Mighty Guides

Sponsored by

RISKSENSE

7 Experts on Threat and Vulnerability Management

Best Practice Advice On How To Prioritize Your Remediation with a Cutting-Edge Approach

INTRODUCTION: THREAT AND VULNERABILITY MANAGEMENT

One of the greatest challenges security teams face is identifying, assessing, and eliminating vulnerabilities before the bad guys find them. Sometimes it seems like the bad guys are winning.

Most major breaches in that past year have occurred through known vulnerabilities that for various reasons went unpatched until it was too late. Organizations know they have vulnerabilities in their systems. They are investing in new tools, yet industry surveys show that few are totally satisfied with their vulnerability-management practice.

Part of the challenge is that managing vulnerabilities requires balancing threats and asset criticality against known vulnerabilities, but these things are all constantly changing. To gain a clearer understanding of these challenges and how organizations are addressing them, we partnered with RiskSense. We approached 7 cyber risk experts with the following question:

"What best-practice advice would you offer to help someone take a proactive, cutting-edge approach to cyber-risk management?"

Of course, the answers depend on a lot of factors, but our experts had a number of useful and revealing things to say about assessing criticality, managing remediation, and applying next-generation tools to the problem. It's interesting that although new technology is a key part of the puzzle, to get the most out of those tools there needs to be close collaboration with business operations. It's essential to have good communications with business people who are not security professionals.

There are no simple answers, but the essays in this eBook contain many observations and valuable lessons from experts actively facing these challenges. I'm sure anyone interested in sharpening their vulnerability management practice will appreciate these insights.

All the best,
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.

Credible advice from top experts helps you make strong decisions. Strong decisions make you mighty.

© 2018 Mighty Guides, Inc. I 62 Nassau Drive I Great Neck, NY 11021 I 516-360-2622 I www.mightyguides.com

FOREWORD

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

Shift your thinking. Narrow down the threats and vulnerabilities to the ones that apply to your IT infrastructure, then further reduce the list to the ones that have active exploits and finally identify your critical devices that should be remediated first. 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 and IoT devices. Leverage human intel, combined with AI and machine learning to guide your remediation efforts and let your security staff focus on the strategic issues to support your digital transformation with an integrated security platform.

This e-book illustrates the value of identifying critical IT assets, and the importance of a prioritization platform that provides you clear guidance on remediation efforts. With the RiskSense Security Score (RS3), you can define your journey to track security metrics that link to your business goals. Security teams and business leaders alike will find value in the perspectives shared here.

Regards,

Srinivas Mukkamala

CEO and Co-Founder, RiskSense

RISKSENSE

The RiskSense Platform embodies the expertise and intimate knowledge gained from real world experience in defending critical networks from the world's most dangerous cyber adversaries.

We help organizations prioritize IT vulnerabilities and threats to reduce cyber risk achieving confidence in your digital transformation efforts. Our mission is to accurately identify and prioritize threats and vulnerabilities, add context to quickly remediate and continuously monitor the results providing organizations with cyber resilience across a growing and dynamic attack surface.

RiskSense offers the only intelligence-driven prioritization of threats and vulnerabilities, helping organizations overcome the complexity of managing today's continuously changing IT infrastructure and ever expanding and complex attack surface. The leader in analyzing threat and vulnerability data across the broadest spectrum of technologies (network, applications, endpoints, databases, and IoT devices) to uncover the most likely attack scenarios. Our platform allows organizations to view assessment findings in real-time, create asset risk profiles, and manage the continuous feed of threat and vulnerability data which is enriched from over sixty independent sources factoring in human Intel to elevate and prioritize remediation actions.

TABLE OF CONTENTS

JUAN MORALES

Senior Director, Global Cybersecurity & Incident Response
Realogy Holdings Corp.

