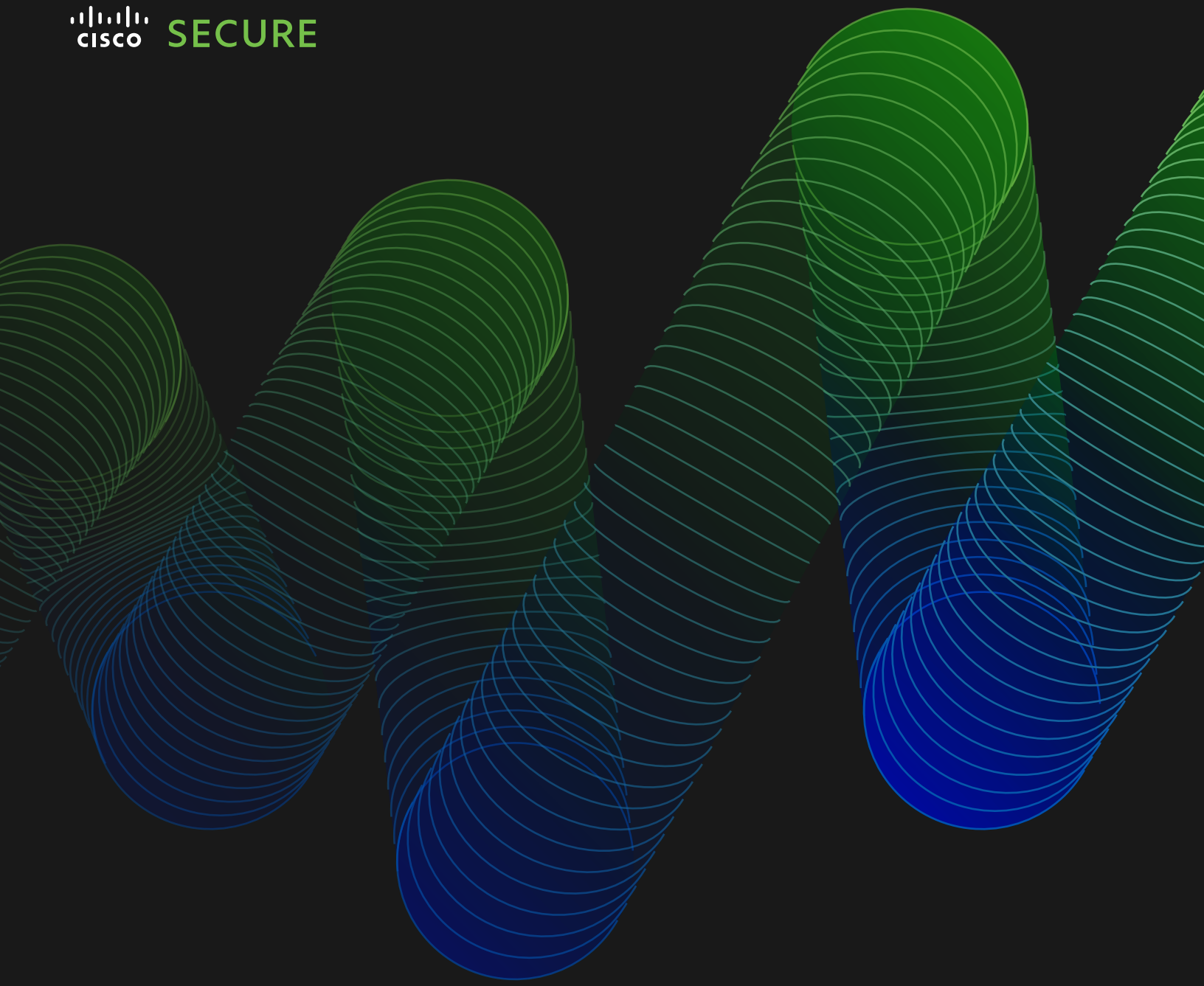
cisco SECURE



Security Outcomes Report

Volume 3

Achieving Security Resilience

Contents

Foreword

When you think of the word **resilience**, what comes to mind? I bet you're thinking of someone or something who has suffered (to quote the Great Bard) the "slings and arrows of outrageous fortune" but has the fortitude and audacity to become even stronger.

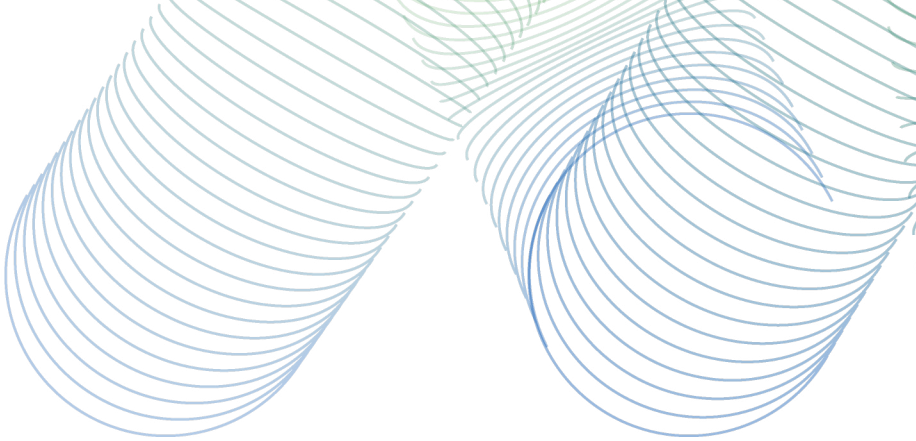
That's a perfectly acceptable definition and I applaud the spirit of it. But when you are talking about securing companies large and small, merely being resilient enough to bounce back after being down may not be good enough. After all, successful cybersecurity breaches like ransomware or intellectual property theft can do outsized harm to companies, their employees, partners, and even their customers. In the 2021 Security Outcomes Report, 41 percent of the companies we surveyed said that they suffered a major security incident or loss within the last two years, showing how wide this problem has become.

Cisco defines security resilience as being able to protect the integrity of every aspect of your business so it can withstand, not just survive, unpredictable threats or changes and emerge stronger. As you will learn in this third volume of our Security Outcomes Report, there is near unanimous agreement among the executives we surveyed that achieving security resilience is critical to their business. And it's no wonder as more businesses are interconnected today, a breach on anyone in the value chain can have a dramatic ripple effect on the others. **No executive wants to be known as the one not having done enough.**

So, please use and enjoy this report. I hope you find it useful in developing your strategies and solutions for achieving your measure of security resilience. Resilient to threats. Resilient to change. Resilient to the unknown. The security industry is certainly not lacking in buzzwords. However, I have a feeling that the word resilient is going to stick around for a while. Maybe not as long as a great Shakespeare play like *Hamlet* but long enough.

– **Shailaja Shankar**
SVP & GM, Cisco Secure

Source: Cisco '2021 Security Outcomes Report: Endpoint Edition'



"Although the world is full of suffering, it is also full of the overcoming of it."

– Helen Keller

Introduction

Security is never an easy job. But the past few years have really upped the ante when it comes to protecting a business from cyber incidents. Today's security defenders not only have to consider increasing threats and an expanding attack surface, but also bigger picture risks such as warfare, climate change, financial instability, and of course, a global pandemic.

In this tumultuous environment, the concept of resilience has risen to the top of most corporate agendas. **How can a company quickly adapt to these rapid, disruptive changes and emerge stronger?**

In this third volume of the Security Outcomes Report, we break security resilience down into digestible and actionable insights. (Because we're sure you have enough on your plate without having to crack the code to resilience on your own.) No one report can cover all there is to know about such a colossal subject matter; but we've surfaced some highlights for you to consider when building and refining your cybersecurity strategy for the road ahead.

Using the data gathered from over 4,700 security professionals across 26 countries, we uncovered **seven success factors** that can boost cyber resilience. The report also analyzes exactly what security resilience means, why it's important, and how businesses are ranking their own resilience.

We hope this data serves as a resource and provides you with more confidence as you set your organization up to thrive no matter what comes next.

Between risk and resilience, there's a bridge. We know the journey can be arduous at times, and we're here to help.

Key findings

Security resilience is top of mind among executives; **96%** of them consider it **highly important** to their business.

Nearly **2/3** of organizations report **experiencing major security incidents** that jeopardized business operations.

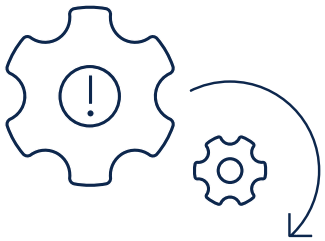
Culture matters.

Organizations that foster a culture of security see a 46% increase in resilience.

Architecture matters.

Organizations with mature zero trust, XDR and SASE implementations all boast significantly higher resilience scores.

TOP PRIORITIES



Preventing incidents and **mitigating losses** are the top two priorities for security resilience overall.

Retaining security talent ranks as the lowest resilience priority, but is **also the most challenging** for organizations of all types.

LOWEST PRIORITY

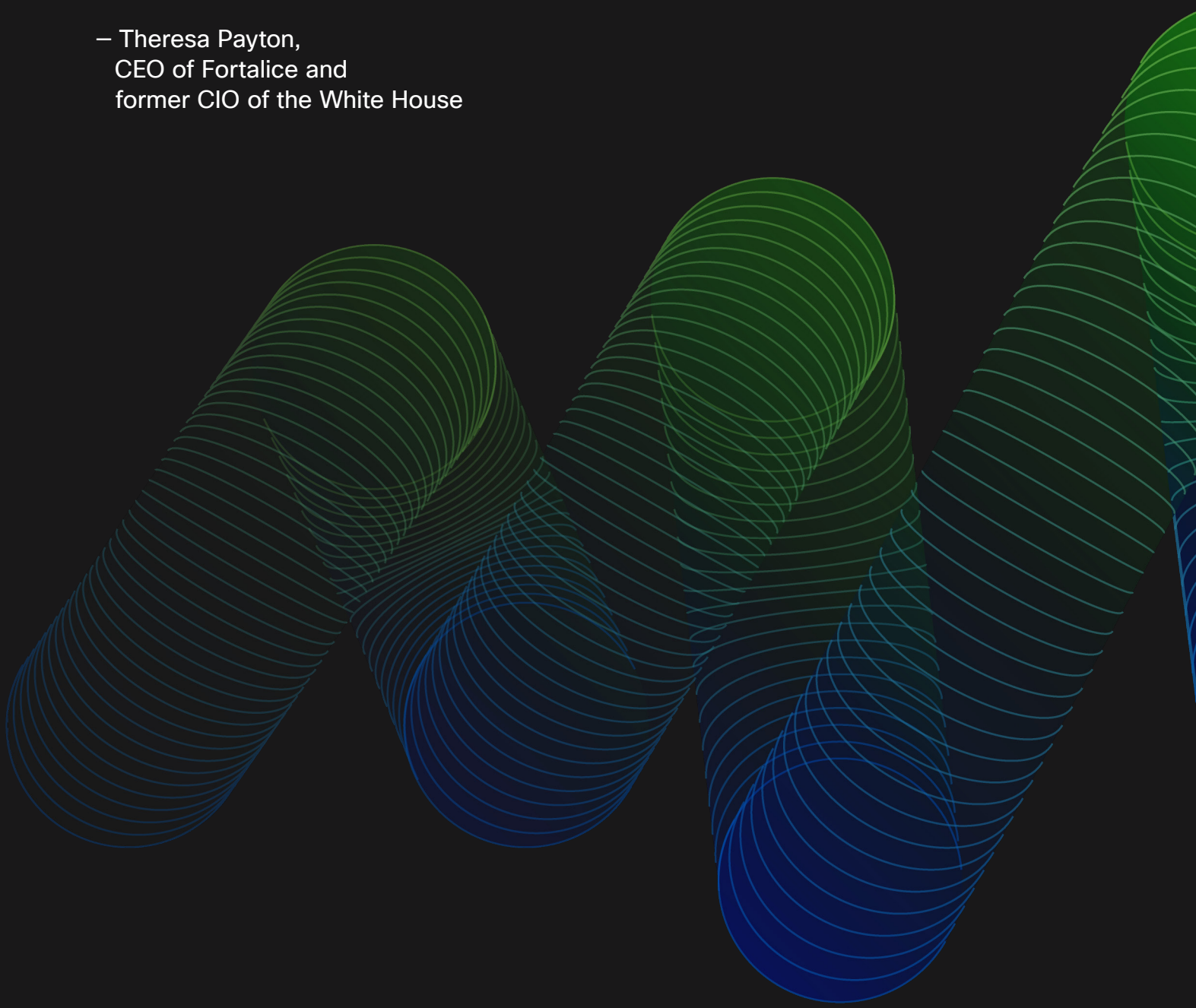
We identified **7** **success factors that**, if achieved, **boost** our measure of overall **security resilience** from the bottom 10th percentile to the top 10th percentile.

About the survey

Sampling method	Cisco contracted a professional survey research firm to field a fully anonymous survey in mid-2022 that utilized a stratified random sampling technique.
Survey participants	We surveyed 4,751 active information security and privacy professionals from 26 countries. Sample demographics can be found in the appendix.
Data analysis	The Cyentia Institute conducted an independent analysis of the survey data on behalf of Cisco, and generated all results presented in this report.

"I'm impressed with the thoughtful approach of the Security Outcomes Report. It provides data-backed guidance on how to best utilize resources to maximize the impact of security programs."

– Theresa Payton,
CEO of Fortalice and
former CIO of the White House



What is security resilience?

Whether or not you consider "resilience" to be a buzzword, it's undeniable that it's on the mind — and probably on the lips — of many inside and outside the field of cybersecurity. But what exactly does it mean? We at Cisco certainly have some thoughts on that topic, but since this is a survey of 4,700+ security practitioners, we'll hand them the mic instead.

"You keep using that word. I do not think it means what you think it means."

– Inigo Montoya, *The Princess Bride*

When asked to describe what security (or cyber) resilience means in the context of their organization, respondents gave a wide range of answers. Yet we do see some common themes among them.

Words such as "withstand," "recover," "anticipate," "adapt," and "adverse" all stand out as core to the concept of security resilience in the minds of respondents. If that sounds oddly familiar, it may be because it's near verbatim from NIST's definition of cyber resilience. That's perfectly fine; there's no such thing as cheating on a survey like this. But it does suggest that the meaning of resilience is murky enough that many security professionals had to look it up. We'll endeavor to make that concept clearer in the sections that follow.

Cyber resilience:
The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.

– Source: NIST SP 800-172

Why is security resilience a big deal?

