CISCO
SECURE

Security Outcomes Study

Volume 2

Maximizing the Top Five Security Practices

Contents

(Re)Introducing the Fab Five

The 2021 Cisco Security Outcomes Study sought to measure what matters most in cybersecurity management. To that end, we examined 25 general security practices and tested how each correlates with the achievement of 11 program-level outcomes. You can view these practice-outcome correlations via an interactive visualization on the 2021 Cisco Security Outcomes Study website, or download the full report.

From the testing, we uncovered that five of the 25 practices stood out from the rest in terms of total contribution to security program success across all measured outcomes.

In the pages that follow, we focus on these "Fab Five" drivers of security program success to identify strategies for maximizing their effectiveness. The "Fab Five" are:

Proactive tech refresh	The organization has a proactive tech refresh strategy to stay up-to-date with best available IT and security technologies.
Well-integrated technology	Security technologies are well-integrated and work effectively together.
Timely incident response	Incident response capabilities enable timely and effective investigation and remediation of security events.
Accurate threat detection	Threat detection capabilities provide accurate awareness of potential security events without significant blind spots.
Prompt disaster recovery	Recovery capabilities minimize impact and ensure resiliency of business functions affected by security incidents.

The broad efficacy of these practices begs the question, "Why?" What makes them so key to unlocking success? What factors make them more or less effective? How should companies implement these practices to maximize outcomes? These are the kinds of questions we want to explore in this iteration of the Security Outcomes Study.

In the pages that follow, we focus on these "Fab Five" drivers of security program success to identify strategies for maximizing their effectiveness. We do this through an independently conducted, double-blind survey of over 5,100 IT and security professionals around the world. We dig into the data, extract salient findings, and share vetted takeaways to help unlock new heights of security achievement for your organization.

Key Findings

We asked over 5,100 IT and security professionals across 27 countries about their organizations' approaches to updating and integrating security architecture, detecting and responding to threats, and staying resilient when disaster strikes. As you might imagine, they shared a wide range of insights, struggles, strategies, and successes. We analyzed every response in multiple ways, extracting key findings like those featured below.

Update and integrate architecture

- Modern, well-integrated IT contributes to overall program success more than any other security practice or control.
- Newer, cloud-based architectures are much easier to refresh regularly to keep pace with the business.
- Organizations that source mainly from a single vendor double their chances of building an integrated tech stack.
- Integrated security technologies are seven times more likely to achieve high levels of process automation.

Detect and respond to cyber threats

- SecOps programs built on strong people, processes, and technology see a 3.5X performance boost over those with weaker resources.
- Outsourced detection and response teams are perceived to be superior, but internal teams show faster mean-time-to-respond (6 days vs. 13 days).
- Teams that extensively use threat intelligence are twice as likely to report strong detection and response capabilities.
- Automation more than doubles the performance of less experienced people, and makes strong teams near certain (95%) to achieve SecOps success.

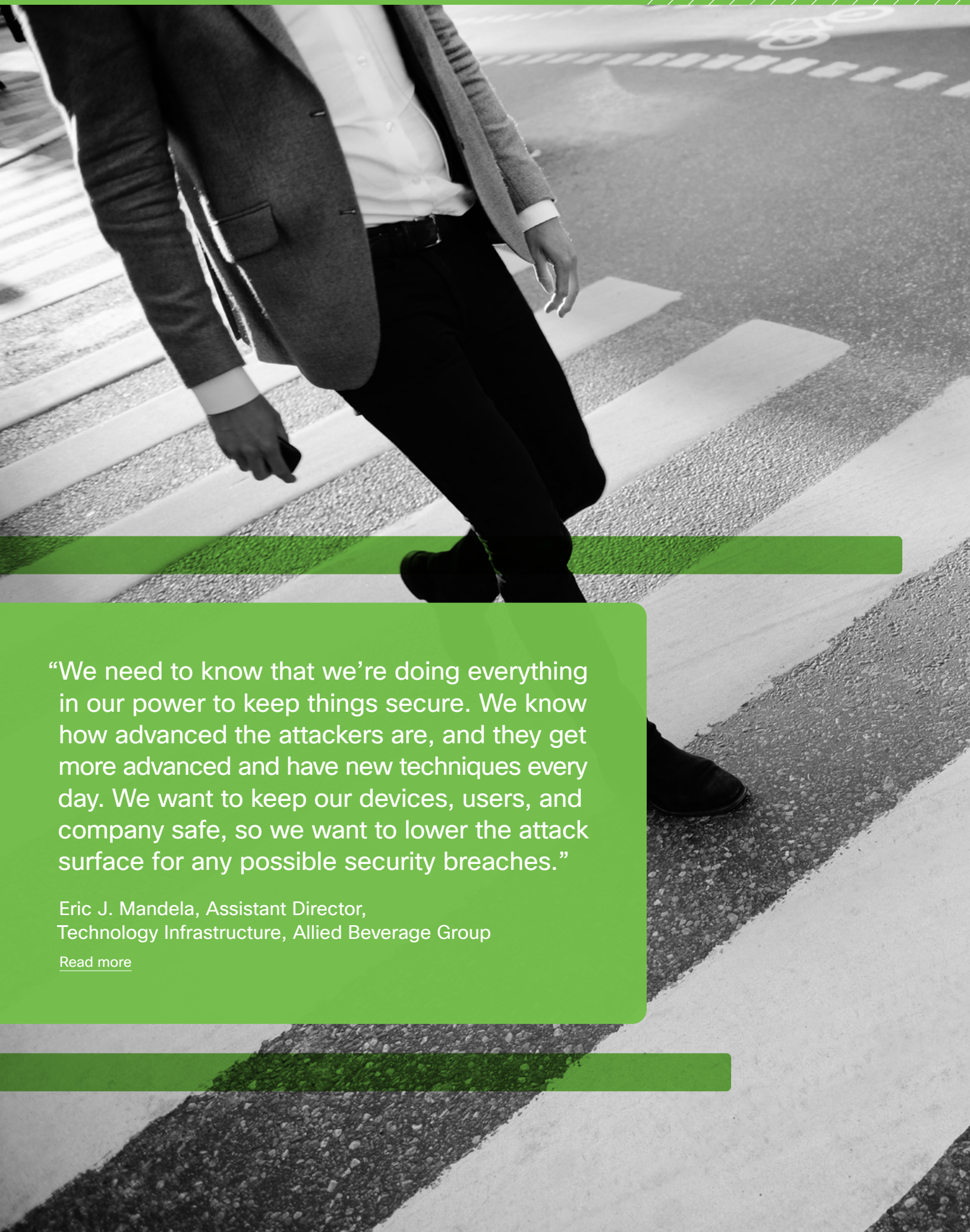
Stay resilient when disaster strikes

- Organizations with board-level oversight of business continuity and disaster recovery are the most likely (11% above average) to report having strong programs.
- The probability of maintaining business resilience doesn't improve until business continuity and disaster recovery capabilities cover at least 80% of critical systems.
- Organizations that regularly test their business continuity and disaster recovery capabilities in multiple ways are 2.5 times more likely to maintain business resiliency.
- Organizations that make chaos engineering standard practice are twice as likely to achieve high levels of resiliency.

About the survey

Sampling	Respondents	Analysis
Cisco contracted a survey research firm, YouGov, to field a fully anonymous survey in mid-2021 that utilized a stratified random sampling technique.	5,123 active IT, security, and privacy professionals from 27 countries responded. Sample demographics can be found in the appendix.	The Cyentia Institute conducted an independent analysis of the survey data on behalf of Cisco, and generated all results presented in this study.

5,123 active IT, security, and privacy professionals from **27** countries responded



"We need to know that we're doing everything in our power to keep things secure. We know how advanced the attackers are, and they get more advanced and have new techniques every day. We want to keep our devices, users, and company safe, so we want to lower the attack surface for any possible security breaches."

Eric J. Mandela, Assistant Director,
Technology Infrastructure, Allied Beverage Group

Read more

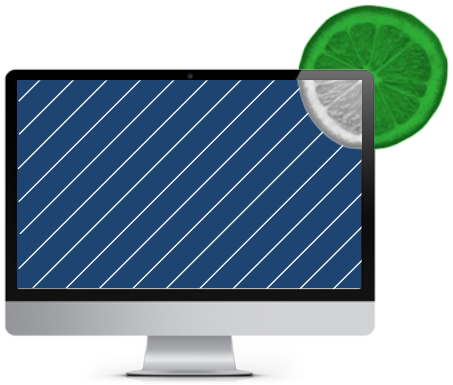
Strategies for Proactive Technology Refresh

Our prior study found that a proactive approach to refreshing and maintaining best-of-breed IT and security technologies contributed more to a successful cybersecurity program than any other practice. That's no small feat considering all 25 of the practices we tested are widely considered "best practices" in their own right. So, we were keen to dig into what makes this practice so effective in this follow-up study.

As we begin digging deeper into tech refresh strategies, let's do a quick sniff test of the freshness of existing infrastructure. We asked respondents what proportion of their active security technologies are outdated. On average, 39% of security technologies used by organizations are considered outdated. Almost 13% of respondents claim that at least 8 out of 10 security tools they use are showing their age.

This fact alone may help explain a lot of the benefits we see from a proactive tech refresh strategy. Ostensibly, newer technologies bring advanced capabilities to bear against an ever-advancing horde of cyber threats. But there's more to it than that, so let's keep digging into questions we asked of the data.

On average, 39% of security technologies used by organizations are considered outdated.



Do infrastructure traits impact refresh initiatives?

In the original study, we speculated that more modern, cloud-based architectures might be more effective because they're easier to manage and have native security measures built in. As a step toward testing that hypothesis, we asked respondents to generally describe their tech infrastructure by choosing a set of scaled descriptors, including:

- Cloud vs. On-prem
- Modern vs. Outdated
- Consolidated vs. Distributed

Do these different architectural traits contribute to the efficacy of tech refresh capabilities? Very much so, according to Figure 1. **Organizations with modern, consolidated, cloud-based architectures are more than twice as likely to report strong tech refresh capabilities than those using outdated, distributed, on-prem technologies.** Before waving that chart around in the next cloud migration strategy meeting, however, take note that organizations with predominantly on-prem environments still perform well above par, provided they've modernized IT.

Sure, being cloud-native makes it easier to unshackle your tech refresh strategy, but being outdated is the more pressing issue here. When keeping older infrastructure fresh becomes an uphill battle, you might make more headway migrating to a new architecture than continuing to retrofit the old. That's not always possible or cost-effective with legacy or critical infrastructure, of course, but the general principle still applies.

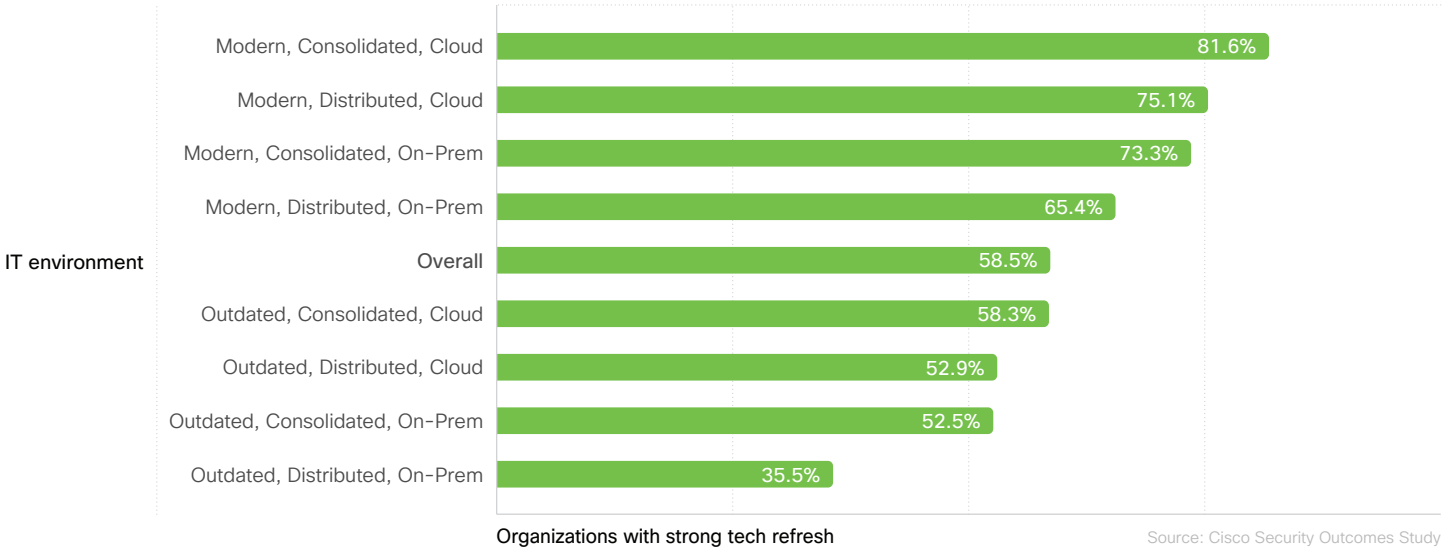


Figure 1: Effect of IT architecture traits on tech refresh performance

81.6% of organizations with modern, consolidated, cloud-based architectures report strong tech refresh capabilities

Do frequent upgrades help security keep up with business?