Juan Morales is the senior director of global cybersecurity and incident response for Realogy. He directs the security operations center, incident response, forensics, eDiscovery, and vulnerability management functions for Realogy. Juan has more than 18 years of experience in IT, InfoSec and technology management, focusing on reducing risk exposure, enabling business success by promoting sound and adaptive security practices with a focus on the fundamentals of cybersecurity. He holds a master's degree in Cybersecurity from Fordham University and CISSP, ISSMP, and CEH certifications.

LinkedIn | Website

The main reason for vulnerability management is that it's not possible to remediate all the vulnerabilities for all the assets in an enterprise completely. It's necessary to prioritize, yet for many companies, just knowing what assets they actually have can be a daunting task. Juan Morales, senior director of cybersecurity at residential real estate services company Realogy, recommends starting out by asking how you identify your critical assets. "Regardless of vulnerabilities, start figuring out what is really important to the business," says Morales. "What is most impactful should it be exploited? What really are the key assets that keep the company going, operationally and financially?"

As you identify those assets, you also need to know where they are located. "That helps to start painting the picture of the criticality, and the context in which they're being used," Morales explains. "You might start doing a bit more in-depth vulnerability scanning of those particular assets, and then you're able to start having conversations with key stakeholders." This gives you a basis for doing more research into vulnerabilities the system is identifying. "Now you have the insight from the organization as far as the criticality of those key assets, tied with the information that the vulnerability-management system is giving you," he adds. He points out the importance of this dialog with business stakeholders, because vulnerability-management systems don't really understand the context of how these systems are being used.

When communicating risk to stakeholders, Morales prefers to quantify it in terms of system availability and financial impact . For instance, you can say that if your company is hit with an exploit that costs $10,000, or $1 million to fix, that's a point in time assessment of a cost to fix, but not a true assessment of the actual impact to the organization. "If the system's not going »

> *Regardless of vulnerabilities, start figuring out what is really important to the business. What really are the key assets that keep the company going, operationally and financially?*

to be available for X number of days or X number of hours, I think then it becomes a lot easier to translate it into an actual risk and potential revenue loss," he says. He also advises keeping it simple. "You're not going to be sharing actual technical vulnerability details. Pictures paint a thousand words. A couple of charts or dashboards with lines showing up or down trends is sufficient for stakeholders to understand the risk." A risk scoring model that translates vulnerability data into business metrics would be invaluable.

There are a couple of important reasons to keep business stakeholders involved in vulnerability discussions. For one thing, they are accountable for the risk in their business. Also, they can be important advocates for driving remediation and getting additional resources needed to address a vulnerability. "We actually distribute our vulnerability-management reports to executives," says Morales. "This is the picture of your assets and systems that you're accountable for, and here are the number of vulnerabilities in your systems. We give them a 30-day look-back of the number of vulnerabilities being fixed, and obviously we want to continue to see a down-trend as we continue to gather those statistics."

Traditionally, security people work with the operations teams and support teams to fix vulnerabilities, but in a perfect world, Morales believes executives should take an active interest in the vulnerability-management discussion. It doesn't always work that way, but the trends are moving in that direction. Morales describes

"Pictures paint a thousand words. A couple of charts or dashboards with lines showing up or down trends is sufficient for stakeholders to understand the risk."

it this way: "You want executives to get a dashboard that has a clear business scoring model that allows them to engage and appreciate how security impacts their business. . You want them to be able to take action and ask the questions. Why is this dashboard looking the way it's looking? Who's not doing what is necessary? Do we need more resources? That's the kind of conversation we want to drive by showing these metrics to the executives." ■

KEY POINTS

1 **A dialog with business stakeholders is important because vulnerability management systems don't understand the context of how assets are being used. Solutions that have a prioritization model and support business criticality of assets is needed.**

2 **By getting business stakeholders involved in vulnerability discussions in business terms they understand, they can help drive remediation and advocate for additional resources needed to address a vulnerability.**

PIETER VANIPEREN

Founding Member
Code Defenders

Pieter VanIperen is a veteran programmer, security expert, and ethical hacker holding multiple certifications. He is a founding member of Code Defenders—a collective that protects the long tail of the internet—and an adjunct professor of Code Security at NYU. He is currently the resident software architect and secure coding expert for several fortune 1000 companies, as well as consulting for law enforcement authorities and advising multiple startups. He is the author of the HAZL programming language and has served as the CTO of several digital companies.

