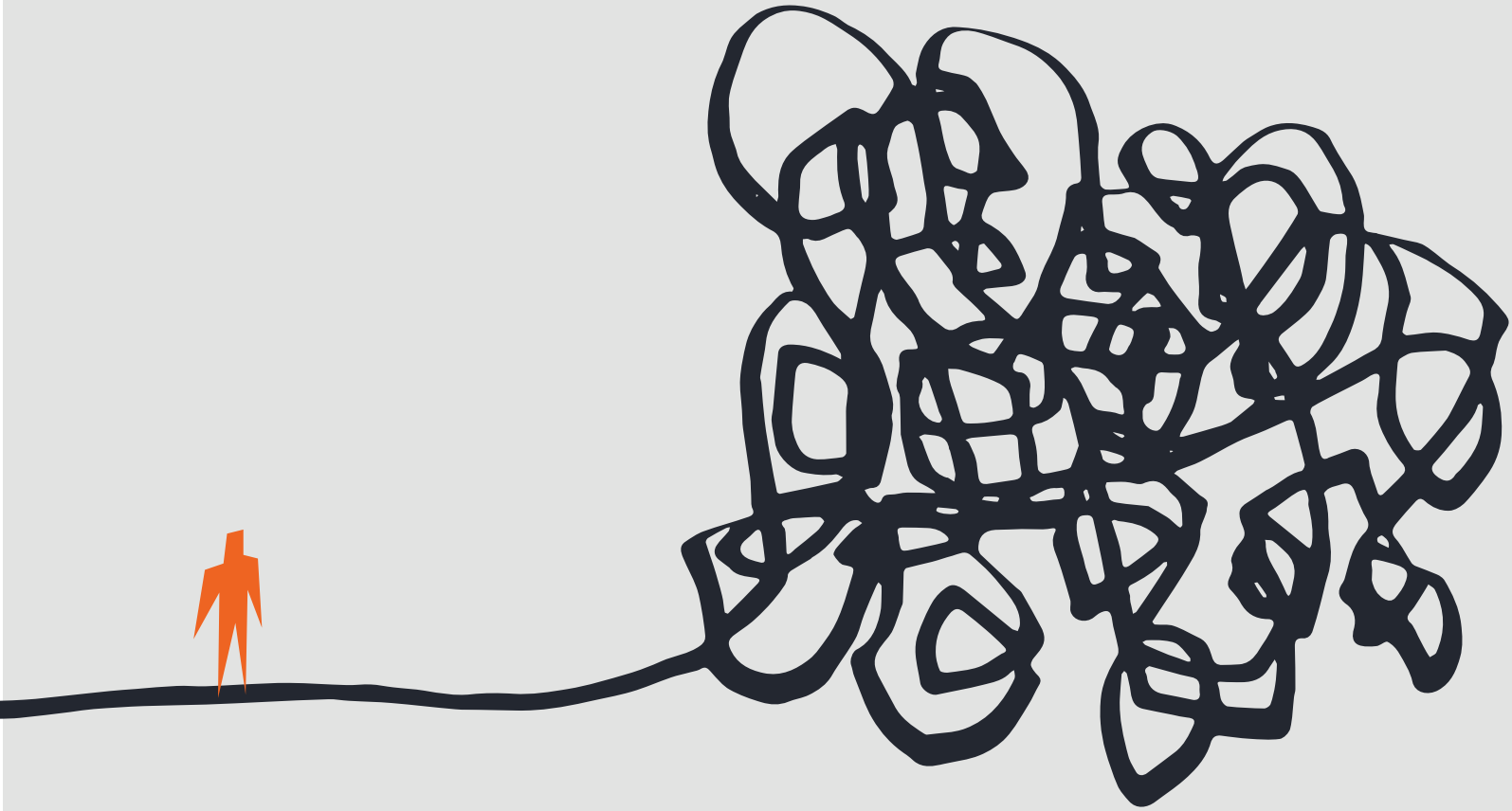
Cyber Resilience ThinkTank

Sponsored by mimecast



Decluttering Your Security Environment

Expert insight: Reduce enterprise security risk by rolling back complexity

Introduction

Your enterprise sits at the center of a significant amount of risk. It's not just about risk the business might take on with funding or product strategy direction. Every day, you as an information security or IT professional, have a front-row seat to the risks presented within your organization's technology infrastructure.

Just as fast as your team can spin up defenses to ward off adversaries, threat actors find a new way to dupe your employees and get their hands on your organization's precious data, intellectual property, customer PII or money.

It's natural to think the answer to these threats would be the acquisition of more technology, more tools and more people to manage them. In essence, more everything.

Research shows this has been the strategy many organizations take; industry reports put the average number of security tools in an enterprise at a staggeringly high 75.

