cisco SECURE

SECURITY

OUTCOMES

study

Contents

Introduction

When we set out to develop this study, our main goal was to provide a practical tool for you, the security leader, to guide your investments, propel you to achieve success in your security program, and better manage risk.

With a global representation (25 countries and over 4,800 respondents), we aim to empirically measure what factors drive the best security outcomes. This is quite different than what we have created in the past in our Cybersecurity Report Series, and we hope that this new approach and tone is refreshing and welcomed.

As we know, security is ever evolving to the point that success can sometimes feel elusive. So we set out to answer some questions in this study: How can we efficiently and effectively manage our cybersecurity risk? How is it that even the largest companies with the biggest security budgets still struggle to achieve certain outcomes? With all the various options out there for achieving a successful cybersecurity program, which ones should practitioners focus on? New technology? More training? Better incident response procedures? The possibilities are endless. How can a security team determine what will work best? And what's to say that won't change? (Spoiler alert, it will.)

This study will provide you with an extra boost of insight and confidence to get focused for 2021 and beyond. The past year has been challenging – even more so than usual, but there are always steps that can be taken to progress your security strategy. Read on to find out which actions may work best for your organization.

About the survey		
Sampling	**Respondents**	**Analysis**
Cisco contracted a survey research firm, YouGov, to field a fully anonymous (source and respondent) survey that ran during the middle of 2020.	We surveyed over 4,800 active IT, security, and privacy professionals from 25 countries. Sample demographics including industries, company size, and region can be found in Appendix A.	The Cyentia Institute conducted an independent analysis of the survey data on behalf of Cisco and generated all results presented in this study.

Approach

- We asked respondents about their organization's adherence to 25 security practices spanning governance, strategy, spending, architecture, and operations.
- We then asked about each program's level of success across roughly a dozen high-level security objectives or outcomes organized into three main categories: Enabling the Business, Managing Risk, and Operating Efficiently.
- Next, we conducted extensive multivariate analysis to identify security practices that correlate strongly with successful program-level outcomes.

To bring this report to life, we've worked closely with many experts around the world, including our CISO Advisory team. If you need any extra incentive to read on, here's a quote to get you inspired:

"This is not a marketing report to toss in your swag bag and ignore; this is a report to cuddle up with and read over and over again. In fact, this report will change how we think about running infosec programs. "

Wendy Nather, Head of Advisory CISOs,
Duo Security at Cisco

Key Findings

Is there evidence that security practices actually do affect program-level outcomes?

Out of the 275 practice-outcome combinations, 45% show significant correlation – meaning a specific practice affected the likelihood of achieving a certain outcome.

The strongest correlation of them all?

A proactive, best-of-breed tech refresh strategy allows you to keep up with business growth.

What about the second strongest correlation?

A well-integrated tech stack improves recruitment and retention of security talent.

Want to achieve overall program success?

Devote resources to proactive tech refresh and integrate your technology.

Want a strong security culture that's embraced by all?

Focus on good equipment, clear direction, accurate alerts, and timely fixes of security issues.

Want to avoid future incidents and losses?

Conduct after-action reviews of major incident response operations.

Which security practices are most difficult to implement?

Across all 25 practices, those in the architecture and operations category appear most challenging to do well.

Where are programs most successful? Where do they struggle the most?

Programs are most successful in meeting compliance regulations. They struggle the most with avoiding unplanned work and wasted effort.

Which function of the NIST Cybersecurity Framework contributes most to success?

The Identify function ranks #1. The Protect function ranks next to last for contributing to a program's overall success.

How did organizations minimize the impact of COVID-19 on operations?

They maintained a modern IT and security infrastructure, invested in role-based training, and kept top executives informed.

Where are we going? Security Program Outcomes

Many security studies (and programs) start by focusing on what we're doing rather than where we're headed. But a successful security program isn't just a set of directions; it's a journey toward a destination. And understanding where we are on the journey helps put everything else in proper perspective.

We've started with an admittedly difficult task – identifying a set of diverse, program-level objectives and related outcomes that security leaders desire to achieve. These outcomes are an aspirational "security destination" so to speak, even if we know we'll never quite get to this ideal. Every security leader and program is different, so we're certain you'll think of various additions and modifications to our proposed list based on your own use cases. At the same time, we hope you'll agree that they're a reasonable and relevant set of strategic outcomes that lay a solid foundation for framing out this study.

Survey respondents were asked to consider and rate how their organization is performing for each outcome in Table 1 on a scale of 'struggling' to 'succeeding.' We recognize that subjective, abstract concepts like 'keeping up with the demands of the business' can be difficult to grasp and rate, so we presented respondents with example evidence for each outcome to guide their assessment (see Appendix B).

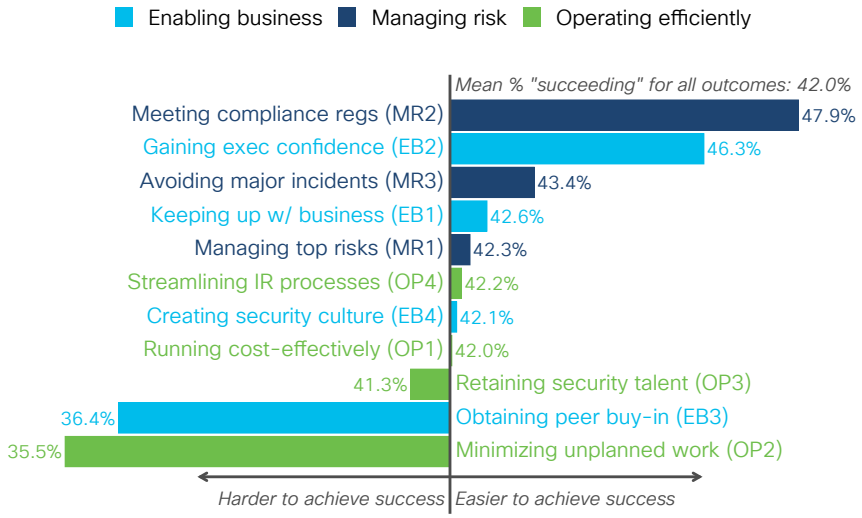
Table 1: Security program outcomes used in this study

Objective: Enabling the Business	Objective: Managing Risk	Objective: Operating Efficiently
• Keeping up with the demands and growth of the business (EB1) • Gaining the confidence and trust of executive leadership (EB2) • Obtaining buy-in from peers and other organizational units (EB3) • Creating a security culture embraced by all employees (EB4)	• Managing the top cyber risks to the organization (MR1) • Meeting regulatory compliance requirements (MR2) • Avoiding major security incidents and losses (MR3)	• Running a cost-effective security program (OP1) • Minimizing unplanned work and wasted effort (OP2) • Recruiting and retaining talented security personnel (OP3) • Streamlining incident detection and response processes (OP4)

Moving beyond context and caveats, let's get back to the question at hand – where on their journey towards a successful security program are the 4,800 organizations represented in this study? Figure 1 shows the percentage of firms that say their security program is successfully achieving each respective outcome in our list. So, roughly 48% of organizations look to be meeting compliance requirements, 46% are gaining executive confidence, and so on, down to the 36% who say their programs are minimizing unplanned work.

The overall rate of success at the program level is 42%, which we can't help but notice also happens to be The Answer to the Ultimate Question of Life, the Universe, and Everything. Coincidence? We think not, which is why we pivoted the entire figure around outcomes exhibiting a success rate above and below 42%. This format helps draw out the consensus among respondents as to which outcomes are easier to achieve (those toward the top) and which are more difficult (toward the bottom).

Figure 1: Percent of respondents reporting their firm is succeeding in each security outcome



Source: Cisco 2021 Security Outcomes Study

The 'maintaining compliance' and 'minimizing unplanned work' are polar opposites on this chart. This won't come as a shock to the many security professionals who see so-called "checkbox compliance" as the epitome of an inefficient security program. And it hints at the inherent trade-offs that exist when pursuing objectives like those we show here. We'll revisit the notion of trade-offs later when we identify program success factors.

The categorical overlay adds another interesting dimension to Figure 1. It's apparent that outcomes within the 'Managing Risk' objective tend to be perceived as less difficult, while those falling under 'Operating Efficiently' are more difficult. Outcomes associated with 'Enabling the Business' run the gamut.

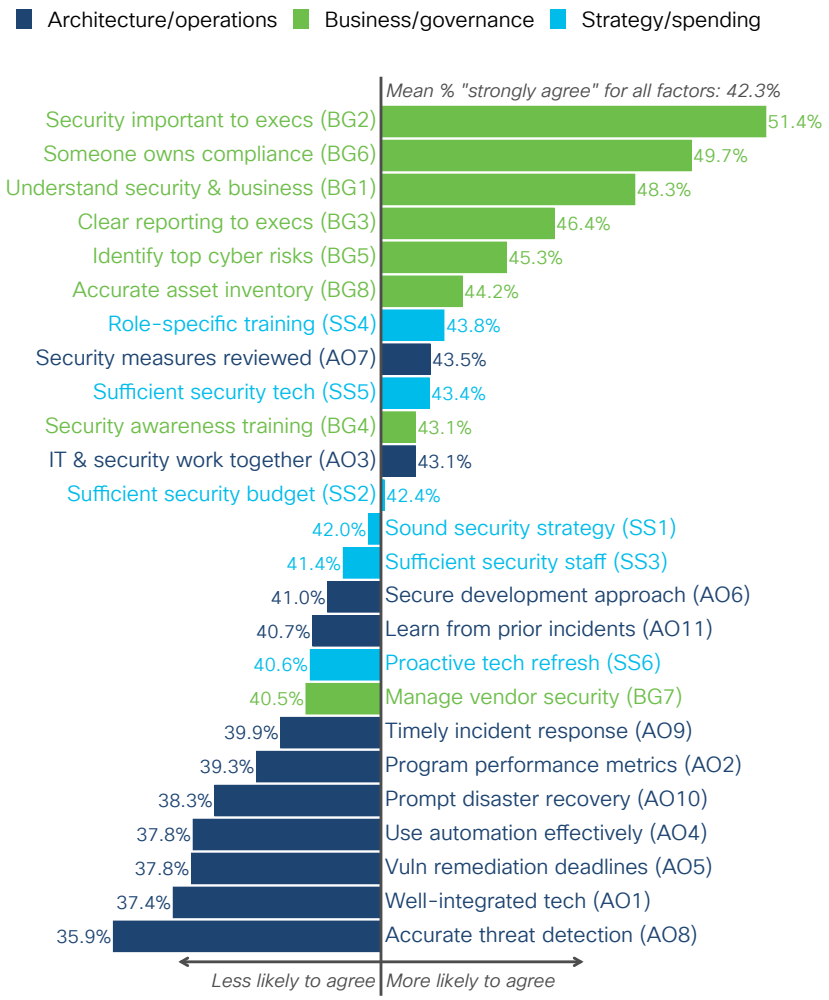
Anyone responsible for leading a cybersecurity program knows that it's not easy to manage cyber risk well AND do so with minimal cost. Given the choice, most organizations take the risk-averse route of spending more to maximize risk reduction.

