hackerone

EBOOK

Navigating the Security Budget Crunch: How Security Leaders Balance Risk and Resilience

From budget constraints to the security stack, this is how security leaders are navigating today's challenges to build and grow effective security programs

Contents

Introduction

CISOs and other security leaders face a host of challenges. From long-term issues like the skills gap and technical debt to more recent developments such as the "resources crunch" created by a difficult economic climate, being responsible for keeping organizations safe is far from an easy job. It's no surprise that 74% of CISOs have experienced burnout in the past 12 months.

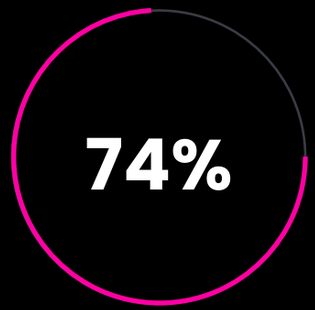
Over the course of a few weeks, we had conversations with 50+ security leaders from a wide range of industries, organization sizes, and geographic locations to find out how they navigate the challenges of the day while protecting against security threats.

This eBook provides insights from our conversations, focusing on five crucial areas:

1. **The Real Impact of the Macro Economy on Security Budgets**
2. **Prioritizing and Handling Talent Management**
3. **Balancing Budgets Against Risk Management and Risk-Based Decision Making**
4. **Engaging Ethical Hackers and Validating Security Controls**
5. **Scrutinizing the Security Stack**

These issues have come up repeatedly in our conversations with CISOs and other security leaders, and we've uncovered some essential strategies to help your security team thrive despite today's challenges.

Using these strategies, leaders can navigate their responsibilities more effectively, align security initiatives with business goals, and build more resilient security programs.



of CISOs have experienced burnout in the past 12 months

1. The Real Impact of the Macro Economy on Security Budgets

After several years of strong security investment, many leaders are now faced with a harsh reality.

Macroeconomic conditions have worsened dramatically, with inflation spiraling across much of the globe and worldwide growth falling from 3.4% in 2022 to 2.8% in 2023, before settling at a predicted 3% in 2024. As a result, 99% of business leaders said their organizations were preparing to cut costs—and security budgets are in the firing line.

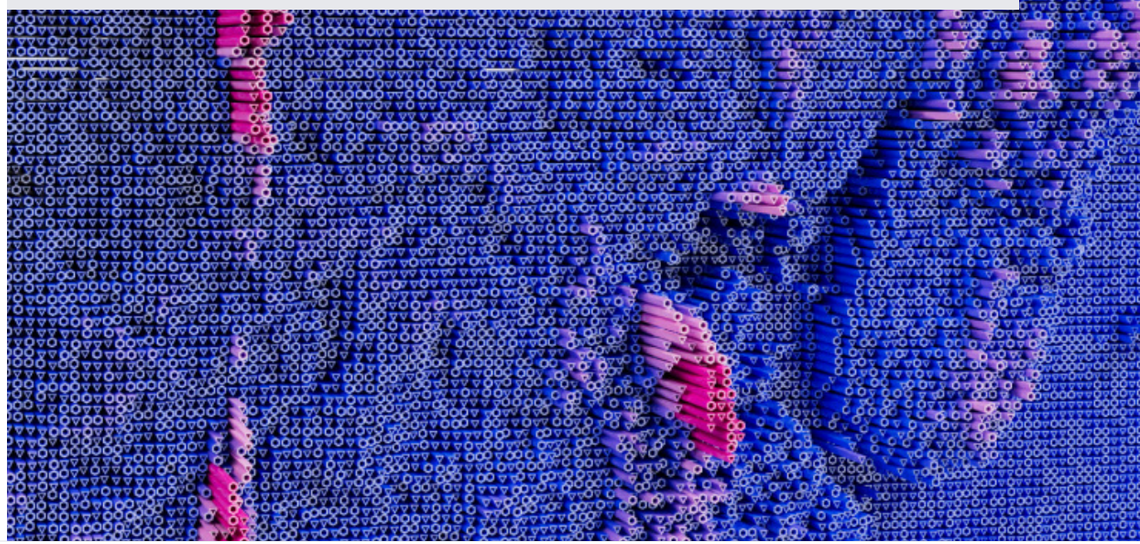
To make matters worse, many organizations poured additional resources into security during the pandemic, prompting security leaders to expand their programs—and the subsequent resources crunch is forcing them to rapidly reprioritize and make many difficult decisions.