According to the 2021 Security Outcomes Study, the outcome most strongly correlated with a proactive tech refresh strategy was enabling the security program to keep up with the demands and growth of the business. In fact, that was the strongest practice–outcome combination across the whole study.

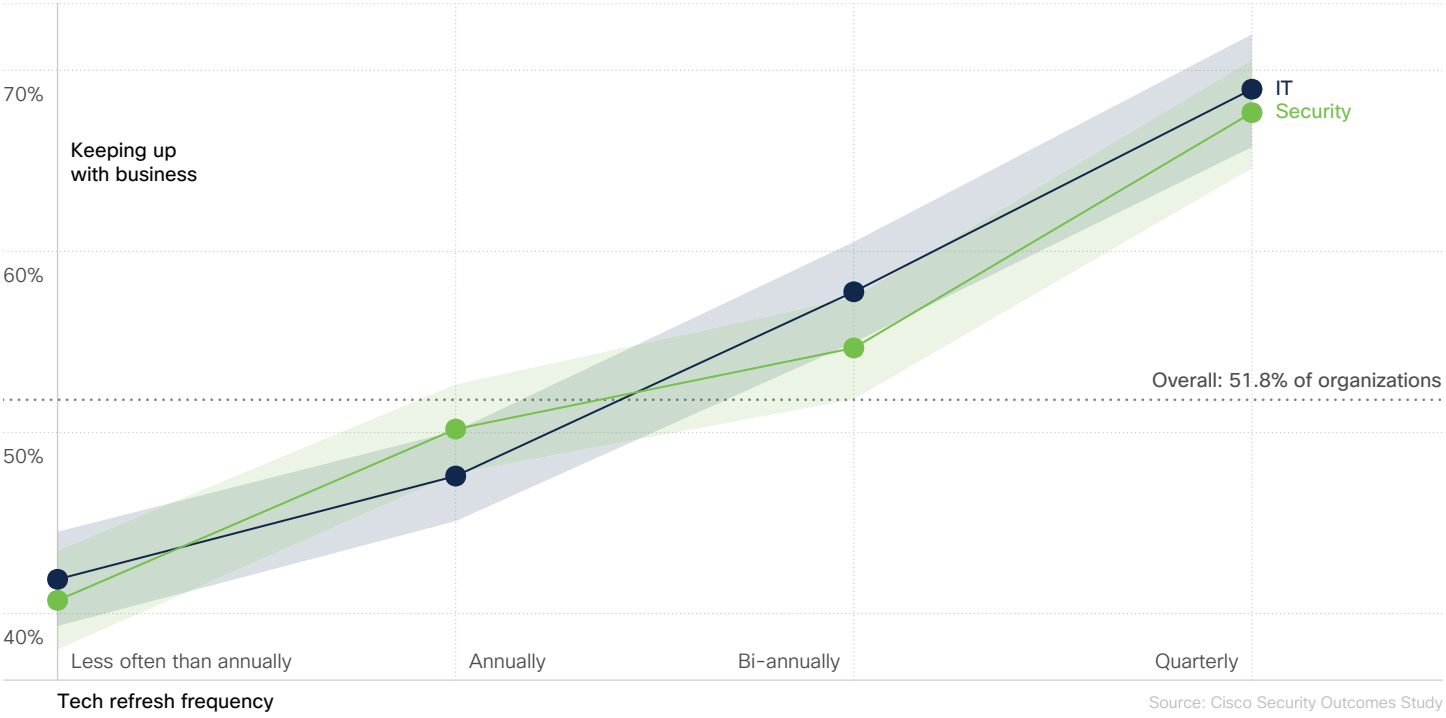


Figure 2: Effect of tech refresh frequency on the security program's ability to keep up with business[1]

We asked organizations about the frequency of their IT and security upgrades, and compared those answers to their security program's stated ability to keep up with the business. Is there a relationship between those two variables?

Yes indeed; we found steady improvement in this key outcome as the cadence of upgrades increased. **Overall, organizations that upgrade IT and security technologies quarterly are about 30% more likely to excel at keeping up with the business than those who only upgrade every few years.** Sounds like a good motivational poster for stressed IT teams: Keep Current and Carry On.

[1] Throughout the report we will label figures with the "Overall" value for a particular practice or outcome. This value represents what the average value is among all respondents who answered that particular set of questions. It is provided for reference, and should guide you to understand who is doing better than average, and who is not up to snuff. We are also displaying uncertainty through error bars or shaded areas on some charts. When those areas overlap the "Overall" line, it means we can't infer that particular aspect of a security program has any effect on the outcome or practice we are examining.

What (or who) should drive tech refresh efforts?

We've established that frequent upgrades contribute to enabling the business, but what – or who – should drive the process of getting those upgrades done? We asked respondents to select their organization's primary drivers for refreshing security technologies, and their responses fell into three broad categories:

- **Vendor-driven:** Schedule is determined by a SaaS provider or is part of a larger vendor consolidation initiative (most common driver)
- **Proactive:** On a predetermined schedule or when new features or use cases warrant an upgrade (second most common)
- **Reactive:** In response to an incident, when tech becomes obsolete, or to satisfy compliance requirements (least common)

These drivers are interesting in and of themselves, but what we really want to know is whether such motives correlated with a stronger approach to tech refresh. The answer is found in Figure 3, which basically says that tech refresh initiatives are more successful when vendors handle them (or are at least actively involved in making them happen). **Less than half of those with a reactive approach report strong refresh capabilities, compared to almost two-thirds of those that sync with vendor refresh cycles.**

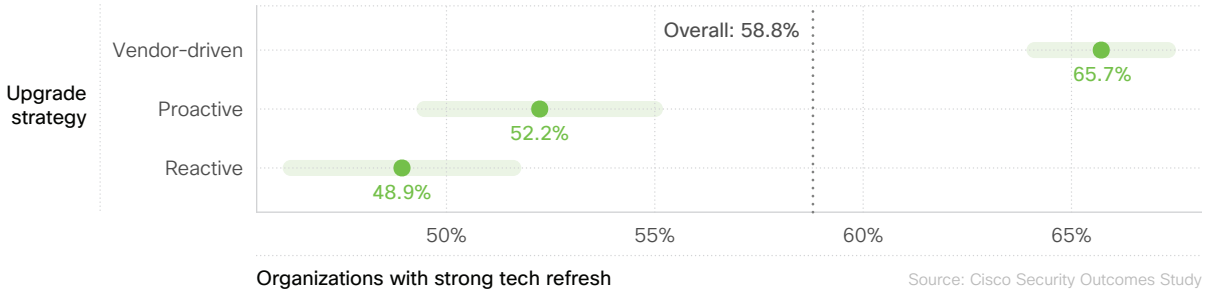


Figure 3: Effect of primary drivers for upgrades on security tech refresh performance

We get it – this all sounds really suspect coming from a vendor of IT and security products. But we honestly had zero influence on this finding. The survey was conducted by an independent, reputable research firm, the respondents had no idea Cisco sponsored the survey, and the well-respected Cyentia Institute analyzed the data to derive what you see in Figure 3. And for good measure, we'll be extra cautious in interpreting these results.

We suspect much of the improvement attributed to vendor-driven approaches ties to cloud/SaaS architectures being more friendly to frequent upgrades. We'll also note that this may be less about vendors being great and more about escaping the internal roadblocks and political quagmires that tend to impede tech refresh schedules.

In the words of Rob Base and DJ E-Z Rock, "It takes two to make a thing go right. It takes two to make it outta sight." Who knew they were security architects! Make your refresh strategy outta sight by harnessing the inertia of your technology solution partners to drive mission outcomes.

65.7% of organizations that sync with vendor refresh cycles report strong tech refresh capabilities

Upgrade for capability or compatibility?

The prior section covered which scenarios prompt organizations to upgrade technologies, and now we'll look at why they choose one solution over another. Figure 4 relays what respondents told us about their selection criteria. Integrating well with existing tech is the clear preference, followed by solutions that offer best-of-breed capabilities or that meet particular needs. Perhaps surprisingly, minimizing cost ranks last.

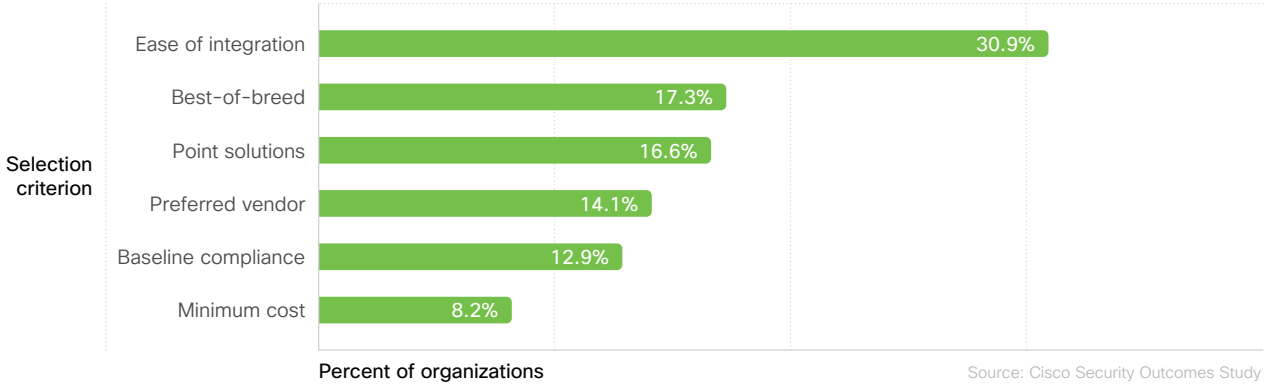


Figure 4: Primary selection criteria when refreshing security products

That's all well and good, but does any of this matter at all in terms of building a successful security program? To answer that, we grouped the selection criteria from Figure 4 into three categories:

- **Minimum:** Minimum cost solution; Baseline compliance
- **Ease of integration:** Integrate with existing tech; Use of preferred vendors
- **Capability:** Best of breed; Point solutions

We then tested these categories against an aggregated score created for each organization based on their level of achievement across the 11 security outcomes. The absolute value of the score has no particular meaning, but it does provide a point of comparison for the different tech refresh strategies. **As seen in Figure 5, prioritizing integration and capabilities both drive outcomes more than selecting products based on minimizing cost or meeting baseline compliance requirements. But an integration-led approach is the only one that significantly outperforms the average.**

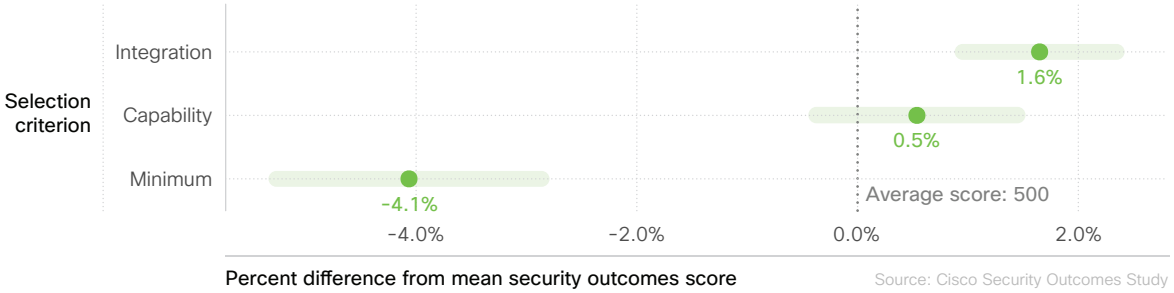


Figure 5: Effect of tech selection criterion on overall security outcomes score

Note that the differences here are pretty small in terms of overall program success. And it's likely that what we're really seeing here is a window into the broader priorities and practices of the security program. But this does suggest that softer issues like why we choose one product over another are worth considering. And if you're struggling to rank features when refreshing or upgrading security solutions, take this as a reasonable justification to push for compatibility and capability over minimizing cost.

