of people, processes, and technology. A vulnerability management practice will possess all of these components, but the question becomes: how well are these moving parts working together? Without a proper balance of these moving parts, a business shouldn’t assume its practice is actually effective.”

Like many security experts, both Riedman and Schautenbuel recognize the value of having a more mature approach to vulnerability management. Schaufenbuel sums it up in this way: “The majority of data breaches are perpetrated through the exploitation of known vulnerabilities. Having a mature and effective vulnerability management program significantly reduces the probability of an organization suffering a debilitating data breach.” In Riedman’s view, it comes down to being able to see what is most important to the business and being able to act on those things. “Significant gains can be had by leveraging vulnerability management tools to tell a story,” he says. “You must use these findings to paint a clear picture of the state of the environment, the risks, and necessary remediation efforts.” ■

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.