What are we doing? Security Practices

We now examine what organizations are doing to meet the objectives discussed in the previous section. To do this, we asked respondents about a set of 25 security practices at their organizations. These practices were drawn from several standards, such as the NIST Cybersecurity Framework (CSF), and were organized into the categories of Business and Governance, Strategy and Spending, and Architecture and Operations. Like the outcomes, these practices are intended to be representative rather than exhaustive. You'll find the complete list of practices that fall under each of these categories in Appendix C.

Figure 2 ranks all practices according to the percentage of respondents who strongly believe their organization is following the tenets of each respective practice. We think the ratings depicted in the chart are rather optimistic, but we won't quibble over that because the adoption of controls and maturity of a cybersecurity program aren't the focus of this study. We're much more interested in how (perceived) security practices relate to the (perceived) outcomes from the previous section. But we're not quite ready to go there yet.

Figure 2: Percent of respondents who strongly agree their firm follows each security practice



Source: Cisco 2021 Security Outcomes Study

We first want to highlight the relative difference among these security practices. The format is the same as that used for outcomes in Figure 1 and pivots around the average level of implementation observed across all controls (42.3%). Those at the top are purportedly easier for firms to implement, while those on the bottom appear more difficult. We'll leave you to pick out specific practices of interest and we'll limit commentary to a few high-level observations.

Once again, we find the contrasting poles to be a fascinating glimpse into the diverse nature of security programs. Security professionals used to have to fight hard for executive attention and support, but respondents indicate that we've come a long way in that regard. On the other hand, some of the fundamentals that the industry has been working on forever, such as threat detection and vulnerability remediation, remain a challenge for many organizations. This is a good reminder that "getting back to the basics" isn't quite as simple as it sounds.

Looking more broadly at Figure 2, we see a general pattern of business and governance factors at the top, strategy in the middle, and architecture and operations at the bottom. The interpretation of that pattern goes deeper than simply "governance is easy; tech is hard." This likely reflects dependencies between these categories – i.e., you can't do the stuff at the bottom well without proper governance and strategy. But there's also the reality that most security incidents have some element of architectural or operational problems at their root. It's hard to do all the things well all of the time.

Looking for some quick wins?

We ran some additional analysis comparing the relative difficulty of the practices depicted in Figure 2 and their correlation with the outcomes listed in Figure 1. Our goal was to find practices that aren't too hard to implement, yet contribute strongly to security program success. Learn more about those quick wins in our #SecurityOutcomes blog series.

How do we get there? Identifying Success Factors

We've considered where we want our security programs to go and what we're currently doing. Now it's time to figure out exactly how to achieve those outcomes. Our overarching question is simple: What contributes to a successful security program?

Since a security program is a complex, inter-dependent system, we analyzed all practices and outcomes to identify relationships among them. For each practice-outcome combination, we calculated the change in probability of achieving outcomes associated with higher levels of adherence to various security practices. This approach allowed us to derive statistically-sound answers to questions like:

- Is there evidence that better security practices correlate with better outcomes?
- Which practices contribute most strongly to successful security outcomes?
- What are the most effective practices for achieving each specific outcome?
- How much more likely are you to achieve *x* if you do *y*?

Some may see these as simple questions with simple answers. But is that really the case? The security industry uses many best practices as part of its overall strategy. Yet we don't always measure how well those practices work, and correlate them with desired outcomes.

No really – how did you correlate practices and outcomes?

Statistics! Many of you may fall asleep (or have recurring nightmares) after reading this, but the answer is careful, rigorous statistics. In particular, we utilize multivariate generalized linear models to understand the effects of each practice on each outcome. That is, we create a logistic regression where each outcome variable is the dependent variable and all the factors are independent variables. This allows us to test when factors make a statistically significant difference and when we might be just seeing the correlation by chance.

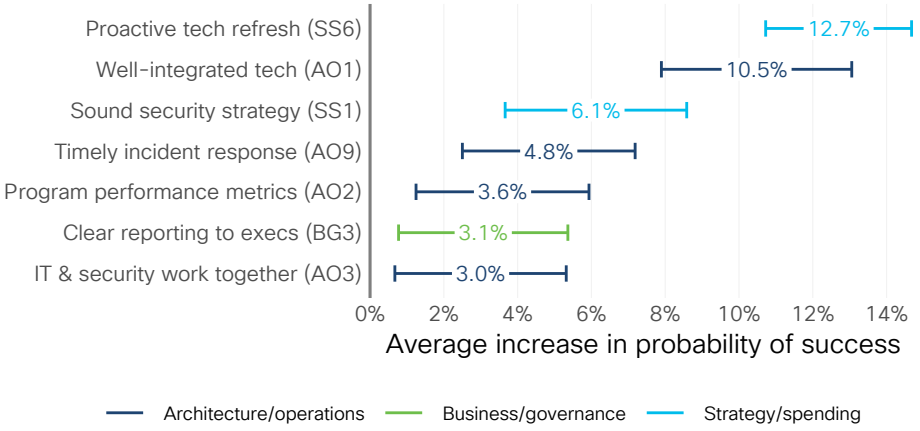
For all you nerds out there, we also go a step further. As you might remember, the regression coefficients for factors in a logistic regression don't quite directly translate to a change in probability. But with a handy little technique called "Average Marginal Effects" we can figure out how much an organization might gain from each factor. The well-known adage "correlation isn't causation" still applies, but this approach effectively spotlights potentially useful practice-outcome associations to consider.

Overall Program Success

Let's start by isolating the 'overall program success' outcome because it encompasses all others. Figure 3 lists factors from top to bottom based on their strength of correlation with the respondent claiming to have a highly successful security program overall. The bars and values indicate the expected increase in probability of overall program success associated with each practice. Because of statistical variation, that increase is expressed as a range of probability. The middle value marks the average (and most likely) increase in the likelihood of program success.

According to these results, organizations wanting to maximize the overall success of their security program should ideally start with a modern, well-integrated tech stack. Most respondents who said their firm's tech refresh strategy emphasizes proactive refreshes using best-of-breed IT and security technologies are 11% to 15% more likely to report successful programs (12.7% on average). Conversely, those who indicated that their firms rarely upgrade infrastructure or only do so when things break showed significantly reduced rates of success. Ensuring that technologies work well together as an integrated defense increases overall success by an average of about 11%.[1]

Figure 3: Practices most strongly correlated with overall security program success



Source: Cisco 2021 Security Outcomes Study

Figure 3 shows the change in probability of overall program success as a range. Read it like this: "A proactive tech refresh strategy increases the chance of reporting a successful security program by roughly 11% to 15%, with an average of 12.7%." Every chart like this can be interpreted in the same fashion.

We fully realize this finding seems suspiciously convenient for a company offering technologies fitting this description, so we'll take this opportunity to reiterate that a professional survey company (YouGov) conducted this survey, participants didn't know Cisco was involved, and an independent research firm (Cyentia Institute) analyzed the data. We're pleased these results validate Cisco's strategy and solutions portfolio, but we played no part in deriving them.

[1]It should be noted that the probabilities associated with practice-outcome combinations cannot be added together. So, we cannot say that proactive tech refreshes AND well-integrated tech up the success rate by 23.2% (12.7% + 10.5%).

We realize that a proactive tech refresh strategy isn't always that easy for some organizations. Some don't have the budget; some need to focus their resources and efforts elsewhere for various legitimate reasons. The good news is that these results DO NOT relegate such organizations to certain failure. It simply means they need to identify alternate success factors that work for their situation. That's exactly what we hope this analysis helps them do.

After all, having a sufficient security budget was one of the factors we tested, but it did not significantly correlate with overall program success. So good security isn't just about the money. Moving beyond the top two factors in Figure 3, it's great to see measurable benefits tied to having a sound security strategy. That's something organizations of all types and sizes can develop. Everything else flows from it.

It's often said that what makes great leaders is the way they respond to a crisis. Figure 3 says that's a big part of what makes a great security program too. A timely incident response requires thorough preparation, smart tools, and tested processes. If you need some justification to improve those capabilities, this chart should help.

The next two success factors go hand-in-hand. Using performance metrics to drive operations, and then clearly reporting that information to executive leadership, contributes significantly to program success. This is the core of the OODA loop, and it works.

