June 2023

Vulnerability management:

A maelstrom of moving targets

CRA | Business Intelligence
A CyberRisk Alliance Resource

LACEWORK

invicti
AppSec with Zero Noise

Contents

ALSO IN THIS REPORT

FOREWORD

All eyes on us

"Come gather 'round people
wherever you roam
and admit that the waters
around you have grown."

– BOB DYLAN

The security technologist and author Bruce Schneier says "a system is only as secure as its weakest point."

Think back to some of the biggest breaches in recent years: Capital One in 2019, SolarWinds in 2020, or Accellion in 2021. Were these organizations haplessly bungling their entire cybersecurity operation? Or did they do nearly everything right against a threat landscape where nearly wasn't enough?

In fielding this survey, our team wanted to get an honest, unfiltered look into what vulnerability management (VM) looks like for the practitioners who swim in that world. What types of vulnerabilities do they track? How do they prioritize them? Do they have a formal program with dedicated VM personnel and tools? Or do efforts resemble an unending game of whack-a-mole, in which security teams must MacGyver whatever is at hand just to get through another day?

We got answers to these questions, but we also got much more: a revelation that respondents are looking inward, not outward. They're not focused so much on the bad guys exploiting these vulnerabilities, so much as they're focused on the home turf failures that allow these exploits to take seed in the first place — lack of support from upper management, IT staffing shortages, policies that favor user convenience over strong security, insufficient funding, legacy systems that resist patching, cloud vulnerabilities, fragmented visibility of IT assets, false positives, lack of automation, the list goes on…

More importantly, these challenges are inseparable from the business mission. Fail to address them, say respondents, and you fail the business. Our hope is that this data advances the conversation so organizations can address these challenges with the same rigor and urgency they address other business priorities, and that they commit to doing so in a way that champions those on the frontline of VM.

"For the times they are a-changin'," Bob Dylan once sang. "And the waters have grown." Will organizations find a way to swim above the currents, or will they sink like a stone?

Vulnerability Management 101

VM is a continuous, repeatable process of identifying, reporting, and remediating cyber vulnerabilities that manifest in the IT environment. Vulnerabilities are any weaknesses that could allow an unauthorized entity to gain a foothold in the network. Insecure code, unpatched IT, misconfigurations, bad business processes, and even lack of user awareness are all examples of vulnerabilities.

A VM program defines the structure, scope and responsibilities of VM. The program enables organizations to track the status of IT assets, prioritize vulnerabilities based on risk and exposure, ensure compliance, measure time to remediation, prevent the reintroduction of known vulnerabilities, and minimize the attack surface overall. A program is essential for configuring vulnerability management to support business processes and objectives.

VM involves a sequence of well-documented procedures. Organizations must assess their attack surface, using automated tools to scan for common vulnerabilities and exposures (CVEs) and monitor health of IT assets. They must then prioritize which vulnerabilities to address first, and then act by eliminating possible exploits. Finally, they should reassess to verify that patches were applied correctly and improve existing policies or processes to prevent reintroduction of vulnerabilities.

> “To improve our VM program, we need to invest in the right technology solutions, establish robust processes and procedures, and allocate resources effectively. Addressing these challenges can help reduce risks to our business-critical assets and ensure the security and reliability of our network.”
>
> – SURVEY RESPONDENT

Four key findings from the survey:

1.

There's no one way to manage vulnerabilities.

Respondents showcase different methods for tracking vulnerabilities and coordinating security updates. For example, 54% use a dedicated VM system for all security, while 41% use separate workflows to track different types of vulnerabilities. Some employ an issue tracker, while others rely on manual communication to get the job done.

2.

Resourcing is a universal challenge.

Most frustration is reserved for how funding and staff are allocated, as well as a perceived lack of automated capabilities to support VM. "We don't have the time, money or staff for these activities, and leadership is not supportive," said one respondent.

3.

Legacy systems have prevented some from patching vulnerable tech.

For the most part, just 51% approve of how their org has decommissioned old IT to ensure proper patch management. In addition to vulnerabilities, poor configuration of systems has multiplied false positives and alerts that some organizations struggle to stay on top of.

4.

Business planning and sound policies should be integral to VM.

Respondents repeatedly mentioned pain points related to organizational growth, asset management, and getting buy-in from both upper management and end users. As one respondent voiced, "Our organization has grown significantly in the last 3 years. With 40,000 colleagues and 13 organizations coming together, the process can be slow and different across each entity, which requires more time and resources to remediate."

1

STRATEGY AND PROCESS

Keeping track of it all

Heraclitus said that no man ever steps in the same river twice, for it's not the same river and he's not the same man. He might as well be speaking about today's IT security landscape, though, with its frequent updates and patches, newly discovered vulnerabilities, and explosive growth in endpoints and Internet-facing assets. How can one possibly keep track of it all?

For respondents, at least, there's more than one answer. Over half use a dedicated VM system to handle all security issues, 44% use a standard issue tracker, and 41% choose to use separate VM workflows. A standard issue tracker appears to be the tool of choice for tracking most things, but at least one-third lack a formal process and manually communicate findings to their internal developers to act on.

When it comes to types of vulnerabilities that are tracked, there's nearly equal attention given to system software Common Vulnerabilities and Exposures (CVEs), network device CVEs, and web application CVEs. However, less attention is given to web app vulnerabilities that are not publicly known or registered in the National Vulnerability Database (NVD) database. What this tells us is that respondents prioritize public databases containing the latest, verified CVEs.