What's the security outcomes score?

We asked respondents about their organization's level of success across 12 different security program outcomes. The first edition of the Security Outcomes Study analyzed these in detail, and you'll see some of them examined individually in this study, too. But we also wanted to create an aggregated score that captures each organization's level of achievement across all 12 outcomes as a measure of how the security program is performing overall. We refer to that as the 'security outcomes score,' and you'll see it referenced a few times in this report.

To get the score, we used a fancy statistics technique called "Item Response Theory." This technique enables us to score organizations based on how they're doing across all outcomes, while at the same time accounting for the fact that some outcomes might be harder to achieve than others. This tried-and-true technique is how standardized test scores are created. The absolute value of the score has no particular meaning, but it does provide a point of comparison among programs.

"CISOs have to be both influencers and educators. If we're going to be as effective as possible, we need to be on the leading edge of the strategy decisions being made in our organizations. But while we're trying to convince people that security is important, that we need the right investments to do it well, and that we should be involved in every aspect of the business, we must also educate. Most executives do not have a background in security, so we need to inform them every step of the way about the types of risks we're introducing with each decision we make."

Helen Patton, Advisory CISO, Cisco @CisoHelen

Hear Helen's take on the evolving role of the CISO in this intriguing episode of our Security Stories podcast

Achieving Well-Integrated Security Technologies

According to our last Security Outcomes Study, well-integrated security technologies that work effectively with broader IT infrastructure contribute to the likelihood of success for all program outcomes. We asked a range of questions designed to dig deeper into the factors behind that laudable feat, starting with the intentions behind security tech integrations.

According to respondents, the most common motive for integrating security technologies is to improve the efficiency of monitoring and auditing. That resonates with us too, as we're familiar with the pain and frustration of having to check numerous consoles or dashboards to piece together some semblance of what's happening across the network. Easier collaboration and automation were also common drivers for integrating security technologies (more on the latter coming up). We tested these motivations against reported tech integration levels and program outcomes, but the correlation wasn't that strong. Perhaps "what" or "how" is more important than "why" when integrating security technologies? Let's pull on that thread a little more in the following questions.

According to respondents, the most common motive for integrating security technologies is to improve the efficiency of monitoring and auditing.

Buy or build for well-integrated tech?

We know from the prior study that integrating security technologies drives outcomes, but what's the best way to achieve a highly integrated tech stack? Buy it that way? Build to suit? Just let it be? Let's see if we can find out.

We asked organizations about their typical approach to security technology integration, and Figure 6 tallies the responses. **Overall, more than three-quarters of organizations would rather buy integrated solutions than build them.** Of those organizations, over 40% choose technologies that come with out-of-the-box integrations into their existing infrastructure. And more than 37% take that one step further and prefer to source solutions from a single vendor so they're natively well-integrated or part of a larger platform. Just over 20% are willing to build integrations themselves, provided the product fits their needs. Few take a laissez-faire approach.

Figure 6: Common approaches to security tech integration among all organizations

Overall, more than **3/4** of organizations would rather buy integrated solutions than build them

Figure 7 evaluates whether any of these integration approaches makes a difference. Here we again see a theme pointing to benefits from collaborating with vendors to keep technology modern and well-integrated. **As seen in the chart, sticking with a preferred vendor is over twice as likely to achieve well-integrated security technologies as a hands-off approach (~69% vs. ~31%).** Furthermore, according to our research, that finding remains consistent across all organization sizes, though the benefits of using a preferred vendor are somewhat higher for small and midsize firms versus large enterprises.

And yes, we're aware that's another suspiciously convenient finding coming from a company with an extensive, integrated security portfolio. Sure, we're pleased to see that this result supports Cisco's strategy…but recall that this was a double-blind study and we didn't manipulate that result at all.

Not surprisingly, organizations that didn't do anything extra to integrate security technologies became a self-fulfilling prophecy. **We do, however, expect that some will be surprised to learn there's virtually no difference among those that buy products with out-of-the-box integrations and those that build integrations on their own.** Just under half (~49%) of organizations using each of these approaches report strong integration levels.

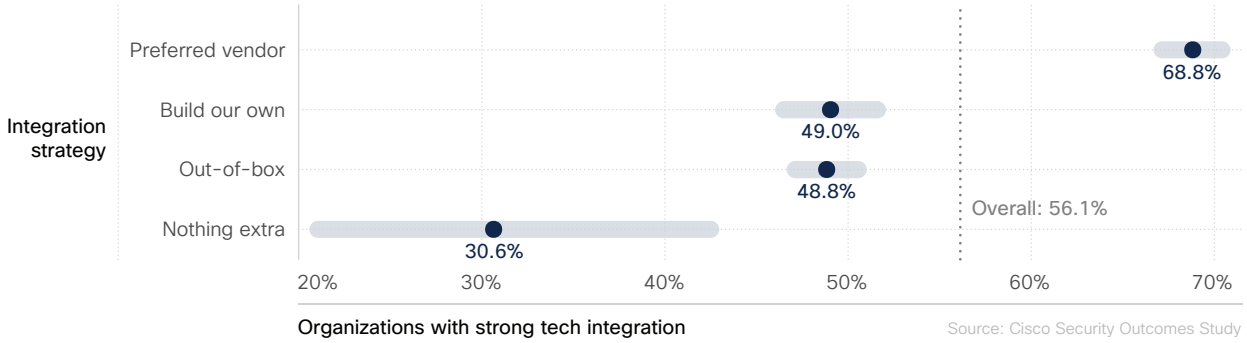


Figure 7: Effect of common integration approaches on level of security tech integration

Cloudy, with a chance of integration

We've heard from many organizations wrestling with the decision whether to begin (or expand) their security tech integration efforts in the cloud or in on-prem environments. If that's you, we have some data that might help that evaluation. The good news is that many survey respondents report good results in both on-premises and cloud environments. That said, it appears to be significantly easier to achieve strong tech integration in the cloud.

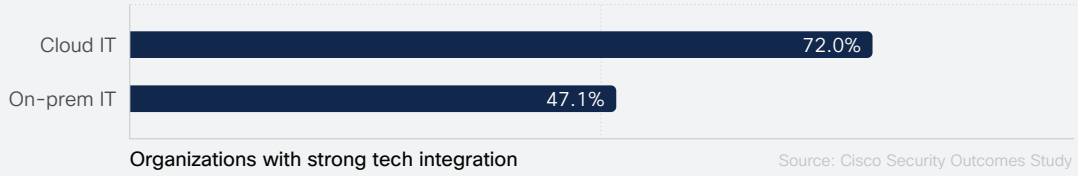


Figure 8: Effect of cloud vs. on-premises environments on level of security tech integration

Does integration aid automation?

Referring back to the start of this section, automation isn't the most common motivation for tech integration. But 44% of organizations did identify it as an incentive. Motivations aside, is there evidence that well-integrated technologies actually do enable better automation of security processes? The evidence put forward in Figure 9 points to that indeed being the case.

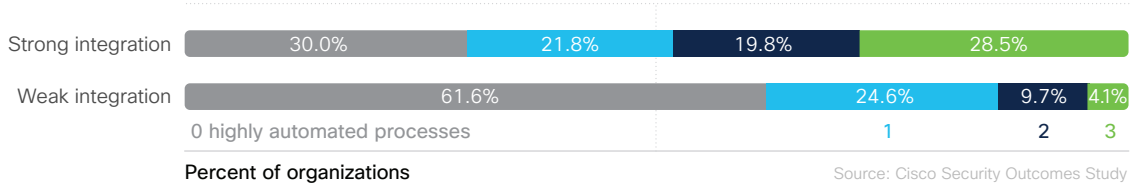


Figure 9: Effect of tech integration on extent of security process automation

The two horizontal bars in Figure 9 distinguish organizations based on their level of security tech integration (strong vs. weak). The color segments represent the number of major security processes (event monitoring, incident analysis, and incident response) supported by mature automation. The proportion of organizations with no automation is more than twice as high among those with weak integration. **Conversely, those with well-integrated security technologies were almost seven times more likely to achieve high levels of automation for all three of these processes (4.1% vs. 28.5%).** That sounds like a compelling motivation indeed!

Which functions should be integrated?

Next, we asked respondents about their level of integration among technologies supporting the five core functions of the NIST Cybersecurity Framework (CSF). They answered on a scale ranging from highly fragmented (siloed technologies that work mostly in isolation) to highly integrated (coordinated technologies that work as a functional unit). Then we created a model to determine the effect on the overall security outcomes score for each organization.

The results in Figure 10 are fairly consistent across the five functions. **Working to defragment and integrate any of the NIST CSF functional areas corresponds to an increase in security program success (+11% to ~15%).** Thus, the answer to our titular question is "all of them." But a highly integrated 'Identify' function boasts the biggest boost if you're wondering where to start.

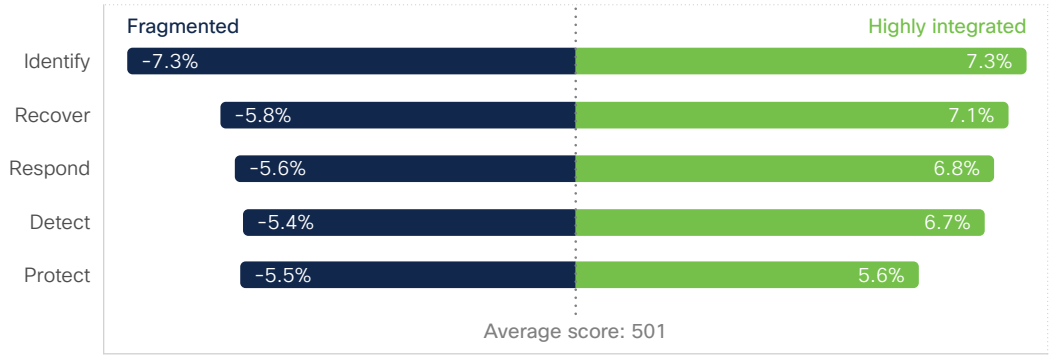


Figure 10: Effect of integrating NIST CSF functions on overall security outcomes score

We can't help but see a connection between this fact and what we learned in the previous section about monitoring, auditing, and collaboration being the strongest drivers for integrating technology. Together, they seem to advocate for the foundational importance of good visibility across the enterprise. It certainly makes sense that a fragmented approach to "developing an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities" (CSF language) won't end well. You'll see this theme further reinforced as we roll into the Threat Detection and Incident Response section.

On integration, identification, and information

Beyond the chart we just discussed, data throughout this study consistently points to the crucial relationship between integration, identification, and information. If you can't identify an asset or threat, you won't know it's there, and therefore won't be concerned enough to establish an informed defense until it's too late.

Figure 11 illustrates this concept well. We compared each organization's reported level of integration within the NIST CSF 'Identify' function to their ability to accurately detect threats in a timely manner. **Organizations with highly integrated systems for identifying critical assets and risks boasted much stronger (+41%) threat detection capabilities.** So, in a real sense, fighting fragmentation and fighting foes go hand-in-hand!