And that brings us to the last of the success factors — IT, development, and security teams working together. No, we don't mean some kind of corporate retreat trust fall exercise while "Imagine" plays in the background. This factor points to the fact that you can't do security well if you can't do IT and development well (and vice versa). And if that's true, doesn't it make sense to communicate and collaborate so everyone's more successful? Figure 3 shows there's a benefit to forging strong alliances across the organizational aisle.

One final thing to note is that the top overall success factors span all categories – operations, governance, and strategy. This suggests that a great security program can't be built solely upon great governance or great strategy or great operations. A winning program requires all of these elements, and the more you do, the better you do. That theme will continue to reveal itself throughout the next few sections as we explore success factors for each of the 11 program-level outcomes.

What appears to be a strong correlation between continually upgrading your tech and program success may spell bad news for organizations that use technology like furniture – meaning it sticks around until it breaks. This indicates that "newer is better" isn't just a lifestyle choice spawned from Silicon Valley.

Read more about this in the Cisco Security Bottom Line Report

NIST CSF Functions

Beyond adherence to specific practices, we also asked respondents about where their security programs place the greatest priority in terms of investment, resources, and effort. We used the high-level security functions defined in the NIST Cybersecurity Framework (CSF) for this.

While the CSF's Protect function isn't at the bottom for every outcome, it ranks next to last for contributing to the overall success of the security program (Identify ranks #1). That's certainly counterintuitive, but we don't see this as suggesting protection isn't important. Rather, it indicates that the best programs invest in a well-rounded set of defenses to identify, protect, detect, respond, and recover from cyber threats. The field has long been protection-heavy; this says that protection alone is not the most effective strategy.

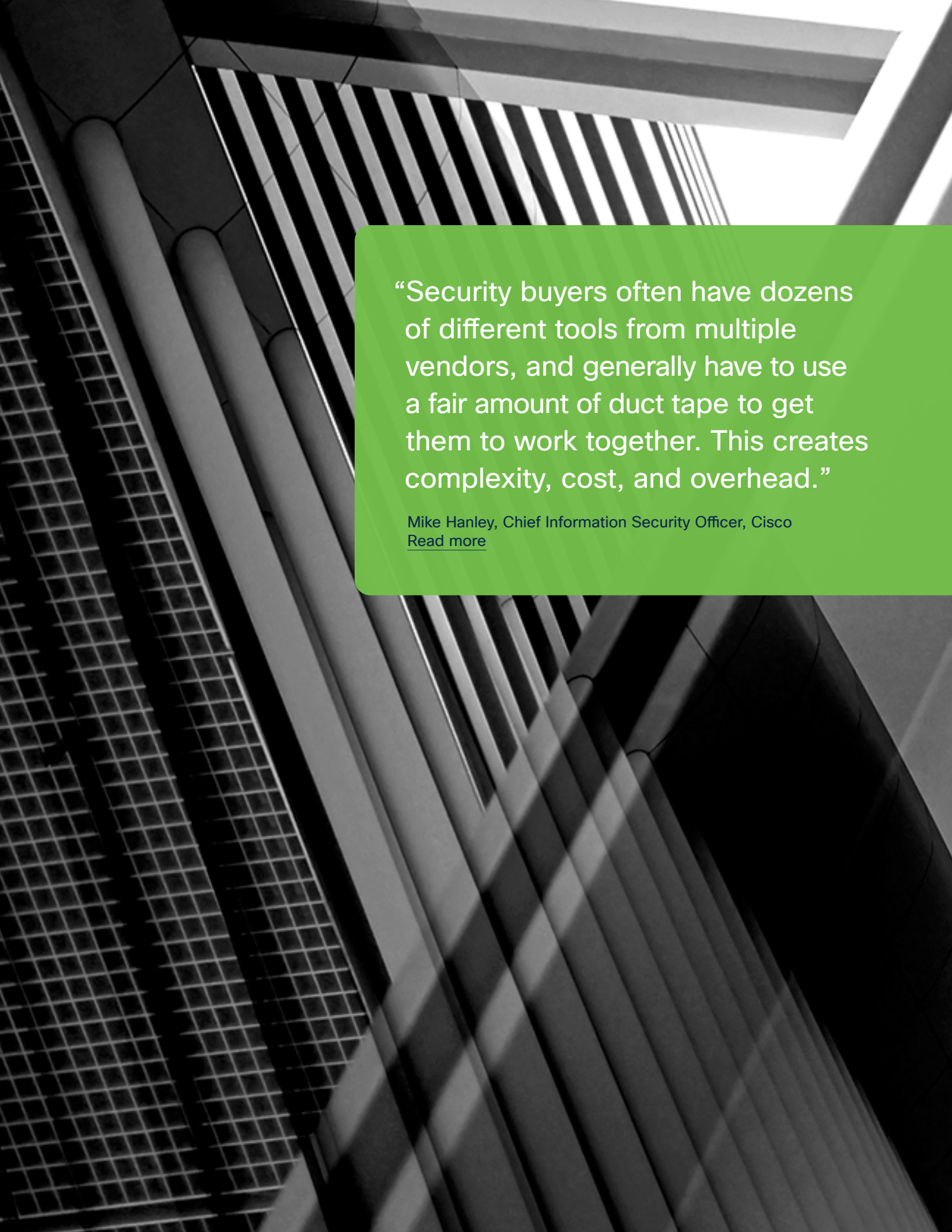
Check out our #SecurityOutcomes blog series to see how all five NIST CSF functions contribute to program outcomes.

Meeting Security Objectives

Having a security program that is successful overall is a worthy goal, but it's also perfectly reasonable (and often necessary) to pursue specific outcomes. Perhaps you looked at the list of outcomes in Table 1 and thought, "I wonder what factors would help us achieve [x outcome]?" If so, this section is for you.

Outcomes are organized into the three categories of: Enabling the Business, Managing Risk, and Operating Efficiently. Under those headings, we provide several security practices that correlate most strongly with respondents asserting their programs are successfully achieving each objective. Those wanting the full list of success factors for any given outcome should sit tight for just a bit; we have something special for you later in the report.

The four practices of Proactive tech refresh (SS6), Well-integrated tech (AO1), Timely incident response (AO9), and Prompt disaster recovery (AO10) significantly contribute to nearly every outcome. Thus, they're very common across all charts in this section. As a way of diversifying insights, we generally focus observations on the top five practices for each outcome besides those four. Please do not take that as us de-emphasizing their importance. There's a strong case that they're THE most important success factors in this study.



"Security buyers often have dozens of different tools from multiple vendors, and generally have to use a fair amount of duct tape to get them to work together. This creates complexity, cost, and overhead."

Mike Hanley, Chief Information Security Officer, Cisco
Read more

Enabling Business

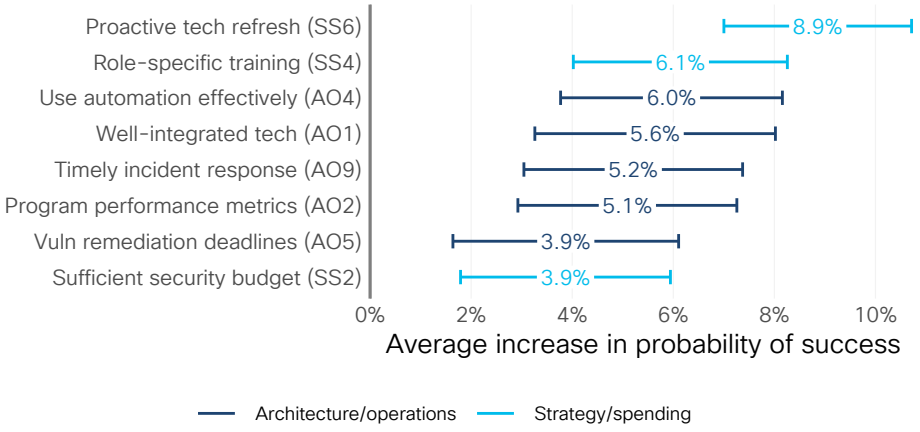
As the label implies, outcomes in this section focus on the security program's mission of supporting and fostering business activities. This category recognizes that security doesn't exist for security's sake; it serves the business. Let's see if we can find tips on how to accomplish that.

Keeping up with the demands and growth of the business

Frequently upgrading to the best available technologies and integrating them to work well together both feature prominently again in Figure 4. Since we've already discussed those practices quite a bit, we'll simply note that this finding makes a lot of sense to us. The whole notion of 'keeping up with the business' means that security must move, change, and adapt along with revenue-generating activities. Anyone who's tried to teach old tech new tricks knows that it's nearly impossible. Outdated, fragmented infrastructure hinders the business, period.

The strong link between role-specific security training and enabling the business is music to our ears. In fact, we made it into a maxim: "Adept people, agile program." Some might argue that this is one of the most fundamental themes in modern security programs. Effective training must be of high quality, consistent with the culture of the business, and tailored for specific audiences.

Figure 4: Top security success factors for keeping up with the business (EB1)



Source: Cisco 2021 Security Outcomes Study

The inclusion of automation in Figure 4 also makes sense to us. Automation helps the security program keep up with the business by eliminating bottlenecks and raising agility across people, processes, and technology. The emphasis on tech modernization, automation, and integration in Figure 4 starts to take on a distinctly DevSecOps appeal.

It may seem odd at first to see incident response (IR) listed as a top business enabler. But IR isn't just about putting out fires and cleaning up the mess. It's ultimately about handling unexpected events with minimal impact to the business. And in that light, it makes perfect sense that it makes the cut in Figure 4.

Ostensibly, a metrics-driven security program is one that's used to adjust course in response to changing conditions. We suspect that's why performance metrics make the list for helping security keep pace with the business. There's no sense in moving quickly if you're not sure where you are or where you're going.