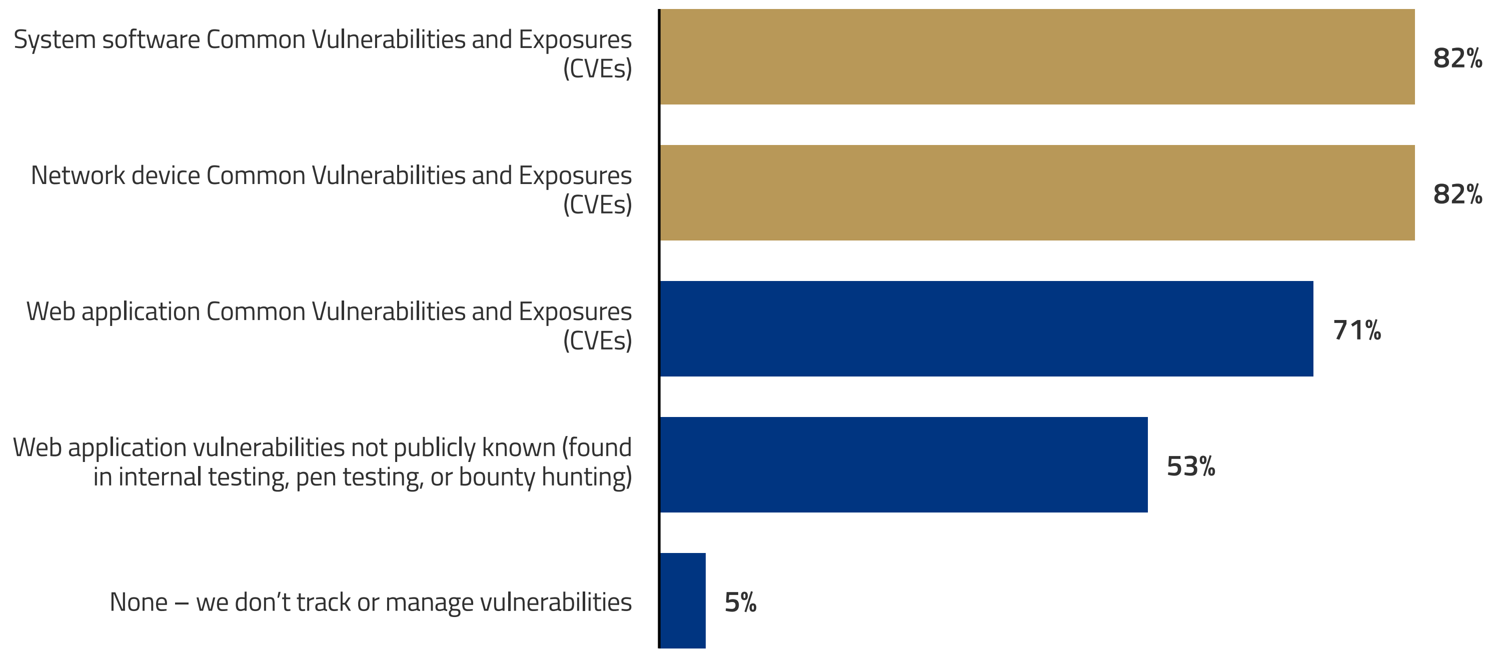
54%

use a dedicated VM system for all security issues

At least 8 in 10 respondents report their organization tracks and manages system software CVEs and/or network device CVEs. Fewer track Web application vulnerabilities found in internal testing, pen testing, or bounty hunting.

> "The lack of a complete and updated asset inventory is another significant VM problem. Because we don't know what we have."
>
> – SURVEY RESPONDENT

Vulnerabilities tracked and managed



Note: Respondents were asked to select all that apply.
Base: All respondents (n=210).
Source: CyberRisk Alliance Business Intelligence (CRA BI), Vulnerability Management Survey, April 2023.

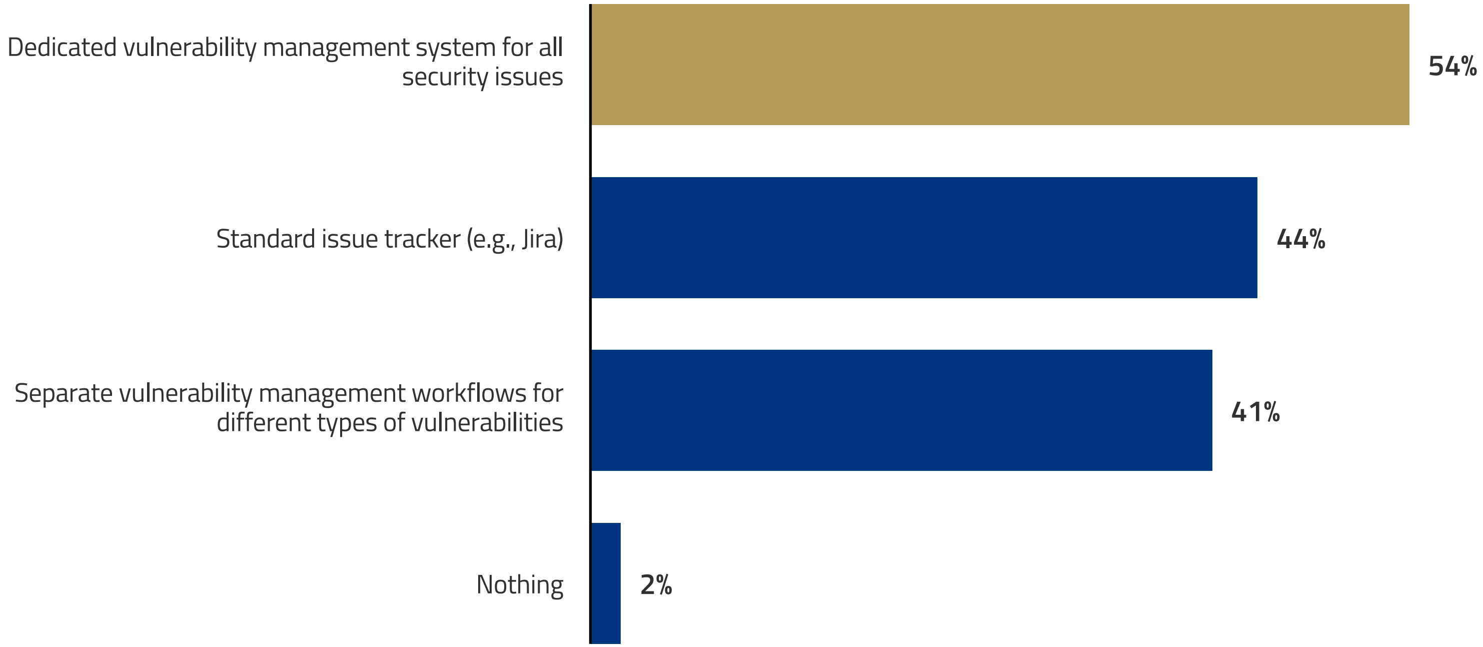
Which of the following types of security vulnerabilities does your organization track and manage?

System software and network device CVEs are the most typical types of security vulnerabilities tracked and managed.

Just over half of respondents report their organization uses a dedicated VM system for all security issues. Slightly less use a standard issue tracker, such as Jira and/or separate VM workflows for different types of vulnerabilities.

> “Some vulnerabilities require a lot more than just patching and updating. These ones are harder to get support from management.”
>
> – SURVEY RESPONDENT