But has this approach led to fewer instances of business compromise, disruption, breaches or successful cyberattacks? The daily news cycle provides the answer in a mind-numbing drumbeat of attack headlines: no.

It's worth questioning if having too many security tools—and not having the right personnel to manage them has the opposite effect when it comes to keeping your company safe. The complexity of your security environment contributes to inefficiencies, ineffectiveness and, ultimately, risk. And your enterprise can't afford more risk.

The Cyber Resilience Think Tank (CR Think Tank) gathered earlier this year to discuss this topic, and what follows are the results of that conversation. They offered their expert advice on how to break through cyberscurity complexity, simplify your tech stack and reduce the risk you face every day.

Cyber Resilience ThinkTank

How Did We Get Here?

As business needs have evolved, technology has been forced to play catch-up. It's an always-on world where employees at all levels require access to systems and data on all devices, at all times. This has led to the explosion of the cloud, along with mobile technology, the Internet of Things, social media and Big Data— a whole universe of business possibilities perpetually available at your employees' fingertips.

These evolving and expanding technological needs have, in turn, created a larger attack surface for adversaries to exploit. So, covering that attack surface with more technology might seem like a natural reaction. Yet industry leaders feel that action is having the opposite impact. Keeping up with the complexity of business has in turn led to complexity in the IT and security world. For some CISOs, having too many things to secure is the biggest issue they face day-to-day.

"In trying to explain what the biggest cyber threat is in an organization, I'd say it's the complexity of the internal environment and the lack of enterprise thinking, operation, strategy and architecture," said Taylor Lehmann, CISO at athenahealth.

Security vendors who offer point solutions may have contributed to this complex environment. Walk the show floor of any major global cybersecurity conference and you'll see that complexity first-hand.

"There's that tussle, that fight for attention," said Dr. Sam Small, chief security officer at ZeroFOX. "I have to tell you that what I do is unique and special, that no one else can solve it, that it's a solution you need to have. Unfortunately, if you buy into that hook, line, and sinker you're creating that complexity."

The industry is profiting off the inefficiency of my business, not because they have a great product," Lehmann said.

For security teams, the complexity can have damning effects. Getting out of triage mode is impossible, and they're triaging repetitive, low-value tasks that grow exponentially with each new alert. Backlogs develop and with that, human error and oversights increase for overworked teams. It's reasonable to expect you'll see churn in your IT organization when your talented people are constantly putting out fires instead of focusing on bigger-picture, transformative projects.

"Controls are a drag coefficient on people, data, and business processes," said Malcolm Harkins, chief security and trust officer at Cymatic. "When you have too much friction in your environment because of the controls, you're actually creating a systemic business risk for your organization."

For Lehmann and others, less complexity means seeing more of what they need to secure.

How Do I Determine What's Important and What's Not?

CR Think Tank Member **Malcolm Harkins'** list of questions you should ask when trying to decide which controls in your security environment you should keep and which you shouldn't:

What Risk
do I have with these controls?

What's the Total Cost
to own and operate them?

What Friction
are these controls causing?

Could Taking Out These Tools
improve my business velocity and efficiency?

"The lower the complexity of the system, the attack surface is more visible, meaning that I know what it is and I can plan and address it."

Taylor Lehmann

CISO, athenahealth

Cyber Resilience ThinkTank

What is the Skills Gap Really?

Ah, the skills gap. You've no doubt heard about it in the IT world and, in particular, the security skill set. There are too many open positions and not enough qualified people to fill them. Average industry standards indicate that the shortage of cybersecurity professionals has risen to nearly 3 million globally, with the Asia-Pacific region alone accounting for more 2 million.

"For most organizations, IT security resources are finite," said **Marc French**, CISO and managing director of Product Security Group. "This includes limited access to funds for personnel and technology, and time is short as well."

CR Think Tank members agreed – the industry fueled the labor shortage by selling solutions that didn't work and now needs to be held accountable.

"[The skills gap] is something we have largely created for ourselves," said Sam Curry, CSO at Cybereason. "It's the complexity issue that has manifested itself in human form. It's hard to find someone who knows these 75 security solutions, sure. You need to find a unicorn, and you never do. But if you didn't have that complexity, you may not need a unicorn after all and a lot more potential opens up."

Cybersecurity vendors may need to look inward when it comes to the root cause of the skills gap.

"Part of the skills gap is an artifact of poor product design," Small said. "We tend to overcomplicate our interfaces, our processes and our workflows and then blame the user when they didn't know about some esoteric feature or setting, or a critical alert that was buried on page four. Machine learning and these technology advancements are great, but there is still something fundamentally important about thoughtful design."

Dealing with the problem of the skills gap comes in many forms, but organizations must consider the appropriate allocation of resources on the biggest threats and protecting the biggest targets as part of dealing with the issue.

"For those without infinite resources, putting your people and technology on the most relevant and most critical possible cyber threats takes on major importance," French said.