It's no surprise that having a sufficient budget helps the security program keep up with the business. This is worth remembering, especially if your business model involves moving fast and evolving quickly. Proper investments in security show promise for aiding that momentum.

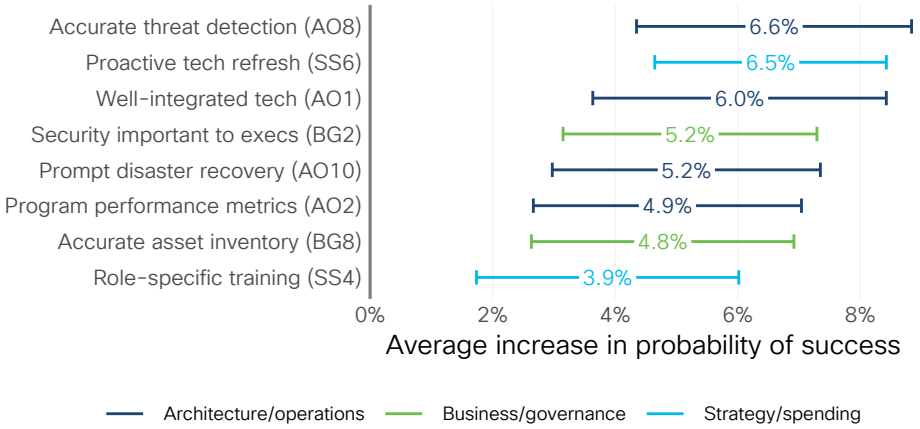
Find out here how Cisco's own CISO is helping to drive the business through security.

Gaining the confidence and trust of executive leadership

Score another point for modern, integrated tech. We can't help but think of executive SOC visits here (and have a sudden urge to clean our desk and look busy), but at least there's some evidence that the "tech tour" song and dance really does work!

Many C-Suite executives view cybersecurity as insurance against landing their company in the headlines for a major breach or business interruption. Those fears may be why accurate threat detection and prompt disaster recovery rise high among factors that correlate with gaining executive confidence. Being able to demonstrate strong visibility and resilience communicates "we got this" to leadership.

Figure 5: Top security success factors for gaining executive confidence (EB2)



Source: Cisco 2021 Security Outcomes Study

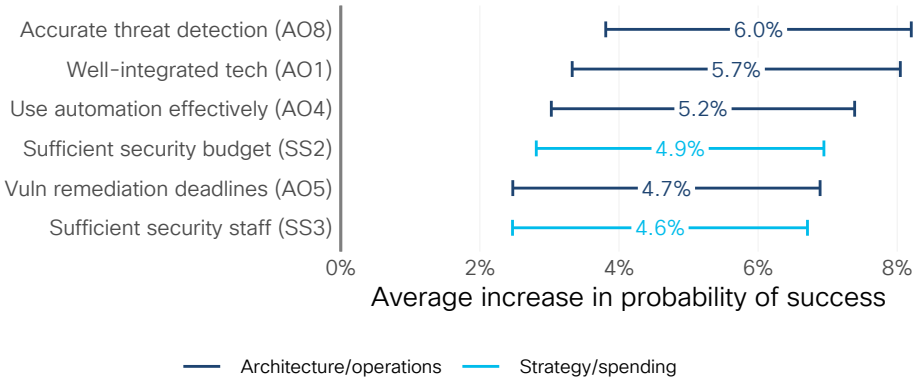
Having an accurate asset inventory, program performance metrics, and role-specific training seem to continue the theme of assuaging executives' fears. Demonstrating that the security team knows where the crown jewels are located, has the skills to defend them, and tracks credible metrics to back up the "we got this" message goes a long way toward earning trust at the top.

Security being important to execs and gaining their confidence seems rather tautological. This is probably a good example of the "correlation isn't causation" adage. If security is important to them, they're likely supporting the program sufficiently and invested in its success.

Obtaining buy-in from peers and other organizational units

Several of the top success factors in Figure 6 we've seen and discussed before. But it's still helpful to see that good security operations (namely detection, integration, and automation) help earn respect and participation from other teams/divisions. You could even argue that they're dependent upon those other teams. These practices reduce friction, increase flexibility, and generally help the security program shed its stigma as the "Department of No".

Figure 6: Top security success factors for obtaining peer buy-in (EB3)



Source: Cisco 2021 Security Outcomes Study

Speaking of stigmas, it's not uncommon that security-related spending hits the budgets of IT and development organizations (sometimes harder than they'd like). This may be why giving the security program a sufficient budget of its own helps with peer buy-in. That same idea is likely why having adequate security staff makes the list. "Oh, I don't have to pay for it or take my people away from what they're doing? Then sure, we'll participate – thanks!"

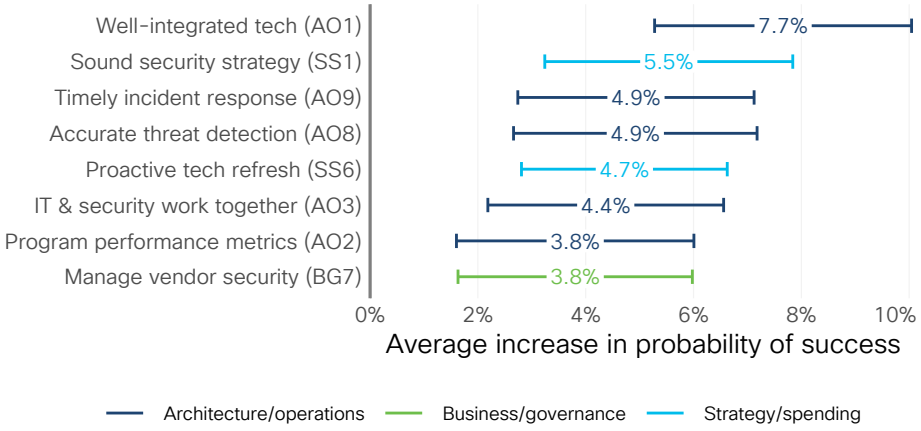
Vulnerability remediation is a concrete example of the dynamic described in the previous paragraph. It's rarely done without collaboration between IT and security teams. Security often finds the bugs, while IT squashes them. It's easy to see why coordinating who's doing what engenders better cooperation among interdepartmental peers.

Creating a security culture embraced by all employees

How do you create a security culture that's actually embraced rather than eschewed by employees? Figure 7 places the following at the top of the list: giving them good tech that meets their needs, a clear sense of direction, and timely fixes when things break (or keeping them from breaking in the first place). It's hard to argue with that message.

Culture doesn't simply mean training, especially the annual online awareness kind that everyone hates. And it certainly doesn't mean 'every time you violate a security policy, we'll punish you by making you go through that training again.' The strategy-culture correlation is worth calling out specifically. This is the only outcome in the 'Enabling the Business' category for which having a sound security strategy significantly increases the probability of success. That may seem odd, but consider that many a frustrated employee has asked something to the effect of "why do we have to go through all of this?" in response to new security policies. A good strategy eases that frustration by getting everyone on the same page.

Figure 7: Top success factors for creating a strong security culture (EB4)



Source: Cisco 2021 Security Outcomes Study

We saw earlier that IT, development, and security teams working together contributes to overall program success, and it's no surprise to see that it benefits culture as well. You can't just impose security on the organization; it must be built into the fabric of the infrastructure and organization itself to really make a difference. Good collaboration among technical teams is essential to that goal.

The inclusion of 'manage vendor security' in Figure 7 gave us pause. The full text of that question, however, offers some insight: "I'm confident that the security practices of vendors in my organization's value/supply chain are in line with our standards OR that we manage them accordingly." We don't think it's reading too far between the lines to infer that firms extending security across their entire supply chain are more likely to have it permeate their culture too.

cisco SECURE

Security Stories

Cisco interviewed Masha Sedova, co-founder of Elevate Security, in our Security Stories podcast.

Listen to this energizing episode and learn how to achieve people-powered security by using data and analytics to invoke cultural and behavioral change in a company's approach towards cybersecurity.

Visit cisco.com/go/securitystories.

Managing Risk

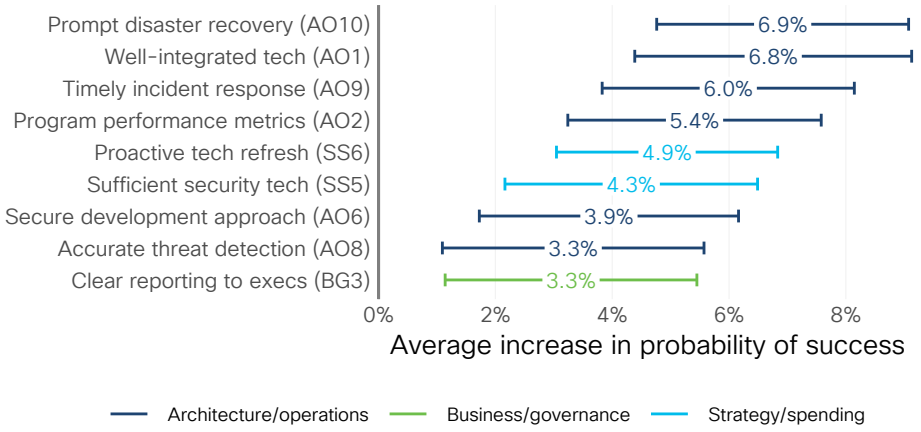
Managing risk is what most people think of when asked about the security program's primary responsibility. Of course, risk is multi-faceted, which is why we chose to examine three outcomes that each provide a distinct perspective on how the organization manages risk.

Managing the top cyber risks to the organization

There's a danger of reading too much into small details like the fact that prompt disaster recovery ranks above the tag team champions of refreshing and integrating tech in Figure 8. But it's possible the data sees something important here and wants to remind us that managing risk isn't just about keeping bad things from happening. It's equally important to minimize the impact when they inevitably do. And that's what prompt disaster recovery is all about.