Vulnerability tracking and management methods/tools



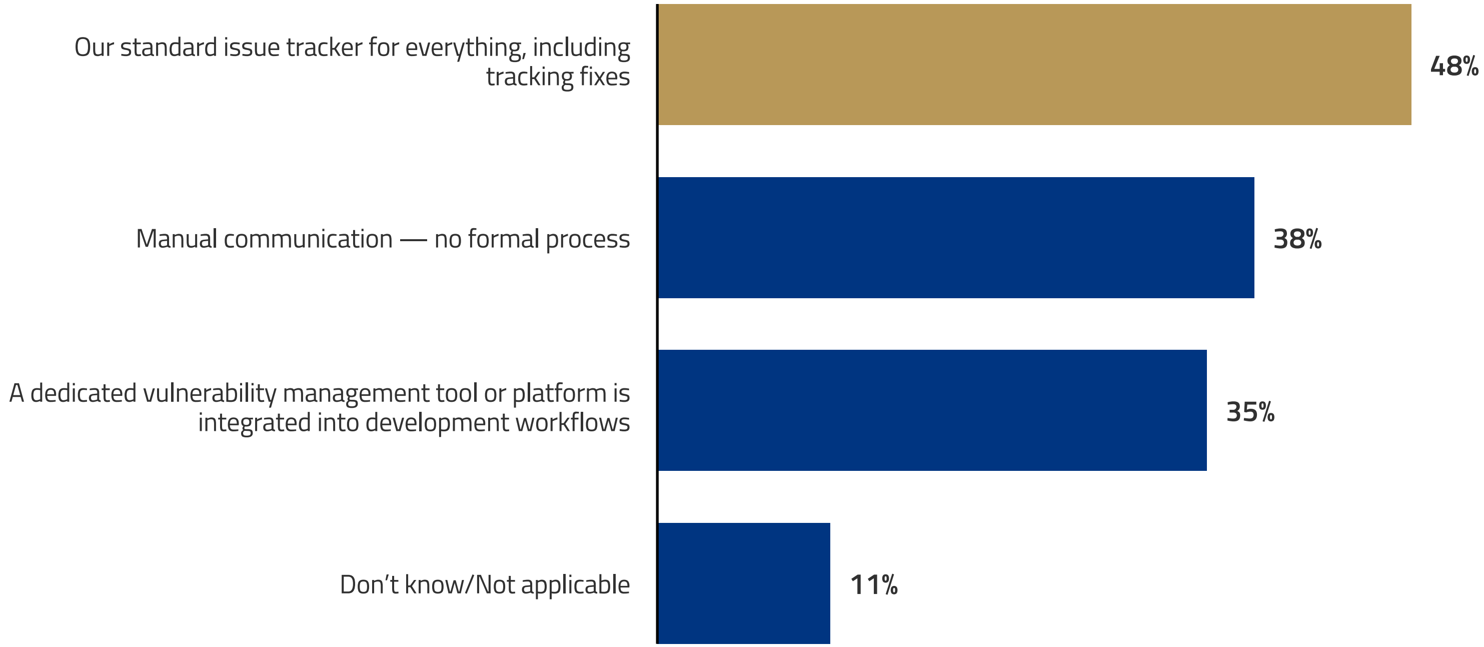
Note: Respondents were asked to select all that apply.
Base: All respondents (n=210).
Source: CyberRisk Alliance Business Intelligence (CRA BI), Vulnerability Management Survey, April 2023.

Which of the following does your organization use to track and manage security vulnerabilities?

Slightly more than half of all respondents say their organization has a dedicated VM system to handle all security issues.

When coordinating security enhancements with internal software developers, nearly half of all respondents say their organization uses their standard issue tracker for everything, including tracking fixes.

Used to coordinate security enhancements with internal software developers



Note: Respondents were asked to select all that apply.
Base: All respondents (n=210).
Source: CyberRisk Alliance Business Intelligence (CRA BI), Vulnerability Management Survey, April 2023.

Which of the following is used by your organization to coordinate security enhancements with internal software developers?

Only 35% say their dedicated VM tool or platform is integrated into development workflows.

> "The sheer volume of changes makes it difficult to keep up with the patching required. Automation is essential, but not always included with standard systems."
>
> – SURVEY RESPONDENT

2

RESOURCES AND SUPPORT

VM capabilities

If we had to summarize respondents' assessments of their organization's VM capabilities, we'd say it was only lukewarm — with more praise given to methods and processes than to resourcing and support from the broader organization.

According to ratings respondents assigned to indicate the extent to which their organization implement various VM methods and processes, prioritizing vulnerabilities appropriately and following best practices for device configuration were top focus areas, with average scores of 5.6 and 5.4 (out of 7), respectively, while formally identifying and remediating vulnerabilities and eliminating legacy systems that would conflict with patch management scored much lower at 5.0 and 4.5, respectively.

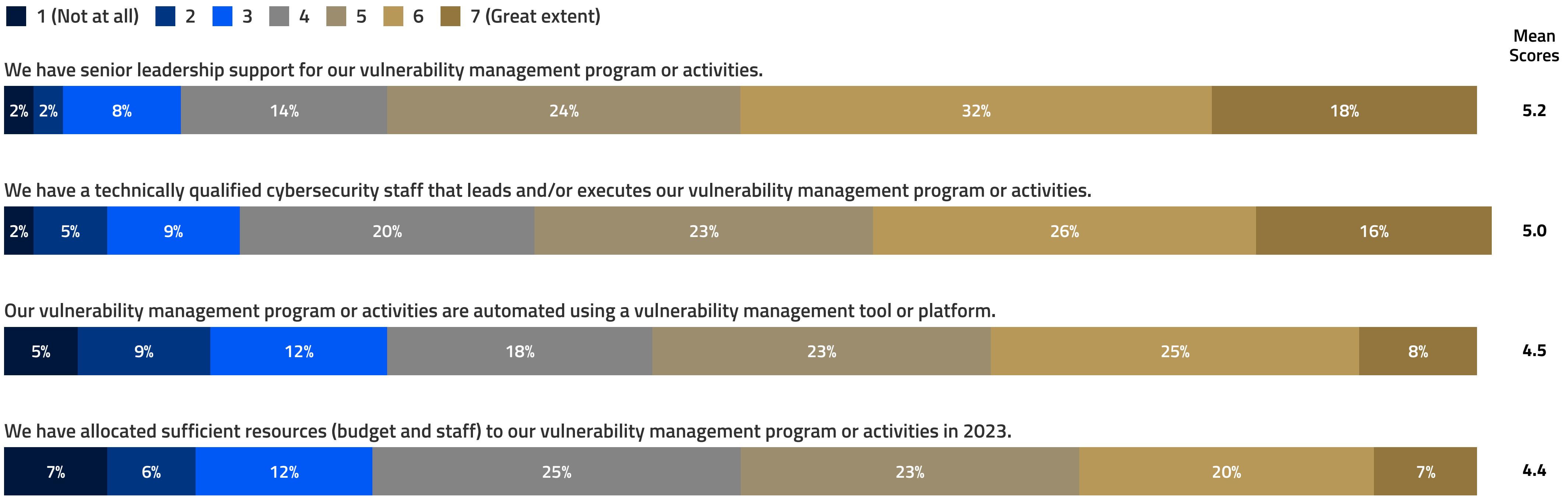
Failure to eliminate legacy IT could additionally be linked to levels of resourcing, which respondents often identified as a roadblock in their VM efforts. At least one in four respondents say VM activities aren't nearly as automated as they could be, while a similar share believe their employer has failed to allocate enough staff and budget for VM activities in 2023.

50%

mostly have senior leadership support for their VM program or activities

50% of respondents indicate their organization's VM program or activities has senior leadership support to a large/great extent.

VM resources



Note: Respondents were asked to rate each on a 7-point scale where 1 is "Not at all" and 7 is "To a great extent."
Chart shows percentage of respondents who provided each rating from 1 to 7; not all totals sum to 100% due to rounding.
Base: All respondents (n=210).
Source: CyberRisk Alliance Business Intelligence (CRA BI), Vulnerability Management Survey, April 2023.