Twitter | Website | LinkedIn

One of the challenges that comes with rolling out vulnerability detection and management technologies is interpreting and acting on the insights they provide. "Having a set of results is great," says Pieter Vaniperen, security architect and a specialist in code security. "But you're going to have a lot of false positives, especially on a first scan. If you're doing an internal scan, you're going to have systems that aren't even accessible to the outside world that are getting flagged."

VanIperen says that in order to use vulnerability scans effectively in a risk-management strategy, you need to be able to triage and analyze risk and there aren't tools that can do that effectively today alone. Doing that requires systems and people. On the human side of the equation, you will need to include people from different parts of the cyber ecosystem. "You will need a cross-functional set of people in order to understand the context of the potential risks you're looking at, to figure out if they are risks, to understand how exploitable and exposed they really are, and how to fix them," he explains. Beyond that, VanIperen says you need to have a system for monitoring events as they are occurring. "You need central logging, and you need training," he adds.

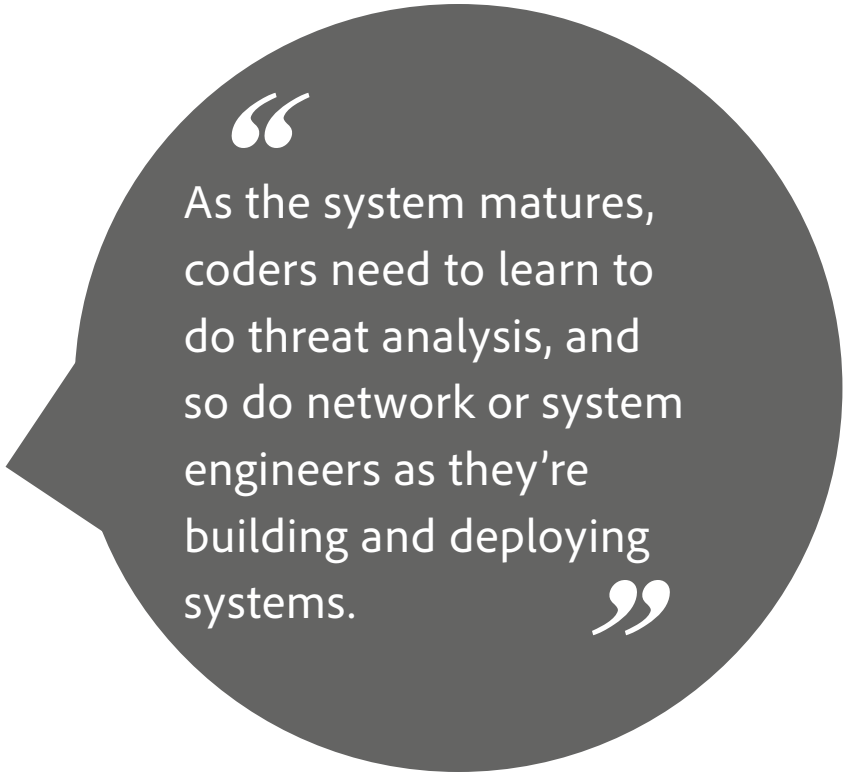
With these capabilities in place, risk assessment and prioritization becomes central to an effective risk-management program. "There needs to be a risk analysis and ranking system," says VanIperen. "Whether that is something like DREAD (damage, reproducibility, exploitability, affected users, discoverability), something like a category score (low, medium, high), or just a scale of 1 to 10, there needs to be something so you can start assessing risk and triaging and prioritizing vulnerabilities." Being able to translate security metrics into business terms is critical

> *"You will need a cross-functional set of people in order to understand the context of the potential risks you're looking at."*

when communicating to management and executives. The objective is to address the highest risks and plug the biggest holes first. As the program evolves, risk assessment becomes something that is built into the IT process within the organization. "As the system matures, coders need to learn to do threat analysis, and so do network or system engineers as they're building and deploying systems. You need to start having secure code reviews, and there need to be standards checklists," says VanIperen.