"The greatest challenge for businesses right now is the requirement to drive down rising costs while maintaining security."

Seema Sangari, Vice President of Security Technical Program Management, Salesforce

99%

of business leaders said their organizations were preparing to cut costs—and security budgets are in the firing line.



What Influences Security Budget Decisions?

The facts are simple: A difficult macro economy may lead to frozen or reduced security resources.

However, it's not as simple as assuming that difficult economic conditions will necessarily mean a cut in your budget. For example, while a large organization may be seeking efficiencies, a venture-backed startup that has already secured funding may have no need to reduce security spending.

"If the organizational culture doesn't support security being everybody's job, it becomes important where you sit. But I have seen situations where the CISO doesn't report to the CEO, but the culture from the leadership team enables the CISO to be effective regardless of reporting structure. There can be a relationship between budget and reporting structure, but if you've got a supportive leadership structure, it matters less."

Helen Patton, CISO, Cisco Security Business Group

Factors that may influence changes to your security budget include:

How security is viewed within your organization

If security is seen as a back-office function, your budget is likely to be at risk during difficult economic periods. Conversely, if security is seen as an essential business driver, you're more likely to see a budget freeze than a budget reduction.

Risk vs. reward

Depending on your organization's industry, location, and profile, the risk associated with a reduction in security spending may or may not be worth the savings. For obvious reasons, high-risk organizations—and those with a strong understanding of their risk profile—are less likely to cut security spending during an economic downturn.

Industry regulation

Organizations in highly regulated industries—and those that engage with voluntary compliance initiatives for business reasons—are always less likely to reduce or freeze.

Changing threat landscape

Difficult economic times naturally lead to changes in the threat landscape, as more people struggle to make money legally and the cost of living rises. In particular, many organizations are seeing increases in business email compromise (BEC), ransomware, and financial fraud. For organizations at high risk of financially motivated attacks, this may prompt business decision makers not to cut security budgets.

CISO reporting structures

One factor that can influence budget decisions is where the CISO (or other security leader) reports. Broadly, CISOs that report to a CFO may be more likely to experience a budget reduction—while CISOs reporting to CEOs may be less likely. While these reporting structures may be a good indicator of budget decisions, there may be a more important factor at play: security culture.

Security culture

The way your organization's leadership views security is paramount. If your board, CEO, and other business leaders are supportive of security and promote the idea that security is everyone's job, it's unlikely that security budgets will be cut significantly during an economic downturn. On the other hand, if your leaders are not supportive of security at a cultural level, they may be willing to cut security budgets to minimize costs.

You're Not Helpless

What if your organizational culture, reporting structure, or leadership team doesn't support your security objectives? Research suggests that only 29% of boards are "deeply involved" in security strategy—so what if your organization falls within the other 71%?

If this is the case, all is not lost—but you may have a rougher road ahead of you. Instead of relying on an existing culture, you'll need to invest time and energy to educate your leaders and peers across the organization on the need for and value of security. This requires two things:

- **Speak the language of the business**

  Typically, this means talking in terms of measurable outcomes (finance, risk, etc.) rather than in more subjective terms (e.g., business enablement).