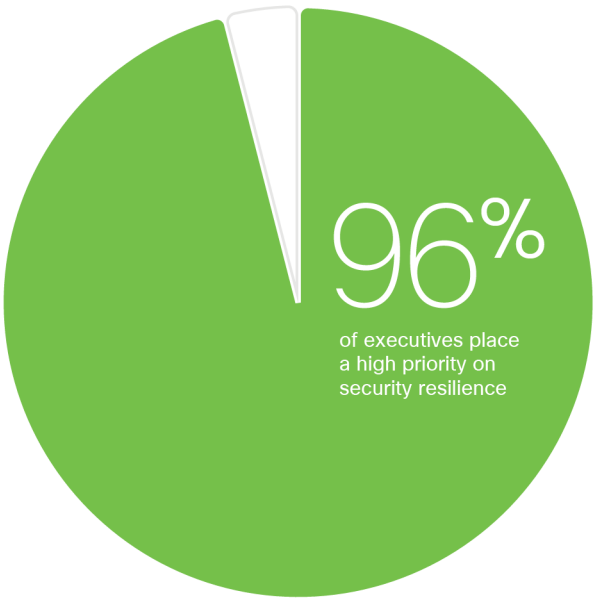
Contrarians among us may read this section title and think, "I'm not convinced that it is a big deal." Fair enough. Since we're not in the business of making empty claims, we'll back that up right at the start.

We asked respondents about the level of interest and importance top executives at their organization place on security resilience. The message couldn't be clearer. **A full 96% of executives consider security resilience highly important.** We think that warrants Really Big Deal status.

Perhaps the high priority placed on security resilience among executives stems from the fact that so many are very well acquainted with the risks. **Nearly two-thirds of respondents reported suffering major security incidents that jeopardized business operations.**

What's more, the majority of these events are said to have occurred within the last two years. From this, we infer that security resilience is not just a big deal in the mouths of thought leaders or the minds of executives. It's a concept that's critically important to a majority of organizations around the world.

Figure 1: How much interest and importance do executives place on security resilience?



Source: Cisco Security Outcomes Report

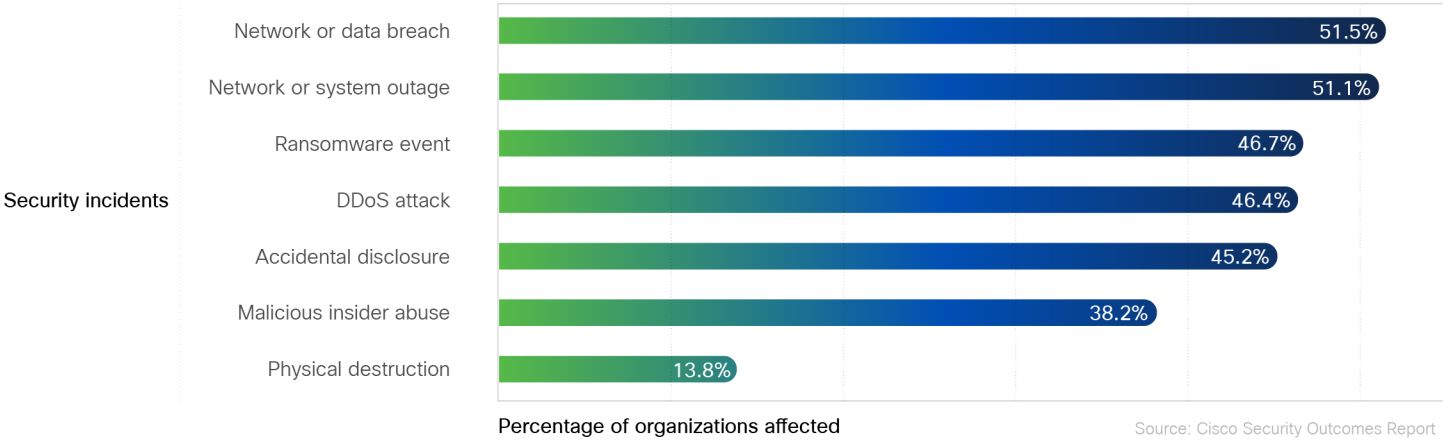
Figure 2: Has your organization experienced a security incident that impacted resilience?

Source: Cisco Security Outcomes Report

We then asked respondents to elaborate on the types of resilience-impacting incidents they experienced. As seen in Figure 3, network/data breaches and network/system outages were both cited by over half of participants that reported prior incidents. Ransomware and distributed denial-of-service (DDoS) attacks were the next most common event types, each affecting about 46% of organizations.

While some of the aforementioned incident types almost certainly involved employees as a vector of attack (e.g., clicking on a phishing email), overt, malicious abuse by insiders was reported by about 38% of organizations. Acts of physical destruction and sabotage were also cited, though substantially less often than the other incident types.

Figure 3: Types of security incidents that impacted resilience

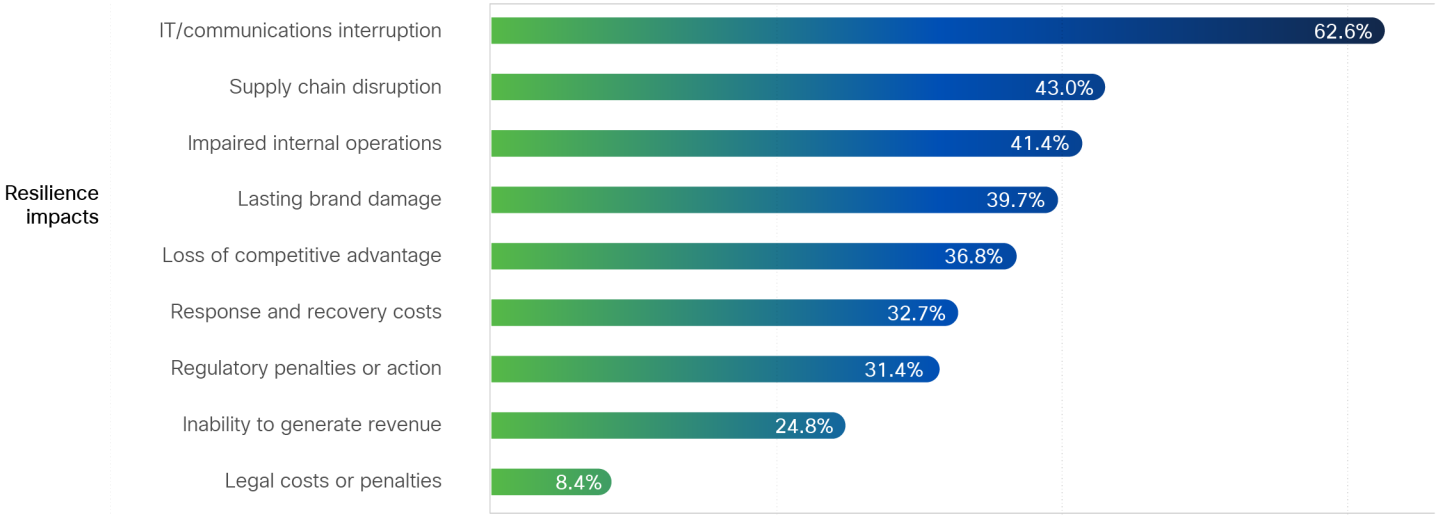


Source: Cisco Security Outcomes Report

Respondents also had a lot to say about how these events impacted their organizations (see Figure 4). Over 60% referenced IT and communications disruptions, as well as the critical role ICT plays in security resilience. Supply chain disruptions landed in the #2 spot for business-level impacts. We've all been living with that pain lately, so it's no surprise that organizations are feeling it too.

While impacts to supply chain operations affect entities outside the victim organization, impaired internal operations (reported by roughly 41% of firms) wreak havoc on the inside. Brand damage sits at or near the top of the "what keeps you up at night" list of many executives, so it's telling that roughly 40% of these incidents result in that outcome. Loss of competitive advantage is another top concern, and it rounds out the top five resilience impacts.

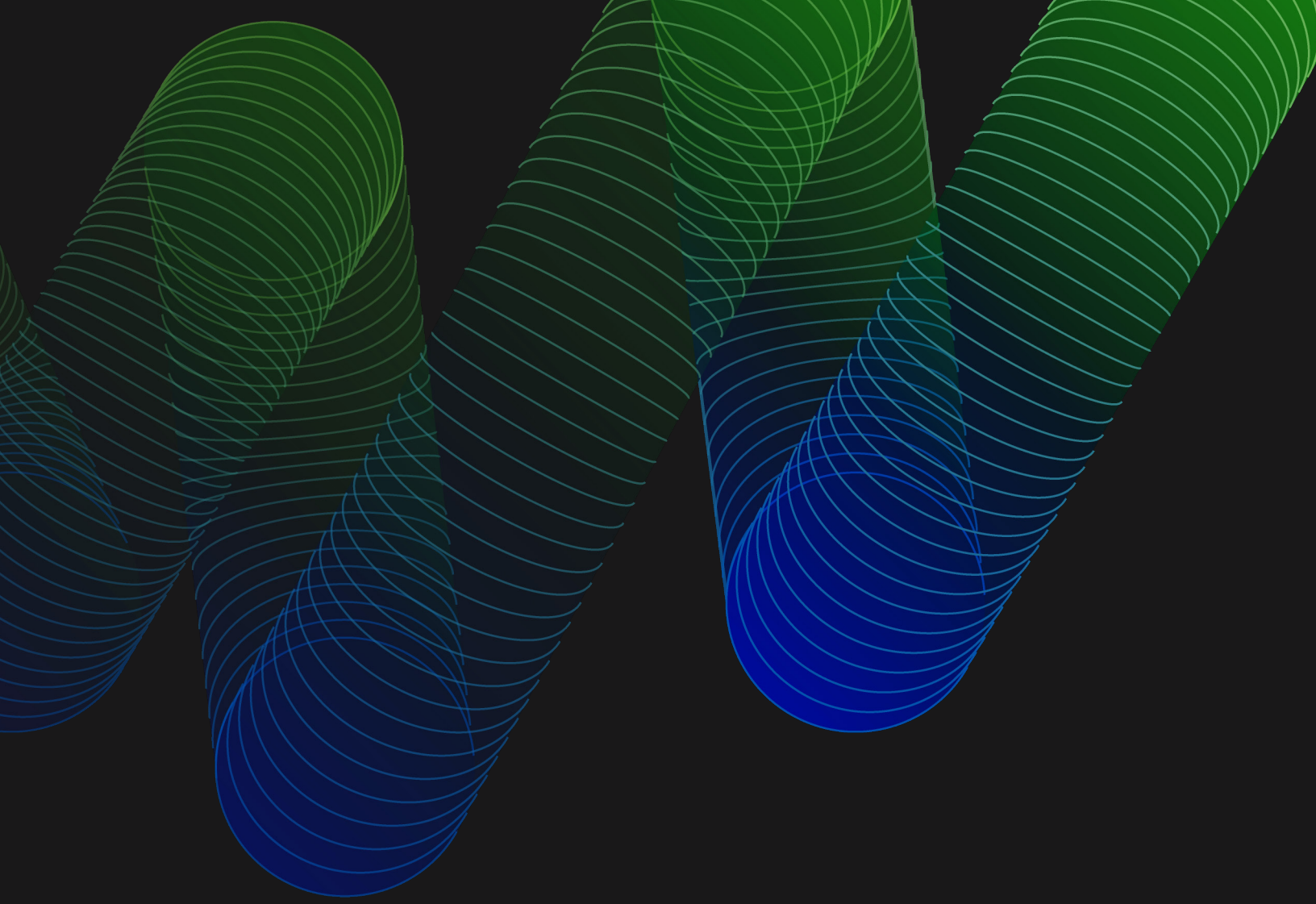
Figure 4: Types of resilience impacts caused by security incidents



Source: Cisco Security Outcomes Report

What can organizations do to avoid such events and improve security resilience? Well, that's one of the main questions we're seeking to answer in this report. Right at the outset, it's clear they're doing one thing above all others – spending money. An astounding 96% of participants say their organizations have increased investments in security in the wake of their most recent major incident.

Now, we all know throwing money at a problem doesn't solve it. But we also know few solutions are free. The important question is which investments give a return and which do not. We'll share what we learned about that a bit later. Before we do, though, let's explore the primary objectives that fall under the umbrella of security resilience.



"Security, after all, is a risk business. We don't secure everything, everywhere, or otherwise business wouldn't get done. But security resilience will allow you to focus your security resources on the pieces of the business that add the most value to an organization, and ensure that value is protected."

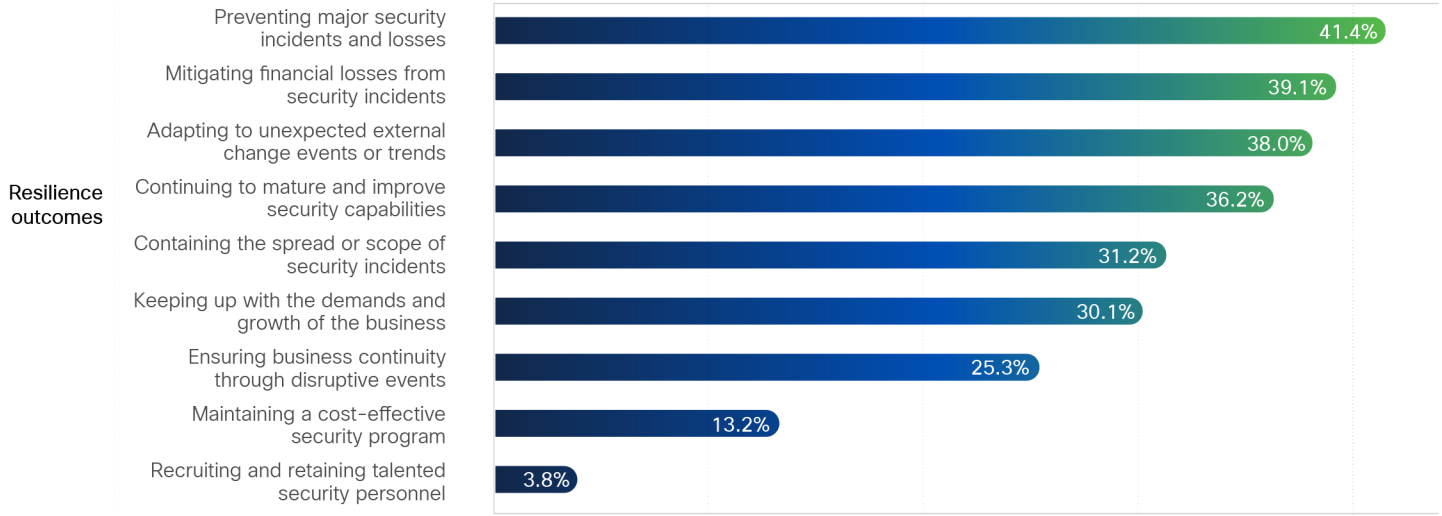
– Helen Patton,
CISO, Cisco Security Business Group

What does security resilience entail?