One thing to keep in mind is that new scanning tools, more complex IT environments, and increased activity logging generate greater quantities of data that must be analyzed to identify legitimate vulnerabilities and risks. New AI systems based on machine learning that are capable of processing vast amounts of data may be the future of cyber risk management. "When you've looked at threat intelligence systems and artificial intelligence analysis that have been out there, some of the most successful systems are self-trained," says VanIperen. But he also points out that when AI based systems become part of a cyber risk-management program, some things change.

For instance, once a self-teaching AI system has built an operational body of risk knowledge it uses to make risk judgements about cyber activity, it is nearly impossible for humans to deconstruct how the AI system is evaluating risk. If for some reason the AI system went off-line, the humans would be inundated with data and have



little criteria for evaluating it. The other challenge is that AI systems can be gamed just like people, and odd situations can return costly false positives. "The best system can be making the right choice 99 percent of the time every day, and then it might encounter a burst of fringe cases that cause it to give unpredictable assessments," VanIperen says. "We continuously train people to know when they're being manipulated. We also need to train the systems to know when they are being manipulated." ■

KEY POINTS

1 **In order to use vulnerability scans effectively in a risk-management strategy, you need to be able to triage and analyze risk, and there aren't tools that can do that effectively today alone. Doing that requires systems and people.**

2 **New AI systems based on machine learning that are capable of processing vast amounts of data may be the future of cyber risk management.**

SURINDER LALL

Senior Director Information Security
Viacom

Surinder is a highly skilled security professional with over 20 years of experience in the technology field. Surinder is one of only a handful of security professionals who has been awarded the coveted LL.M - Legum Magister (Master of Laws). This coupled with his extensive experience and qualifications within the fields of compliance, governance, and Information security allow him to be an effective strategist throughout the security, compliance and governance life cycles.

LinkedIn

"If you don't know specifically where the risks are or how they impact the business, then you're going to have considerable issues in mitigating any of that risk," says Surinder Lall, senior director of information security at Viacom. "If you don't know where it's coming from, how you're going to address it, and what platforms you need to put in place, you could be randomly performing vulnerability scans on your IT infrastructure for hours on end and running generalized reports but not really getting anywhere." This is especially challenging in the media space where technology and new ways of monetizing content are always necessitating innovative security strategies.

In a complex IT environments that have tens or hundreds of thousands of infrastructure components, each with its own set of vulnerabilities, the key to prioritizing mitigation activity lies in risk assessment. "First you have to understand what you're trying to protect," says Lall. This involves defining what has real commercial value to the business, because that's where you need to focus mitigation efforts. "Security departments often scan everything except the most critical things because they're afraid they might break something. My argument is if you don't break it then someone else will," he notes.

Defining asset criticality comes down to the commercial consequences of exposing that asset, and how that translates into a loss for the business. "There's no simple formula," Lall says. "It's more art than science." That includes considering costs associated with asset exposure, such as loss of customer trust and the consequential damage to business. But it also includes regulatory considerations. "You have to factor in legal liabilities too," he explains. "So think about GDPR [the EU's General Data Protection Regulation], and look at the massive fines that could result if »

> *Security departments often scan everything except the most critical things because they're afraid they might break something. My argument is if you don't break it then someone else will.*

something is not fixed."

