CISCO
SECURE

Thriving as a Small or Midsize Business with a Strong Cybersecurity Strategy

SECURITY OUTCOMES

study

CISCO The bridge to possible

The 2021 Security Outcomes Study – Small and Midsize Business Edition

What makes for successful cybersecurity? Is there evidence that security investments result in measurable outcomes? How do we know what actually works and what doesn't? These are the types of burning questions guiding Cisco's 2021 Security Outcomes Study, which pulls together the experiences of over 4,800 IT, security, and privacy professionals around the world. This document is an offshoot of the larger study that focuses on small and midsize businesses (SMBs).

Defending organizations against cyber threats is tough for any business, regardless of size. But it's particularly true for SMBs because their resources are typically limited, and they must be laser focused on only making investments that will bring impactful results. The stakes are higher, and prioritizing what's most important is critical for success. Helping to identify those priorities is what this report is all about.

Read on to discover how SMBs compare to larger enterprises when it comes to security, and what key factors contributed to successful security planning in companies like yours.

Contents

Key Findings 4
About the Survey 7
Security Outcomes for SMBs 9
Overall Security Success Factors for SMBs 11
It's Good to Dream Big 14
Achieving Specific Outcomes 14
Key Success Factors for Small Businesses 15
Enabling Business 16
Managing Risk 18
Operating Efficiently 19
Resources for Successful Security in Small Businesses 20
Key Success Factors for Midsize Businesses 23
Enabling Business 24
Managing Risk 26
Operating Efficiently 27
Resources for Successful Security in Midsize Businesses 30

Key Findings

If you take one thing from this study, it should be that good things do come in small packages.

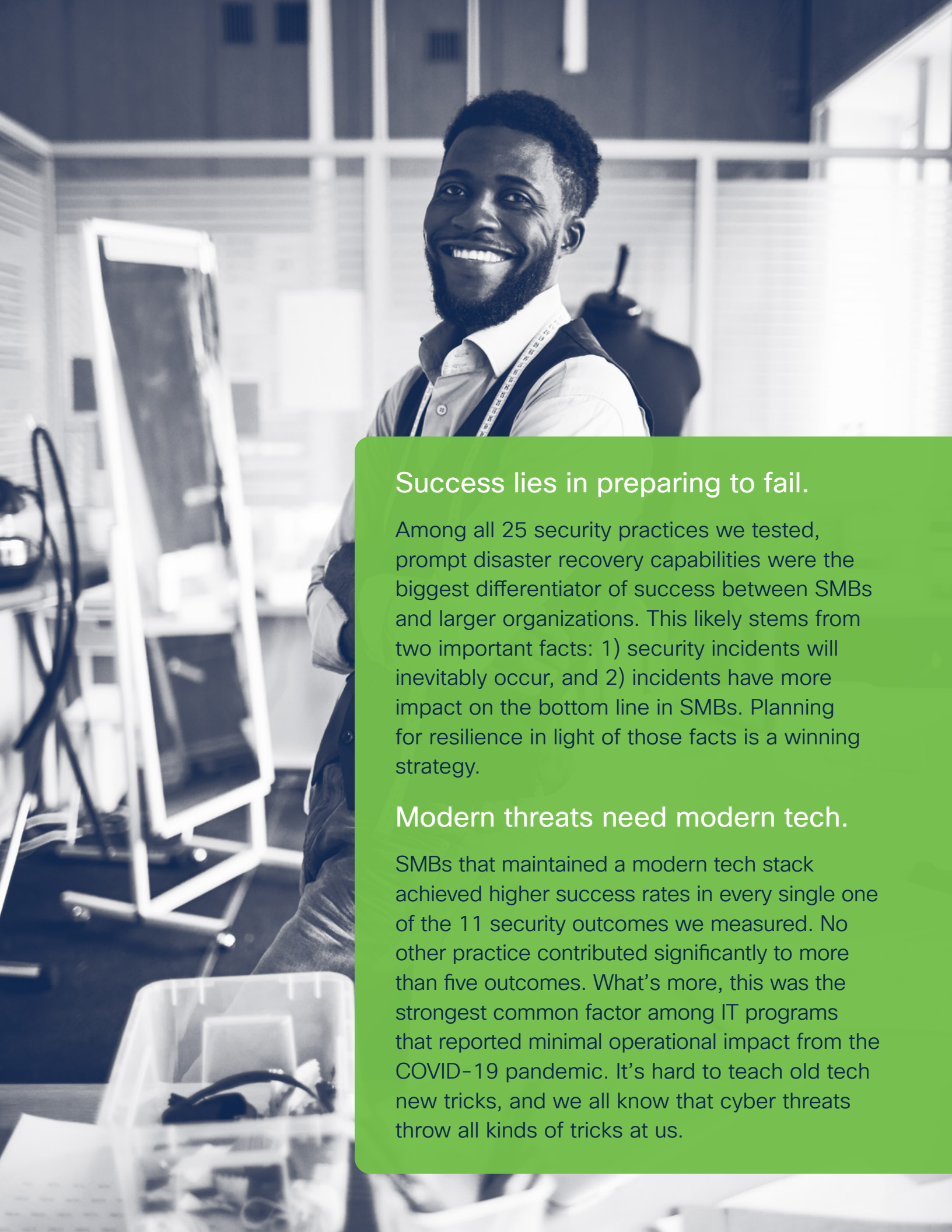
From vendors to practitioners, the cybersecurity industry has a bad habit of assuming bigger means better. But this study makes a convincing case that your company's smaller size doesn't hinder the possibility of big wins when it comes to building successful approaches to security. Here's a few quick examples of what we learned from the collective input of 850+ of your SMB peers.