There's no question it will take time, effort and energy to train the next generation of cybersecurity leaders. And many jobs in IT security are, in fact, unfilled and may stay unfilled for a long time. But industry influencers agreed this gap doesn't exist just because of a lack of skill. The complexity of their environments is part of the problem.

Take Action to Simplify Your Environment

Now that you've recognized the issues around complexity in your security environment, it's time to begin the process of decluttering. Think of it as a spring cleaning for your IT infrastructure.

There are many ways to approach this decluttering, but we've culled the advice from cybersecurity experts down to several points to focus on as you begin this process.

1. Know what you have, use it, connect it.

Odds are, if you're running 75 security solutions in your environment, some of them are redundant. In fact, many of those solutions probably had capabilities you didn't even know about when you bought them.

Turning on all the relevant features and assessing what you may or may not need in your entire environment is a key step.

"You may be surprised by what the tech you already have is capable of doing," Small said. "Instead of standing up a whole new point solution, a little bit of data transformation and a little bit of architecture can go a long way."

Security leaders also recommend taking those tools and integrating them into other platforms. Choosing platforms with powerful, extensive API capabilities is critical.

"I care about platforms," said Peter Tran, VP and Head of Global Cyber Defense & Security Strategy at Worldpay. "So, from a vendor perspective, I weed out a lot. You can pitch all the nice little toys you want. But I just want to be able to ingest it, aggregate it and de-dupe it and give to my analyst in an automated fashion. That gives us the ability to make data-driven decisions faster."

"I'm more interested in finding fabric then finding things that plug into the fabric," Small said.

2. Don't bite off more than you can chew.

Consider a plan where you take a methodical approach to see incremental improvement over a finite period.

"Throw the old stuff out?" pondered Harman CISO Maurice Stebila, "Do you dare?"

Instead of tossing everything at once, Stebila suggested keeping those tools that reduce dwell time and put less people behind it. Push the responsibility to each business unit in your organization, Stebila said – they need to take accountability.

"Apply the law of marginal gains first on your environment," said Tran. "You have to make use of what you have now to make sure it is aligned properly to where you want your visibility…It doesn't happen overnight."

Because of regulations in the fintech world, Tran is required to keep close tabs on his security infrastructure.

"We have no choice when it comes to spring cleaning," Tran said.

But even if the changes he makes are minute, over time they can add up to a more secure, less complex environment. Such an approach may be a good idea across all industries and verticals.

"Innovation comes through program starvation," Harkins added. "You can't possibly buy all the tools. Worry about operation efficiency versus spend."

3. Consider your resources.

When adding new services to your security stack, ensure that it's right for your environment, your resources and who you have on hand to manage it all.

"As a rule of thumb, if you have implemented and are managing more than two tools per IT/security professional on your team, it may be time to reconsider your approach," French said. "You have to consider your force multipliers in this count (that includes your MSSPs, champions, proxies and vendors). Then, consider if you've truly implemented these IT security tools in question to their fullest capability. If you haven't done that, you've likely created a bigger cyber risk as a result with a false sense of security."

Set strict standards for what you're going to introduce, and ensure complexity is part of that equation, Lehmann said. "We rate everything we buy based on complexity reduction."

Once you're using a tool, Think Tank members advise that you look at the results of what it actually does as opposed to what it says it does.

"It's a little like gardening," Harkins said. "It's like weeding and feeding. You see what yields you're getting off the investment. If you're not getting the yield, then you've got to try a different approach. It might be because you're not operating the tool to its full capacity, it may be because you bought on a marketing glossy and a lab-based proof of concept versus really seeing how it operated in a production environment."

Features and capabilities are one thing. But they must deliver a result, and in Harkins' words, if you're not measuring for a result, you're measuring for the wrong thing.

"As a rule of thumb, if you have implemented and are managing more than two tools per IT/security professional on your team, it may be time to reconsider your approach."

Marc French
CISO, MANAGING DIRECTOR, PRODUCT SECURITY GROUP

Cyber Resilience ThinkTank

"They know and understand tech, had critical thinking skills and the desire. I don't need to see certificates or degrees."

Sam Small
CSO, ZeroFOX

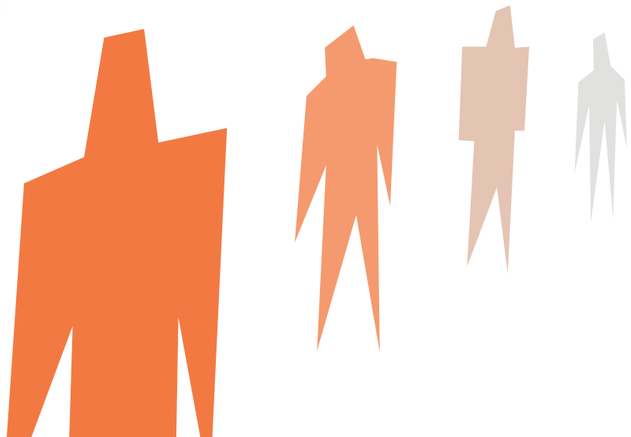
Hiring the Next Generation of Security Pros

The Cyber Resilience Think Tank experts don't believe pulling graduates with the highest GPAs straight from prestigious universities is totally necessary when it comes to staffing a security program. In fact, the right person may have just served your morning latte.