You also have to consider the seriousness of different threat vectors, for instance the likelihood that a particular vulnerability will be exploited. But this is extremely difficult to quantify, and changes continually. And even a perceived low-risk vulnerability can have a big impact if it results in a breach, just as the impact of a low-value asset exposure can far outweigh the value of the asset itself. Given these intangibles and the need to prioritize, Lall says most organizations focus on the substantial threats. "They focus on how to protect themselves against legal liability, such as violations of GDPR, PCI DSS [Payment Card Industry Data Security Standard], and the big laws. And they focus on how to mitigate risk to the obvious higher-value assets."

Lall sees AI-assisted vulnerability-scanning tools as useful in providing more continuous monitoring of asset activities, especially solutions that factor in business criticality. But he says a manual process is still required to teach them which are the high-value assets. "AI hasn't reached the maturity where it's able to look at something and say 'hey, this is sensitive stuff.'" Some systems are able to identify keywords and number configurations, but it comes back to how those assets are used in the business. The machine-learning process needs to occur over time, using data classification and business-based risk scoring. ■

> "You have to factor in legal liabilities too. So think about GDPR, and look at the massive fines that could result if something is not fixed."

KEY POINTS

1. **Defining asset criticality comes down to the commercial consequences of exposing that asset, and how that translates into a loss for the business.**
2. **A low-risk vulnerability can have a big impact if it results in a breach, just as exposure of a low-value asset can have business impacts far greater than the value of the asset itself.**

IN A LARGE ORGANIZATION, KNOW THE RISK OWNERS AND ADAPT TO THEIR NEEDS

NICK GREEN

Vice President , Information Security EMEA/APAC
Live Nation Entertainment & Ticketmaster

Nick Green is vice president of information security at Live Nation Entertainment and Ticketmaster. Live Nation is the largest producer of live music events in the world, producing 29,000 events globally and managing over 3,200 artists. Ticketmaster is one of the world's top 10 e-commerce sites, selling more than 484 million tickets annually. He is passionate about security fundamentals, automation, and deploying solutions at scale to meet the challenges of global organizations.

in
LinkedIn

Nick Green, who is responsible for IT security at Live Nation Entertainment and Ticketmaster in all regions outside North America including Europe, Asia, Australasia, and Africa, is involved in pretty much every security issue facing all of Live Nation's brands and business groups. This encompasses a huge global network handling very high transaction volumes. Managing vulnerabilities across business units and geographical regions is an enormous task that includes scanning, ranking and reporting risks, and remediation monitoring.

Before any of that is possible, Green says you have to know what your network encompasses. "You've got to find all your systems and applications," he says. "Within Ticketmaster, we've built custom systems that take in all this data from all different kinds of sources." Building an inventory includes identifying an owner for every asset. "You need to make sure you can attribute each one of these systems or applications to an owner," Green explains. "We pay special attention to making sure the owners are people, not teams. The owner is the person you talk to when something's not getting fixed."

Once you know what you've got, then you can get serious about scanning and managing vulnerabilities. "We use a well-known scanning tool, but we have to feed that tool with inventories from all kinds of sources," he says. "We feed it everything from DHCP scopes to network router tables, to other discover metrics. So there's a whole array of tools that feed into our vulnerability scanners."

Vulnerability scanning is just the beginning. You have to rank risks and report them out to asset »

> *"We use a well-known scanning tool, but we have to feed that tool with inventories from all kinds of sources."*

owners for remediation. When it comes to ranking risks, Green says, "There are a number of risk frameworks and methodologies out there. We've tended to take the best of a lot of them and customize them to keep it as simple as possible. You want to avoid getting caught up in analyzing vulnerabilities to the point where you're trying to put actual dollar figures on them, and you're reaching out to 10 different people to find out what's important. A lot of the risk decisions are based on business knowledge. It would be valuable to have a security risk score that worked similar to a credit score so business owners could more easily interpret the results."