SMB security is taking care of business. Would you believe that SMBs can teach enterprises a thing or two about effective security?

You should, because the data shows that small and mid-market teams are more successful than their larger counterparts in building security approaches that enable the business! This study drives home the concept that security and the overall business share an integral relationship in SMBs.

Don’t lose sight of your priorities.

Focus is critical to executing any strategy, but that’s especially true when resources are limited. Small and midsize companies that said they had a sound strategy in place to guide security initiatives were significantly more likely to report successful outcomes. Furthermore, having a good security strategy was comparatively more important for SMBs than larger enterprises.



Success lies in preparing to fail.

Among all 25 security practices we tested, prompt disaster recovery capabilities were the biggest differentiator of success between SMBs and larger organizations. This likely stems from two important facts: 1) security incidents will inevitably occur, and 2) incidents have more impact on the bottom line in SMBs. Planning for resilience in light of those facts is a winning strategy.

Modern threats need modern tech.

SMBs that maintained a modern tech stack achieved higher success rates in every single one of the 11 security outcomes we measured. No other practice contributed significantly to more than five outcomes. What's more, this was the strongest common factor among IT programs that reported minimal operational impact from the COVID-19 pandemic. It's hard to teach old tech new tricks, and we all know that cyber threats throw all kinds of tricks at us.

About the Survey

Over 4,800 active IT, security, and privacy professionals from around the world participated in our 2021 Security Outcomes Study. Of those participants, 857 represented SMBs, and their responses form the basis of this follow-up report.

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. About 18% of respondents represented SMBs.	The Cyentia Institute independently analyzed the survey data on behalf of Cisco and generated all results presented in this study.

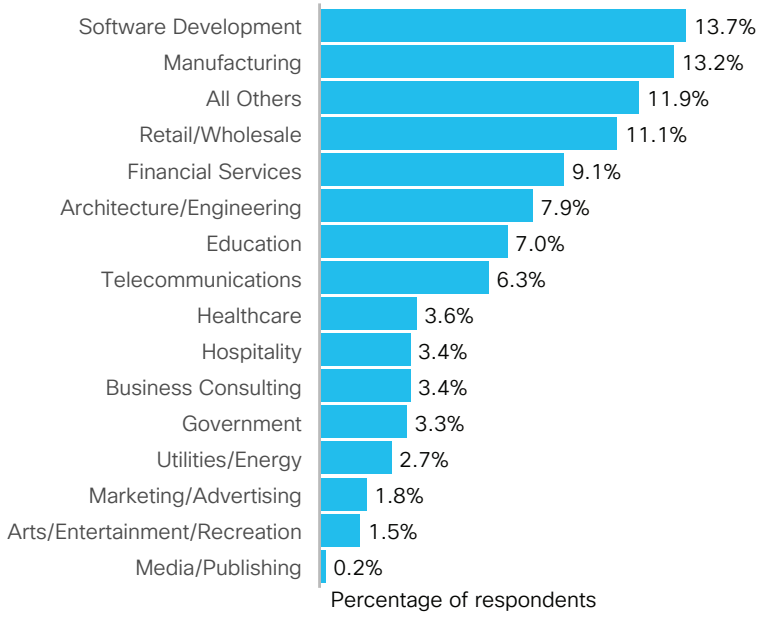
Approach

- We asked respondents about their organization's adherence to 25 security practices spanning governance, strategy, spending, architecture, and operations.
- We then asked about each company's level of success across roughly a dozen high-level security objectives or outcomes organized into three main categories: Enabling Business, Managing Risk, and Operating Efficiently.