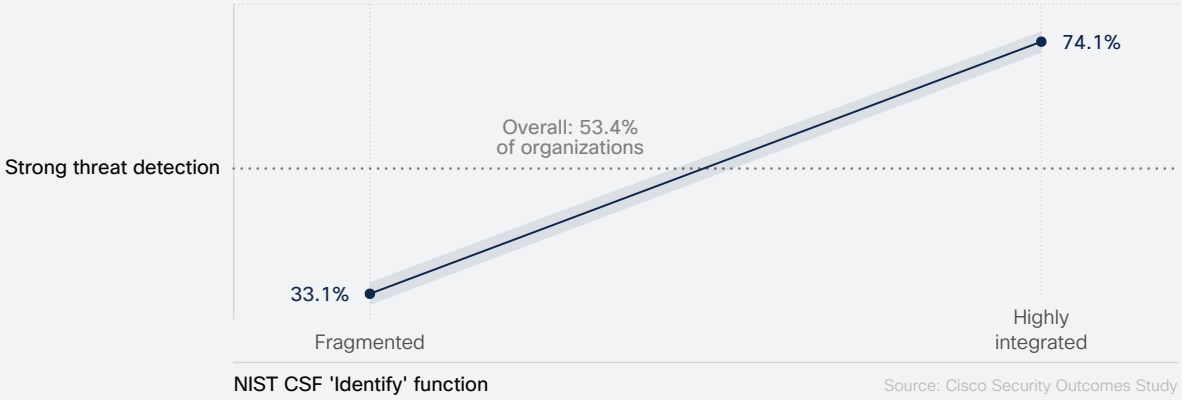
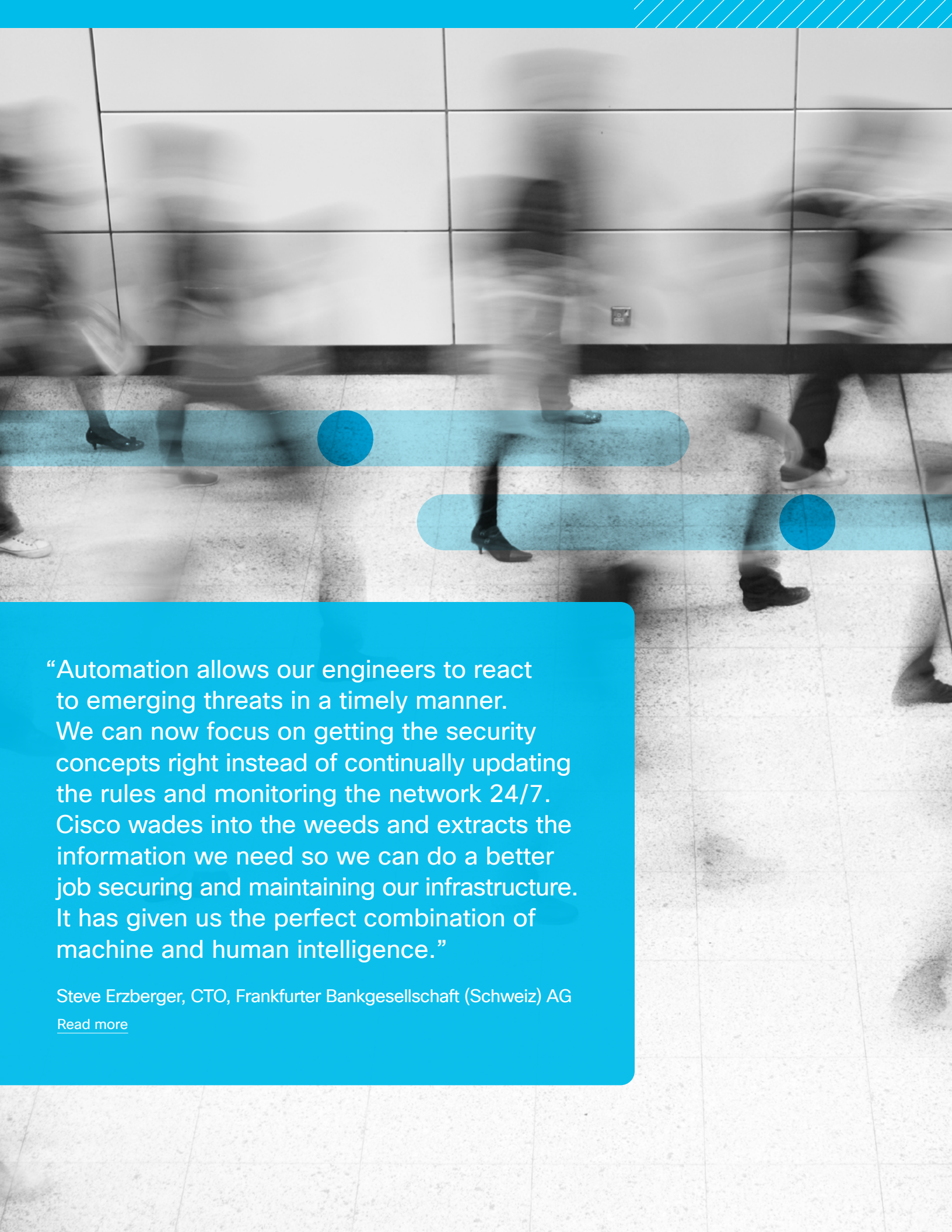


Figure 11: Effect of integrating the NIST CSF Identify function on threat detection capabilities

Organizations with highly integrated systems for identifying critical assets and risks had **+41%** stronger threat detection capabilities



"Automation allows our engineers to react to emerging threats in a timely manner. We can now focus on getting the security concepts right instead of continually updating the rules and monitoring the network 24/7. Cisco wades into the weeds and extracts the information we need so we can do a better job securing and maintaining our infrastructure. It has given us the perfect combination of machine and human intelligence."

Steve Erzberger, CTO, Frankfurter Bankgesellschaft (Schweiz) AG

Read more

Developing Threat Detection and Incident Response Capabilities

This section covers two separate security practice areas that both made the Fab Five in their own right. But because threat detection and incident response (IR) often share people, processes, and technologies under the banner of security operations (SecOps), we asked a set of common questions between them. Thus, it makes sense to analyze them within the same section for this study.

Nearly all (about 92%) of organizations with strong people, process, and technology achieve advanced threat detection and response capabilities.

Prioritize people, process, or technology?

Speaking of people, processes, and technology (aka the p-p-t triad), let's start our investigation there. Security functions are often described as a combination of all three elements, particularly in the domain of threat detection and incident response. But is any part of this security trinity more critical than the others? You know where this is going; let's jump into the analysis.

Starting from the bottom of Figure 12, we see that only about a quarter of programs lacking strength in all facets of the p-p-t triad express confidence in their SecOps. Gaining strength in any one area – people, process, or technology – boosts that percentage up to roughly 60% to 64%, depending on which one. Strong people appear to grant a slight edge, but the overlapping confidence intervals caution against making too much of that fact. The important takeaway is that any of these offer a good starting point for building better detection and response capabilities.

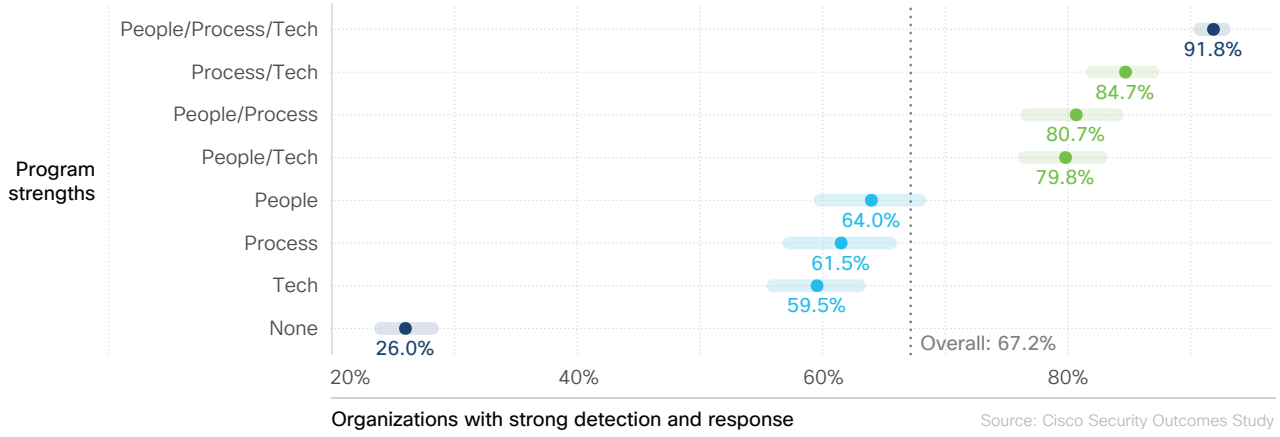


Figure 12: Effect of strong people, process, and technology on threat detection and incident response capabilities

Continuing up Figure 12, doing two things well moves SecOps programs solidly above the average and improves capabilities by about 15% to 20% over those that just do one thing well. Once again, it doesn't really matter which people, process, technology pairing you choose. You just need strength in any two. It's nice to know that there's some freedom of choice in tailoring your organization's SecOps roadmap, isn't it?

And that brings us to elite programs in Figure 12 that manage to attain the SecOps trifecta. **Nearly all (about 92%) of organizations with strong people, process, and technology achieve advanced threat detection and response capabilities.** That's a 3.5X performance increase compared to SecOps programs that don't get any of those right! So, start wherever you can make the most headway, but don't stop until you reach the p-p-t pinnacle.

Organizations with strong people, processes, and technology see a **3.5X** performance increase for threat detection and response over those lacking strength in all of these areas

Do zero trust and SASE enable better SecOps?

We understand that abstract descriptors like “strong technology” make it difficult to form concrete takeaways from the findings above. That’s why we posed a couple follow-up questions about specific architectures. We asked respondents about their adoption of zero trust and secure access service edge (SASE) to better understand how those approaches affect threat detection and incident response capabilities (and therefore security program outcomes).

Figure 13: Effect of zero trust and SASE architectures on threat detection and incident response capabilities

Organizations that claim to have mature implementations of zero trust or SASE are about 35% more likely to report strong SecOps than those with nascent implementations. These results corroborate the evidence we shared earlier about the many benefits modern architectures can bring to cybersecurity programs.

Do more heads mean fewer headaches?

We know that good people are important to building strong threat detection and incident response capabilities. But is it better to focus on adding more people or adding to the skills of the people you have? Obviously, that doesn't have to be mutually exclusive, but the question remains–do we see any evidence that quantity or quality is more important when it comes to developing successful SecOps teams?

To answer that, we first calculated a ratio of SecOps staff to overall employees for all organizations. We then compared that ratio to the reported strength of detection and response capabilities. Figure 14 depicts the outcome of those calculations, and while it doesn't fully answer the question of quantity or quality, it does offer some takeaways.

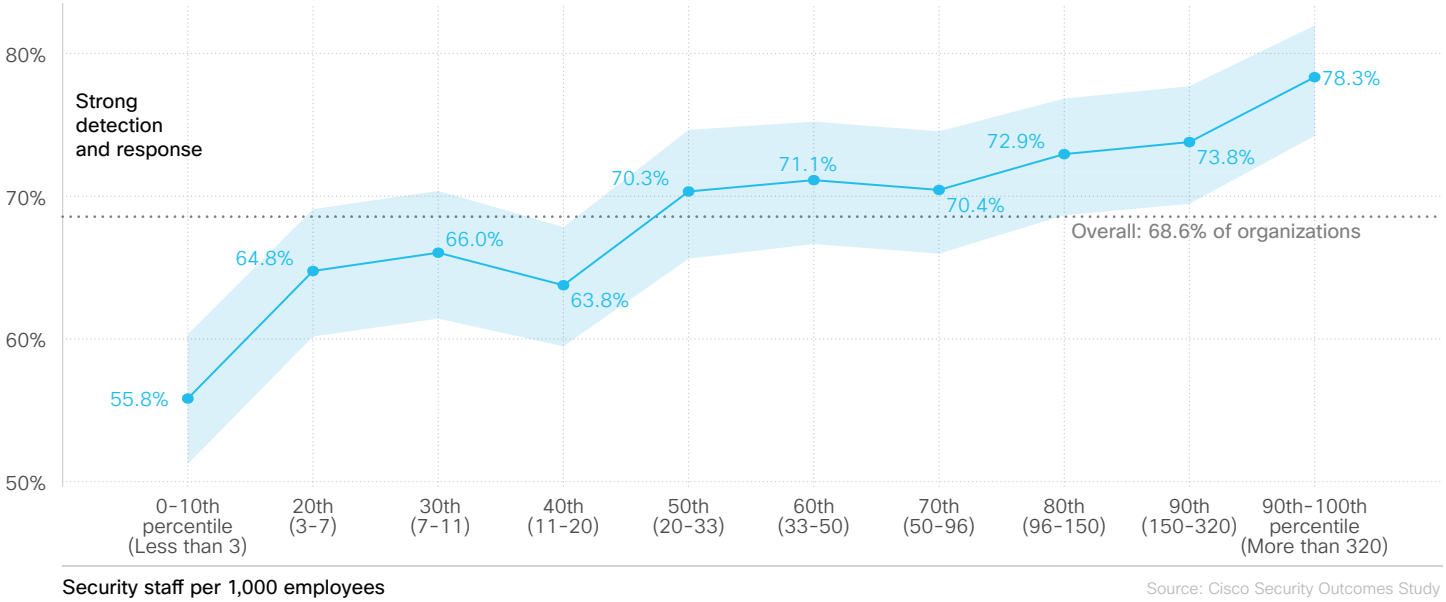


Figure 14: Effect of security staffing ratio on threat detection and incident response capabilities

First among these takeaways is that security staffing ratios do correlate with better threat detection and response. Organizations with the highest ratios are just over 20% more likely to report stronger capabilities than those with the lowest. BUT–see how the dotted line marking the overall average crosses through much of the shaded confidence interval in Figure 14? That basically means that organizations not on the extreme ends of the staffing scale (the majority of them) are equally likely to report strong SecOps programs.