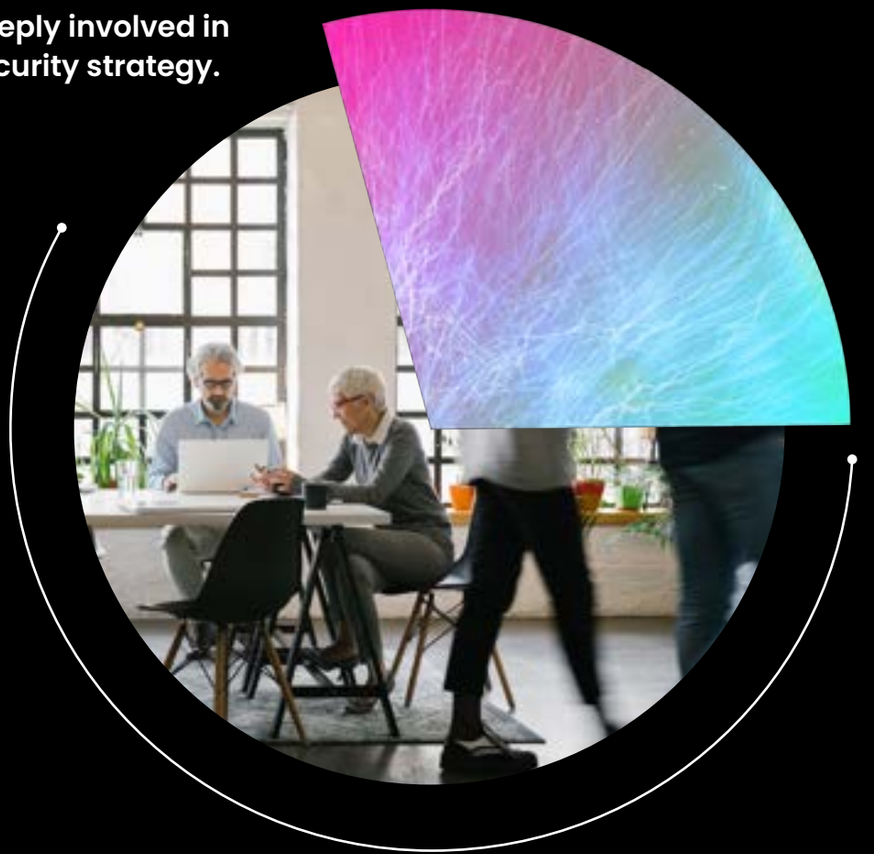
- **Use a data-driven approach**

  There must be clear thinking and evidence behind your budget requests or push-backs. For example, what risks would arise from a loss of budget? How would additional budget create measurable value for the business?

While there's no guarantee you'll be able to substantially change your leaders' stance on security, approaching the topic in a business-focused way gives you the best possible chance of protecting your budget during times of economic uncertainty.

71%

of boards are not deeply involved in security strategy.



2. Prioritizing and Handling Talent Management

Hiring and leading high-quality talent is among the most important responsibilities of any security leader. It's also one of their biggest challenges—and it only becomes more challenging during difficult economic periods. As a security leader, it's generally not possible to hire for all of the roles you'd ideally like on your team...and even if you could, a host of other challenges stand in the way.

What to Do If You Can't Find Experienced Security People

Every security leader has experienced the impact of the cybersecurity skills gap. What can you do when ideal security practitioners and skills aren't available or are out of budget?

George Gerchow, CISO and SVP IT, Sumo Logic, takes a three-pronged approach:

- **Hire developers,** even if they don't know much about security initially.
- **Hire prior military personnel,** who typically have a strong understanding of processes and general situational awareness.
- **Hire IT people** who are good at automation and awareness, and are always on the lookout for challenges and how to fix them.

In George's experience, this combination—along with experienced security practitioners—is a powerful way to build your team while ensuring you have the diverse expertise needed for ongoing success.

Coping With Limited Financial and Human Resources

Limited resources are a perennial challenge in security. It's simply never possible to have enough people to do everything that needs to be done—but that's no excuse for leaving the organization at risk. Our security-leader conversations have uncovered the core tactics to help alleviate this challenge:

Think about where you want your team to spend its time

Naturally, this requires a clear understanding of where they currently spend their time. Once you have that, identify those areas that are most significant, and that clearly require human input or oversight—and prioritize allocating human resources in these areas.

Leverage automation

There are many areas of security that—while important—aren't a good use of human resources. Typically these are repetitive, simple processes that can quickly eat up a huge amount of time if left unchecked. To avoid this, identify these areas and look for ways to leverage automation and AI to improve efficiency and free up your team.

Build relationships with IT and the business

Many issues that present roadblocks for security are also a challenge for other areas of the business—particularly IT. Aim to build key relationships and work together to remove these roadblocks—for example, by simplifying the IT environment to remove operational and security complexities.