From the last section, we know that security resilience is a big deal among the big bosses, but what does it actually entail? What traits or achievements indicate that an organization is resilient? In preparation for this survey, we asked a group of security leaders about their goals and objectives for security resilience. We then reviewed their responses and grouped them into nine main security resilience outcomes.

Returning to our present global survey, we asked participants which of those nine key resilience outcomes their organizations considered to be the most important (they could select up to three). Figure 5 tallies their responses.

Figure 5: Most important security resilience outcomes as selected by participants



Source: Cisco Security Outcomes Report

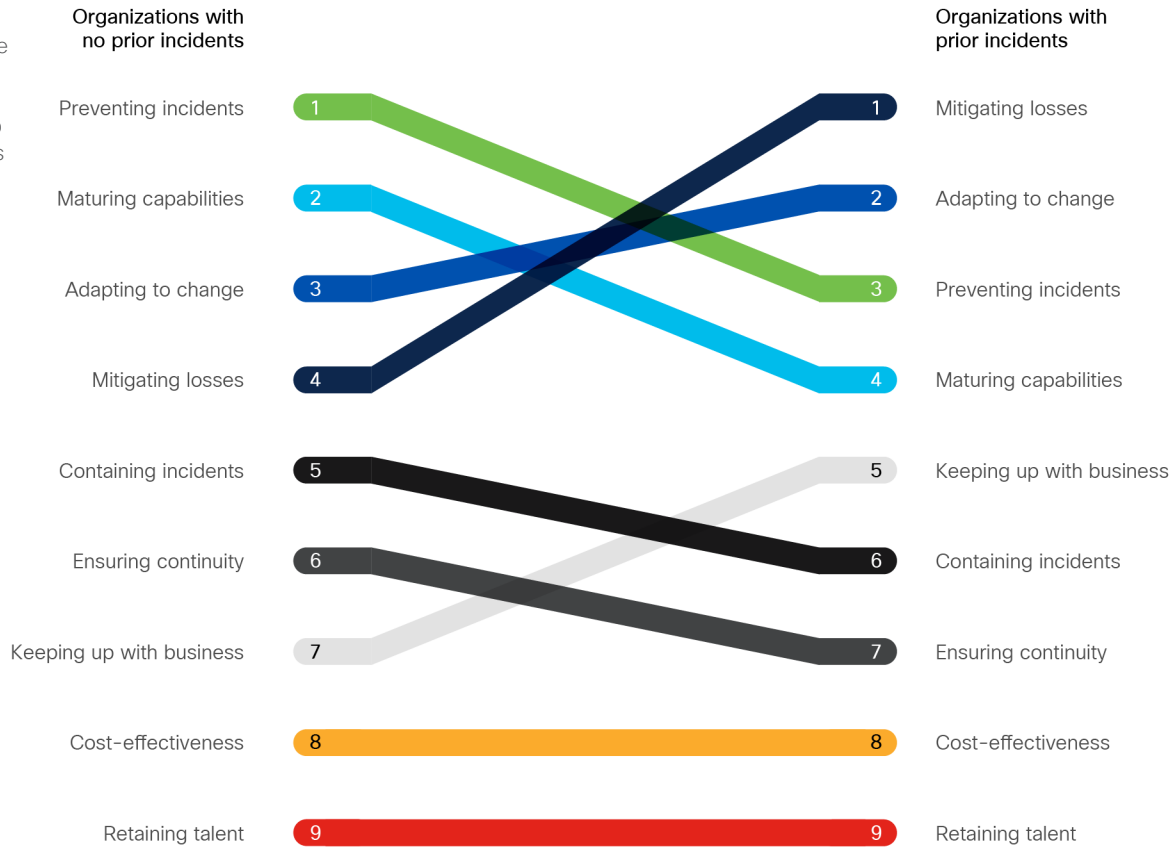
We find it somewhat surprising that preventing incidents is the top selection, given that general consensus seems to place resilience as a "right of boom" concept. But in combination with mitigating financial losses, the top two picks target the classic definition of risk – probability and impact.

Next up, adapting to unexpected events calls back to themes depicted in the free-form responses shared earlier. We can't help wondering if recent experience with the COVID-19 pandemic pushed that one up the list.

We'll refrain from commenting on all nine outcomes and instead skip down to the last one. Recruiting and retaining security talent was only seen as a primary aspect of security resilience by 3.8% of respondents. Perhaps respondents see talent retention as HR's responsibility or a long-term objective rather than critical to a resilience-impacting event. But ample and trained security staff are a critical success factor for resilient organizations, as we'll elaborate on later.

As you might imagine, experience shapes one's perception of what security resilience entails. Recall earlier when we said that 62% of respondents experienced a resilience-impacting security incident. According to Figure 6, those events may have triggered a reordering of priorities.

Figure 6: Ranking of perceived importance of security resilience outcomes for organizations with no prior incidents versus with prior incidents.



Source: Cisco Security Outcomes Report

Mitigating losses moves from #4 among organizations without major incidents to #1 for those who've lived through them. Adapting to change events and keeping up with the business bump up as well. Preventing incidents and capability maturity take a backseat.

You may also be wondering if perceptions of security resilience differ based on demographic and firmographic characteristics. Here again the data answers in the affirmative. We'll use the respondent's role as the filter for this one to compare CISOs and Security Directors with security professionals in technical roles.

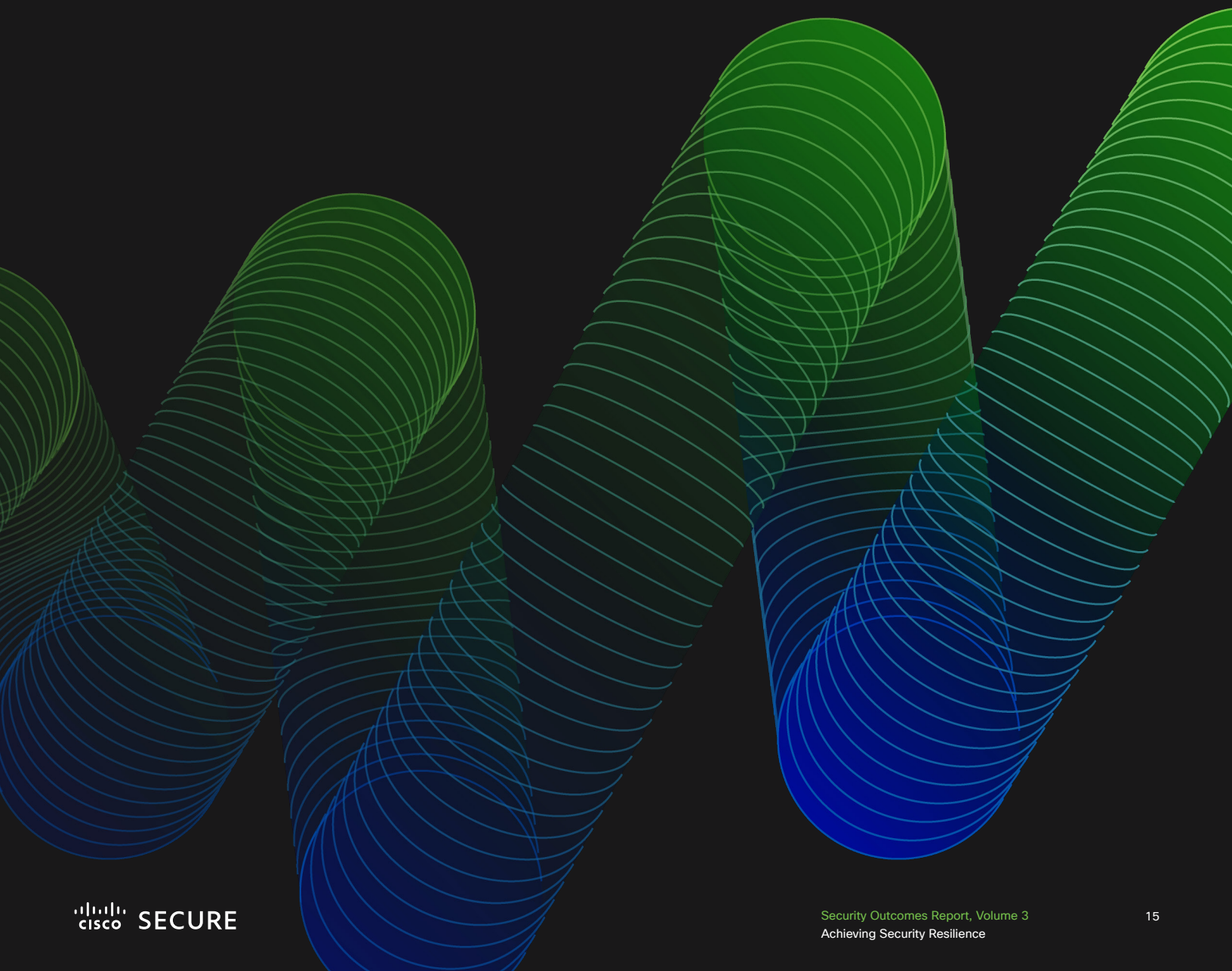
Figure 7: Ranking of perceived importance of security resilience outcomes by work role

Source: Cisco Security Outcomes Report

Differences in opinion emerge right from the start. Security leaders prioritize mitigating financial losses, containing the spread and scope of events, and not hindering the business. More technical and operational security respondents rank those 2nd, 5th, and 6th, respectively and place the highest importance on preventing major incidents. That's not to say either group is right or wrong; it's natural that they focus on different aspects of security resilience. But it's probably a good idea to establish shared priorities and delineate responsibilities to ensure everyone works as a team to achieve better outcomes.

"We have the tired, deprecated notion of building systems that have five nines for their ability to stay up. When we're talking about security resilience, it's more towards building [systems] to fail in that, if a system goes down, it will continue to operate despite having any technical issues."

– Dave Lewis,
Advisory CISO, Cisco Secure



The state of security resilience

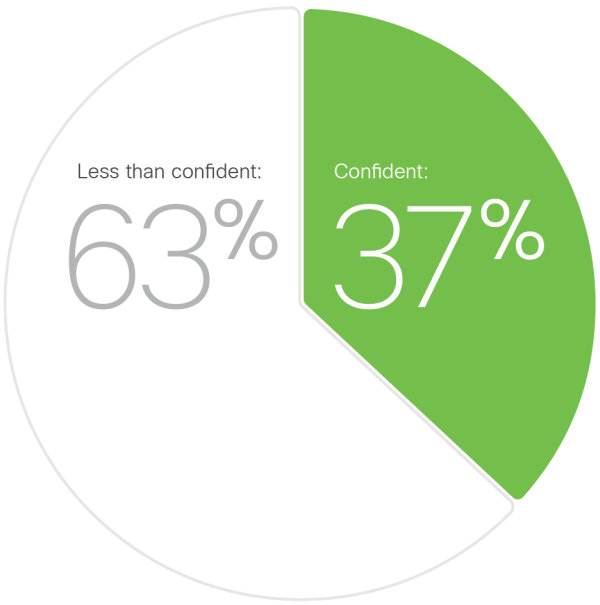
We asked respondents how confident they were that their organization would remain resilient through a worst-case (but still plausible) cyber event if it occurred today.

A little over a third expressed strong confidence, with the remaining two-thirds expressing some level of doubt about how their organizations would fare.

Asking a subjective question like that is an interesting gut check on the state of security resilience, but we'll need to be more specific and measured if we want to accomplish our goals. Since we have input from respondents on a set of desired security resilience outcomes, let's see where organizations stand in terms of achieving those outcomes.

We asked respondents to rate their organization's performance for each objective using a four-point scale (failing | struggling | performing | excelling). To help them do that more objectively, we provided a description of each outcome along with example evidences of what failure and/or excellence might look like. These descriptions and examples are included in Appendix B for those curious about the details or interested in adapting these for use within your own organization.

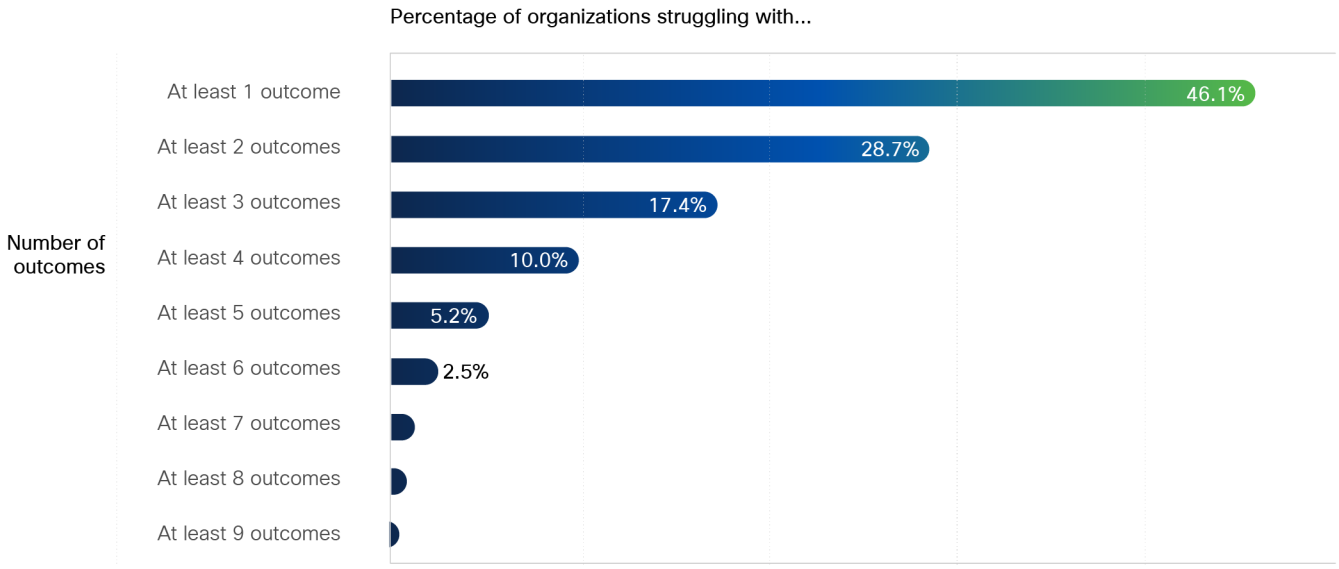
Figure 8: Confidence in ability to remain resilient through a worst-case cyber event



Source: Cisco Security Outcomes Report

In general, the majority of respondents gave their organizations at least a "performing" rating overall. But don't take that to mean all is hunky dory in the world of security resilience. As seen in Figure 9, almost half of the survey participants say their organizations are struggling or outright failing to achieve at least one of the nine security resilience outcomes. Over a quarter are having difficulty with two or more, 10% report at least four outcomes giving them trouble, and so on. From that, we conclude that there are a lot of organizations out there underachieving in key areas of security resilience.