Reporting threats—which involves tracking risks and releasing them into the business pipeline—can be tricky in a complex business environment. Different business units may be using different reporting platforms and incident ticketing systems. "I'm always bending to the needs of the business groups," says Green, "because if I want somebody to work on something, I have to present it to them in the format they require. I can't dictate how different business groups work." Variations between different business groups also impact vulnerability remediation, because the business units may not agree with the security team's risk rank and prioritization. Green tracks everything through a central ticketing system that ties to the ticketing systems used by particular business groups. "Sometimes we'll go to them with a high-priority vulnerability. It's easy to fix. It goes through the pipeline and boom, it's fixed the next day or the next hour. Sometimes they might push back and say, 'This

isn't really a problem, and here are the reasons why.' We adjust the risk on that and prioritize it accordingly," he says.

Green conducts vulnerability scanning daily, weekly, or monthly, depending on the systems, but more granular, closer to real-time scanning has costs. "You start talking about a lot of data and a lot of infrastructure," he cautions. "If you're trying to scan a network as large as ours daily or in real time, there's a heavy cost associated with rolling out that kind of platform." ■

KEY POINTS

1 **Before meaningful vulnerable management is possible, you must know what you are protecting. This means building an asset inventory that includes asset owners.**

2 **If a business group does not agree with the security team's risk rank and prioritization, it should be able to explain why.**

BOBBY ADAMS

Senior Security Architect
TD Ameritrade

Bobby Adams is an intuitive technical leader offering hands-on skills and experience in enhancing system capabilities for both private and government organizations. He has a natural ability to determine solutions to minimize system vulnerabilities and improve security functions.

Website | LinkedIn

One of the biggest things I see in complex IT environments is people being paralyzed by all the analysis that needs to happen and all these tools that are telling you there are lots of threats in the environment," says Bobby Adams, who heads a team responsible for security architecture at a large brokerage firm. Paralysis sets in when people are faced with too many alerts and not enough resources to analyze or remediate them properly.

Adams believes the best way to address this problem is to apply a holistic cycle that tracks incidents and vulnerabilities from discovery to remediation and involves the entire enterprise. "Taking a holistic approach to security throughout an enterprise environment is key," he says. "You need to get that holistic life cycle in place and make sure that you have buy-in from all the other technical teams. You need that because you can't do security by yourself."

What does this kind of holistic cycle look like? Adams outlines these key elements:

- Document your program and get agreement from all stakeholders, including network administrators, server administrators, their management, and directors. Stakeholder buy-in across the enterprise is critical.
- Perform accurate scans routinely or even continuously across the entire enterprise.
- Tightly integrate scanning tools with other tools such as the configuration management database so that security tools are constantly aware of all assets on the network. "You can actually orchestrate and automate a lot of that kind of integration," Adams points out.
- Aggregate all threat intelligence from all tools and vendors into one centralized tool

You need to get that holistic life cycle in place and make sure that you have buy-in from all the other technical teams. You need that because you can't do security by yourself.

that automates threat intelligence. "Aggregating that threat intelligence to a single pane of glass makes it a lot easier to analyze what's happening in your environment," Adams says.

- Validate and prioritize vulnerabilities. Many scanning tools provide information about the severity of vulnerabilities, which should be part of your aggregated threat intelligence.
- Remediate vulnerabilities and install patches on a prioritized basis as quickly as possible. Also, validate through continuous scanning to see that those remediations are in place. "That vulnerability management life cycle is extremely important. You need to do it in a timely manner, and continuously," he stresses.
- Track scanning and remediation metrics to measure the effectiveness of your program.

Continuous scanning is an important part of Adams's program for both detection and validating remediation. "We're continuously scanning for those old vulnerabilities all the time. We don't remove those from our scanning signature. We're looking for how many have been detected, how many have been patched, and then we track that over time." Adams also likes to compare data from different tools. "I like to have multiple results from multiple tools. If I can use a tool that's not really a vulnerability scanner, but it can provide useful data, I will absolutely use that."