Diversify skill sets

More important than an individual's skills and experience is how they fit into the wider team. As a security leader, you should aim to find people whose skills bridge gaps in your existing team, even if they lack experience in security. It helps to match junior team members with more experienced "buddies" to help them find their footing within the team and begin to grow in their roles.

Core Functions vs. "Nice-to-Haves"

You can't do everything. To avoid misallocating resources, be very clear on what value your security program brings to the wider organization—and which security functions are essential to deliver it. Once you understand this, examine your existing program to determine:

- **Core functions** that must be prioritized and maintained at all costs.
- **"Nice to have" functions** that could be sacrificed if necessary.

Particularly when budgets are tight, this knowledge will allow you to double down on core activities, maintaining the most important business-value functions while allowing "nice to haves" to wind down.

"As a CISO, the hardest thing is what you're *not* going to do."

George Gerchow, CISO and SVP IT, Sumo Logic

Supporting Team Growth

The security leaders we've spoken with emphasize the importance of supporting team members to self-lead their growth and development. This means:

Engaging with individuals to find out how they want to grow. Provide opportunities for individuals to grow and expand their skill sets beyond the constraints of their existing roles.

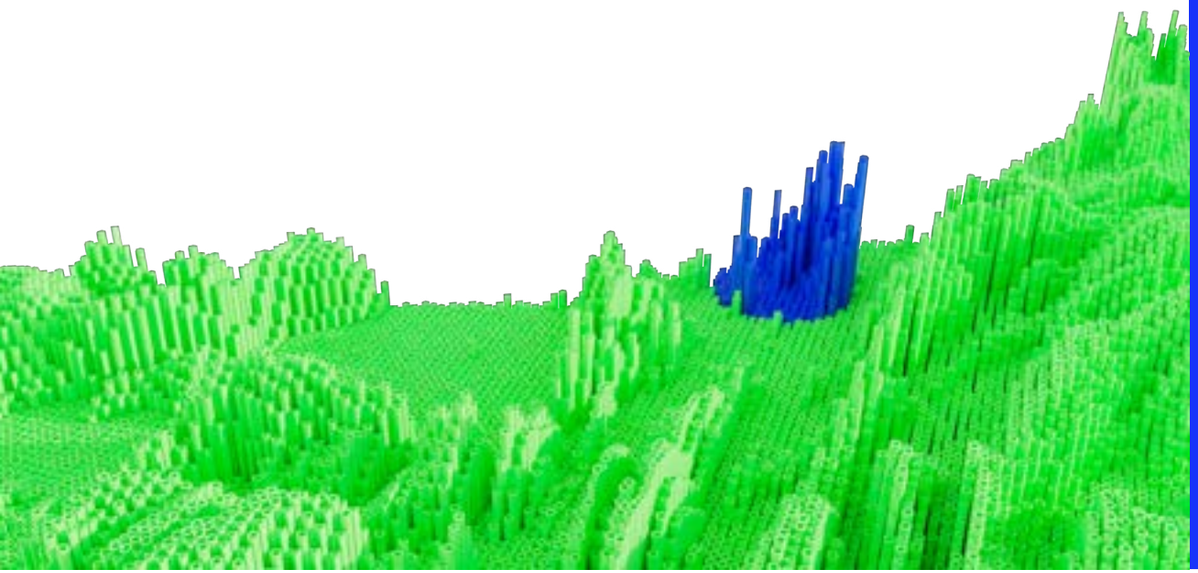
Giving them autonomy and authorization to identify risks and security issues, and addressing those without having to go through too much procedure. This may be difficult in organizations with more rigid governance structures, but it allows individuals to exercise their problem-solving skills and develop in ways that aren't easily supported by formal training.

Filling Skills Gaps and Short-Term Needs With Contractors

Some skills are simply too difficult to find in permanent employees. A current example of this is AI specialists—it's simply too difficult for many organizations to find high-quality permanent employees with these skills.

In these cases, consider using contract or loaned resources to address temporary needs and augment your core team without incurring excessive long-term costs.