Figure 9: Proportion of organizations struggling with security resilience outcomes



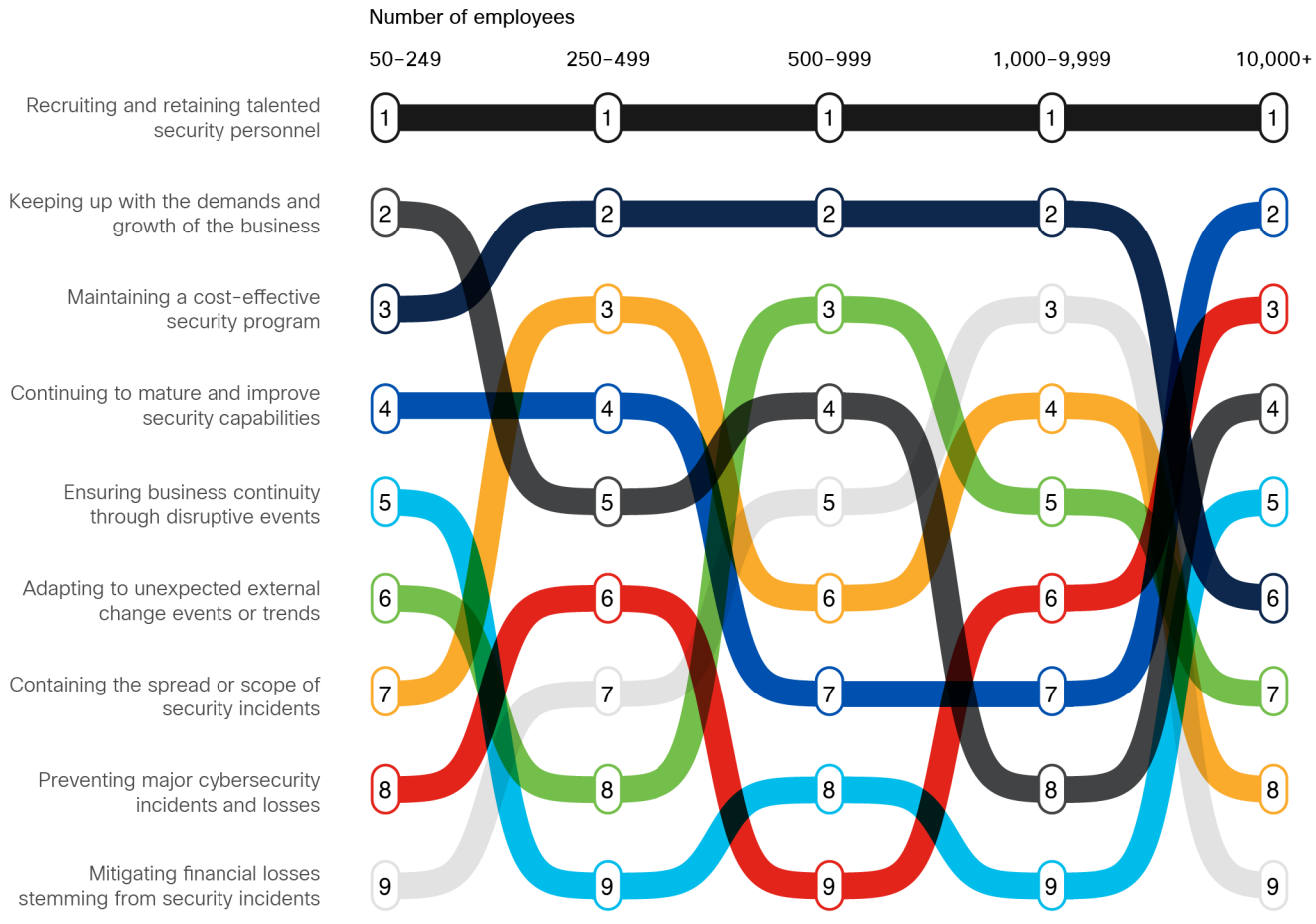
Source: Cisco Security Outcomes Report

We saw earlier that perceptions vary on the relative importance of these security resilience outcomes, so it's no real shock to learn that performance varies as well for different types of organizations. Take Figure 10, for example, where we compare the proportion of participants struggling with each outcome across different organization sizes. Firms of all sizes agree that recruiting and retaining security staff is the biggest challenge, but the consensus ends there.

We find this view particularly interesting because it gives the sense that areas of struggle change as organizations grow. For instance, mitigating financial losses is purportedly least challenging for the smallest firms. (Maybe because they're more worried about going out of business than losing money?) But it creeps successively up into the top three for organizations with 1,000–9,999 employees. And then it crashes back to last place for the largest enterprises. (Maybe because they have extra financial security from high revenues?)

On the other hand, some things seem to never change with growth. As mentioned above, organizations of all sizes apparently struggle more to recruit and retain security talent than with any other outcome. That's rather ironic since they also unanimously rate that outcome as the lowest priority for security resilience. A self-fulfilling prophecy, perhaps? Or maybe just blunt pragmatism. *("Sure, it's hard to keep good people, but I'm far more concerned about avoiding major incidents and losses.")*

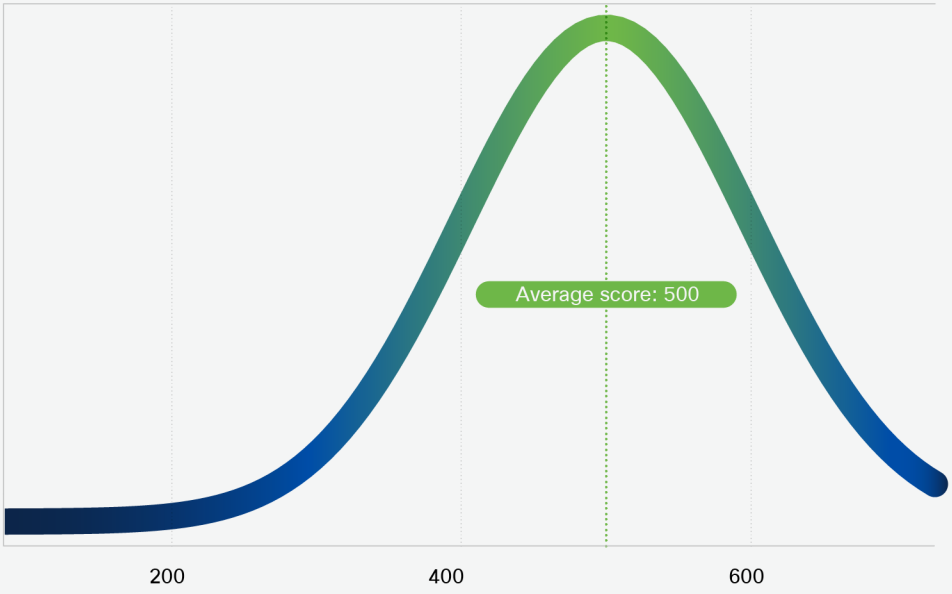
Figure 10: Most challenging security resilience outcomes ranked by organization size



Source: Cisco Security Outcomes Report

In addition to assessing performance for individual outcomes, we wanted an overall measure of security resilience for each participating organization. So we created a security resilience score based on each organization's achievement across all nine outcomes. If you'd like to know how we did that, check out the callout below. But the gist is that a higher score means higher performance across greater numbers of security resilience outcomes. We will use this score extensively in the next section to measure the efficacy of various success factors in improving security resilience.

Figure 11: Distribution of security resilience scores across participants



Source: Cisco Security Outcomes Report

Measuring the overall security resilience score

In addition to assessing each outcome, we wanted an aggregate score that captured an organization's level of achievement across all nine outcomes as a measure of its overall security resilience. We refer to that as the 'security resilience score,' and you'll see it referenced a lot in this report.

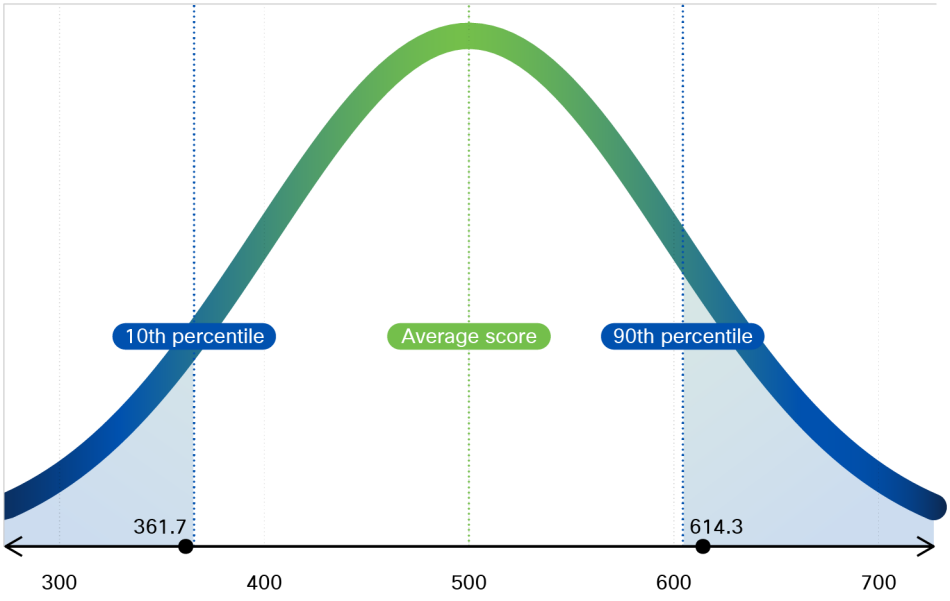
To get the score, we used a statistics technique called Item Response Theory. (We did the same thing for the security outcomes score in the last volume.) This technique enables us to score organizations based on how they're doing across all outcomes, while at the same time accounting for the fact that 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 reliable point of comparison among programs. The distribution of security resilience scores is shown in Figure 11, with the average falling right at 500.

Seven success factors for resilience

We come now to the part for which you've all been waiting/reading. With a score representing overall security resilience across nine outcomes for each of the 4,700+ organizations, we now explore how to improve it. We approached that by analyzing a bunch of potential organizational, IT, and security factors to test how they correlate with stronger security resilience.

Through that process, we identified seven data-backed success factors for security resilience. How much difference did they make? Glad you asked. Organizations that exhibit these factors scored within the top 10% of all security resilience scores measured across all participants in our report. On the other hand, organizations missing the majority of them fall to the bottom 10th percentile. Nobody wants that benchmark.

Figure 12: Effect of adherence to seven success factors on overall security resilience score



Source: Cisco Security Outcomes Report

Organizations implementing these success factors see their resilience jump from the 10th to the 90th percentiles.

So what are these lucky seven factors for strengthening security resilience, and how can your organization benefit from them? Be forewarned – there's really no luck about it! Like Denzel Washington once said, "Luck is when an opportunity comes along and you're prepared for it." The remainder of this section should help with that preparation.

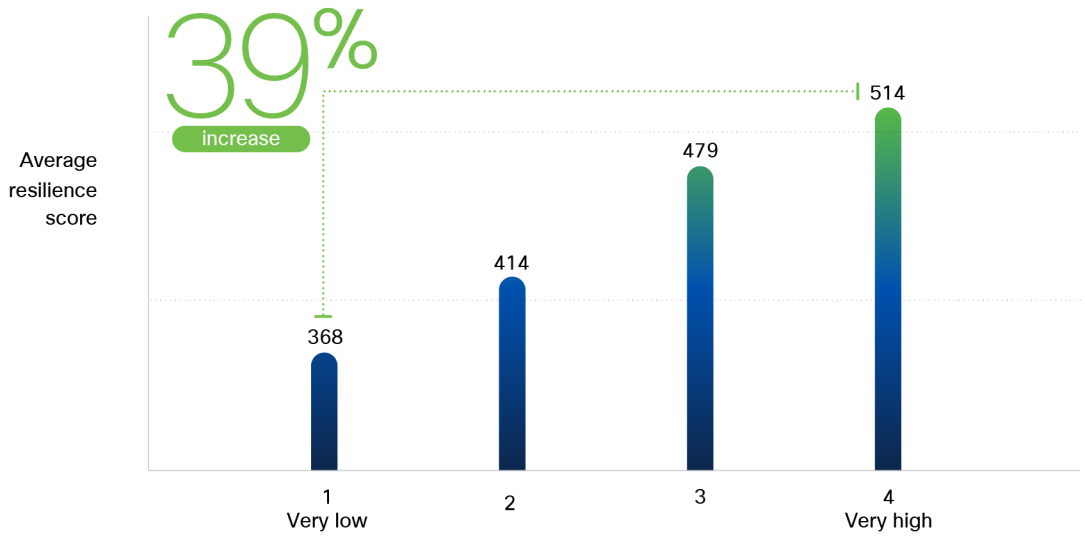
1. Establish executive support

Granted, this factor is rather hackneyed in cybersecurity circles, but its effect cannot be dismissed offhand. Organizations that report poor support from top executives exhibit security resilience scores that are 39% lower than those with strong backing from the C-suite. The real puzzle, of course, is how to garner the support of executives.