All these inputs provide a lot of data and threat intelligence that require deeper analysis. Adams's team is looking for ways they can automate their incident response front end to perform an even more in-depth investigation of all the alerts. He wants to create incident cases, have automated security orchestration and automated incident response, and be able to present all that in one place, drawing from every single tool in the environment. "I think the most critical thing is getting that data in front of the eyes of the people who need it the most," says Adams. ■

KEY POINTS

1 **Many scanning tools provide information about the severity of vulnerabilities. This needs to be part of your aggregated threat intelligence.**

2 **Continuous scanning is an important part of any vulnerability management program for both vulnerability detection and validating remediation.**

JOHN TRUJILLO
AVP, Technology
Pacific Life Insurance Company

John Trujillo has 30 years of experience in the IT industry. He began his career in application development and then migrated to enterprise infrastructure and information security. Since 2001, he has worked for Pacific Life Insurance Company, where he leads the information security and IT infrastructure practices for his business unit. He holds a BS in Computer Information Systems and an MBA from the University of Redlands.

in
LinkedIn

John Trujillo believes vulnerability and risk management for digital assets is part of a larger business challenge. "If I lose a system to a physical event or I lose a system to a logical attack, the business ultimately doesn't care. In the aggregate, you need a comprehensive risk assessment and management program, of which security is a critical component."

From that perspective, the question becomes how you evaluate vulnerabilities of your digital assets to decide which ones are most critical. "I think you need to understand the business function of the assets that you're securing," says Trujillo, who heads the information security and IT infrastructure in his unit at Pacific Life Insurance Company. "You have to understand the costs of losing any given configuration item, and then have that configuration item roll up into applications, which in turn roll up to the business processes." He believes any vulnerability-management program needs to be integral to business process and enterprise architecture. "You need a program that at its inception partners with the enterprise architecture, because the enterprise architecture has to be constructed in such a way that your risks are mitigated."

To accomplish this, and to have effective risk management, there need to be standards, perhaps similar to a credit score around how risks are identified, how they're ranked, and how they are either accepted or remediated. This would include having remediation plans tied to business risk criticality, so that higher risks have higher priority, and there is enough information for business decision makers to decide how to handle certain risks. "After a certain amount of time you either have to remediate the thing or re-accept it formally. But all of the specifics around that are dependent on your particular industry and your particular company's appetite for risk," Trujillo explains. »

> *"You need to understand the business function of the assets that you're securing."*

Given the growing complexities of enterprise architecture and the increasing reliance on web applications and extended networks to conduct routine business, effective vulnerability management depends on more continuous scanning and analyzing much larger volumes of data. Trujillo believes new tools are emerging to make this possible. "I definitely see a time where AI-assisted penetration testing is going to help companies do that continuous penetration testing," he says. "Today I can't afford to hire 1,000 hackers to bang on my environment. So we accept that risk to the degree that it is a risk."

If it's not feasible to hire an army of hackers, it's also difficult and costly to analyze all the data their efforts would generate. And it's not just data from continuous vulnerability scanning. There is also data from all the security and activity logs that are available for analysis. "Humans are the weak link," says Trujillo. "But when you get to a place where machines can do it, it becomes feasible for a company to start moving toward that kind of continuous vulnerability testing and automating the prioritization of remediation. Now I can start aggregating all my data and logs into a data link and have AI and machine learning start analyzing it."