But not everything is a long-term need. Specific challenges such as SolarWinds and Log4j create urgent work for a defined period of time, and smart leaders call on contractors to help.



"Ethical hackers really added value for us when it came to Log4j. In addition to directing our internal teams to focus on instances where we were exposed, we also ran a targeted campaign with a pool of hackers to identify any instances that were still not mitigated. This is how we stay ahead of the game."

Seema Sangari, Vice President of Security Technical Program Management, Salesforce

3. Balancing Budgets and Risk-Based Decision Making

Security is a perpetual trade-off between spending and risk. The lower the budget, the more risk the organization must accept. So, how do you strategize for this trade-off?

The Board Sets the Standard

Security budget is a reflection of the board's decision about what they want the organization's risk profile and posture to be. For example:

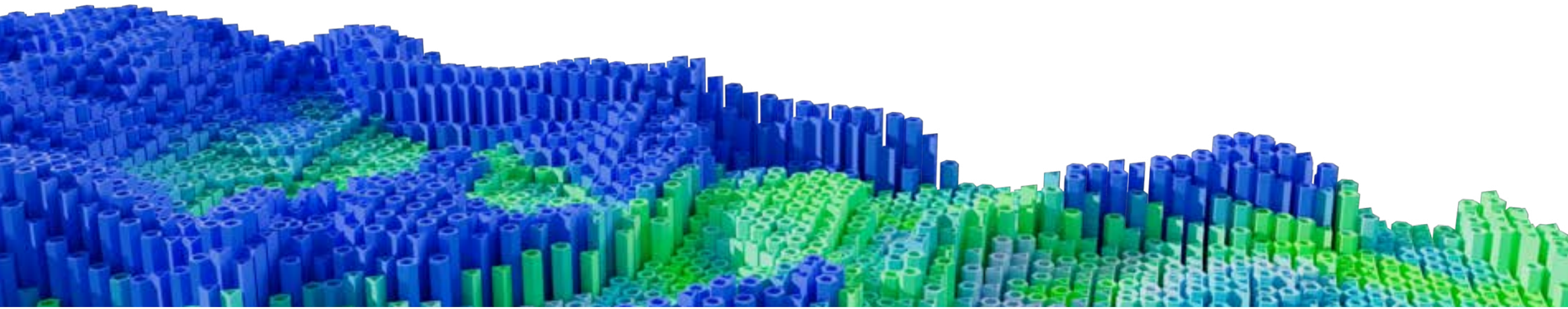
- **Do they want to focus purely on compliance activities?**
- **Do they want to be "good enough"?**
- **Do they want to be industry-leading?**

For example, the CISO's role is to advise the board on what must be done and what could be done depending on the available budget. Once the board has made an informed decision, the CISO executes according to the will of the board.

"A business leader can make this call to not fund a security thing, but they need to let the insurance company and the board know because they're making a risk decision on behalf of the company. Money is the proxy for a risk decision, and it shouldn't be up to a single person to make that call."

Helen Patton, CISO, Cisco Security Business Group

In simple terms, money allocated to security reflects a risk-management decision. The lower the budget, the higher the risk accepted by the organization. This decision might even be made above the CISO's head, but they must be sure to properly advise business decision makers about the potential consequences.



Choosing What *Not* to Do

As we've already discussed, some of the hardest decisions to make involve what not to do. A common example in deciding whether to replace a solution that isn't optimal. When your budget is tight, you may want to consider sticking with a sub-optimal but adequately performant solution that would consume a lot of resources to replace.

"There will always be solutions that might not be perfect, but they do the job. Maybe they do 50% or 80% of the job. But if those solutions have taken a couple of years to implement, is it the right time for you to scrap them and start from the beginning with a new solution? This consumes effort for you and your business partners. Or is it something you can live with, and bridge the gap with something else?"

Viswa Vinnakota, CISO, Xerox

Of course, leaving a substandard solution in place could create risk for the organization. To mitigate this, you must understand where gaps exist, and ensure they are filled in other ways—for example, through other tools or human-led processes.