This is one of only two outcomes for which having sufficient security tech and proactive refreshes both contribute significantly. We interpret that as the data doubling down on the message that the best tools in the best shape give the best chances of managing critical risks.

Figure 8: Leading security success factors for managing top risks (MR1)



Source: Cisco 2021 Security Outcomes Study

As long-time proponents of security metrics, we're glad to see that having a data-driven program improves the management of risk. The "you can't manage what you can't measure" quote is overused, but not without good reason. It holds true in so many domains, including cybersecurity.

We were genuinely surprised to see that this is the only outcome showing a strong correlation with a secure development approach for applications. But it makes sense since software flaws are inherent to so many cyber risks.

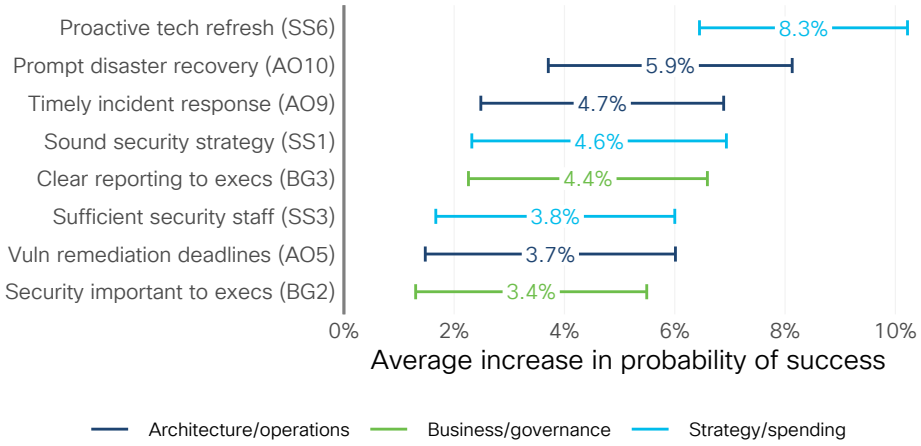
This is also the first time clear reporting to execs plays a role, so it seems fitting to touch on that. It's doubtful that just reporting on the activities and effectiveness of the security program to leadership effectively reduces exposure to critical risks. That said, it does imply some level of oversight and accountability, which may act as a forcing function for the security program to walk the talk. Of course, we could be seeing the equivalent of a Jedi mind trick: "Here are the assurances you're looking for; we can go about our business."

Meeting regulatory compliance requirements

Proactive tech refresh has become a permanent fixture in these charts, but its leading position for meeting compliance regulations is kind of a head scratcher. Do modern, best-of-breed solutions check a bunch of boxes or create a superb audit trail? We're not entirely sure, but it's certainly something to note.

Several practices in Figure 9 could be viewed as go-to evidence that the security program is covering its bases – creating a sound strategy, remediating vulnerabilities on time, responding quickly to incidents, and swiftly recovering from major events. Ticking off those boxes goes a long way in remaining compliant.

Figure 9: Top security success factors for meeting compliance regulations (MR2)



Source: Cisco 2021 Security Outcomes Study

Executives are keenly aware of legal and regulatory risks, which is why the topic is often front and center in board-level security reporting. In reference to the inclusion of "clear reporting to execs" in this chart, perhaps security leaders that can clearly communicate the status and effectiveness of the security program to executives can likely do so for regulators as well. Or perhaps those very executives are better able to communicate with regulators, thus helping with compliance.

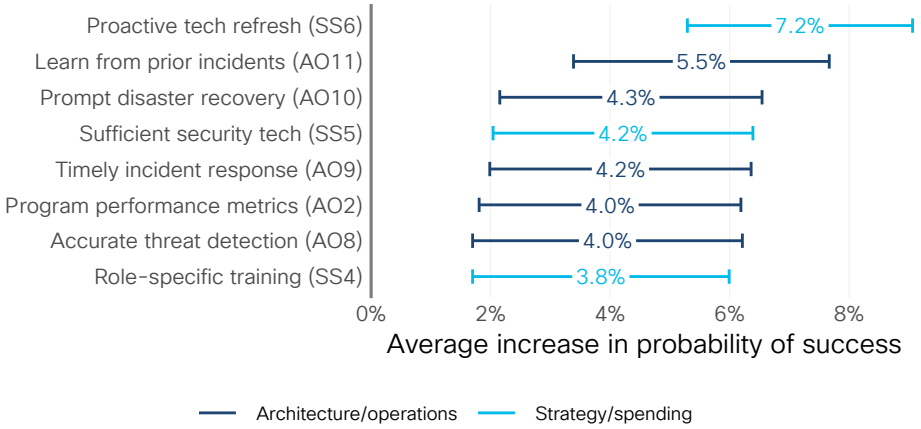
We haven't made it a practice of discussing practices that do NOT correlate with outcomes, but we just can't ignore this one. Having someone on staff who owns compliance was one of the factors we analyzed. But it didn't improve the chances of success for any outcome, including this one. Granted, just having a person with a compliance title isn't going to make the regulators happy...but still. If it should contribute to any objective, it should be this one.

Avoiding major security incidents and losses

To us, Figure 10 proclaims a clear "attackers are always innovating; we must also" message. The ability to avoid major cybersecurity incidents and losses appears strongly dependent on maintaining modern, highly effective IT and security infrastructure backed by nimble response and recovery capabilities.

One of the side benefits of a proactive refresh strategy is that tech stacks are being touched regularly and not being left undocumented and out of date. The history of major breaches is replete with examples of organizations that overlooked, lost track of, or otherwise weren't closely maintaining systems that allowed attackers to establish a foothold in their environment. Stagnant infrastructure makes it all too easy for bad actors to get comfy and stick around.

Figure 10: Top security success factors for avoiding major incidents (MR3)



Source: Cisco 2021 Security Outcomes Study

Speaking of breach history, Figure 10 says we shouldn't just be studying the big public incidents for clues on how to avoid them, but should also look at our own incidents (and near misses). A learning security culture that conducts after-action reviews of major incidents and carries those lessons forward is better positioned to address future events.

In addition to helping manage top cyber risks, it appears performance metrics also improve a security program's chances of dodging the breach bullet. Along with accurate threat detection, this combination provides holistic situational awareness. Knowing the adversaries' capabilities and activities as well as that of your own defenses helps level the asymmetric nature of the playing field.

Last but not least, role-specific training adds to the program's ability to avoid major incidents and losses. To put this in proper perspective, the data shows that training is about as effective as threat detection for minimizing the risk of breaches. Now, which one of those gets more funding in your organization? Training is one of those things often put forth as necessary for success, yet it's often one of the first things to go when budgets get tight. If you need evidence to convince your organizational leadership that it's in their best interest to invest in their people, it's in this chart.

Spotlight on Major Incidents and Losses

Having a major security incident or data loss doesn't mean the security program is failing (nor does a lack of them prove success), but it's certainly a top-of-mind metric for organizational leadership. We asked respondents who said their firms were struggling to avoid incidents to provide additional detail on those struggles. The most common types of security events reported were data breaches, ransomware, and service outages.

We were also interested in learning about the impacts of those events. Operational impacts were most common, which makes sense because major events force people (and systems) to stop their normal business activities in response to the incident. Regulatory action comes in next, along with brand damage, harmed business relationships, lost revenue, and legal actions. Get more detail on incidents and losses in the #SecurityOutcomes blog series.

Operating Efficiently

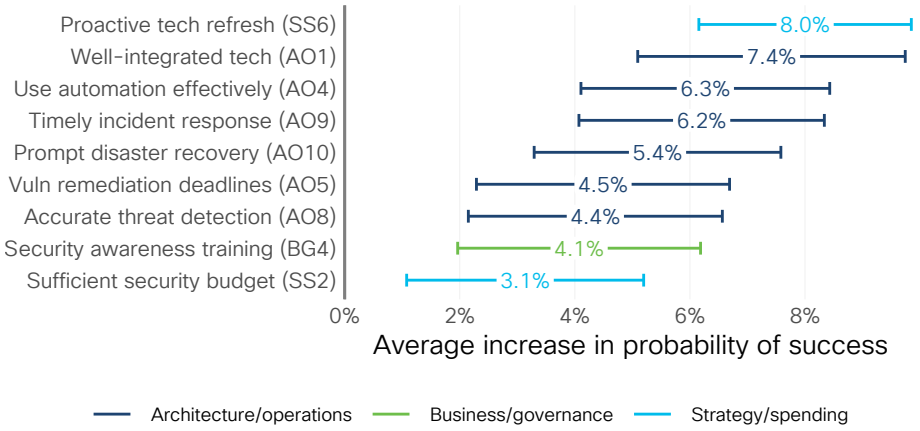
Beyond enabling the business and managing risk, the ability to operate efficiently often sets great security programs apart from the good ones. This last set of outcomes in our study addresses cost-effectiveness, executing strategy, talent management, and IR processes. Important stuff, right? Let's see what can give your program the edge.

Running a cost-effective security program

It initially seems counterintuitive that a proactive tech refresh strategy would contribute to maintaining a cost-effective security program. But as we've said before, this practice isn't just about making it rain security Benjamins. It's a strategy that ensures your team has the best tools to help them perform to the best of their ability. And the next two practices in Figure 11 – integration and automation – are difficult to achieve if your security tools are not kept up to date. The best tools are more effective, easier to manage, and therefore less costly over the long run.

We've also seen the next two practices in Figure 11 several times already. If you've ever gone through a major security incident, you know that an absurd amount of time and money can be spent during the response and recovery process. Ensuring those capabilities are primed and ready to fire when needed contains both the incident and associated costs.