What does all that actually mean? Well, we can say with confidence that organizations with huge security teams are significantly more likely to achieve strong detection and response capabilities than those with skeleton crews. But headcount alone won't make all your SecOps headaches go away or guarantee success. Furthermore, even the differences between the smallest and largest staffing ratio don't account for the performance boost associated with having strong people resources in the previous section. **Thus, we're left to infer that quality is equally–perhaps even more–important than quantity when it comes to building strong threat detection and response teams.**

Security teams continue to face a severe staffing shortage.

With shrunken resources and rising threats, many cybersecurity professionals are experiencing extreme stress and burnout. What proactive measures can we take to help their well-being? In this eBook, we asked industry leaders and practitioners to share their insights and stories on managing mental health.

SecOps staffing: Yours, mine, or ours?

So, SecOps success isn't merely about headcount, but do staffing models affect outcomes? All things being equal, is it better to outsource, insource, or share responsibilities for threat detection and response? Let's see how the data answers that question—but be warned—it kind of speaks out of both sides of its mouth on this one.

We asked respondents about their staffing models and then compared that with the rating of their detection and response capabilities. **As seen in Figure 15, organizations with predominantly insourced or outsourced teams were much more likely (+20% to 30%, respectively) to report strong SecOps programs than those with a mixed staffing model.** Since most organizations said they used some form of mixed model, we thought it would be worth looking at this from a different perspective before dooming them all to failure just because the survey (seems to) indicate this outcome.

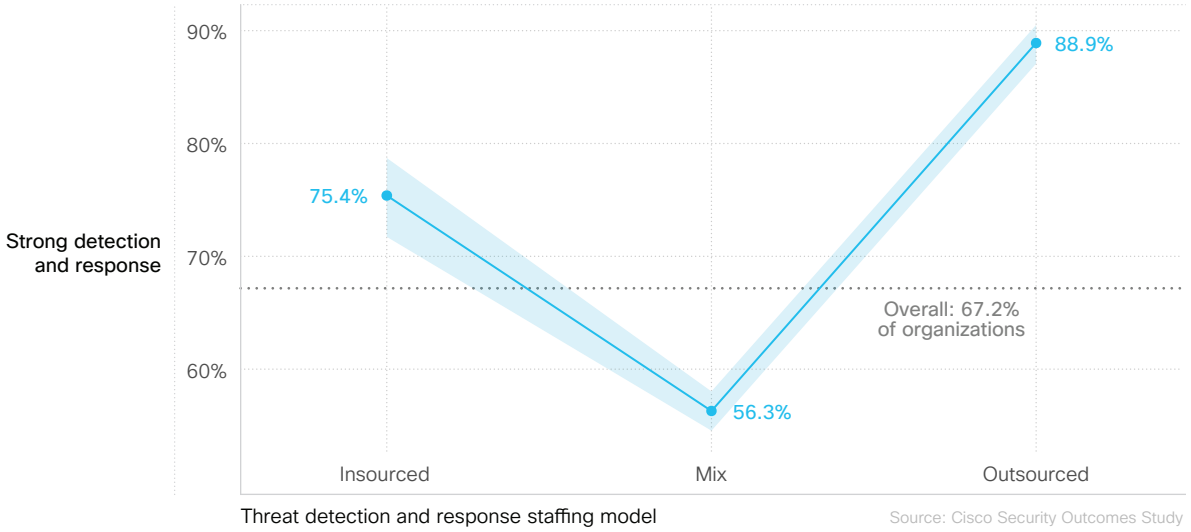


Figure 15: Effect of staffing models on perceived threat detection and incident response capabilities

Organizations with predominantly insourced or outsourced teams are **20 to 30%** more likely than those with a mixed staffing model to report strong SecOps programs

In addition to asking respondents to rate the perceived strength of detection and response capabilities, we also tried to obtain more objective metrics for comparison. One of those is Mean Time to Respond (MTTR), or the average time to remediate or contain a security incident. In our background analysis outside this report, these metrics often tend to directionally agree with the subjective assessments. But the two perspectives contradicted each other in this case, as is evident from Figure 16.

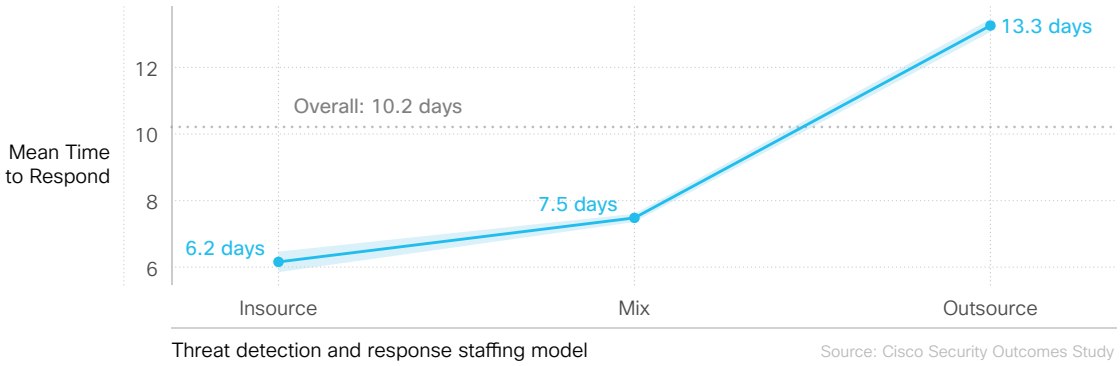


Figure 16: Effect of staffing models on Mean Time to Respond to security incidents[2]

Based on Figure 16's side of the story, organizations with internal threat detection and response teams enjoy an MTTR that's less than half that of outsourced models (about 6 days vs. 13 days). Those with hybrid staffing models land in the middle (about 8 days), with MTTRs that aren't quite as quick as internal teams but much faster than their mostly outsourced counterparts.

Obviously, we have a bit of a quandary here. Which measure (perspective vs. metric) is right and, more importantly, which one should you listen to in terms of making sourcing decisions. We're going to be intentionally dodgy here and say "both" and "neither" (hey—don't blame us for following the data's conflicting lead here).

Of course, remediation has many elements and dependencies to it. The organization may be dependent on a vendor to issue a patch/bug fix to fully resolve a vulnerability. That patch then needs to be lab tested in their environment before being deployed into production. Suffice it to say there are a lot of moving parts involved.

In truth, it's hard to know for sure what's going on here. Maybe trying to collect metrics via a survey is misleading. Maybe MTTR and capability ratings are different enough that it's possible to have a "strong" detection and response program overall, yet slower remediation rates. Maybe those programs are slower because they're more thorough. Maybe coordinating with outsourced staff just takes longer. Maybe there's a sense of confidence because "we're paying the experts to do this and they've got it covered." Maybe we're seeing a SecOps version of the Dunning-Kruger Effect. It's probably all this and more. And because of that, we suggest using this section to spark discussions rather than make decisions.

[2] We use the geometric mean in this chart as it is more representative of a "typical" value. The reported MTTR was typically less than 2–3 weeks, but occasionally respondents reported months (or years!). Using the geometric mean manages to represent "typical" better without being skewed by those extremely large values.

Is it smart to use intelligence?

Speaking of the Dunning-Kruger Effect, that's a perfect setup for this section. We asked respondents about the use of cyber threat intelligence in their SecOps program. Most organizations (85%) say they're using intelligence at some level, but less than a third (31%) claim to be using it extensively. Does that intel lead to better, smarter, faster threat detection and response? Well...let's look at Figure 17.

Curiously, most organizations that don't use threat intelligence at all seem to think they're doing pretty well. The old adage of "ignorance is bliss" comes to mind here, especially since dipping a toe in the intel waters apparently dispels those notions (about 84% down to 46% confidence). **Organizations that make extensive use of threat intelligence are nearly twice as likely to report strong detection and response capabilities compared to those with lower usage. And in an example where capability ratings and metrics agree, those that leverage intel more heavily achieve MTTRs that are about half that of non-intel users.**

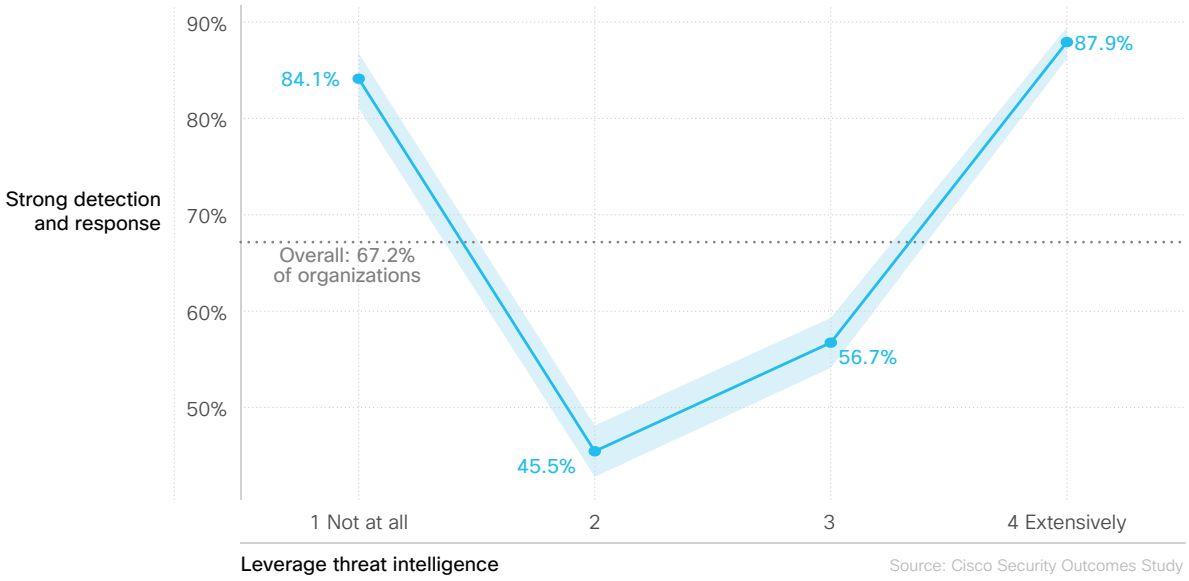


Figure 17: Effect of cyber intelligence usage on threat detection and incident response capabilities

Psychologist and best-selling author Daniel Kahneman once said, "We're blind to our own blindness. We have very little idea of how little we know." Figure 17 suggests that once organizations know a little bit about the threats arrayed against them, they realize there's a lot they don't know. More extensive use of threat intelligence begins building back that confidence—except now it's not so blind.

Organizations that make extensive use of threat intelligence are nearly **2X** as likely to report strong detection and response capabilities

Is automation a substitute for people?

After reading this title, you might have assumed it was a rhetorical question. Not so fast. At the risk of drawing the ire of the entire security community, we're going to go out on a (data) limb here to suggest that automation can, in fact, replace people. BUT keep reading before you decide to delete this report and add us to your blocked contacts list. <deep breath>

Figure 18 incorporates elements you've seen before in separate charts—security staff and automation. The two lines compare two different types of SecOps programs. The first (dark blue line) represents organizations that DO NOT have strong people resources, while those that DO enjoy that luxury are represented by the bright blue line. In both scenarios, moving from left to right shows the effect of increasing levels of automation on threat detection and IR capabilities.