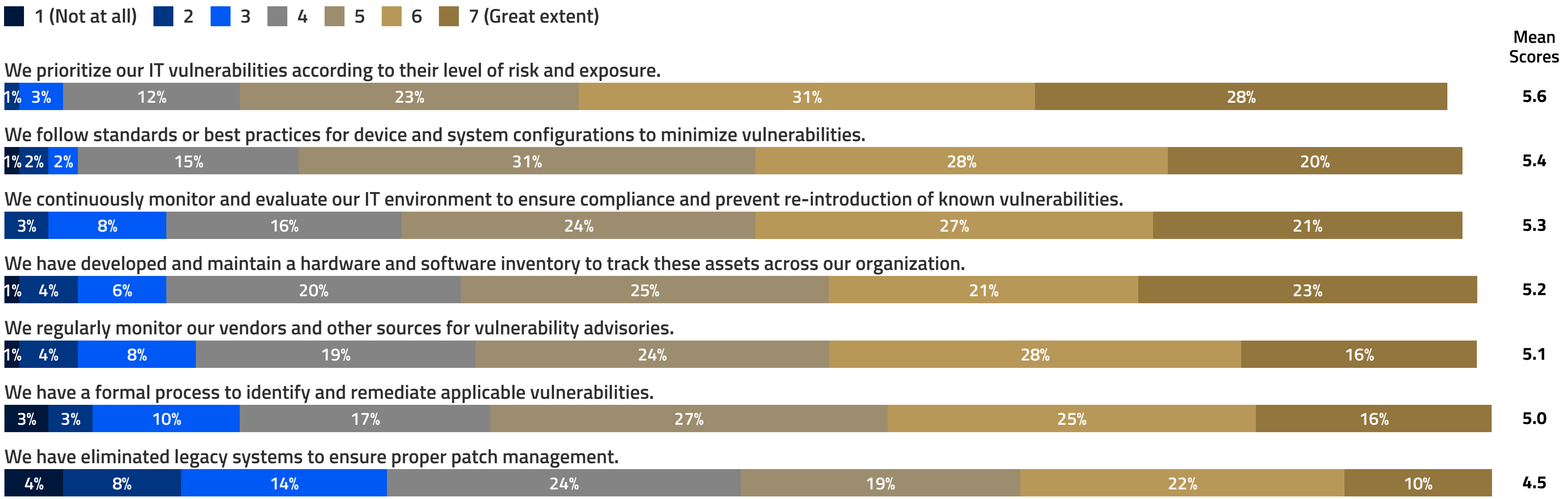
To what extent does each of the following describe your organization's vulnerability management resources?

Respondents' mean scores for VM resources range from a low 4.4 for allocation of VM budget and staff to 5.2 for senior leadership support for VM programs or activities.

The overall mean score for VM resources is 4.8.

59% of respondents say that for the most part, their organization prioritizes their IT vulnerabilities according to their level of risk and exposure.

VM methods and processes



Note: Respondents were asked to rate each on a 7-point scale where 1 is "Not at all" and 7 is "To a great extent."
Chart shows percentage of respondents who provided each rating from 1 to 7; not all totals sum to 100% due to rounding.
Base: All respondents (n=210).
Source: CyberRisk Alliance Business Intelligence (CRA BI), Vulnerability Management Survey, April 2023.

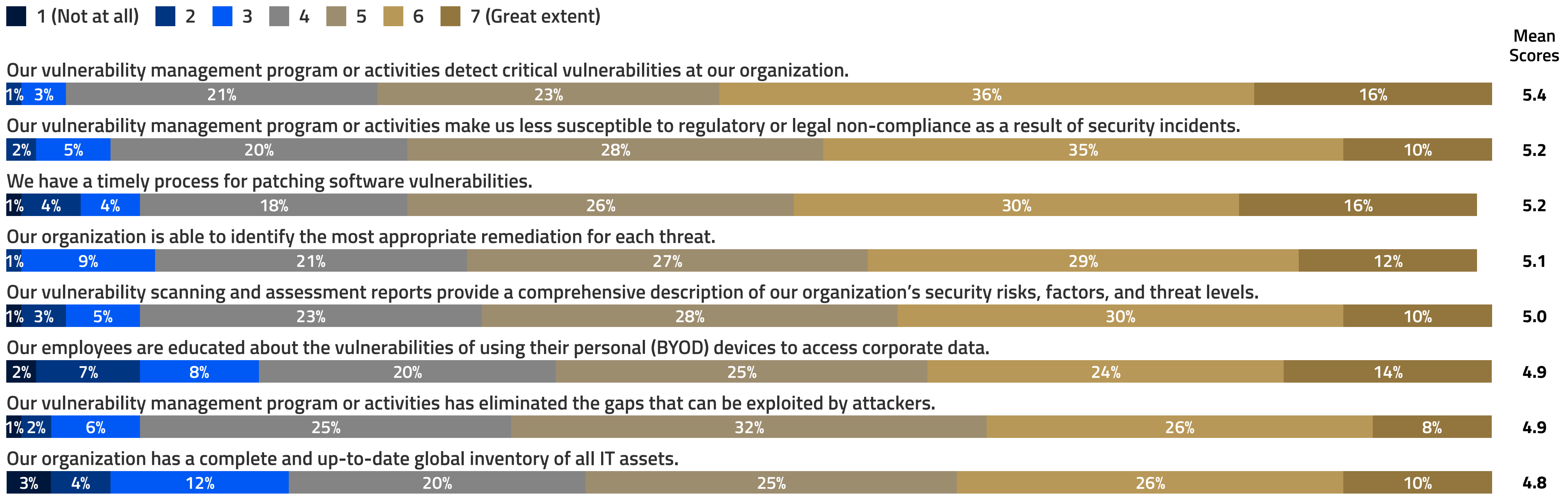
To what extent does each of the following describe your organization's vulnerability management methods and processes?

Respondents' mean scores for VM methods and processes range from a low 4.5 for eliminating legacy systems to ensure proper patch management to 5.6 for prioritizing IT vulnerabilities according to their level of risk and exposure.

The overall mean score for VM resources is 5.2.

Only 34% of respondents indicate their VM program has to a large/great extent eliminated the gaps that can be exploited by attackers.

VM outcomes or results



Note: Respondents were asked to rate each on a 7-point scale where 1 is "Not at all" and 7 is "To a great extent."
Chart shows percentage of respondents who provided each rating from 1 to 7; not all totals sum to 100% due to rounding.
Base: All respondents (n=210).
Source: CyberRisk Alliance Business Intelligence (CRA BI), Vulnerability Management Survey, April 2023.

To what extent does each of the following describe your organization's vulnerability management outcomes or results?

Respondents' mean scores for outcomes/results range from a low 4.8 for having a complete and up-to-date global inventory of all IT assets to 5.4 for their VM program's ability to detect critical vulnerabilities.

The overall mean score for VM outcomes or results is 5.1.