Figure 11: Top success factors for running a cost-effective security program (OP1)



Source: Cisco 2021 Security Outcomes Study

Few tasks in security are more tedious than vulnerability management and triaging countless false-positives. It's not without reason that these two functions sit at the bottom of Figure 2 among the least well-implemented practices we examined. They're hard and consume a lot of resources. Thankfully, Figure 11 offers hope for the weary by showing that remediation deadlines and detection accuracy boost efficiency.

There's a Goldilocks zone for security budgets when it comes to this outcome. Too little, and you can't get everything done no matter how hard you try. Too big, and wastefulness tends to creep in. But when the budget is juuussst right, the program's capabilities fit the mission perfectly and operations run at maximum efficiency.

Overall, it appears that a cost-effective security program is easiest to achieve with well-designed architecture supported by efficient operations.

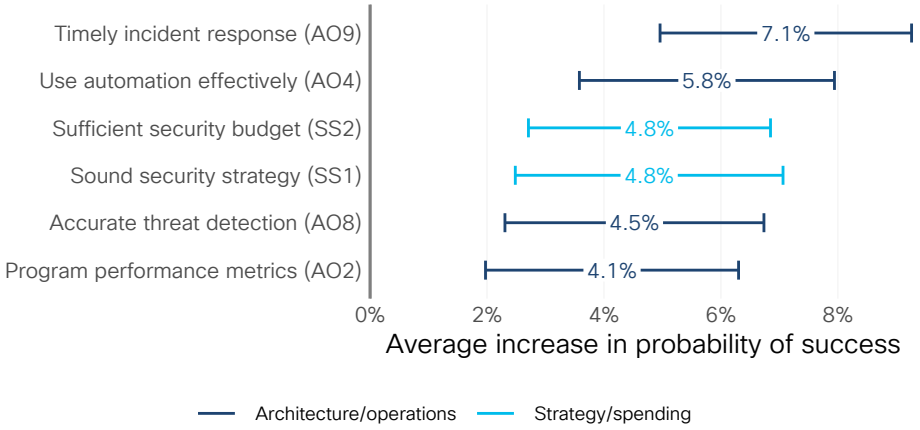
Minimizing unplanned work and wasted effort

This outcome is similar to running a cost-effective program, but is focused more on executing the strategy without major setbacks or deviations. It makes sense then that having a good strategy in the first place makes the top five practices correlated with this objective. Having a budget that's sufficient to enable that strategy helps a lot too.

Additional factors in the chart – timely response, effective automation, and accurate threat detection – offer a first-mover advantage in the day-to-day execution of that strategy. Poor threat detection and response are particularly prone to rabbit holes. As mentioned before, a disjointed incident response process and chasing down endless false-positives lead to wasted time, staff burnout, and a host of other value-diminishing effects. The primary purpose of security automation and orchestration is to counteract operational dead-ends and bottlenecks. It's good to have validation that it does indeed accomplish that purpose.

Also important for achieving this objective, performance metrics can force hard questions about the direction of the security program and provide instrumentation to determine when it's veering off course.

Figure 12: Top security success factors for minimizing wasted effort (OP2)



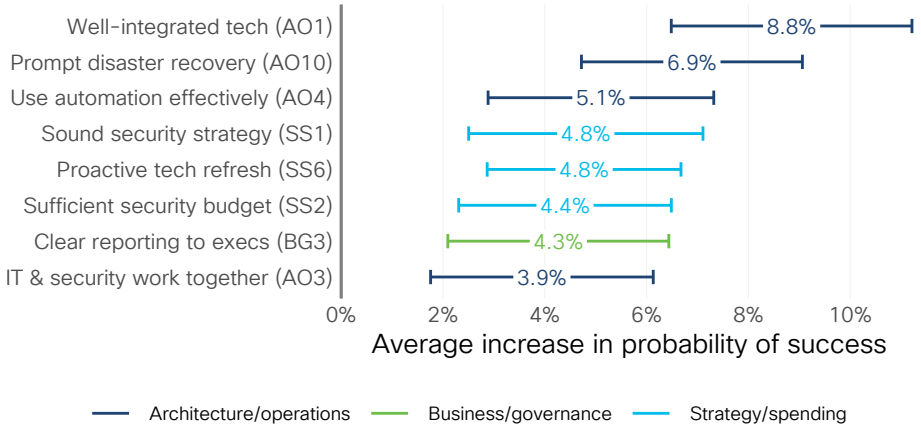
Source: Cisco 2021 Security Outcomes Study

Recruiting and retaining talented security personnel

There's a lot of talk in the industry about the difficulties of recruiting and retaining security staff. Here's a formula that might help: have the budget to hire top talent, develop a strategy that makes sense to them, surround them with good peers, and give them the tools they need to succeed. Diversity in your talent, and their backgrounds, skills, and opinions is essential to create a culture where your staff feels included, respected, and ready to grow their careers.

To be honest, the tech-heavy nature of the practices listed in Figure 13 caused us to do a double take. We expected to see a somewhat softer list of success factors. But as it often does, the data urged us to reconsider our presuppositions. After doing that, we concede that it makes good sense that architecture and operations play an important role in attracting and keeping top security staff. Absolutely no one enjoys wasting their time and talents overcoming bad tech.

Figure 13: Top success factors for retaining security talent (OP3)



Source: Cisco 2021 Security Outcomes Study

Regarding wasted time and talents, security automation is worth calling out here. Some position automation as a replacement for people, but those who know how to use it effectively understand that it relieves rather than replaces talent. Relieving staff from mundane tasks frees them up for more challenging, enjoyable, and valuable work. And these results indicate that security professionals appreciate that.

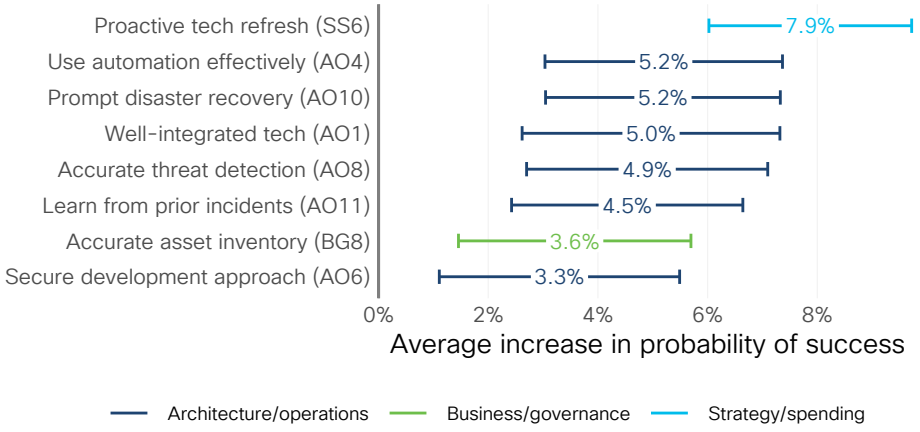
IT and security teams working together is another factor that deserves mention. A culture of collaboration isn't easy to build, but it's worth it for so many reasons. Figure 13 adds talent retention to that stack of justifications.

> There's more than one path into cybersecurity. In this eBook, Diversity in Cybersecurity: A Mosaic of Career Possibilities, we interviewed notable cybersecurity professionals to find out how they got their start, and ask what tips they would share with their younger selves.

Streamlining incident detection and response

This final outcome is more tactical than many of the others and, at least as far as the label goes, overlaps with the 'timely incident response' practice. Reviewing the description and example evidence for this objective in Appendix B, however, clarifies that streamlined IR can be an end as well as a means. And as prominently as IR, threat detection, and other core SecOps practices factor into the outcomes presented in this section, it's reasonable to wonder how we can improve those capabilities.

Figure 14: Top security success factors for streamlining IR processes (OP4)



Source: Cisco 2021 Security Outcomes Study

Part of the answer is the same one that's been reinforced so often in this study: modern, well-tuned security architecture supported by mature operations. We're ready to call that table stakes by this point. We're more interested in what ups the ante for a winning hand, as revealed by the last three factors in Figure 14. We've seen the value of learning from prior incidents once before (for avoiding major incidents and losses), and it's good to see it pop up again here. While it seems obvious, you'd be surprised how many IR teams don't take the time to really do this. This is also only the second outcome for which having an accurate asset inventory serves as a key success factor. Having heard "we didn't even know that (compromised) server was still around" and "we're not sure where that application lives" a time or two, this correlation makes perfect sense. It's hard to respond well when you don't know where assets sit, who owns them, how they're configured, etc.

Streamlining IR processes isn't what typically comes to mind when seeking to justify adoption of a secure development lifecycle. But this practice implies better integration between security and development teams/processes through DevSecOps. This, in turn, leads to more robust and resilient applications, better shared understanding of the attack surface, and greater awareness of flaws and how to address them when issues arise.

Curtailing the impact of COVID-19

We asked participants about how the COVID-19 pandemic impacted their organizations, which could be viewed as another outcome in the 'Operating Efficiently' grouping. Firms that were most successful in minimizing the impact of COVID-19 on their operations and cyber risk posture had the following characteristics:

1. They had a proactive tech refresh strategy emphasizing frequent upgrades to best-of-breed IT and security technologies.
2. They had adequate security staffing levels and invested in their people through role-based training programs.
3. They kept top executives informed through clear reporting on the activities and effectiveness of the security program.

We interpret these results to suggest that an organization's ability to maintain resiliency through unexpected events like the COVID-19 pandemic is strongly dependent upon a modern, high-performance tech stack maintained by capable personnel with strong accountability from organizational leadership. See what else we discovered about this important topic in the #SecurityOutcomes blog series.