However as you move to more automated, AI-driven tools

"When you get to a place where machines can do it, it becomes feasible for a company to start moving toward continuous vulnerability testing and automating the prioritization of remediation."

for vulnerability scanning and analysis, you need to have a solid vulnerability-management program in place. "All your governance has to be in place, your policies and procedures have to be in place, because you have to know where it is you want the machine to look, and what you want it to look for," Trujillo concludes. ■

KEY POINTS

1 **To have effective risk management, there needs to be standards around how risks are identified, how they're ranked, and how they are either accepted or remediated.**

2 **As you move to more automated, AI-driven tools for vulnerability scanning and analysis, you need to have a solid vulnerability-management program in place.**

TO MANAGE VULNERABILITIES EFFECTIVELY, DEFINE BUSINESS PRIORITIES AND IDENTIFY CRITICAL ASSETS

JAYESH KALRO

Director, Global Practice, CA Services
CA Technologies

Jayesh Kalro combines a strong technical background with business-management skills. He has led regional technical teams from diverse backgrounds, and has experience working with North America, Latin America, Europe, and the Asian market. With proven ability in building high-performing teams, he feels at ease communicating with all levels of management both internally and externally.

LinkedIn

For Jayesh Kalro, vulnerability management comes down to clarifying business priorities. "Your business defines your set of priorities, and your data is the most important thing that you're trying to protect. Where is that data stored? Those are your critical assets." says Kalro, the director of global practice at CA Technologies. Many vulnerability-management tools provide you with a scanning tool that can serve as the starting point for identifying vulnerabilities and threats, but you really have to look at the vulnerabilities, enrich that data with threat intel sources, and active exploits to assess your true risk posture. Identifying vulnerabilities is just the first step in managing your organization's risk effectively.

Most businesses want to prioritize identification of vulnerabilities relating to external-facing business, financial data, or customer data. "You want to make sure that these areas are secure and that they are your highest priority for remediation," he says. If you are using separate tools to aid in prioritization, then you will need to decide what is most important to the business and use that as your criterion. "In 99 percent of cases, businesses know that they want to protect their customer data," Kalro explains. "Companies cannot compromise anything with respect to their customers because it directly impacts their business. No one wants to make headlines because of a breach associated with customer data loss."

Successful vulnerability management also relies on strong processes. "How do you prioritize? How do you get that data and make sense of the data? I would say that having a strong process is something that a lot organizations miss out on," Kalro says. Smart vulnerability-management software can produce a report of key vulnerabilities to address, but from that point on resolution depends on proper internal processes. For example, one follow-up process would »

> *"Your business defines your set of priorities, and your data is the most important thing that you're trying to protect."*

be to have that report automatically kick off a help-desk ticket and assign it to a security engineer or administrator who would fix the vulnerabilities, then close the loop by monitoring that the patch was implemented successfully and provide a dashboard of risk measurements to management.

There are some ways that, in Kalro's opinion, businesses can speed up the process of identifying and acting on vulnerabilities in their environment. "You can build a process to collect all of this information, and you could pretty much automate the whole thing as long as you have the right data available," he says. Mapping the organization's most critical assets and the vulnerabilities associated with them can go a long way toward helping a business prioritize effective risk management. The real value will be seen when you have visibility to active exploits that could directly impact assets critical to your business. This supports a clear path to prioritization of what to remediate first. Finding a solution to provide this level of detail eliminates much of the work that security teams currently tackle and never finish.

Kalro has seen a couple of organizations capitalize on automation to speed up their vulnerability-management processes. "Because they had the process laid down, they were able to react with more

agility and speed," he says. This process proved valuable at one company when a person was suddenly let go. The security team received a notification about that person's termination and then simultaneously deactivated his access privileges across all the systems he had used. This process, which used to take days, was completed within a matter of hours, and the business was able to more effectively manage the risk of a potential insider threat.

It can be challenging for today's businesses to manage the vulnerabilities in their environment, particularly if they are operating with lean resources and juggling multiple priorities. But by defining their most critical assets and the vulnerabilities connected to them and then automating the processes for managing those vulnerabilities, they can manage these risks far more effectively and thus better protect their organizations from the threats they face. ■

KEY POINTS

1. **Businesses must first define their priorities in order to effectively manage vulnerabilities in their environment.**
2. **Automation can provide businesses with a powerful way to speed up their response time and react to threats with greater agility.**
3. **Understanding active exploits in your IT infrastructure provides a clear path to an improved cyber risk profile**