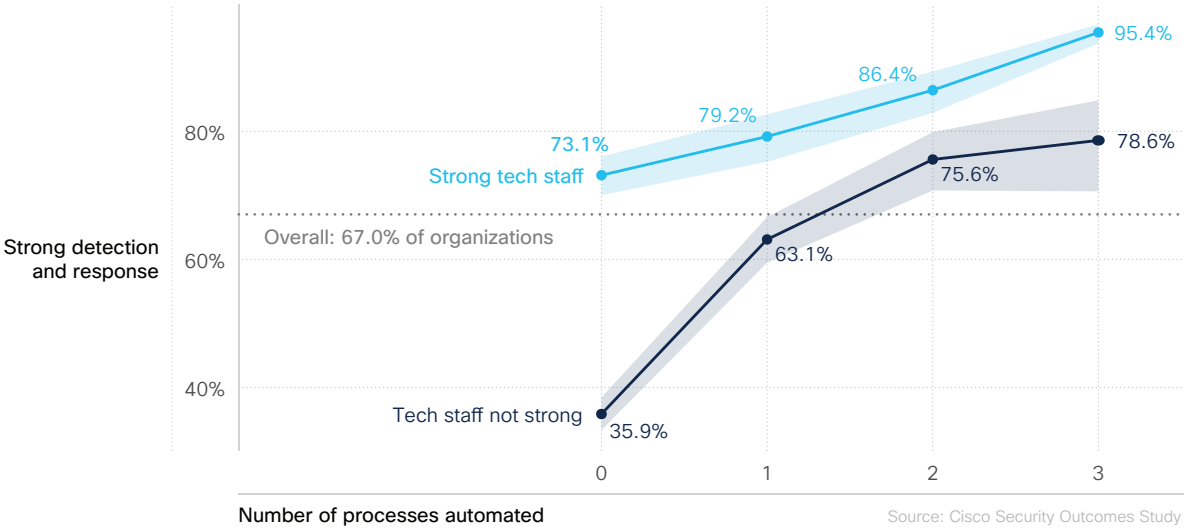


Figure 18: Effect of staffing and automation strength on threat detection and incident response capabilities

Let's start with the Have Nots. Only about a third of organizations that lack strong security staff and don't automate any major processes report strong detection and response capabilities. That jumps a lot when one of the three process areas we inquired about (threat monitoring, event analysis, incident response) is automated. Automating two of those further ups the value, and automating all three more than doubles the performance of less experienced staff alone. **Over three-quarters of SecOps programs that don't have strong staffing resources are still able to achieve robust capabilities through high levels of automation.**

Now trace your eye or finger from the rightmost point on the dark blue line to the first point of the bright blue line. Did you catch the implication? **A SecOps program with a weaker staff that employs advanced automation rates close to the same as one with a strong staff and poor automation.** Or said differently, strong automation can be a substitute for a strong staff. See—we wouldn't lie to you!

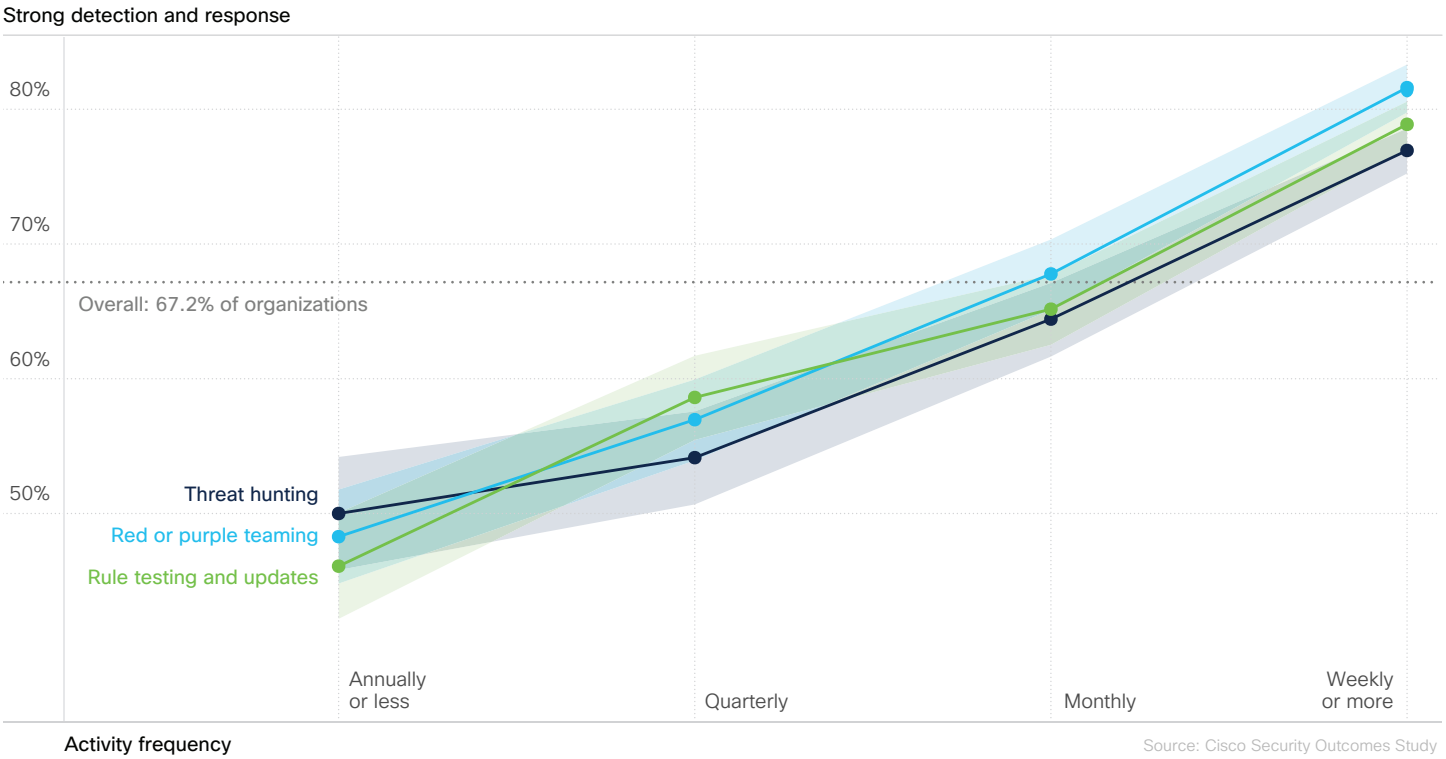
But man vs. machine isn't really the main point or most important lesson from Figure 18. Following the blue line through successive levels of automation provides very compelling justification for pursuing both objectives. Security programs that manage to assemble a strong team AND automate major threat detection and response processes are almost assured (more than 95%) of SecOps success. So, don't use automation as a substitute for a talented workforce. Use it to augment your talent by allowing them to focus on high-priority activities.

How often should we tweak, hack, and hunt?

One could name any number of recurring activities that could potentially improve threat detection and response programs. In an informal poll we took on that topic, three were recommended more than any others:

- Testing and updating detection rules and use cases
- Proactively hunting for signs of malicious activity
- Engaging in red and/or purple team exercises

We asked respondents how often their organizations conduct each of those activities and then checked that against the reported strength of threat detection and response capabilities. The resulting trend in Figure 19 couldn't be any clearer.



Source: Cisco Security Outcomes Study

Figure 19: Effect of activity frequency on threat detection and incident response capabilities

Rule tweaking, red/purple teaming, and threat hunting all follow a similar trajectory. The more they're done, the more they benefit SecOps programs. **Organizations that conduct these on at least a weekly basis see a roughly 30% lift in performance compared to those that do them annually or less.** So, how often should your organization do them? The simple answer is "more often is better."

Organizations conducting these activities on at least a weekly basis see a roughly **30%** lift in performance

"Security is changing all the time and we need to follow these security trends. [Previously], we lost a lot of time in solving security issues and incidents. Now that we've simplified our process and saved time during investigations, we can follow the new security trends and integrate new security solutions to provide a more secure infrastructure for our educational network."

Bahruz Ibrahimov, Senior Information Security Engineer, AzEduNet

Read more

Ensuring Prompt Disaster Recovery and Resilience

It's interesting how the "top of mind-ness" of different aspects of cybersecurity ebb and flow over time. After taking a backseat to data breaches and cyber espionage for a number of years, the topic of business continuity and disaster recovery (BCDR) is once again front-and-center. And there's good reason for it. Rampant ransomware, outages of major hosting providers, and so on have forced major changes in strategies for ensuring resiliency in the face of relentless threats.

The 2021 Security Outcomes Study ranked prompt disaster recovery as the fourth strongest contributor to building successful cybersecurity programs. It showed significant correlations with all 11 outcomes except one (security culture). With that in mind, let's examine strategies for maximizing the effectiveness of this practice and ensuring resilience.

Rampant ransomware, outages of major hosting providers, and so on have forced major changes in strategies for ensuring resiliency in the face of relentless threats.

Should disaster recovery have board-level oversight?

We were curious to know who had ultimate oversight of disaster recovery capabilities. It turns out the buck stops fairly evenly with the CIO, CISO, and other non-IT members of the C-Suite, with about a quarter of organizations' BCDR processes reporting up to each. Board-level visibility is a little less common than those, but still present in 18% of organizations in our survey.

When we compared these answers to each respondent's assessment of their business continuity and disaster recovery capabilities, it became apparent that the question of oversight isn't just a curiosity. **Per Figure 20, organizations with board-level oversight of BCDR are the most likely (11% above average) to report having strong programs.** Business continuity and disaster recovery functions that topped out with the CIO exhibit the lowest rates that fall significantly below the average.

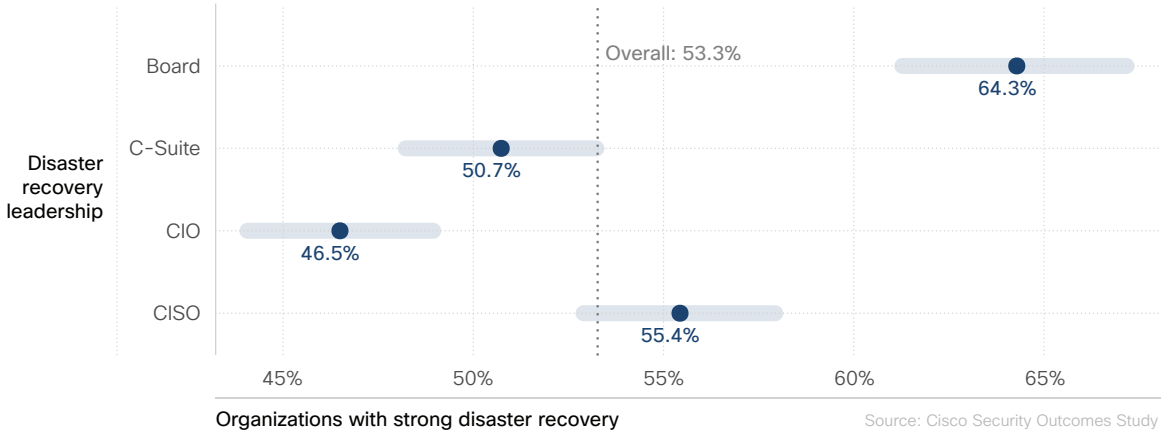


Figure 20: Effect of top-level organizational oversight on disaster recovery capabilities

There are many plausible explanations for the results in Figure 20. We suspect organizations answering to the board on disaster recovery matters likely have heightened concerns over operational risk and resiliency. Those concerns presumably translate into tighter oversight, stronger support, and bigger budgets. So, if your organization is struggling to improve disaster recovery capabilities, it might make sense to build them top-down rather than bottom-up.

What about the day-to-day operation of disaster recovery?

In addition to ultimate oversight, we also asked who's responsible for running the more tactical aspects of disaster recovery. **Operations residing within cybersecurity or specialized business continuity teams tend to report the best performance.** Programs run by IT generally fell below those. Interestingly, board-level visibility seems to act as a rising tide that lifts all boats. Success rates were statistically equal regardless of where day-to-day responsibilities fell as long as ultimate oversight went up to the boardroom.

Is the scope of disaster recovery important?