Align With Business Objectives

In a given year, a security leader can only expect to get a handful of new initiatives or capabilities over the line. When allocating limited resources, leaders should always ensure they are supporting business objectives. You'll have many opportunities to invest in things that appear to be excellent initiatives—but if they don't support the business, there's really no need for them.

For example, if the organization goes through a lot of mergers and acquisitions, the security team's ability to support due diligence processes is paramount and needs to be allocated the right resources to ensure security.

Similarly, for high-profile organizations, protecting their reputation may be crucial. This means prioritizing certain types of risks over others—for example, a risk that could create reputational harm may be prioritized over one that's likely to have a purely operational or financial impact.

"At Zoom, our products serve as essential communication tools for customers worldwide, and therefore we prioritize the strength and resilience of our products. Our commitment to security led us to develop the Vulnerability Impact Scoring System (VISS), which we use to interpret risk specific to our company, alongside CVSS. Since VISS is tailored to our company's needs, it helps us to prioritize the issues that really matter."

Michael Adams, CISO, Zoom

4. Engaging Ethical Hackers and Validating Security Controls

A common thread in our discussions with security leaders is their use of ethical hackers to help address strains and challenges in their security programs. From reducing costs to validating security controls, below are the most common ways security leaders work with the global hacker community to achieve their objectives.

Filling Skill Gaps

Security leaders frequently call on the hacking community to fill skills gaps within their teams. It's simply not possible to retain full-time employees with all of the necessary skills to keep your organization safe—and the ethical hacking community is on hand to provide any skills you're missing.

However, it's not just about additional testing skills. The leaders we've spoken to recommend going beyond individual reported vulnerabilities and engaging with hackers to learn how they identified and exploited a vulnerability, and how the organization can prevent that vulnerability from recurring.

Over time, these conversations with hackers will help you understand your attack surface more thoroughly, and enable you to identify ways to harden your attack surface against a broad array of threats—whether through human expertise, tools, process changes, or something else.

Security leaders frequently call on the hacking community to fill skills gaps within their teams. It's simply not possible to retain full-time employees with all of the necessary skills to keep your organization safe.

Addressing Unidentified Risks and Validating Security

The products, solutions, and infrastructure that make up modern IT environments are complex and interconnected. No matter how good your IT operations, security practices, and CI/CD pipeline are, you can't anticipate all risks—and the combination of different IT assets inevitably creates a risk profile that is difficult to understand and protect.

To address this, security leaders need a way to uncover unanticipated risks within their IT environments—but this is far from easy, and generally can't be done exclusively in-house. It's simply too easy for security teams to overlook risks and threats due to gaps in knowledge, skills, or experience.

Again, the ethical hacking community can help. Having a large, diverse group of security experts continuously evaluating your attack surface dramatically increases the chances of finding unexpected weaknesses, allowing your team to address them before they can be exploited by cybercriminals.

At the same time, hackers provide independent validation of your security maturity. You may have products or controls in place to address a risk, but are they adequately mitigating that risk in the real world? Ethical hackers help validate this through continuous and varied testing, allowing you to proactively tighten or replace controls that aren't performing adequately.

"We're stronger together, and no one security team can know enough to be fully effective."

Helen Patton, CISO, Cisco Security Business Group

CISCO

Time and Cost Savings (Doing More With Less)

Engaging with the ethical hacker community is an easy way to improve security testing coverage while controlling costs and saving time. The breadth of testing skills available is far greater than any security team can retain in-house, or even what can be obtained by engaging with penetration testing providers.