3

CHALLENGES AND OBSTACLES

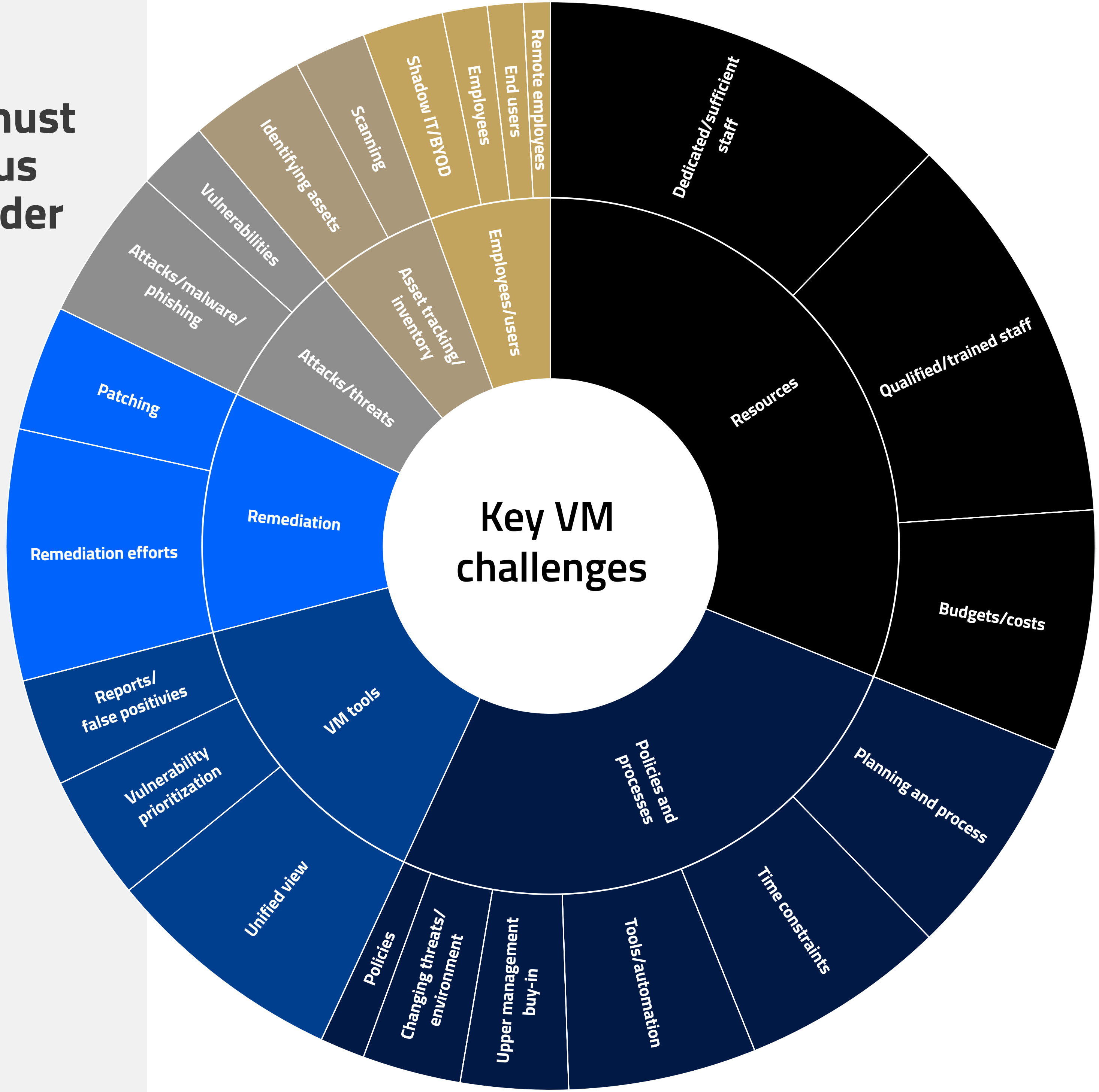
Prevailing in an ever-changing threat environment

The challenges standing in the way of effective VM are many.

From specific pain points (like the lack of a centralized inventory of IT assets or the use of spreadsheets to manually catalog vulnerabilities), to broader HR problems (like inadequate staffing and lack of user training), to failed business processes (like communication between teams and internal stakeholders) — respondents pulled no punches in detailing the myriad issues plaguing their organizations.

Taken together, these obstacles stunt VM programs and overwhelm security teams, making it extremely difficult to address weaknesses proactively, particularly when new threats emerge on a daily basis. "Staying ahead of the constantly changing threat environment is by far the most difficult aspect of our cybersecurity management, even with the advanced tool set that we have," said one respondent.

Organizations must overcome various challenges in order to implement an effective VM program.



What are your organization's challenges or issues in effectively using vulnerability management to reduce the risks to your business-critical assets?

Note: Respondents were asked to describe any challenges or issues with strategy, technology, solutions, or processes they would like to resolve to improve their organization's VM program or activities.
Chart shows main topic categories (inner ring) and topics within those categories (outer ring).
Chart segments are sized based on number of respondent comments mentioning these subtopics.
Source: CyberRisk Alliance Business Intelligence (CRA BI), Vulnerability Management Survey, April 2023.

VM challenges

Organizations are confronted with a variety of roadblocks in implementing an effective VM program. Survey respondents reported everything from inadequate human and financial resources to ineffective policies and processes, remediation and patching issues, employee and user awareness and behaviors, and keeping up with persistent and changing threats and attacks.

Resources

"Personnel and financial resources are the biggest barriers affecting VM. In many ways they are related. In order to truly be good, I will need more of both."

VM tools

"Alert fatigue from the tools, automated fixes cause issues with custom apps."

Asset tracking/inventory

"We do not have a complete and accurate asset inventory that we have confidence in."

Policies and processes

"Lack of management buy-in. Their idea that being a small business will make us less of a target is wrong. Everyone is a target and security needs to be an ongoing spend, not a one-and-done purchase. A firewall is not enough anymore."

Attacks and threats

"The main challenge is just keeping up with the various styles of attacks and generally staying informed."

Remediation

"Not all our VM tools are integrated with our patch management tools. Remediation is more of an automated process on those that are. Manually tracking progress on remediation efforts is tedious."

Users/employees

"We have struggled with [our] system in part due to employees all using BYOD devices and their unwillingness to allow us to enable and enforce certain management polices."

4

STORIES FROM THE FRONTLINES

VM challenges, lessons learned, and best practices/tips

This section features first-hand accounts from two cybersecurity leaders — a CTO and a CISO — who shared their perspectives in follow-up interviews about handling various VM issues at their respective organizations. We heard about the challenges they are encountering in the field as well as lessons learned from their experiences. They also offered some valuable best practices and tips for improving overall security posture and VM health.

Whether learning from the bombshell discovery that was Log4j, navigating shortages in resources and personnel, or identifying broken business processes, these cybersecurity pros made clear they are eager to update the vulnerability management playbook to address the latest generation of complex security challenges.

Challenges: Dealing with legacy tech

Aging legacy technologies can present liabilities to vulnerability management programs. These systems may not 'play nice' with newer technologies and struggle to scale with modern workload requirements. Eventually, they lose the dedicated support of vendors responsible for patching them, which makes them more susceptible to an attack.