You probably won't be shocked to learn that disaster doesn't conveniently strike only when or where you're ready for it. Cybersecurity disasters are no different, which is why conventional wisdom in the field is to prepare for all eventualities as best you can. That's easier said than done, of course.

Attesting to that fact, less than three out of ten organizations say their disaster recovery functions cover at least 80% of critical systems. Half fall into the 50% to 79% zone, and a little under 20% admit coverage rates lower than that. At first blush, that doesn't seem too bad. Afterall, most organizations have the majority of their critical systems covered. Unfortunately, that fact ignores the pesky tendency of disasters to strike in unexpected places. Our data suggests that this happens more often than we'd like to admit.

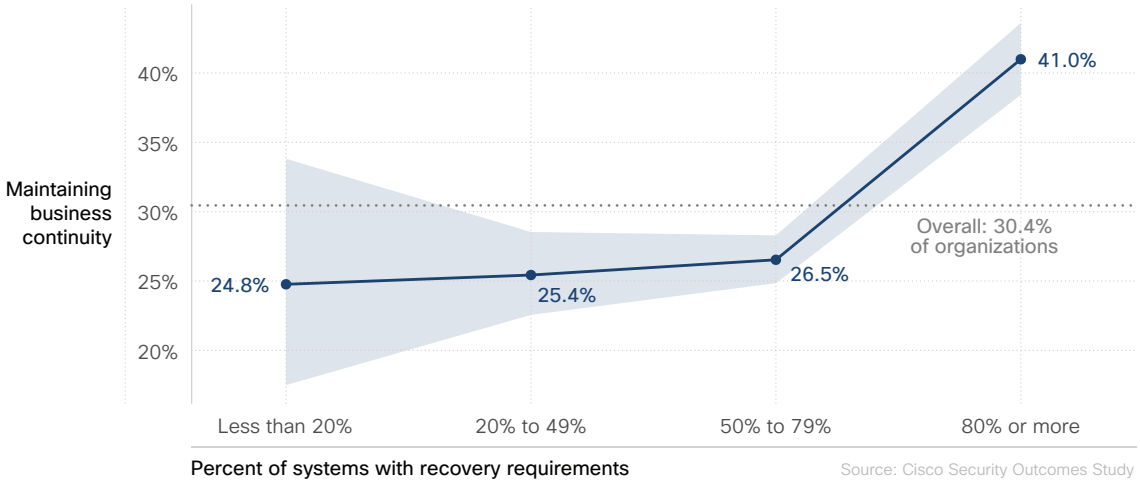


Figure 21: Effect of critical asset coverage on disaster recovery capabilities

Figure 21 measures a new outcome added for this study aimed at measuring the organization's ability to maintain business continuity through disruptive events. It turns out that it's one of the three outcomes respondents report struggling with the most. That makes it all the more important to find effective ways of improving the likelihood of success.

There's an important message in Figure 21 about maintaining business continuity. **Namely, there's virtually no improvement in the probability of achieving this outcome until BCDR capabilities cover at least 80% of critical systems.**

This almost certainly goes back to disasters' uncanny propensity to strike where we're not ready. The lesson here is that we can't expect investments in business continuity and disaster recovery to result in immediate or equivalent outcomes. That's probably not a welcome message, but then again, disaster is never a welcome messenger.

Does practice make for perfect disaster recovery?

We'll tip our hand for this question and give the answer right up front. No, it unfortunately does not. But it does make it a lot better than not practicing at all. How much better? Keep reading...

A well-known military adage says, "No plan survives first contact with the enemy." It turns out that rolls over quite well into the cyber battlefield, and there are many different ways of testing BCDR capabilities, including plan walkthroughs, tabletop exercises, live testing, parallel testing, and full production testing. We asked respondents about how often their organizations engage in such exercises, and compared that to their likelihood of maintaining business continuity.

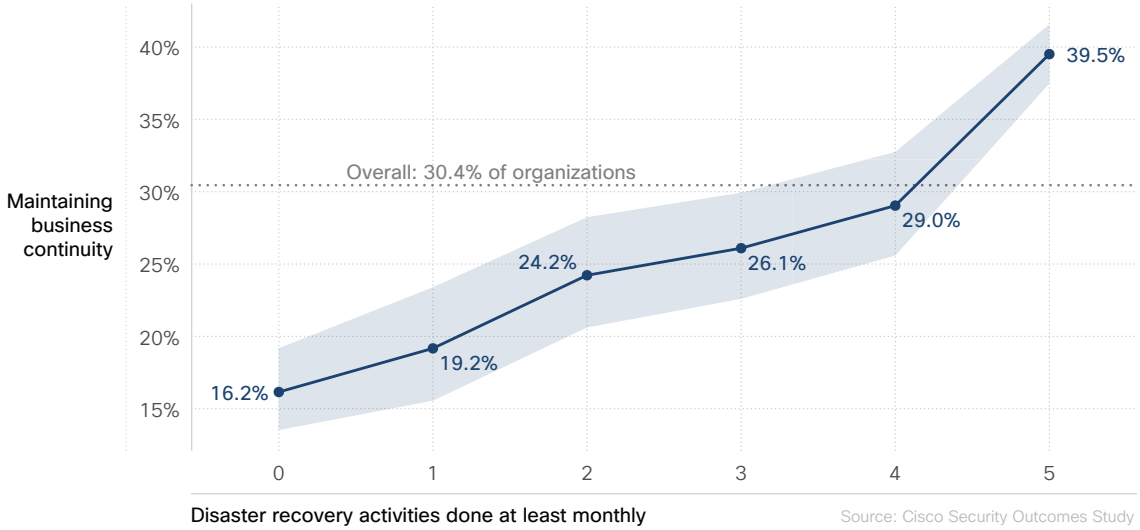


Figure 22: Effect of testing exercises on disaster recovery capabilities

None of these practices stood way above the others in terms of efficacy, but all of them collectively contributed something to better resilience. **Organizations that regularly engaged in all five types of disaster recovery testing were almost 2.5 times more likely to successfully maintain business continuity than those who did none.** The takeaway? Don't leave resiliency to chance. Stress test your business continuity and disaster recovery capabilities regularly from multiple different angles.

Organizations regularly engaged in all five types of disaster recovery testing are **2.5X** more likely to successfully maintain business continuity

Should we unleash the chaos monkey?

On the topic of stress testing your disaster recovery plan, let's maximize the "stress." We're talking about chaos engineering, whereby systems are periodically disrupted (intentionally) to test their ability to withstand unexpected conditions and events. Could tossing a monkey wrench into your IT and security systems help make your organization more resilient? Well, you've come to the right place to find out.

We asked respondents about the extent to which their organizations engage in chaos engineering, and learned it was more common than we expected. Of note, we noticed a relationship between this practice and tech integration. Per Figure 23, over two-thirds of organizations for which chaos engineering is standard practice report highly integrated technologies supporting their recovery capabilities. Whether integration necessitates or enables chaos engineering is unclear. As with so many things in this field, it's probably a bit of both. Keep an eye on this emerging discipline—especially if you're responsible for BCDR in a complex and highly integrated IT environment.

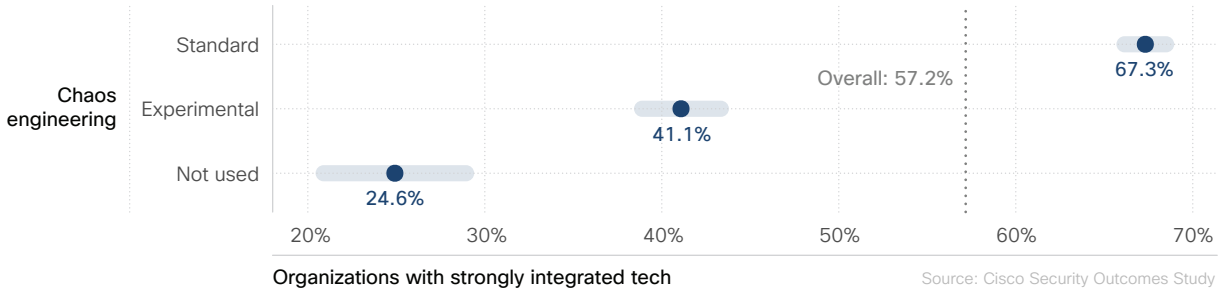


Figure 23: Relationship between chaos engineering and level of IT integration

Comparing the extent of chaos engineering with the outcome of maintaining business resiliency in Figure 24 offers a compelling reason to invite the chaos monkey into your network. **Organizations that make chaos engineering standard practice are twice as likely to achieve high levels of success for this outcome than organizations that don't use it.** If that result shocks you, you're not alone. The good news is that you can shock the monkey before it shocks you again by putting it to work for you through the practice of chaos engineering.

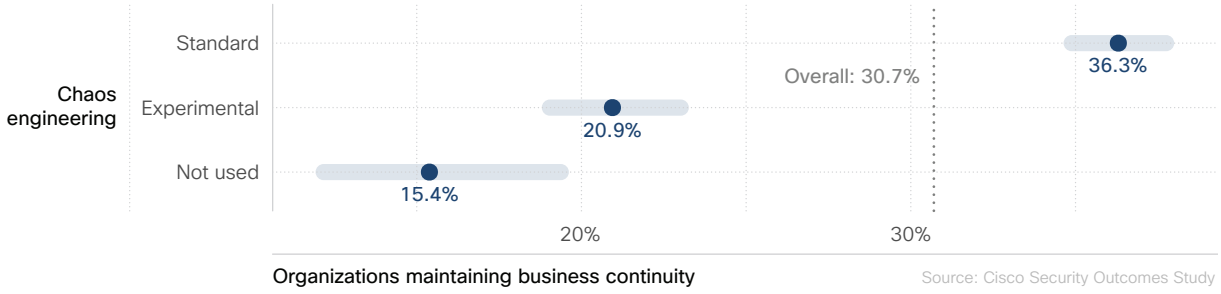


Figure 24: Effect of chaos engineering on maintaining business resiliency

Conclusion and Recommendations

We started with security practices identified as highly effective in a previous study, gathered more information via a new survey to learn what makes them most effective, and shared those lessons with you. It's our hope that you're leaving this report with several practical tips on how to make your cybersecurity program more successful.

But it never hurts to reflect on the findings of a study like this and hear what others took away from them. We asked our experienced CISO Advisory team to weigh in on each of the practice areas examined. We've included their top recommendations below. You can find additional insights and takeaways in our Security Outcomes Study blog series.

Proactive tech refresh

"The issue of security debt is significant. For the CISO, the way forward is to develop a 'Buy, Hold, Sell' strategy. Recognize what you have, define an adaptable architecture, reduce dependency risk, and implement a review loop for future refresh cycles."

Richard Archdeacon, Advisory CISO, Cisco

Well-integrated technology

"We know modern, well-integrated IT contributes to overall security program success, so here are some actions you can take to improve your environment: Look for cloud-based security solutions, investigate automation opportunities, ensure purchasing requirements include tech integration capabilities."

Helen Patton, Advisory CISO, Cisco @CisoHelen

Timely incident response

"Strong staff provide IR teams with an edge. This is a good starting point but needs to be done in conjunction with other elements. When enterprises combine strong people, process, and technology, they achieve advanced threat detection and response capabilities."

Dave Lewis, Advisory CISO, Cisco @gattaca

Accurate threat detection

"Choose the best-skilled people for your SecOps teams, because that matters more than just the number of headcount. If you can't get the expertise level you need, automation can help you bridge the gap with your junior staff and get results that are just as strong as if you had more senior staff."

Wendy Nather, Advisory CISO, Cisco @wendynather

Prompt disaster recovery

"The findings in this report highlight the value of business continuity and disaster recovery capabilities, but don't run them in isolation from other security functions. The prioritization and risk-ranking of resources should be shared with other risk management functions. Similarly, tightly integrate asset management and threat management to ensure all teams are working off the same playbook."

Wolfgang Goerlich, Advisory CISO, Cisco @jwgoerlich

About Cisco Secure

Cisco has long established itself as the worldwide leader in technology that powers the internet, while building an open, integrated portfolio of cybersecurity solutions along the way. We believe that security solutions should be designed to act as a team. They should learn from each other. They should listen and respond as a coordinated unit. When that happens, security becomes more systematic and effective. Our customers have trusted us for years as both the world's largest provider of IT infrastructure and networking services and the world's largest enterprise cybersecurity business.