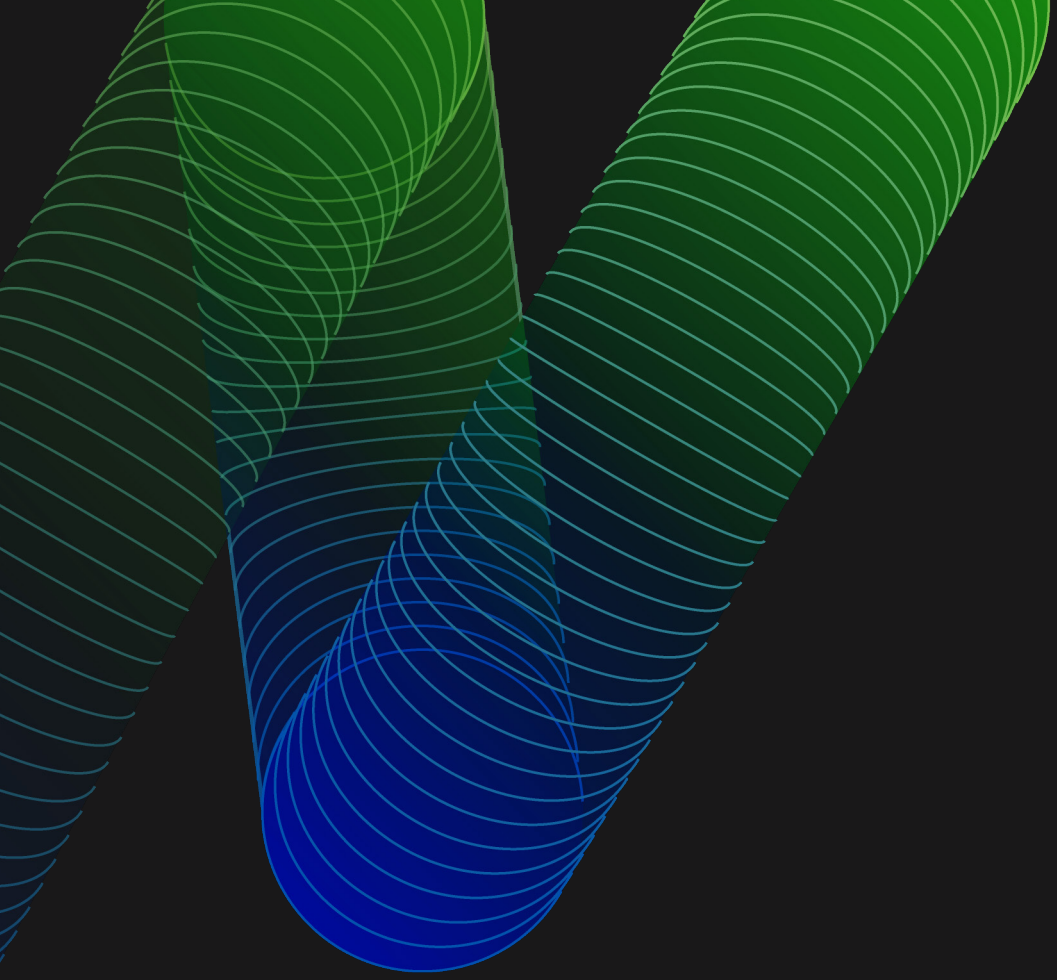
Our data suggests that security programs that are tightly aligned with the core mission of the business have stronger executive-level support and improved resilience to boot (+32% to overall score). Thus, bridges to the C-suite are built upon a solid understanding of how the business works and how security initiatives can make it work even better. Support goes both ways in any relationship, after all.

While on the topic of relationships, we'll mention another observation from our analysis. We asked respondents where the responsibility for security resilience sits in their org chart. And for the most part, reporting lines don't seem to make a big difference. But we did notice that organizations in which the CEO, CRO (Chief Risk Officer), and CISO were closely involved had significantly higher security resilience scores than those where the buck stopped with other C-level executives (e.g., CIO, COO, CTO, CFO).

Figure 13: Effect of executive support on security resilience



Source: Cisco Security Outcomes Report



"CISOs must strengthen relationships with the executive team. By improving business alignment and getting executive buy-in for budget and headcount, organizations can improve their security resilience. Good relationships lead to good security programs, and good programs lead to great relationships."

– Wolfgang Goerlich,
Advisory CISO, Cisco

2. Cultivate a culture of security

Leaders looking to improve security resilience might start at the top by establishing executive support, but they shouldn't stop there. They should endeavor to cultivate a culture of security throughout the organization, because our data shows that organizations able to do that will see a 46% boost in resilience scores over those with poor security culture.

±46% difference in average resilience scores between organizations with poor versus excellent security culture

That is, of course, much easier said than done. And it's a fair question to ask what is meant by a strong security culture and how that was assessed in our report. We provided the following guidance to respondents to help them assess and rate the strength of their organization's security culture:

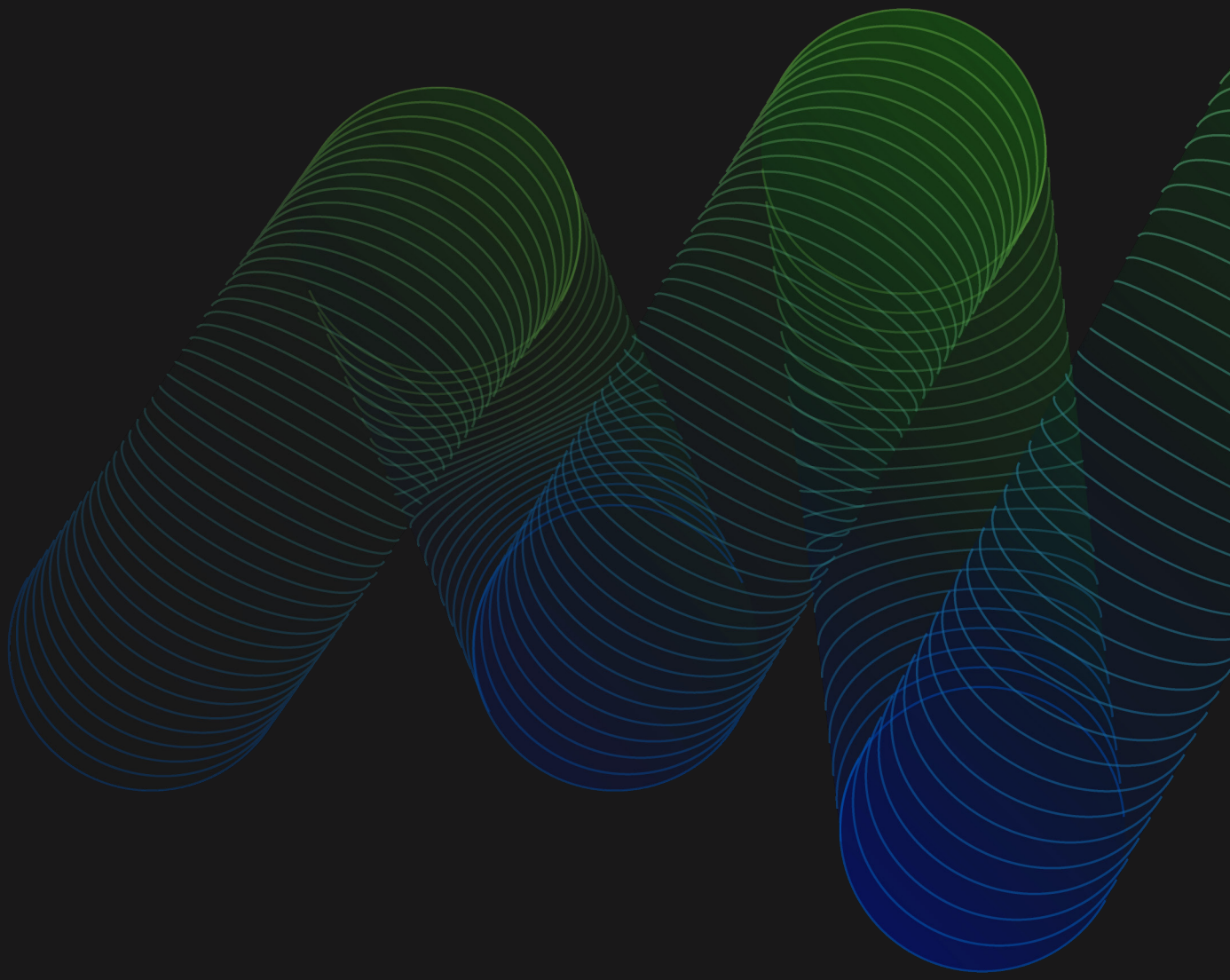
> In a strong security culture, employees are treated as part of the solution rather than the problem. Security staff understand their role in the context of the organization and non-security staff know they have a role to play too. This may be seen by regularly reporting phishing attempts, potential malware, and other incidents. Security isn't a negative theme in employee satisfaction surveys or exit interviews. Conversely, frequent security policy violations and workarounds are evidence of poor security culture.

That's not intended to be an exhaustive description of what a strong security culture looks like because it will look different in every organization. But it at least level sets what respondents had in mind when they rated the strength of their security culture, and hopefully sparks ideas for measuring your own.

Reading between the lines of that description, you may get the sense that it's important for a security program to clearly communicate its policies and rationale with the rest of the organization. Respondents giving their organizations high marks on that front showed a 27% increase in security resilience scores over those who said their security programs can't articulate what they're doing and why they're doing it. It's hard to build a strong culture when everyone's using a different set of blueprints.

"Security awareness is disappearing as a topic to be replaced by an emphasis on security culture, changing the DNA of the organization and making every colleague a member of the extended security family. Simple training is being seen as a tick-box compliance exercise while communicating and changing the values of the organization is now seen as a core objective by many CISOs."

– Richard Archdeacon,
Advisory CISO, Cisco



3. Hold resources in reserve

We saw earlier that recruiting and retaining talented security personnel was widely perceived as the least critical security resilience outcome, and yet also the most challenging. Prior volumes of the Security Outcomes Report have pointed to several measurable benefits tied to the people pillar of cybersecurity programs, and this one is no different.

Surprisingly, we did not find a strong correlation between the overall size of security staff and level of security resilience, even when controlling for total number of employees in the organization. What does appear to make a difference, though, is maintaining excess internal staff and resources in order to better respond to unexpected cyber events. Organizations able to do that achieve 15% higher security resilience scores on average than those without "flex" resources to tap into when needed.

How exactly do organizations maintain excess internal resources when it's already difficult to hire and retain baseline security staffing? Unfortunately, we didn't ask for those details in the survey but it's now on the list for future research.

±15% difference in average resilience scores between organizations that **do versus don't maintain excess internal staff for incident response**

±11% difference in average resilience scores between organizations that **do versus don't retain external incident response services**

If maintaining excess internal staff to handle unexpected events isn't feasible for your organization, all is not lost. Our analysis also points to an 11% average improvement in security resilience among firms that retain external incident response (IR) services. Consider getting those retainer contracts in place with a credible IR service provider so help is just a phone call away.

You may be thinking that if extra internal resources or external IR services each offer benefits, then perhaps they're even better together. That indeed appears to be the case. Having both internal and external resources ready to go in a major cyber event gives another 13% bump to security resilience scores over having just one or the other.

4. Simplify hybrid cloud environments

Cloud architecture and migration have been big topics for quite some time now among IT and security teams alike. Many have gone all-in on the cloud from infrastructure to software, while some remain staunchly entrenched in their on-premises environment. But which of those strategies is more conducive to security resilience? Would you believe that the answer is both?

We asked participants if, in general, their IT infrastructure was hosted on-premises or in the cloud (or varying levels of hybrid models). Then we correlated those answers with each organization's security resilience score. Cloud-heavy organizations averaged 526, while those predominately on-premises averaged 525. In other words, we see no difference in security resilience outcomes between heavy on-premises versus heavy cloud environments.

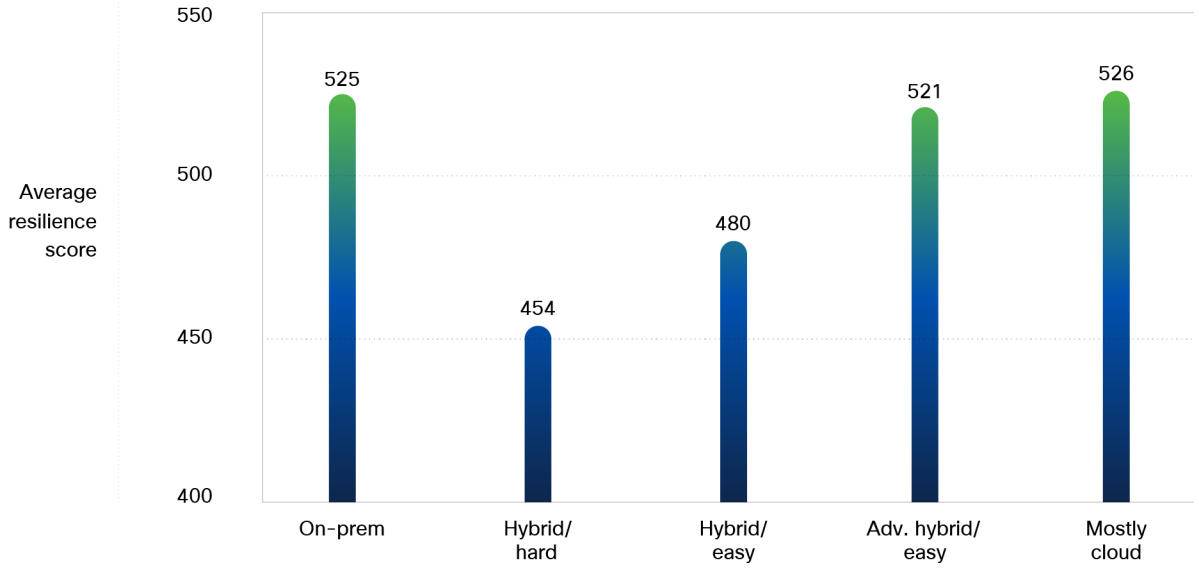
±15% difference in average resilience scores across hybrid cloud environments that are simpler versus harder to manage

Where we do see a difference is *in-between* on-premises and cloud environments. Organizations in an early-stage hybrid model post security resilience scores that fall an average of 14% lower than their predominately on-premises peers. In the voice of Ned Ryerson from Groundhog Day, "Watch out for that first step [to the cloud]; it's a doozie!"

There is, however, evidence that it's possible to make that first step into the cloud a little less of a doozie. Organizations that, in a separate question, rated their hybrid environment as easier to manage and secure appear to cushion the negative hit to resilience that typifies the early phases of cloud migration. Their resilience scores dropped by just 8.5% rather than 14%. What's more, the benefits of simplified management of hybrid environments grow along with greater levels of cloud adoption.

Organizations with more extensive hybrid environments exhibit resilience scores that are statistically on par with the on-premises (or fully cloud) baseline — provided they're able to simplify management. If not, those resilience gains are erased as the organization languishes in that hard-to-manage hybrid state. Overall, there's a 15% difference in resilience scores between early hybrid cloud environments that are difficult to manage and advanced cloud deployments that are simpler to manage.