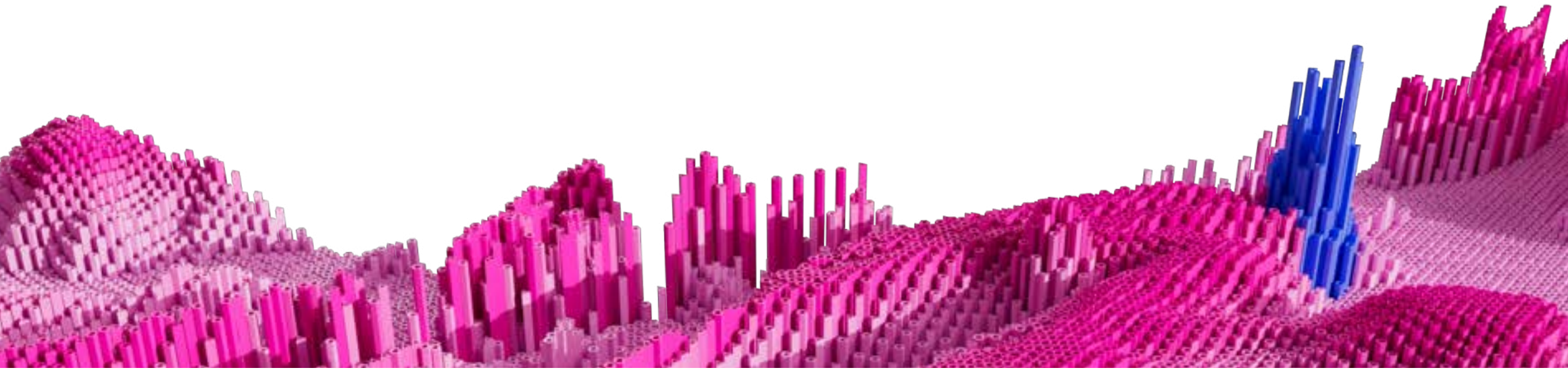
"One thing people don't consider, including companies that want to sell us pentesting, is the advantage of running everything through one platform. Having one platform for a very wide range of offensive security testing avoids the need to onboard lots of different vendors, platforms, and so on. This creates a significant time and cost saving."

George Gerchow, CISO and SVP IT, Sumo Logic

Creating Trust With a Vulnerability Disclosure Program (VDP)

Some of the leaders we've spoken to mentioned their initial hesitance to work with hackers for fear of opening up their organization to external eyes. However, after working with the global hacking community, they noted that—far from being dangerous—hacker-driven vulnerability disclosure and bug bounty programs contribute substantially to organizations' security profiles, and create a higher level of trust with customers and partners.

By inviting expert hackers to scrutinize your asset landscape, you can tighten your security controls and address gaps without having to wait for vulnerabilities to be highlighted by a real-world cyberattack.