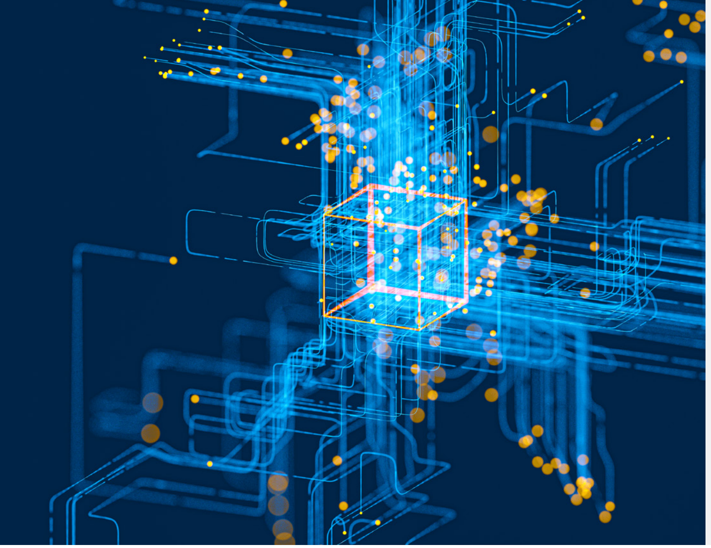
"On [Amazon] EC2 we have systems where unfortunately no more updates are available. **Applications were only developed to support certain types of operating systems or third-party plugins that you can't update without breaking the native functionality.** This creates exploitable packages that are available for script kiddies or hackers to use. And so we're stuck in that unfortunate manual type of monitoring for abnormal behavior, using layered compensating controls on those assets.

The hardware itself is even more difficult because once those are deployed out into the field, there's little to no update unless a customer returns the device, or they want to give up or upgrade their device. They're maybe not deploying the latest and greatest firmware at the time, but it's still something that's supported. Then over time that ages out, and there's a downstream effect of not having to support the device out in the field. We're left in this scramble where we're really good about doing stuff that's new — like enhancing through automation — but the stuff that was deployed before those processes were in place are still a pain, such as tracking them in the annotating platform and managing the risks and exceptions and exposures."

"We're an 88-year-old organization, so there's been decisions and cans kicked down the road which continue to support legacy solutions. **It's also a little bit of our organizational culture, which doesn't want to say no to our customers or our vendors and partners, and that typically leaves you in a situation where you have one solution that's being supported on really outdated and obsolete technology, creating the most amount of risk.**

Look at Windows Server 2008 as an example, which had its end of life [years ago] when Microsoft announced they weren't going to support it anymore. Well, we just last week retired all of our Server 2008 servers, all the while we've been obtaining specific patches from Microsoft to apply them. That's an example of where your risk posture goes out of the roof, because a zero-day on that is nowhere close to anything else that you get out in the industry.

We're on a mission to try and remove obsolete technology from our organization. I have a significant amount of support, but that's just something that we're not good at. We're really bad at retiring and rationalizing solutions. And so my strategy over the next few years is to really tackle that. If we did that, we would operate it less. And if you operate it less, you have less capacity going towards operating the solutions and more going towards building new capability."



Challenges: Automating VM

Automating vulnerability management can help organizations respond to threats much faster and deliver richer context for decision-making. While providing a more efficient alternative to manual processes, it's important for organizations to configure automation to serve the business so as not to create more problems than it can solve.

"Our security engineers that we have doing security automation are so critical to stitching together the outputs that come from scans, from API calls, and normalizing the actual information if it's really critical or high. **But where we're still struggling, and I think a lot of companies are struggling, is automating vulnerability management to pair up with the business value or materiality or context.** Not all tools can ingest the right level of tags or the right level of materiality. So there's still a little bit of normalization if it doesn't fall into the right bucket of criticality. But for the most part, it's pretty well automated.

When it comes to my team, in order to be the most effective and not slow down the velocity of our teams and their sprints, we have to embrace automation, and in such a way that integrates it into the existing team's processes.

What we've done is taken on the actual creation or modification of Terraform templates, when we're referring to standard build images or to third-party services that they're using. If we've identified a component that requires resolution, either through patching or through updating the base image or the third-party repository or open-source project that we're pulling from — if there's validation that's required from the analysis tools, we'll get it and actually modify the scripts to adjust the automated builds. Depending on the confidence level coming out of the tool with its operating system, we're taking recommendations straight from our cloud platform that does vulnerability management and adjusting the scripts."

"Automation for us is relatively new over the last couple of years. I think Covid drove us to have better insights over different threats and different vulnerabilities. And being in a highly regulated space, we needed to have something like that, because otherwise your only way to address it is through labor and staff — and that becomes time-intensive. So having that level of automation is necessary to us.

The first thing about automation is that it's costly, because you go through an effort to automate your entire code base and your entire posture. It's taken us a good part of over two and a half years to even have 50% to 60% of the coverage that we were looking for.

Is it perfect? Absolutely not. **There's a lot of unknowns, bad responses, a lot of alerting and a lot of noise in the system.** A lot of false positives that we're trying to get better at and fix and work with the vendor on what we're seeing. But the level of transparency has been incredible, because now we have dashboards and reports that we're talking about and it's not just someone's gut feeling of 'I think this should be done a certain way.' So we're looking at data and trying to react to it, versus reacting to someone's more qualitative feeling around it."

Challenges: Getting complete visibility of all IT assets

The modern operating environment is fast-moving and fraught with numerous complexities. From endpoints and sensors, to multi-cloud environments and microservices, it's critical for organizations to keep a watchful eye over their entire inventory of IT assets.

"I desire information down to the data element level within the databases, but what I have visibility into stops short at the asset itself. I know there's a database, I know there's an EC2 instance, I know those serverless calls go on. But the difficulty we have in maintaining parity with the speed of business is how fast those serverless calls are updated when information is going across them in the databases themselves. If I have information that sits side by side, then one might be sensitive, one might be public, one might be restricted — and not everything is following the right types of tags, with the right types of data hygiene. We're still behind on getting down to that level of granularity and then being able to track and assign ownership.

We have a pretty good handle at a macro level, but I still don't have the complete visibility that makes me comfortable enough that I'm making the best, most-informed decision. And that's what we're striving towards: getting down to that service and data element layer on where all of our information resides so we can know who's actually using it and what the lifecycle of that data looks like. Those are really the next steps in the evolution of our [vulnerability management] program.

It's not going to be in a single pane of glass — that will never exist and it never has. We've been after that for how many years or decades in security? What I care about is a high-enough level of efficacy on the regex or the identification processes, how tight they can fit in and integrate into my existing data structures, and how easy it is for me to pull that data out and massage and manipulate it. Because if I can get a hook in or an access to the platform that's pulling that information, then I can plug that in and pair it up against all my other data stores."

"We use a combination of an integration platform as a service to plug in all our different tools and move workflows amongst our different capability sets. We use a variety of automation techniques across all of our data sources to make decisions, and push and pull information back to the dashboard. And we've tried to stay out of going all in on a 'single pane of glass' from any one provider because it just doesn't exist.