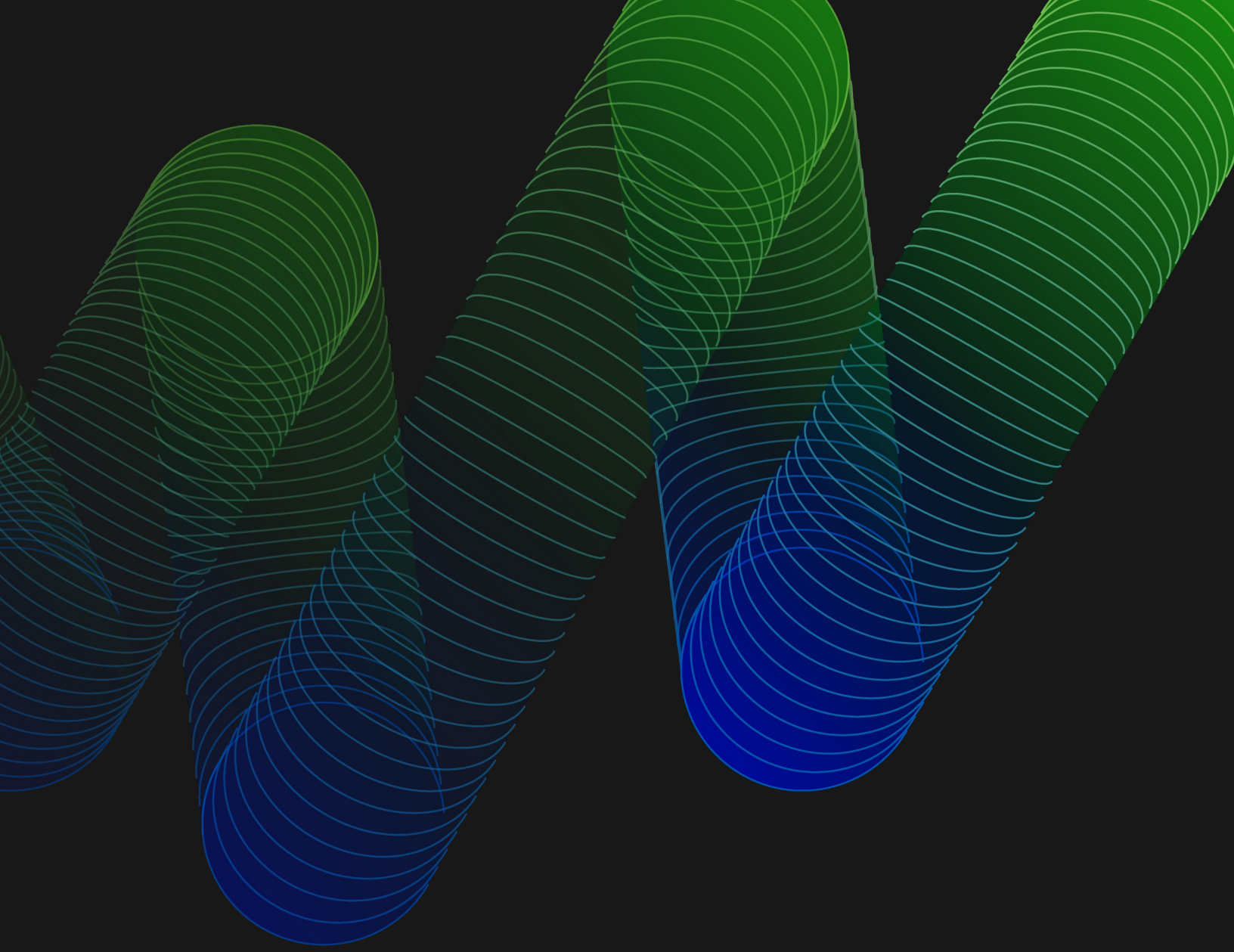
Figure 14: Effect of cloud adoption and ease of management on security resilience



Source: Cisco Security Outcomes Report

From that, we infer that keeping things simple and friction free is a key success factor for transitioning to the cloud. Since hybrid cloud deployments are a necessary part of that journey, ensuring you have the right tools and services in place to manage these complex environments will help your organization remain secure and resilient throughout the journey.

It's worth noting that the general pattern described here applies to organizations of all sizes. There's not much measurable difference in security resilience between the cloud vs. on-premises extremes for any sized organization. But both SMBs and large enterprises alike struggle with resilience in hybrid cloud infrastructures. One difference we did note is that larger organizations are three times as likely to rate their environment as complex and difficult to manage, meaning their move to the cloud could translate into a bigger hit to security resilience if not managed well.



"The challenge is that most of the time, security practitioners can't influence how quickly organizations move from on-prem to the cloud. If you can't change the tech, the only other levers you can pull are the people and the process."

– Helen Patton,
CISO, Cisco Security Business Group

5. Maximize zero trust adoption

In today's business environment, work is done from anywhere, which means security must exist everywhere to fully protect the business. Traditional security approaches that trust anything (devices, users, infrastructure, etc.) inside the corporate network can't deliver that level of protection. Thus, an approach that eliminates blind trust has arisen. A zero trust model establishes trust in users and devices through authentication and continuous monitoring of each access attempt, with custom security policies that protect every application.

The obvious question, then, is whether we see any evidence that a zero trust model improves security resilience. And to that question, we're glad to respond with a definitive "yes." Respondents with mature zero trust implementations boosted their security resilience rating by 30% over organizations that haven't started that journey! Furthermore, zero trust correlated with significantly higher success rates for 8 out of the 9 security resilience outcomes we discussed earlier.

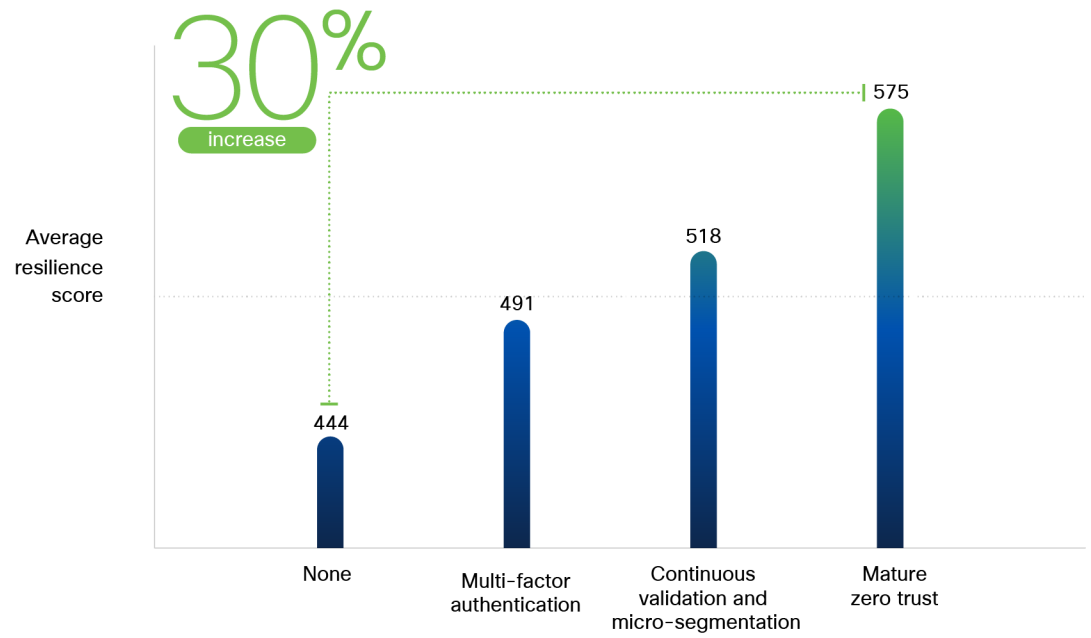
±30% difference in average resilience scores between organizations with non-existent and mature zero trust implementations

A mature zero trust implementation doesn't happen overnight, nor are the full benefits to resilience reaped all at once. It's a journey. We don't have the space in this report to draw up a detailed map of that journey, but we do have a ton of resources to help those interested in getting started. What we will do is highlight some key steps to demonstrate the progressive benefits of maturing zero trust adoption.

The first step of the zero trust journey for many organizations is verifying users and devices through multi-factor authentication (MFA). Among our respondents, rolling out MFA correlates with an 11% improvement in security resilience scores.

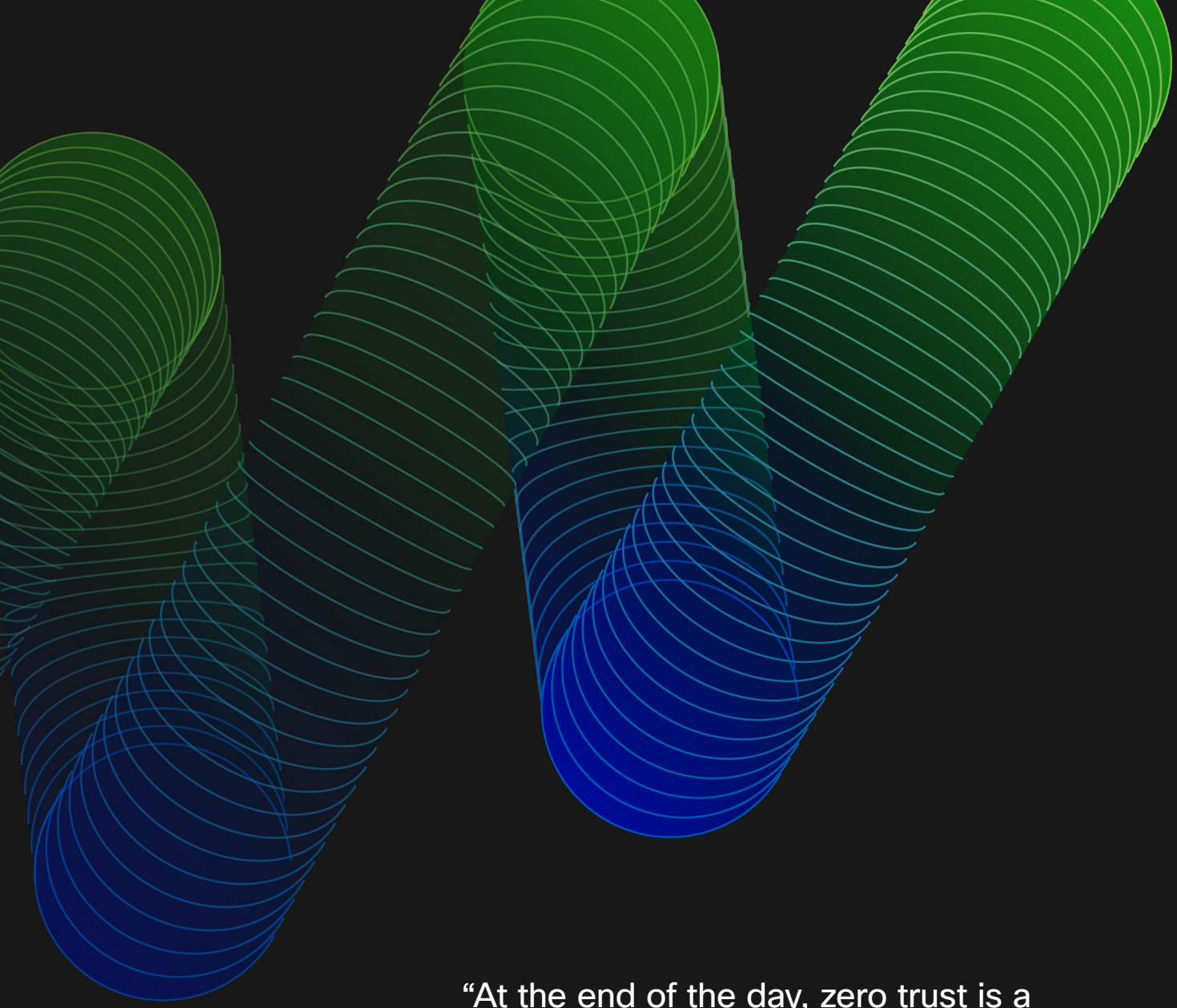
Many organizations continuing their zero trust journey will also implement continuous validation of users and devices along with micro-segmentation of workloads. According to our data, those that do add another 6% to their security resilience score. Don't dismiss those gains, and remember that large percentage increases get harder as base scores get higher.

Figure 15: Effect of zero trust implementation milestones on security resilience



Source: Cisco Security Outcomes Report

Let's look at one more milestone on the zero trust journey, this one nearing the finish line. Here, organizations have bolstered MFA, continuous validation, and micro-segmentation with adaptive policies, extensive monitoring, and orchestration of user workflows. That brings us to what we labeled as a "mature" implementation of zero trust to achieve the full 30% improvement in security resilience scores referenced above.



"At the end of the day, zero trust is a philosophy that can be applied to any technology. Technology by itself is not enough and every organization's journey will take a different route to their destination of choice. Finding the right mix of technologies to implement its core principles is what will ultimately unlock the full benefits of zero trust security for a more resilient business."

– Wendy Nather,
Head of Advisory CISOs, Cisco

6. Extend detection and response capabilities

It shouldn't take more than browsing through the latest headlines to get the sense that modern cyber threats come at you from a multitude of vectors. But if you're a skeptic and need more convincing, you can dive headlong into the hundreds of adversary techniques and sub-techniques listed in the MITRE ATT&CK framework. The point is that all of these tactics and techniques require multiple vantage points in order to detect and respond to them effectively.

Extended detection and response (XDR) delivers visibility into data across networks, clouds, endpoints, and applications while applying analytics and automation to detect, analyze, hunt for, and remediate today's and tomorrow's threats. You can probably guess where this is headed. Do we see measurable improvements to security resilience as detection and response capabilities extend to cover more threat vectors and enterprise assets? Let's find out.