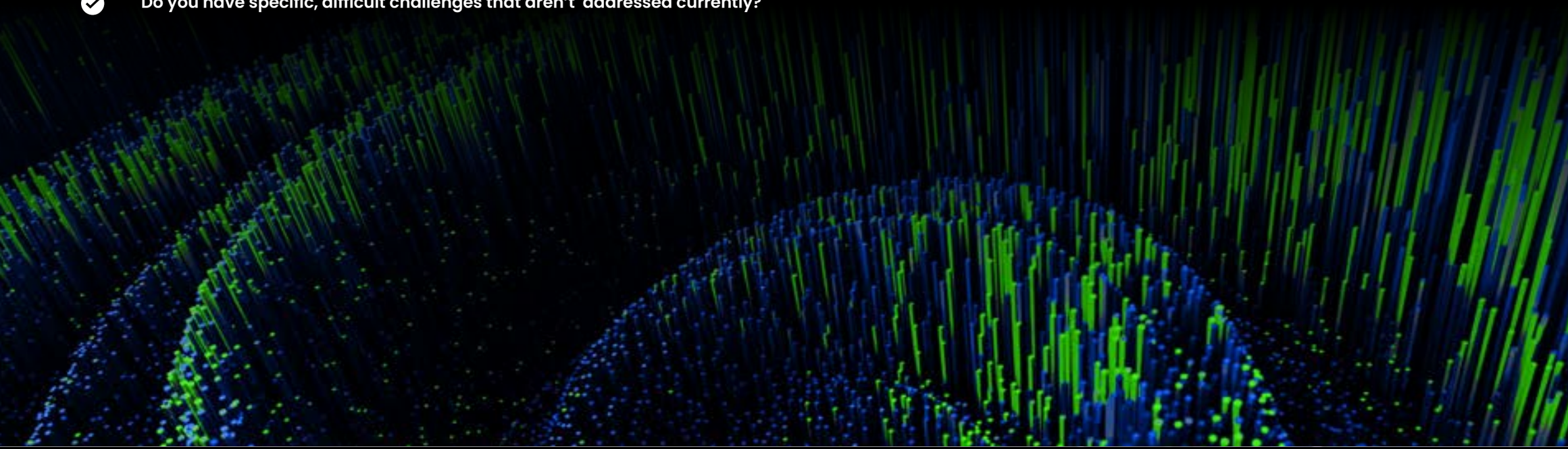
5. Scrutinizing the Security Stack

Whatever your challenges—whether you need to reduce costs, mitigate risks, or address specific thorny challenges—you should begin by examining your security stack. Important questions to consider include:

- **How does your security stack lay on top of your IT architecture?**
- **Do you have solutions working in silos?**
- **Are you overspending on certain tools that don't address core needs?**
- **Are there opportunities to modernize your stack?**
- **Could you consolidate your stack by working with an all-in-one platform?**
- **Where does the majority of your security value come from?**
- **Do you have specific, difficult challenges that aren't addressed currently?**

There are no one-size-fits-all solutions—your stack is your stack, and reflects your organization's specific risk profile, priorities, IT environment, and business objectives. However, it's highly likely that there are opportunities for change or improvement that can bring you closer to your goals.

For example, consolidation is a common tactic to reduce costs. However, if you have a high-priority challenge that isn't addressed by your current stack and/or isn't easily solvable with an off-the-shelf solution, you may be able to influence a small vendor's product roadmap to meet your need.



Best of Breed or Good Enough?

In a perfect world of limitless budgets, we'd all buy the best possible solution to our problems. However, as we discussed earlier, not all problems are equal—in some cases you need a comprehensive solution, but in others you just need to check a box.

In the latter case, a good option is to approach existing providers to see if they can meet your needs. This avoids unnecessary costs and disruption from onboarding a new vendor or solution.

Security vs. IT

Often, security teams are forced to spend heavily to address the risks posed by technical debt or poor operational processes outside security. For example, you may currently be responsible for securing multiple tools in the same category, when in reality the organization could consolidate. The more efficiently your organization manages its IT environment, the less you'll need to spend to secure it.

How do you effect these changes? The simplest solution is to influence decisions via budgetary processes. The organization doesn't want to spend unnecessary resources on duplicate or overlapping systems, and streamlining creates savings on two fronts: the cost of unnecessary systems themselves and the cost of securing them.

"We found out we had seven LMS systems, and we're not that big a company. Once you start diving into IT, there's technical debt all over the place. They sometimes satisfy the business too much. Working with line-of-business owners is essential so you can start to take these unnecessary things out."

George Gerchow, CISO and SVP IT, Sumo Logic

sumo logic

However…It's Not All About Money

One of the striking takeaways from our conversations with security leaders was that—despite the current economic climate—they spent very little time talking about money.

Yes, times are tough. Yes, budgets may be frozen or even reduced. But still, leaders are overwhelmingly talking about the importance of nailing down core security functions, including:

Managing risk

Living with uncertainty

Building and developing strong teams

While budgets may be an issue, there have never been enough resources to do everything. Today—as always—security leaders face the challenge of securing their organizations against cyberthreats by making the best possible use of limited resources.

Does that job get harder when resources are tighter? Of course.

However, leaders choose to focus on the challenges they have control over, adopting a creative approach to ensure their organizations are protected from cyberthreats.

Hear from some of the CISOs in this eBook by watching this on-demand webinar.

hackerone

HackerOne pinpoints the most critical security flaws across an organization's attack surface with continual adversarial testing to outmatch cybercriminals. HackerOne's Attack Resistance Platform blends the security expertise of ethical hackers with asset discovery, continuous assessment, and process enhancement to reduce threat exposure and empower organizations to transform their businesses with confidence. Customers include Citrix, Coinbase, Costa Coffee, General Motors, GitHub, Goldman Sachs, Hyatt, Microsoft, PayPal, Singapore's Ministry of Defense, Slack, the U.S. Department of Defense, and Yahoo. In 2021, HackerOne was named a 'brand that matters' by Fast Company.

Book a meeting with an expert today.

Contact Us