It's difficult to get the single pane of glass view. We recently just wrote some software for any leader to have access to what their team is using and what devices have been provisioned for them and whether they've been returned or not returned. Asset tagging has been part of our process for a long time, and so I think we have visibility into it. But all of these things can keep getting better because the endpoint is where the challenges typically occur.

I can't certainly sit here and say that I know exactly what those 10,000 devices that interact with our network have going on at any point in time. So we have some visibility and are continually getting better, but I'd say it's not a huge challenge for us."

Lessons Learned: The Log4j wake-up call

In 2021, security researchers discovered a critical vulnerability in the Apache Log4j logging library that allowed attackers to execute malicious code remotely by exploiting the library's processing of log messages containing specially crafted strings. As Log4j is one of the most popular packages for Java and present on billions of devices, researchers estimate that finding all new instances of this vulnerability across enterprises and vendors could take years. The cybersecurity leaders we interviewed shared these perspectives on Log4j.

Adjust the methodology as needed

"A lot of us in the industry changed our methodologies during the whole Log4j fiasco. In one sense, it was a very positive event that tested our automation. But here's the kicker — they changed the fixes how many times within that first week? I think it was three times before they ultimately had a fix that really addressed the underlying issues. And we were pushing up against the limits of pace. **When you're trying to automate or push that many critical fixes in a short period of time that have unknown effects that you're not able to test, you have to adjust your response**. So that's what we did, in order to do more testing and allow for greater changes."

Plan for more lag time

"That was probably the biggest lesson learned: more lag time. The business wanted more testing and vacant time to see whether they had to make just one change or whether there were going to be multiple changes within a short window. **While it was good to understand the complexity of issues like that, it was bad from the standpoint that within any vulnerability management program — no matter how close you're automating — there's still a limit to how many changes engineering teams want to have to their production systems in a short period of time.** Log4j caused us to scale back the velocity on those."

Test and vet third parties

"With Log4j, we were probably luckier than most because we hadn't updated to the most recent version. So the impact on our blast radius was a lot smaller for us. **But it's just something that we never thought of — a third party vendor, and there are solutions, libraries and things they use.** As a result, it brought third-party vendor management into high visibility. The importance of testing their posture, their solution, and how they remediate or what type of lifecycle they are on."

Lessons Learned: Tying VM to the business

While IT security teams may steer the ship, vulnerability management is a business-wide responsibility and challenge that demands vigilance, support and understanding from the whole crew (i.e., business leadership and non-technical end users).

Keep the lights on

"Vulnerability management should be lumped in the bucket of 'keep the lights on' as operational support for the availability of your products with customers. That's the way we've approached it from day one. **The DevOps team, and the software engineering and IT teams are really good about keeping customer-facing services either up to date or n-minus-one.** And that same process supports patches and updates."

Change the behavior

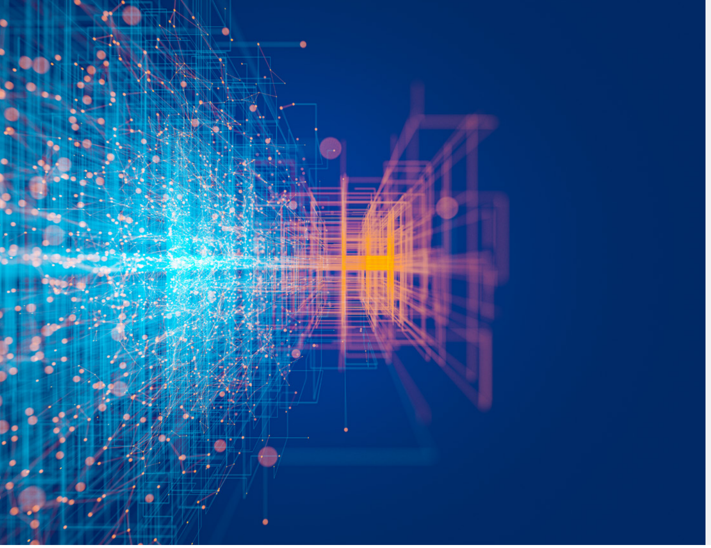
"The hardest thing was helping folks change behavior to think about what could be built into their automation templates. But once you've refined the process so that they know what they're now responsible for and you've given them the guardrails to operate within, it becomes much easier. The business has come to understand that those are as equally important as providing services that follow your five nines principle in uptime or in pushing out an enhancement."

Stress visibility and ownership across the business

"Unless vulnerability management turns into everyone's problem, you're leaving things behind that can significantly help you. It's not just about risk reduction. In today's day and age, the impact to your business can be significant—whether that's through ransomware, the inability to actually operate or being completely denied from service. **Every time you don't take action to better your vulnerability posture, you're leaving something out there for bad actors to exploit and cause serious damage to not just your reputation, but your business.** It's extremely important to create that visibility across the organization and not just make it IT's problem."

Advocate for availability of services

"A lot of it goes back to culture. Why does it help to make sure something's up to date? **Because you want your customers to be able to access your services at the highest frequency and percentage of available time.** And the fewer instances and the less potential there is to disrupt that, the less opportunity somebody has to take your service offline."



Lessons Learned: Prioritizing vulnerabilities

While the cybersecurity leaders we interviewed are generally confident in their ability to prioritize vulnerabilities, there are other resource needs and intangible requirements that do not receive the same level of consideration.

Translate the impact of risk exposure

"If I had an easier way to inform the business on the tradeoffs that they're making or the value that they're delivering based on the information I'm bringing to them from something that's not being taken care of in an automated fashion, it would make those prioritization decisions much easier from a product and from a SCRUM perspective. **The biggest challenge is translating material cost and impact into risk exposure (or cyber value at risk) for identified issues.** It's too manual and it doesn't have to be."

Agree on the priorities

"Operational downtime associated with something being exploited is completely different than prioritizing fixes. When you start talking about compensating controls and all the things related to VM that you can't automate your way out of, having an easier way to pair that up against what the exposure is and how material it is from a risk perspective — that's something I can tie together. **Then, when I communicate that to audit or risk committees, everybody is at least aware of what's prioritizing the work and the tradeoffs we're making.** There's less room for somebody to call anybody out on using their personal judgment because we now have that organizational agreement on what exposure and vulnerability and downtime means."

Implement reserve capacity

"The ability to prioritize is probably the biggest concern for the organization. Over my last year, I've been able to implement some reserve capacity to address governance, compliance and automation types of tasks and efforts where that's the only focus. But there's still this notion of running towards where the dollars are at, and it does cause some concern. **We're also moving from a project to a product world, and in the product world, there's a lot of product owners that are coming from a business and still learning about technology.** Recognizing what a good platform can do or what a compliant solution can do is something that they still need to learn."

Best practices and tips for VM

Here is a summary of the best practices and tips for VM shared by the two cybersecurity leaders we interviewed.