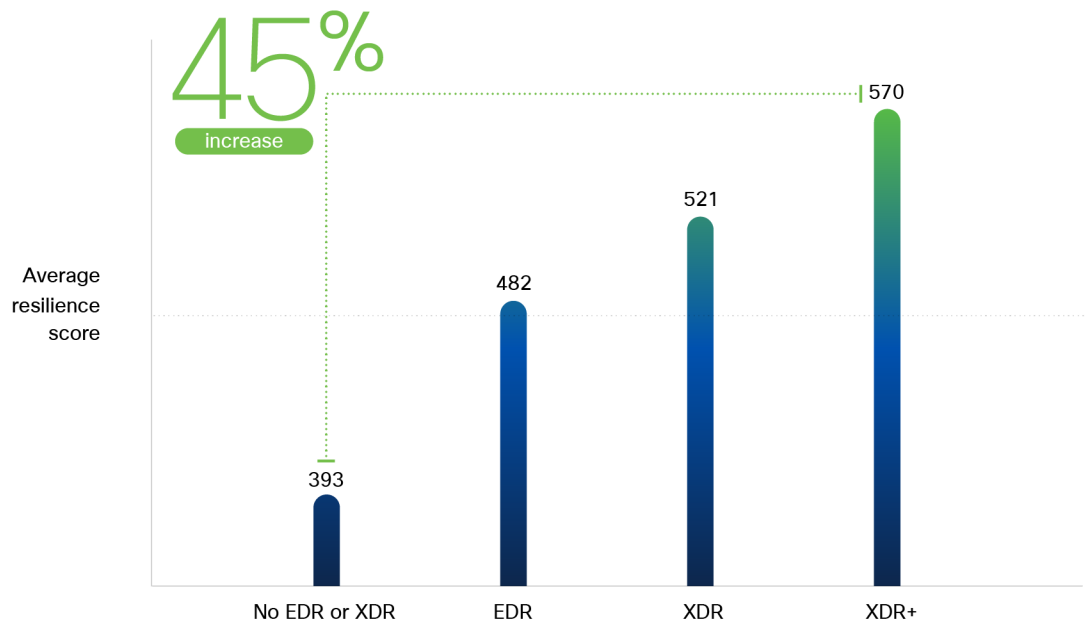
±45% difference in average resilience scores between organizations with non-existent versus mature XDR implementations

To test that, we'll establish a baseline for organizations that haven't made progress with XDR or even its predecessor, endpoint detection and response (EDR). The security resilience scores of those organizations average 393. To put that in perspective, this puts them in the 14th percentile for security resilience among all participants. Obviously not where most want to stay.

Since many view EDR as a foundational component of XDR, we'll consider that milestone #1 on the journey. Organizations that report rolling out EDR upped their overall security resilience score by 23% over the baseline. Not bad at all. But also not really XDR, so let's keep going.

Participants that report having the basic elements of XDR in place add another 10 percentage points to their security resilience score, rising 33% higher than organizations with no EDR or XDR deployments. By "basic," we mean that they have detection and response capabilities at the endpoint and network but haven't yet integrated it all together.

Figure 16: Effect of XDR implementation milestones on security resilience



Source: Cisco Security Outcomes Report

Extending capabilities is great, but anyone who's worked in security operations knows the challenges that come with wider and deeper visibility. The ever-increasing volume of events that must be triaged and responded to is what leads to many security incidents that we read about in those headlines. In our view, there are two major things that integrate the base components of XDR into a cohesive solution: cyber threat intelligence and automation/orchestration.

Detection and response capabilities work best when they know what to look for and how to find it. Many look to quality cyber threat intelligence for that purpose. Security automation and orchestration is the connective tissue of mature XDR implementations. Together, they take XDR to the next level. Organizations with all of these capabilities significantly improved their performance in all nine resilience outcomes and boasted a 45% better overall resilience score than those with no progress toward XDR.

7. Take security to the edge

The acceleration in hybrid work – including a mobile workforce, the proliferation of devices, and the hyper-distribution of applications over multiple cloud providers – has resulted in growing challenges to securing this widespread interconnectivity that outpaces human scale. The current prevailing secure connectivity model is inadequate to address these challenges. As a result, end users and IT professionals alike face a reality where their experiences are both fragmented and exposed.

Secure access service edge (SASE) offers a strategy to converge networking and security into a cloud-delivered service, simplify operations, and remain resilient in the face of ever-changing business demands. Do we have evidence from our report that SASE does indeed correlate with improved resilience? Yes!

±27% difference in average resilience scores between organizations with non-existent versus more mature SASE implementations

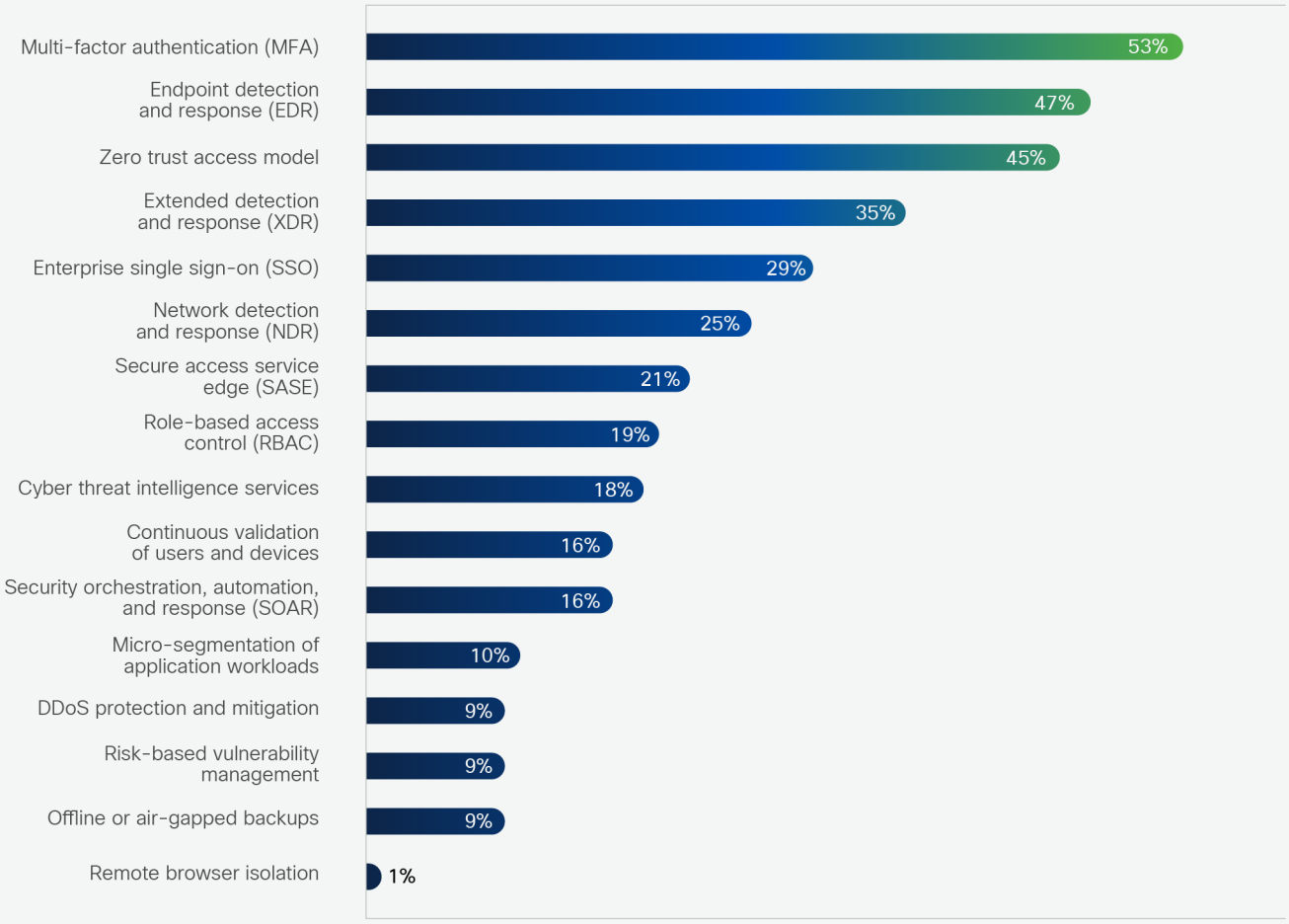
We didn't get into the specifics of classic components of SASE implementation (see Gartner's definition), but we did inquire about participants' general progress in that direction. Organizations claiming to have SASE deployments exhibit overall security resilience scores that are, on average, 15% higher than those that have no plans or progress on the SASE front. We also found that SASE implementation correlates with higher success rates for eight out of the nine individual security resilience outcomes.

But wait, there's more! Cisco expands on Gartner's definition of SASE to include advanced threat detection and response capabilities, among other components. Since we did ask about those capabilities, we were curious to see if organizations that incorporated them along with their SASE implementations were even more resilient. Turns out they did indeed climb to new heights of security resilience, raising their scores to 27% higher than the baseline of organizations that haven't started rolling out SASE.

Showing some initiative

Parallel to this larger survey, we asked a focus group of IT and security executives to share their top three current initiatives for improving the cyber resilience of their organizations. Here's what they had to say.

Figure 17: Top initiatives for security resilience



Source: Cisco Security Outcomes Report

The cybersecurity (resilience) framework

Originally the result of a 2013 United States Executive Order aimed at securing critical infrastructure, the NIST Cybersecurity Framework is now used by many different types of organizations the world over to reduce cyber risk and improve resilience. Because of that widespread usage, we thought it would be useful to assess how relevant activities defined in the Cybersecurity Framework affect our nine security resilience outcomes.

To enable that, we asked each participant to rate the implementation level of a subset of 13 capabilities derived from activities defined in the Cybersecurity Framework. These capabilities were selected by our experts based on their potential relevance to security resilience. Then we crunched the data to determine correlations between each capability and each of our security resilience outcomes. The results of that are captured in the effects matrix presented below in all its data nerdery glory.

Figure 18: NIST Cybersecurity Framework activities correlated with security resilience outcomes

	Key systems/data are tracked and have security requirements (ID.AM)	Top cyber risk scenarios have been identified and assessed (ID.RA)	Response abilities contain the expansion of security events (RS.MI)	A sufficient cyber insurance policy is maintained (N/A)	Recovery strategies include management of public relations (RC.CO-1, RC.CO-2)	Response/recovery testing includes services by third-party providers (RC.SC-5)	Response/recovery plans are regularly updated (RS.IM, RC.IM)	Delivery of services is ensured during/after a cyber event (ID.BE-5)	Response/recovery plans include coordination with external parties (RS.CO-4)	Threat detection capability provides awareness of potential security events (ID.AE)	Response personnel have been trained to handle a security event (RS.CO-1)	Response capabilities enable timely/effective investigation of events (RS.AN)	An incident response and recovery plan exists/is known about (RS.RP, RC.RP)
Containing the spread or scope of security incidents	10.6%	9.0%	8.6%	5.4%	5.4%	4.9%	5.3%						
Recruiting and retaining talented security personnel	9.7%	7.2%	5.0%	5.8%	6.1%			4.6%				5.1%	
Mitigating financial losses stemming from security incidents	9.9%	8.4%	4.1%	5.0%	6.7%	4.4%	4.1%						4.7%
Adapting to unexpected external change events or trends	10.7%	6.5%	6.2%	5.1%	5.4%	4.9%	4.6%	4.1%	4.2%			6.5%	
Keeping up with the demands and growth of the business	11.6%	8.3%	4.4%				4.7%	7.4%		8.9%		4.0%	4.7%
Continuing to mature and improve security capabilities	8.1%	6.9%	7.4%	4.9%	6.1%	5.8%	6.6%	4.5%	4.3%				
Preventing major cybersecurity incidents and losses	11.1%	8.2%	7.5%	4.9%				5.3%	4.7%	5.5%	4.3%		5.4%
Ensuring business continuity through disruptive events	7.9%	7.8%	4.0%	4.3%	4.2%	4.8%	4.0%		9.5%		5.2%	4.9%	
Maintaining a cost-effective security program	8.3%	6.8%		5.0%	5.7%	8.1%		4.6%	5.0%		5.5%	4.3%	

Source: Cisco Security Outcomes Report

Anywhere you see a blue square means the intersecting NIST capability and security resilience outcome have a statistically significant correlation. The percentages within those blue squares denote the increased likelihood of successfully achieving that outcome among organizations with the most effective implementations of that capability. In other words, participants that do a great job tracking key systems and data are almost 11% more likely to excel at containing the spread and scope of security incidents (top left square). All the others can be interpreted the same way.

As with our original security outcomes matrix for Volume 1 of this series, this chart is a Choose Your Own Adventure kind of thing. If you'd like to know how to improve specific resilience outcomes, then pick one along the lefthand side and scan across to find data-backed options for accomplishing that. If, on the other hand, you're curious how a certain activity within the Cybersecurity Framework might strengthen your organization's resilience, then pick something at the top and scan down the list of intersecting outcomes.

In that spirit, we chose our own adventure through the matrix to come up with the observations listed below. These are by no means the only takeaways, and we don't want to spoil or bias your own exploration. So if you'd rather not have our thoughts in your head, just skip to the Conclusion.

Observation 1

Know what you're defending... and what you're defending against

Yes, this is a security platitude along the lines of "just patch your systems." And yes, this concept has filled many PowerPoint decks with mention of "protecting your crown jewels" and Sun Tzu quotes. But maybe there's a legitimate reason for that.

It's hard to dismiss the data's message here. Tracking key systems and data is the #1 most effective activity overall. Identifying top cyber risk scenarios is #2. That means two activities that fall under the NIST Cybersecurity Framework Identify function may do more for improving your security resilience than functions normally associated with resilience like Detect, Respond, and Recover. Food for thought (and action!), right?

Observation 2

Cyber resilience isn't just about you

Upon reviewing the Cybersecurity Framework activities that correlate with resilience outcomes, it's hard to ignore the sense that a significant amount of an organization's success ties to external parties. Backing up your defenses with a sufficient cyber insurance policy ranks #4 overall. Managing PR during the incident response and recovery process is #5. Testing essential third-party services follows at #6, and #8 ensures those services continue to be delivered during a cyber event. Finally, coordinating response plans with external parties lands in ninth place.

So, by all means – get your own ducks in a row in preparation for unexpected, disruptive cyber events. But don't be left as a lone sitting duck when that day comes. Practical experience, along with this data, clearly demonstrates that the true extent of cyber resilience goes far beyond your own perimeter and people.

Observation 3

People and plans have a high ROI

The mention of people at the end of the last point segues into another theme that jumps out at us from the matrix above. Namely, multiple Cybersecurity Framework activities involve people or plans (which are created with people in mind).

One activity establishes that an incident response plan be created and communicated to employees. Another requires that plan to be updated regularly rather than simply gathering dust on a shelf (or a shared drive). And we've already mentioned the importance of response plans covering coordination with external parties. Of course, none of these plans are worth anything if response staff aren't adequately trained on how to carry them out.

There are a lot of technical solutions out there to help organizations improve their security resilience. But behind every single one of those solutions are people who configure, maintain, and operate them during a cyber crisis. Help your organization by helping them know what to do and how to do it.

Observation 4

It's not all about the money, but...

...mitigating financial losses from a security event is the most important resilience outcome to CISOs and organizations that have experienced a major incident in the past. It's helpful to note, therefore, that our analysis reveals that 8 of the 13 Cybersecurity Framework activities increase the chances of successfully achieving that outcome.