Cisco Secure is built on the principle of better security, not more. It delivers a streamlined, customer-centric approach to security that ensures it's easy to deploy, manage, and use – and that it all works together. We're driven by the fact that people and our customers are at the heart of what we do. We understand that customers want to cut through the complexity and noise and feel confident in their security, focusing on outcomes. This requires simplification without being simplistic. Our cloud-native platform is a giant leap forward in that.

We empower the security community with the reliability and confidence that they're safe from threats now and in the future with the Cisco SecureX platform. We help 100 percent of the Fortune 100 companies secure work – wherever it happens – with the broadest, most integrated platform. Learn more about how we simplify experiences, accelerate success, and protect futures at cisco.com/go/secure.

Appendix: Survey Sample Demographics

In this appendix, we've included sample demographics from the 5,123 qualified responses to this survey. We hope this helps those trying to discern the representativeness of these findings.

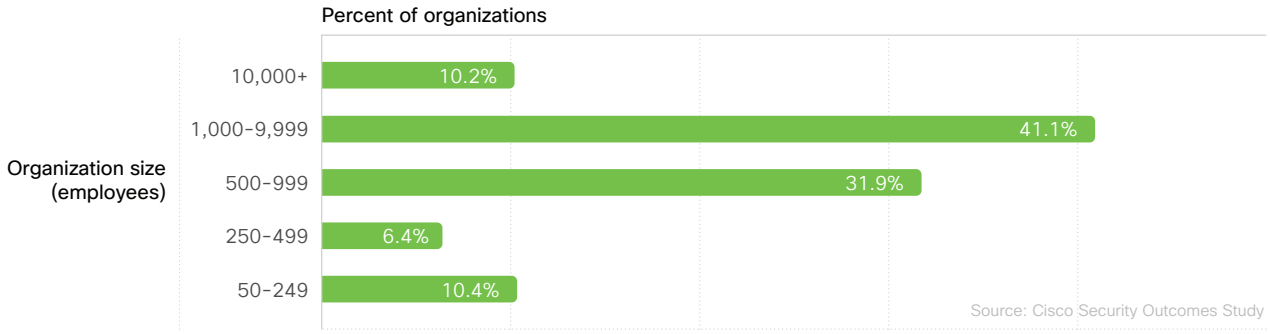


Figure A1: Number of employees for participating organizations

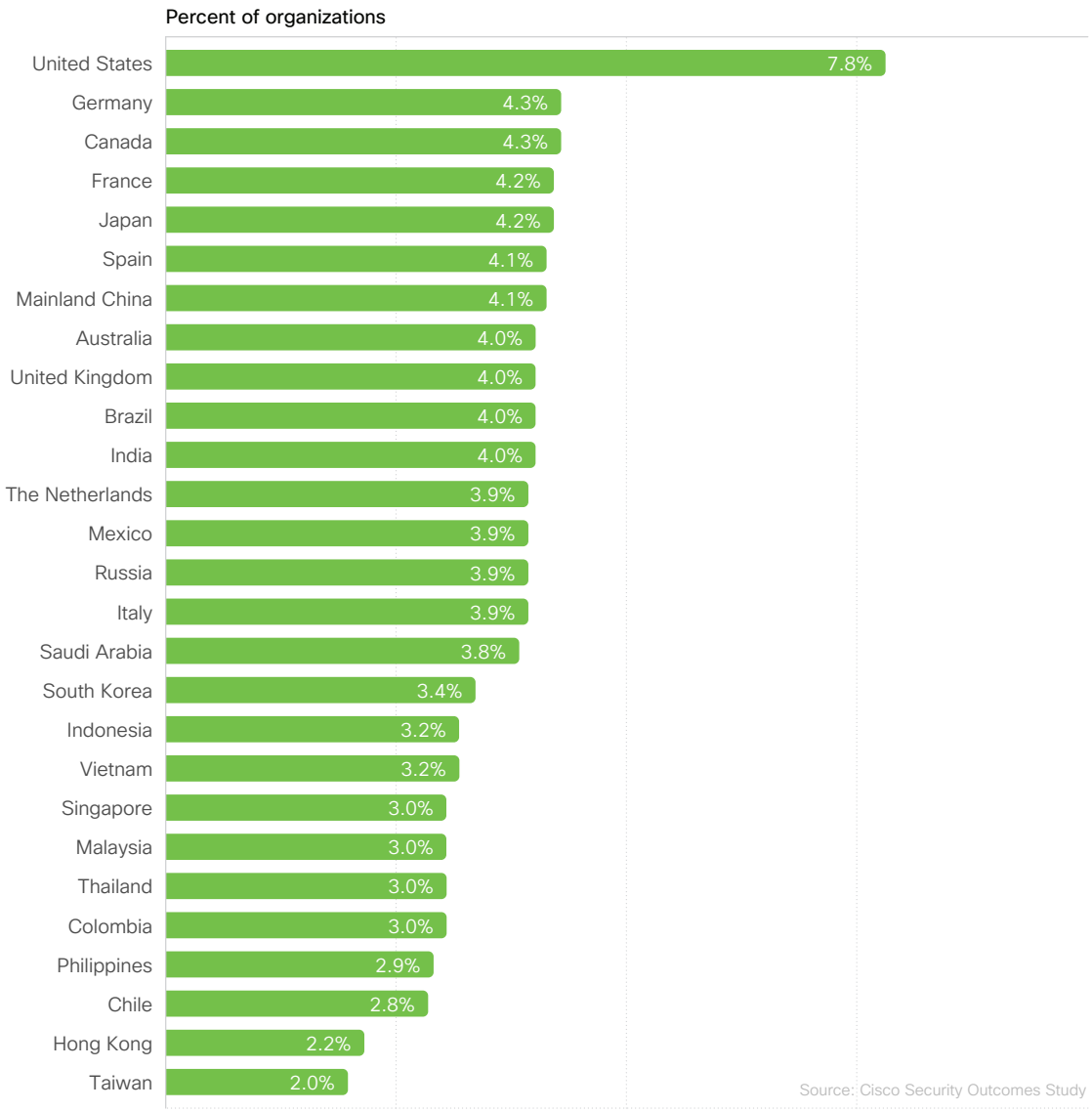


Figure A2: Markets in which participating organizations are headquartered

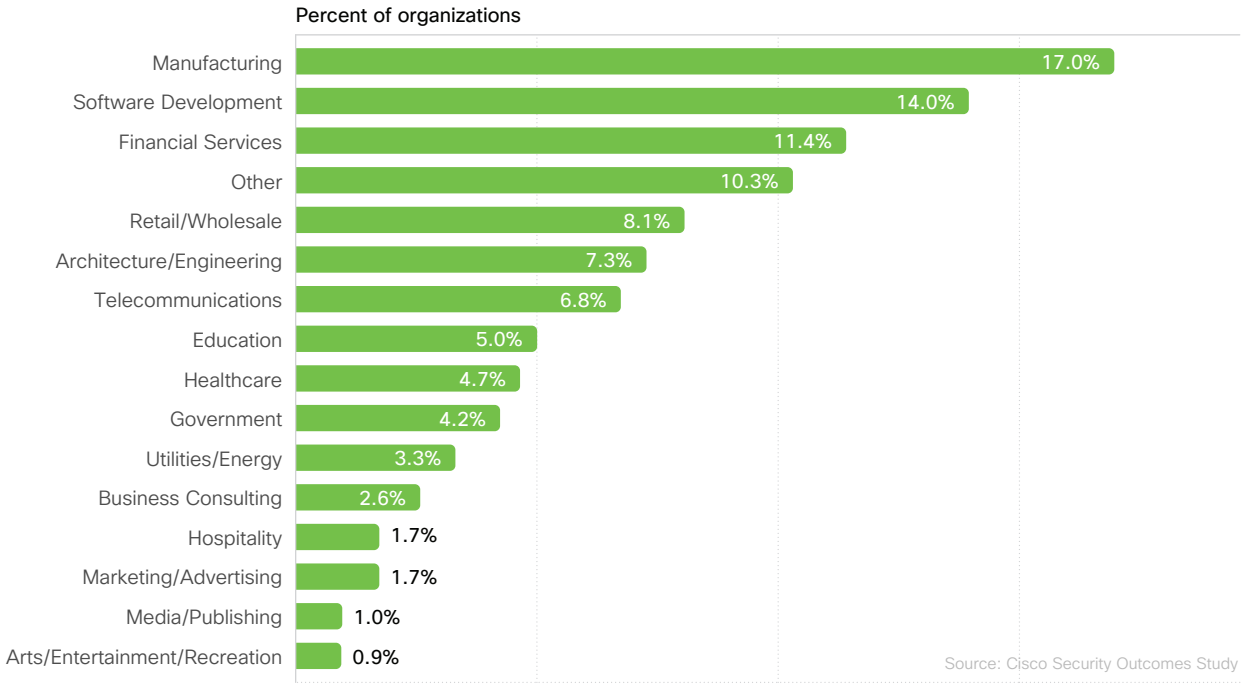


Figure A3: Industries represented by participating organizations

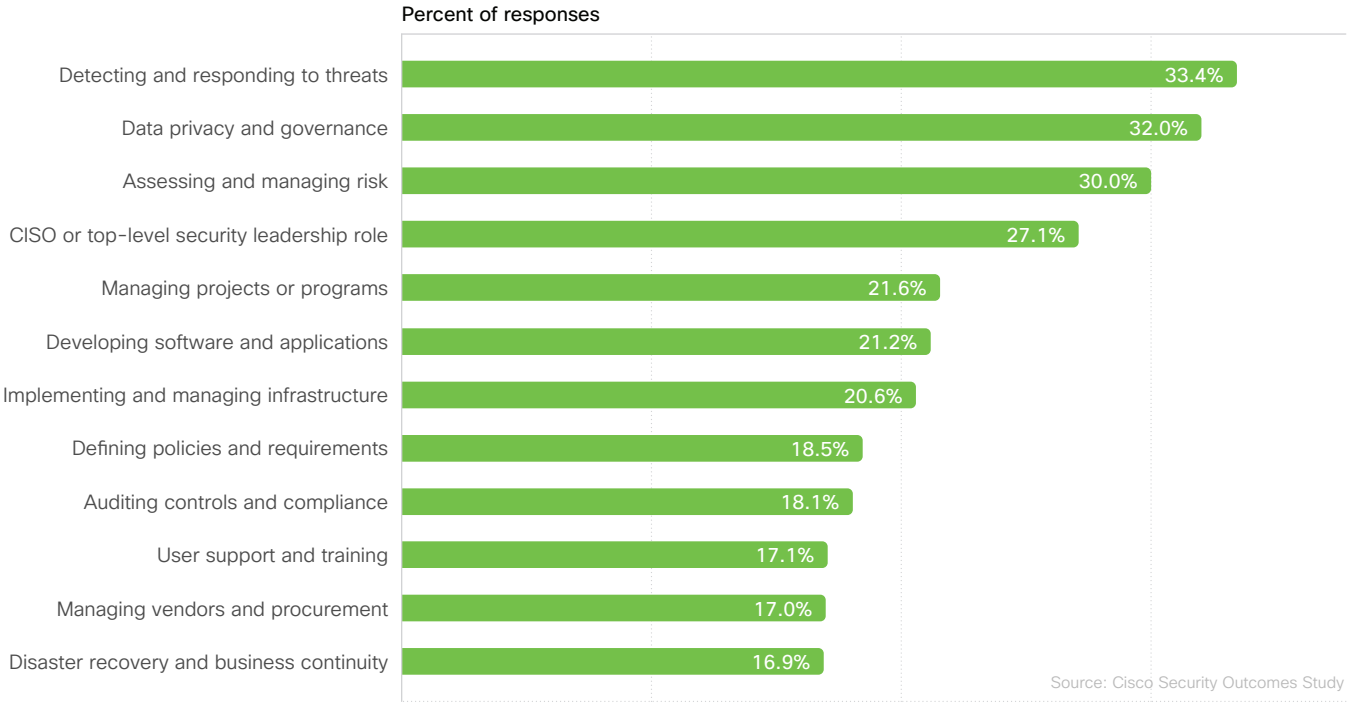


Figure A4: Primary job responsibilities among respondents

CISCO
SECURE

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA), Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Published December 2021

The bridge to possible