Start with the known knowns

"Don't worry about what's happened in the past. Identity your known knowns, build processes for them, and then figure out what you can improve going forward. **Once you have a solid, workable process that meets some of your MVP [minimum viable product] characteristics that you've defined, get folks comfortable with that.** You can always go back and take things off your backlog and retroactively fix. "

Go big on zero trust

"Start adopting the zero-trust mindset. **Above and beyond, it's about knowing where your business workflows map to your data applications, assets and services. Not all vulnerabilities are created equal, not all impacts are equal.** You got to know how the business makes money, you got to know how people work. So just have a solid understanding of that before you start automating and building in fixes defined to your protect surface."

Include objectives that raise awareness of your VM policy

"Your policy or vulnerability management program should have objectives associated with it. The literacy that comes with it, whether that's for educating your employees, your customers, your partners, is a very important aspect of it. We tend to forget that software aside, humans are probably the ones that make the most mistakes. **So having objectives that make room for the human element and account for their education is a critical aspect.**"

Make quantitative-based decisions

"Look for a tool or solution that raises visibility and automates how you get insights through data. Rather than basing your decisions on a qualitative feeling, get to more quantitative decision making. **Tools that provide dashboard visibility or regular reporting can add transparency and enable your team to react to data rather than just reacting to a gut feeling.**"

Be realistic about what you can control

"This is 90% behavior, 10% knowledge — and our tools and our partners can give us knowledge pretty quickly. It's all about how you handle it, and how easily you make it for the business to consume. Many folks have a purist mindset — which can be good — but they don't translate that actual practice. **You have to be a pragmatist when resolving issues because businesses operate in a state of constant risk.** As long as you're following a set process that folks agree on, you're doing your job. It's all about making it better — just stay focused and do the right things that you can control."

Survey methodology

The data and insights in this report are based on an online survey conducted in April 2023 among 210 security and IT leaders and executives, practitioners, administrators, and compliance professionals in North America from CRA's Business Intelligence research panel.

The objective of this study was to explore the issues and topics related to vulnerability management, including strategy, methods/processes, capabilities (tools and resources), and challenges.

Additionally, two cybersecurity professionals leading their organization's IT and/or cybersecurity practices volunteered to participate in a confidential follow-up phone interview to share their VM experiences, challenges, lessons learned, and best practices/tips for VM.

Notes:

Not all figures add up to 100% as a result of rounding percentages.

The respondent profile is as follows:

IT or IT security roles/titles:

- CISOs/CROs/CIOs/CTOs (11%)
- VPs/SVPs/EVPs (7%)
- Directors (25%)
- Managers (31%)
- IT/security admins (19%)
- Analysts/consultants (7%)

Organization sizes:

- Small (1 to 99 employees) (10%)
- Medium (100 to 999 employees) (27%)
- Large (1,000 to 9,999) (41%)
- Enterprise (10,000 or more) (23%)

Industries:

- High-tech, IT software, and telecom (18%)
- Education (17%)
- Financial services (11%)
- Healthcare (10%)
- Manufacturing (10%)
- Retail, trade, eCommerce, and financial services (8%)
- Professional services (consulting, legal, etc.) (5%)
- Government (5%)
- Other (media/communications/advertising, transportation/warehousing, non-profit, utilities, construction, agriculture, and real estate) (16%)

Other CRA Business Intelligence reports

1. Controlling the Chaos: The Key to Effective Incident Response (May 2023)
2. Identity and Access Management: Can security go hand-in-hand with user experience? (April 2023)
3. Finding the Way to Zero Trust (March 2023)
4. Wanted: A Few Good Threat Hunters (February 2023)
5. Third-Party Risk: More Third Parties + Limited Supply-Chain Visibility = Big Risks for Organizations (January 2023)
6. Threat Intelligence: Critical in the Fight Against Cyber Attacks, But Tough to Master (December 2022)
7. Ransomware Ready: Organizations Fight Back with More Aggressive Strategies and Technology (November 2022)
8. Harsh Realities of Cloud Security: Misconfigurations, Lack of Oversight and Little Visibility (October 2022)
9. Zero Trust Adoption Faces Ongoing Headwinds (October 2022)
10. Endpoint Security: Security Pros Concerned About the Proliferation of Non-Traditional Devices and Endpoints (September 2022)
11. Organizations Adopt Aggressive, More Proactive Vulnerability Management Strategies in 2022 (August 2022)
12. Threat Intelligence: The Lifeblood of Threat Prevention (July 2022)
13. CRA Study: Attackers on High Ground as Organizations Struggle with Email Security (July 2022)
14. Security Teams Struggle Amid Rapid Shift to Cloud-Based Operations (June 2022)
15. CRA Study: XDR Poised to Become a Force Multiplier for Threat Detection (May 2022)
16. CRA Study: Zero Trust Interest Surges, But Adoption Lags as Organizations Struggle with Concepts (April 2022)
17. CRA Study: Managing Third-Party Risk in the Era of Zero Trust (March 2022)
18. CRA Ransomware Study: Invest Now or Pay Later (February 2022)
19. CRA Research: A Turbulent Outlook on Third-Party Risk (January 2022)

CRA Business Intelligence contacts

Bill Brenner
VP of Content Strategy and Research
bill.brenner@cyberriskalliance.com

Dana Jackson
VP of Research
dana.jackson@cyberriskalliance.com

Daniel Thomas
Custom Content Producer
daniel.thomas@cyberriskalliance.com

About CyberRisk Alliance

CyberRisk Alliance (CRA) is a business intelligence company serving the high growth, rapidly evolving cybersecurity community with a diversified portfolio of services that inform, educate, build community, and inspire an efficient marketplace. Our trusted information leverages a unique network of journalists, analysts and influencers, policymakers, and practitioners. CRA's brands include SC Media, Security Weekly, ChannelE2E, MSSP Alert, InfoSec World, Identiverse, Cybersecurity Collaboration Forum, its research unit CRA Business Intelligence, the peer-to-peer CISO membership network, Cybersecurity Collaborative, and now, the Official Cyber Security Summit and TECHEXPO Top Secret. Click here to learn more.

About Lacework

Lacework is the security company for the cloud. The Lacework Cloud Security Platform is offered as-a-Service and delivers build-time to run-time threat detection, behavioral anomaly detection, and cloud compliance across AWS, GCP, Azure, and Kubernetes services, workloads, and containers. Trusted by enterprise customers worldwide, Lacework significantly drives down costs and risk, and removes the burden of unnecessary toil, rule writing, and inaccurate alerts.

About Invicti

Invicti Security — which acquired and combined DAST leaders Acunetix and Netsparker — is on a mission: application security with zero noise. An AppSec leader for more than 15 years, Invicti's best-in-DAST solutions enable DevSecOps teams to continuously scan web applications, shifting both left and right to identify, prioritize and secure a company's most important assets. Our commitment to accuracy, coverage, automation, and scalability helps mitigate risks and propel the world forward by securing every web application. Invicti is headquartered in Austin, Texas, and has employees in over 11 countries serving more than 4,000 organizations around the world. For more information, visit our website or follow us on LinkedIn.