We won't list all of those activities – you can do that on your own and then refer to NIST documentation for additional details and implementation guidance. What we will do is emphasize that the effective activities highlighted in the matrix span governance, people, process, and technology-based controls. This corroborates the theme that minimizing losses and maximizing resilience requires much more than a one-dimensional point solution.

Conclusion

So there you have it. Are you feeling more resilient yet? Or at least like you're on the road to resilience? Building security resilience requires a lot of hard work, but it starts with a plan.

As you set up your organization to thrive no matter what comes next, we're ready to support you in developing and executing on that plan — and finding clarity in chaos. Whether you're struggling with risk assessment, ransomware, regulatory compliance, response and recovery, or other security challenges, you don't have to go it alone.

For further insights:

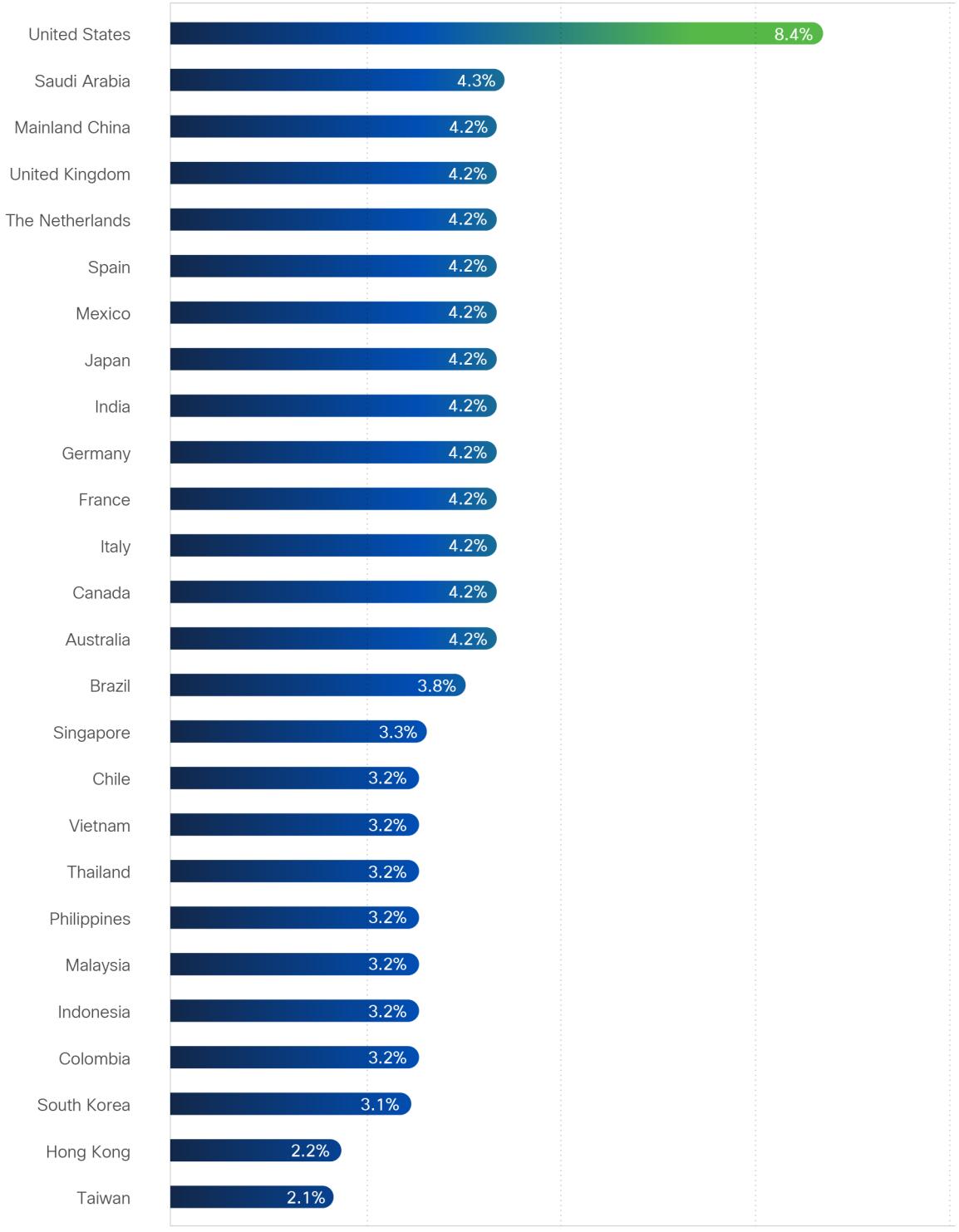
- Explore our series of data-driven, research-based studies
- Learn more about protecting your business with security resilience

About Cisco Secure

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 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.

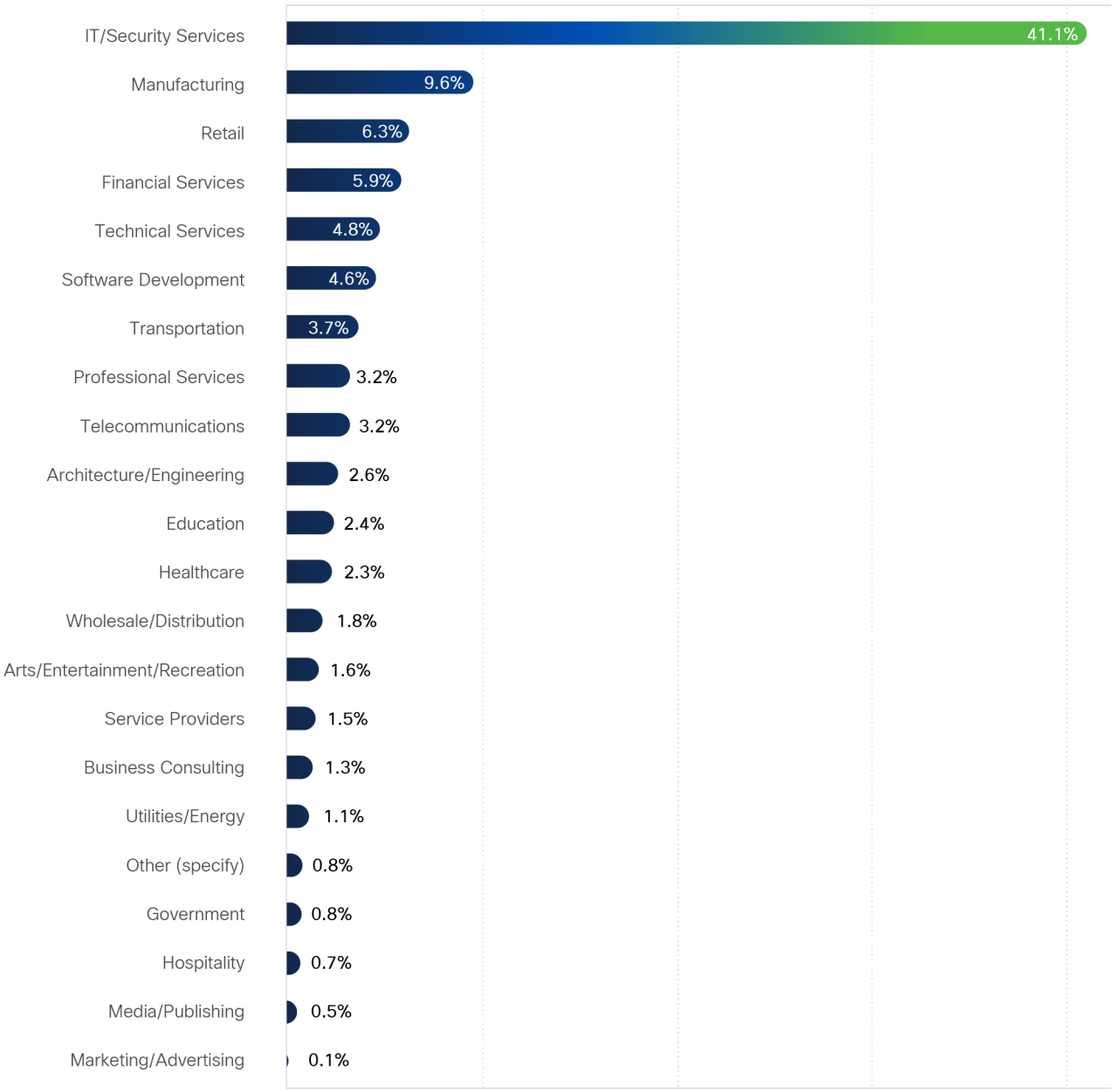
Appendix A: Participant demographics

Figure A1: Markets in which participants primarily work



Source: Cisco Security Outcomes Report

Figure A2: Industries represented by participating organizations



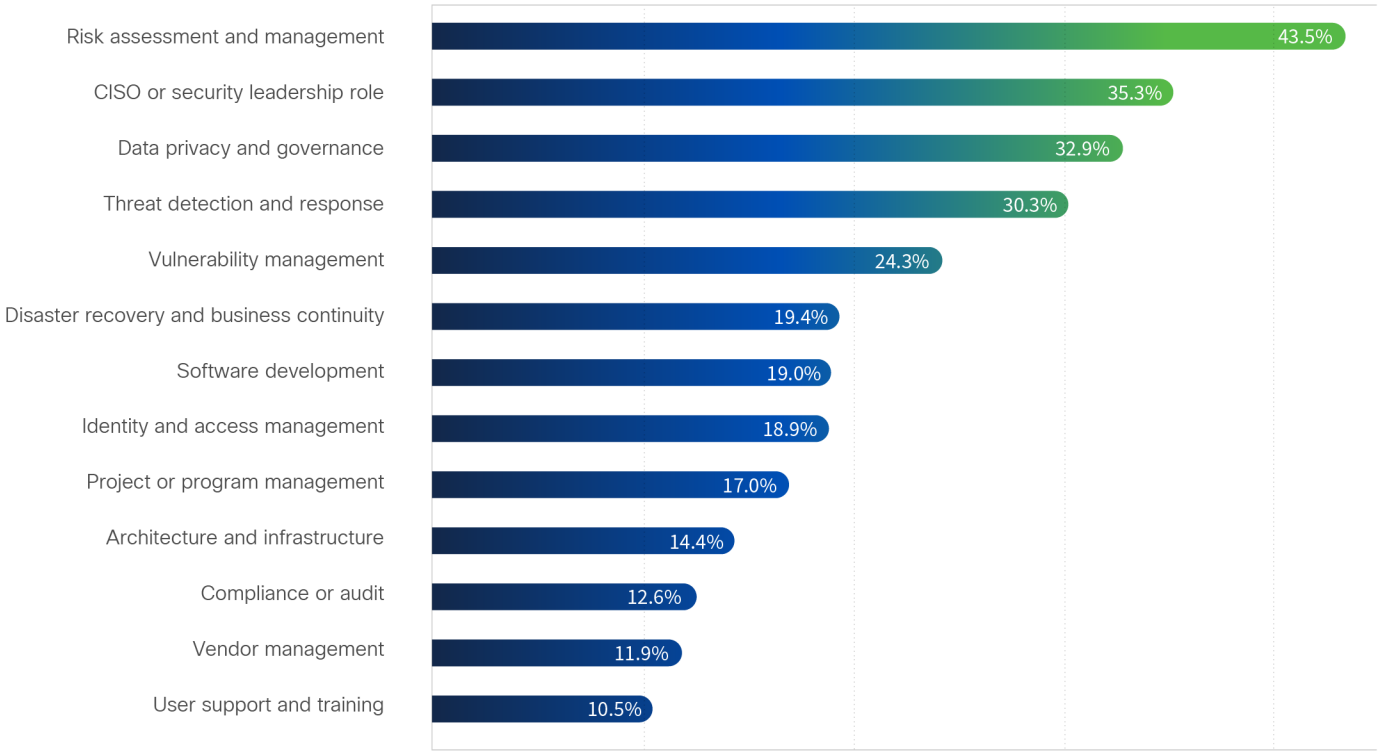
Source: Cisco Security Outcomes Report

Figure A3: Number of employees for participating organizations

Percentage of respondents

Source: Cisco Security Outcomes Report

Figure A4: Primary security role and responsibilities among respondents



Percentage of respondents

Source: Cisco Security Outcomes Report

Appendix B: Security resilience outcomes

1. **Containing the spread or scope of security incidents:** When security incidents do occur, their scope is contained by controls and processes that limit lateral movement, privilege escalation, dwell time, propagation to other departments, etc. A track record of keeping incidents in check that might otherwise have been much bigger or recent tests that validate these capabilities would be an indicator of success here.

2. **Mitigating financial losses stemming from security incidents:** When security incidents do occur, their cost is reduced through controls and processes that mitigate their extent of impact and associated losses. Examples include plans and procedures to recover quickly, limit brand damage, reduce downstream losses to other parties, avoid litigation, transfer risk through cyber insurance, etc. Hoping for the best or a strategy of "we'll deal with what may come" would be a sign of struggle.

3. **Adapting to unexpected external change events or trends:** The security program is agile and able to respond effectively to changing conditions triggered by unforeseen and uncontrollable events outside the organization. Adapting well to the sudden transition to a remote workforce during the COVID-19 pandemic and handling the subsequent trends of hybrid work and quickening digital transformation would be evidence of success.

4. **Keeping up with the demands and growth of the business:** 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 as a business roadblock or purely as a cost center by business execs, it's a sign of struggling to meet this goal.

5. **Continuing to mature and improve security capabilities:** The security program establishes goals, tracks progress, and seeks to continually improve its efficacy over time. The program may not yet be mature in all areas but should know where it most needs to improve and have a plan to get there. A stagnant security program that's falling behind modern threats or a philosophy of being "done" after the next control is implemented would be signs of struggle.

6. **Preventing major cybersecurity incidents and losses:** We expect that an organization that's highly successful in achieving this goal has not had a serious or highly impactful security incident (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 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.

7. **Ensuring business continuity through disruptive events:** System failures, network outages, and other technology disruptions have minimal impact on critical business operations. The organization is able to successfully navigate sudden and unexpected events that force extensive or rapid architectural and/or process changes.

8. **Maintaining a cost-effective security program:** Executive leaders view the security program as having good ROI. No recurring rumblings about the overly high costs of security. Low rate of shelfware purchases. Staffing is lean yet not starved. A plan among executives and security leaders to reduce the security budget without increasing risk would be a good sign of success here.

9. **Recruiting and retaining talented security personnel:** 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.

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 2022

The bridge to possible