"I've hired great T1 analysts whose last job was as a barista at Starbucks," Small said. "They know and understand tech, had critical thinking skills and the desire. I don't need to see certification or degrees."

Lehmann agreed: "I have a zero-college degree policy for kids coming out for entry level positions. Think about who they're going up against. Most of the adversaries follow the path of interest, motivation and critical thinking skills."

They have zero formal education. It's about matching that level of knowledge and critical thinking."



Cyber Resilience ThinkTank

"It's a little like gardening," Harkins said. "It's like weeding and feeding. You see what yields you're getting off the investment. If you're not getting the yield, then you've got to try a different approach."

Malcolm Harkins
CHIEF SECURITY & TRUST OFFICER, CYMATIC

Three R's for Simplifying Your Security Environment

Peter Tran
VP, Head Of Global Cyber Defense
& Security Strategy
Worldpay

CR Think Tank Member Peter Tran's three actions to take when considering how best to simplify your environment:

Realign...

your resources if they aren't providing the proper visibility into your environment.

Reinvest...

in services that have performed to the standards you've set.

Retire...

services completely if they are no longer working or relevant.

The Bottom Line

Simplicity must be the name of the game for keeping your enterprise safe from adversaries. By not going this route, you open yourself up to an inordinate amount of risk, beyond even what attackers are doing on a day-to-day basis.

When thinking about solutions, consider those that will lead to less complexity, less bandwidth and skills needed to manage and lower total cost to your organization.

Ensure that the tools you've already bought are being used to their greatest capabilities and capacities and integrate them with your existing systems. You can even consider outsourcing some functions if needed.

Going this route **will free up your people to focus on the big picture items** and systems work, and allow your skilled workers to shine. They'll be happier as a result.

However, it falls on the organization to make these changes—and accept the outcomes.

"The one thing you can never outsource—even if you outsource your entire security structure to an MSSP—is your accountability and your decision-making," Harkins said.

"At the end of the day, you own it."

Cyber Resilience ThinkTank

What is the Cyber Resilience Think Tank?

The Cyber Resilience Think Tank is an independent group of industry influencers dedicated to understanding the cyber resilience challenges facing organizations across the globe, and together, providing guidance on possible solutions.

They define cyber resilience as: "an organization's capacity to adapt and respond to adverse cyber events—whether the events are internal or external, malicious or unintentional in ways that maintain the confidentiality, integrity and availability of whatever data and service are important to the organization."

Malcolm Harkins
Chief Security & Trust Officer
Cymatic

Juan Harmse
Head Of Resilience Strategy & Engagement
ABSA Group

Taylor Lehmann
CISO
athenahealth

Gary Hayslip
CISO
Softbank Investment Adviors

Sue Lapierre
VP, Information Security Officer
Prologis

Peter Tran
Vice President, Head Of Global Cyber Defense & Security Strategy
Worldpay

Dr. Sam Small
CSO
ZeroFOX

Maurice Stebila
CISO, Digital Cyber Security, Compliance & Privacy Officer
Clicksoftware
Harman International

Jakub (Kuba) Sendor
Software Engineer
Yelp

James Lugabihl
Senior Director, Global Security
ADP

Ari Schwartz
Managing Director Of Cybersecurity Services
Venable

Stephen Ward
CISO
Home Depot

Dawie Wentzel
Head Of Forensic Investigations
Absa Group

Chris Wysopal
Chief Technology Officer
Veracode

Sam Curry
CSO
Cybereason

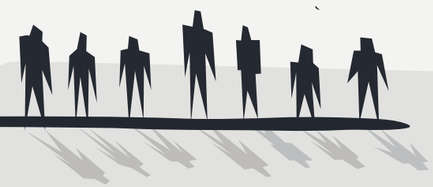
Greig Arnold
CISO
Vista Consulting Group

Bill Brown
CSO
Clicksoftware

Marc French
CISO, Managing Director
Product Security Group

Josh Douglas
VP Product Management Threat Intelligence
Mimecast

Scott Eigenhuis
Associate Director, Information Security
Illumina



For more insights from the Cyber Resilience Think Tank
Visit **mimecast.com/ThinkTank**

Cyber Resilience ThinkTank
Sponsored by mimecast®

Printed on Recycled Paper.