"As a crisis, COVID-19 has undoubtedly created additional security threats as the workforce spends more time working in unusual circumstances. We needed to do three major things: equip staff and students with the appropriate work tools, overlay sensible security measures, and train the workforce on the threats and then message those threats again and again. Engagement was key – a gentle 'drip, drip' of solid and sensible advice to keep their homes cyber-safe."

Mick Jenkins, CISO of Brunel University London

A Roadmap for Success

Earlier in this study, we urged those wanting to see beyond the top success factors to hold that thought and we'd circle back to it. Here's where we make good on that promise. Figure 15 displays all security practices discussed in this report along the bottom and all program-level outcomes on the left side. See the Appendix for the full question text for both practices and outcomes.

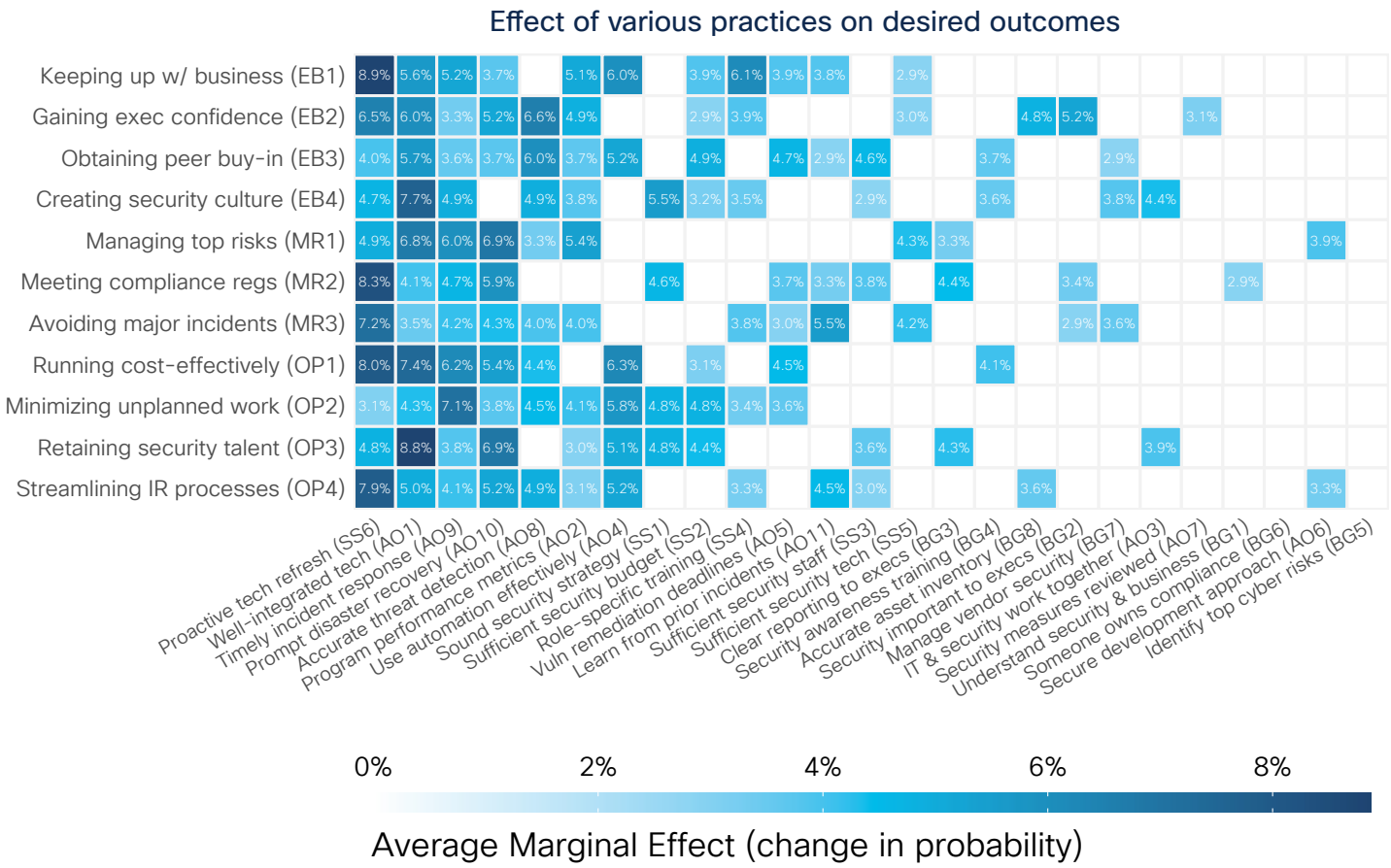
Colored squares indicate a statistically significant positive correlation between the intersecting practice and outcome (white squares mean no correlation). The intensity of shading indicates the average increase in probability of success for each practice-to-outcome combination. The values underlying the shading correspond to those shown in the preceding charts.

Rather than include a bunch of recommendations from us, we thought we'd conclude the report the same way we started it – by letting the data speak for itself. We designed this chart to help you visualize the big picture and begin to build an evidence-based roadmap to a more successful security program. It's the ultimate Choose Your Own Security Adventure.

Here's a couple tips for planning that journey:

- Focus on individual rows if you'd like to identify practices that the data suggests can help your program achieve particular outcomes.
- Focus on individual columns if you'd like to see the potential benefits to your program (outcomes) associated with a particular practice.
- Note that some practices have a broad influence on many outcomes, while others offer more narrow or specific benefits.

Figure 15: All security practices correlated with each security program outcome



Source: Cisco 2021 Security Outcomes Study

Blank squares in Figure 15 don't necessarily mean the practice in question is useless for achieving outcomes. It just means that, on average across all respondents, the effects weren't statistically significant. Segmenting the data by industry, region, or organizational size changes the effects substantially. In other words, your mileage may vary. If you're interested in some of those views, you can find additional insights in the regional and vertical reports at cisco.com/go/SecurityOutcomes

Thank you for investing your valuable time in reading this Security Outcomes Study. There's no shortage of security industry reports out there vying for your attention, and we hope this one provided some actionable, data-driven insights to help you build a more successful security program. Let us know if we can support you in any other way in that noble pursuit and join us in the conversation using #SecurityOutcomes on social platforms.

About Cisco Secure

Cisco has long established itself as the networking leader, 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 B2B 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, easy to manage, and easy to 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 protect what's now and what's next with the most comprehensive, integrated cybersecurity platform on the planet. Learn more about how we simplify experiences, accelerate success, and protect futures at cisco.com/go/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

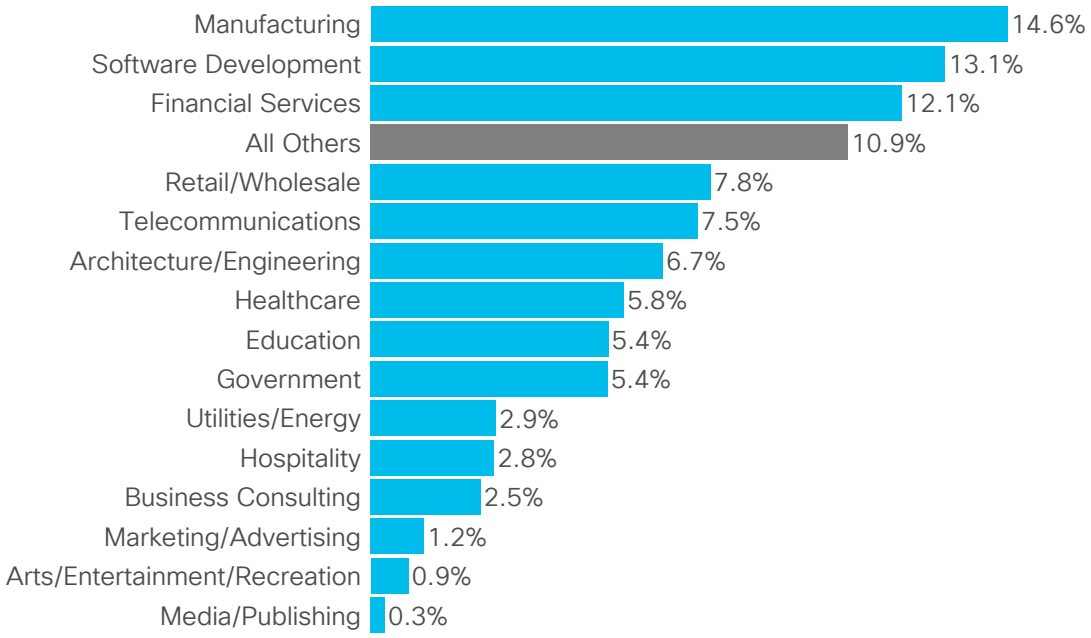
Published December 2020 RPT_12_2020

cisco SECURE

Appendices

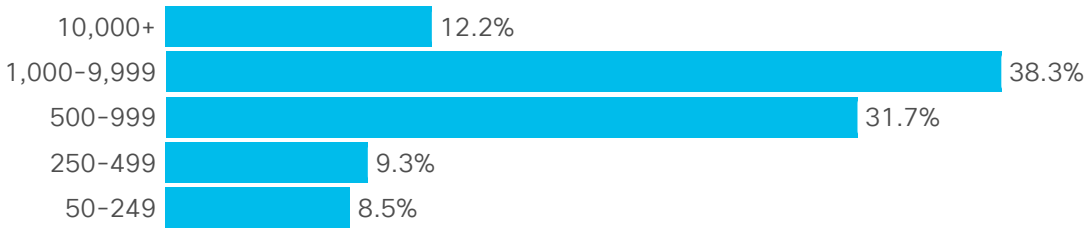
Appendix A: Sample Demographics

Industries represented:



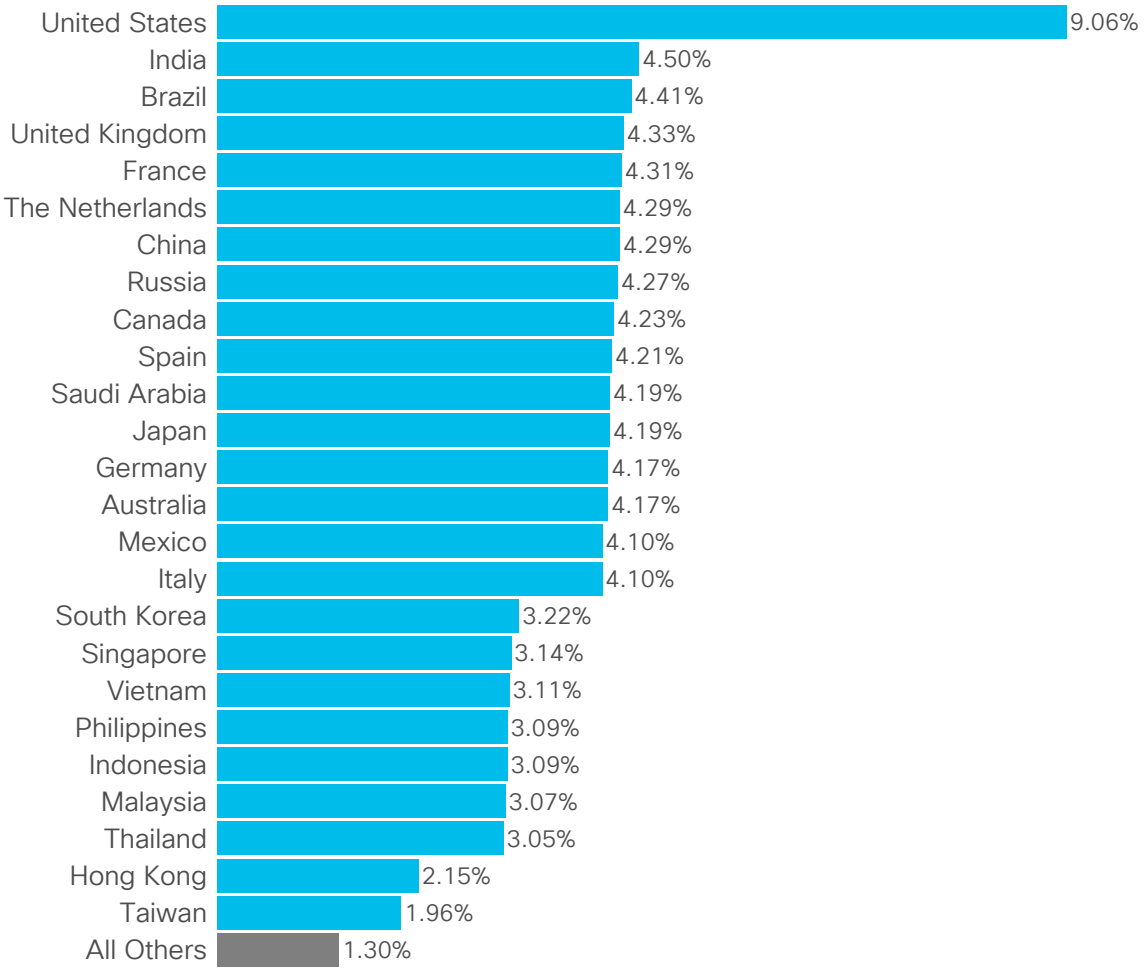
Source: Cisco 2021 Security Outcomes Study

Company sizes represented (number of employees):



Source: Cisco 2021 Security Outcomes Study

Countries represented:



Source: Cisco 2021 Security Outcomes Study

Appendix B: Full Listing of Security Outcomes

Enabling Business	
EB1	Keeping up with the demands and growth of the business
	Example and Evidence of Success: The security program responds well to changing business needs and doesn't impede new lines of revenue. In some cases, security may provide competitive advantage or even be a net revenue generator. If security is viewed purely as a cost center or the "Department of 'No!'" by business execs, it's a sign of struggling to meet this goal.
EB2	Gaining the confidence and trust of executive leadership
	Example and Evidence of Success: Security leaders meet regularly – and favorably – with top executives and the Board of Directors. The relationship between business and security leaders is one of mutual respect and collaboration. If security is often in the hot seat with executives or regularly denied reasonable requests for support, it's a sign of struggling to meet this goal.
EB3	Obtaining buy-in from peers and other organizational units
	Example and Evidence of Success: Security enlists other divisions in building a cooperative defense of the organization. Communication and collaboration is strong with a fair sense of "give and take" for the greater good. Non-security leaders or divisions may have security-related performance measures. A culture of inter-departmental complaints and contention is a sign of struggling to meet this goal.
EB4	Creating a security culture embraced by all employees
	Example and Evidence of Success: Employees are treated as part of the security solution rather than the problem. Security isn't a negative theme in employee satisfaction surveys or exit interviews. Non-security staff regularly report phishing attempts, potential malware, and other incidents. Frequent security policy violations and workarounds are a sign of struggling to meet this goal.
Managing Risk	
MR1	Managing the top cyber risks to the organization
	Example and Evidence of Success: Top risk scenarios have been agreed upon by executives and security leaders and mitigation plans exist for those risks (or they've been accepted). Potential cyber risk exposure is currently within the risk appetite established by leadership. There's no evidence that risk management capabilities are failing (e.g., frequent near misses, control deviations, response/recovery testing failures, etc.).
MR2	Meeting regulatory compliance requirements
	Example and Evidence of Success: There's an absence of avoidable security findings from auditors and regulators. The organization is diligently tracking and addressing changing regulatory requirements. There's evidence that the organization understands what's required, acknowledges any findings and deficiencies, and is spending/working to mitigate them.
MR3	Avoiding major security incidents and losses
	Example and Evidence of Success: We expect that an organization that's highly successful in achieving this goal has not had a major security incident (of high internal and/or external visibility) in the last couple years. Furthermore, there's no reason to suspect that it's merely a matter of time until a major data loss event occurs. Minor and even moderate incidents are expected, but the question here is whether the organization has and will continue to stay out of the headlines.

Operating Efficiently	
OP1	Running a cost-effective security program
	Example and Evidence of Success: Executive leaders view the security program as having a good return on investment (ROI). There are no recurring rumblings about the overly high costs of security. There's a low rate of shelfware purchases. Staffing is lean but sufficient. A plan among executives and security leaders to reduce the security budget without increasing risk would be a good sign of success here.
OP2	Minimizing unplanned work and wasted effort
	Example and Evidence of Success: Strategy execution proceeds without frequent setbacks and deviations. Security budget is spent proactively rather than reactively. Employees spend their time on higher-level, more valuable tasks rather than being mired in the mundane. Constant firefighting mode or a program that "can't get out of its own way" is a sign of struggling to meet this goal.
OP3	Recruiting and retaining talented security personnel
	Example and Evidence of Success: The organization has a positive reputation in the security community as being a good place to work. Open security positions are generally filled quickly and without undue incentives. Talented staff move up instead of move out and attrition rates remain low. Employee satisfaction is consistently high.
OP4	Streamlining incident detection and response processes
	Example and Evidence of Success: There's a general sense that security operations run efficiently. Triaging security events isn't a guessing game and doesn't take forever. Responding to and remediating incidents is well-organized rather than chaotic. Metrics like time-to-detection and time-to-remediation are tracked and are trending down over time.

Appendix C: Full Listing of Security Practices

Business and Governance	
BG1	I have a clear understanding of how the security initiatives I'm involved in support my organization's business needs and objectives
BG2	I have good reason to believe that my organization's top executives view security as important to business objectives
BG3	My organization's top executives receive clear reporting on the activities and effectiveness of the security program
BG4	All employees in my organization receive effective security awareness education on threats, policies, and procedures relevant to their duties
BG5	I know what my organization considers to be our top cyber risks and believe that we've accurately assessed those risks
BG6	Someone in my organization is responsible for managing security and privacy compliance requirements
BG7	I'm confident that the security practices of vendors in my organization's value/supply chain are in line with our standards OR that we manage them accordingly
BG8	My organization maintains an accurate inventory of key systems and data and classifies those assets based on their security requirements and business criticality
Strategy and Spending	
SS1	Our security program maintains and communicates a sound overall strategy to successfully achieve its mission
SS2	Our security program has the financial budget needed to successfully achieve its mission
SS3	Our security program has the personnel needed to successfully achieve its mission
SS4	Our security personnel receive the role-specific training needed to successfully perform their duties
SS5	Our security program has the technology and tools needed to successfully achieve its mission
SS6	My organization has a proactive tech refresh strategy of frequent upgrades to best available IT and security technologies
Architecture and Operations	
AO1	Our security technologies are well integrated and work effectively together
AO2	Our security program uses performance metrics to drive operational decisions and actions
AO3	My organization's IT, development, and security operations personnel work effectively together
AO4	We use automation effectively to improve the efficiency of security operations and personnel
AO5	My organization meets established SLAs or deadlines for remediating disclosed vulnerabilities in systems and software
AO6	My organization takes a rigorous approach to developing and continually maintaining the security of our internal applications
AO7	Our security measures are actively monitored and regularly reviewed to verify and maintain their effectiveness
AO8	Our threat detection capabilities provide accurate awareness of potential security events without significant blind spots
AO9	Our incident response capabilities enable timely and effective investigation and remediation of security events
AO10	Our recovery capabilities minimize impact and ensure prompt restoration of assets affected by security incidents
AO11	We make a special effort to identify lessons learned from responding to incidents and use them to improve security measures for future events

CISCO

SECURE

The bridge to possible