The definition of what constitutes a "small" or "medium" business differs around the world, so we've adopted the following definitions for use in this report:

- Small: 50 to 249 employees[1] (8.5% of respondents; n=409)
- Medium: 250 to 499 employees (9.3% of respondents; n=448)
- Large: 500 to 999 employees (32% of respondents)
- Enterprise: 1,000+ employees (50% of respondents)

Figure 1: Industries represented among participating companies



Source: Cisco 2021 Security Outcomes Study

[1] Note that firms with less than 50 employees were not included in the target sample for this study.

From that, it's clear that the 2021 Security Outcomes Study skews toward larger organizations. SMBs collectively represent only about 18% of the sample, but keep in mind that this percentage tallies to 857 respondents. (A little over 400 of those hail from small businesses, and about 450 land in the medium category.) The uneven representation makes it hard to hear what those smaller (yet important) firms have to say, which is precisely why we're producing this supplemental report focused on the SMB audience.

Another thing to keep in mind is the types of SMBs that participated. An industry breakdown is given in Figure 1. It may help to refer to this as you consider various findings of this study and how they apply to your company.

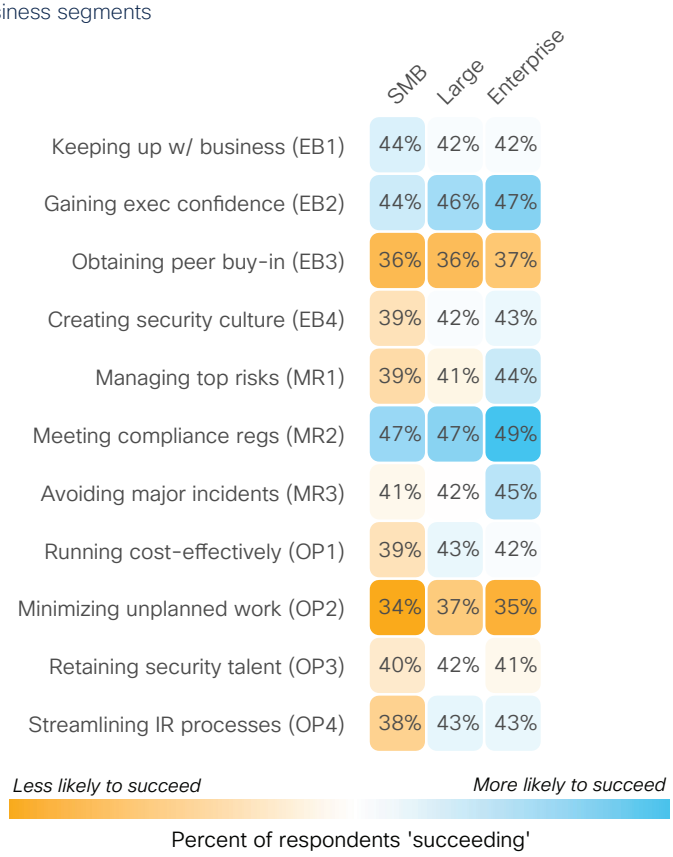
"It doesn't matter whether you are a multinational investment bank or a small 130-person operation like ours—going forward, every financial institution has to adhere to the same rules and compliance standards. Cisco Secure simplifies the work of our security experts and network engineers."

Steve Erzberger, CTO at Frankfurter Bankgesellschaft (Schweiz) AG

Security Outcomes for SMBs

Given the title of this study, it makes sense that we begin with the end in mind—security outcomes. We asked respondents to rate their organization's level of success across 11 diverse, high-level security outcomes that companies generally seek to achieve. We organized these outcomes under three main objectives: Enabling Business, Managing Risk, and Operating Efficiently.[2] Identifying security practices that increase the chance of achieving these outcomes is the main goal of this study. But let's first see how SMBs fare relative to their larger brethren across these objectives.

Figure 2: Comparison of reported success rates for each security outcome among business segments



Source: Cisco 2021 Security Outcomes Study

The percentages in Figure 2 indicate the proportion of organizations in each size segment rating their companies as highly successful for each outcome. So, for example, 44% of SMBs say security is successfully keeping up with the business within their organization (upper-left). We'll come back to that little factoid in a moment.

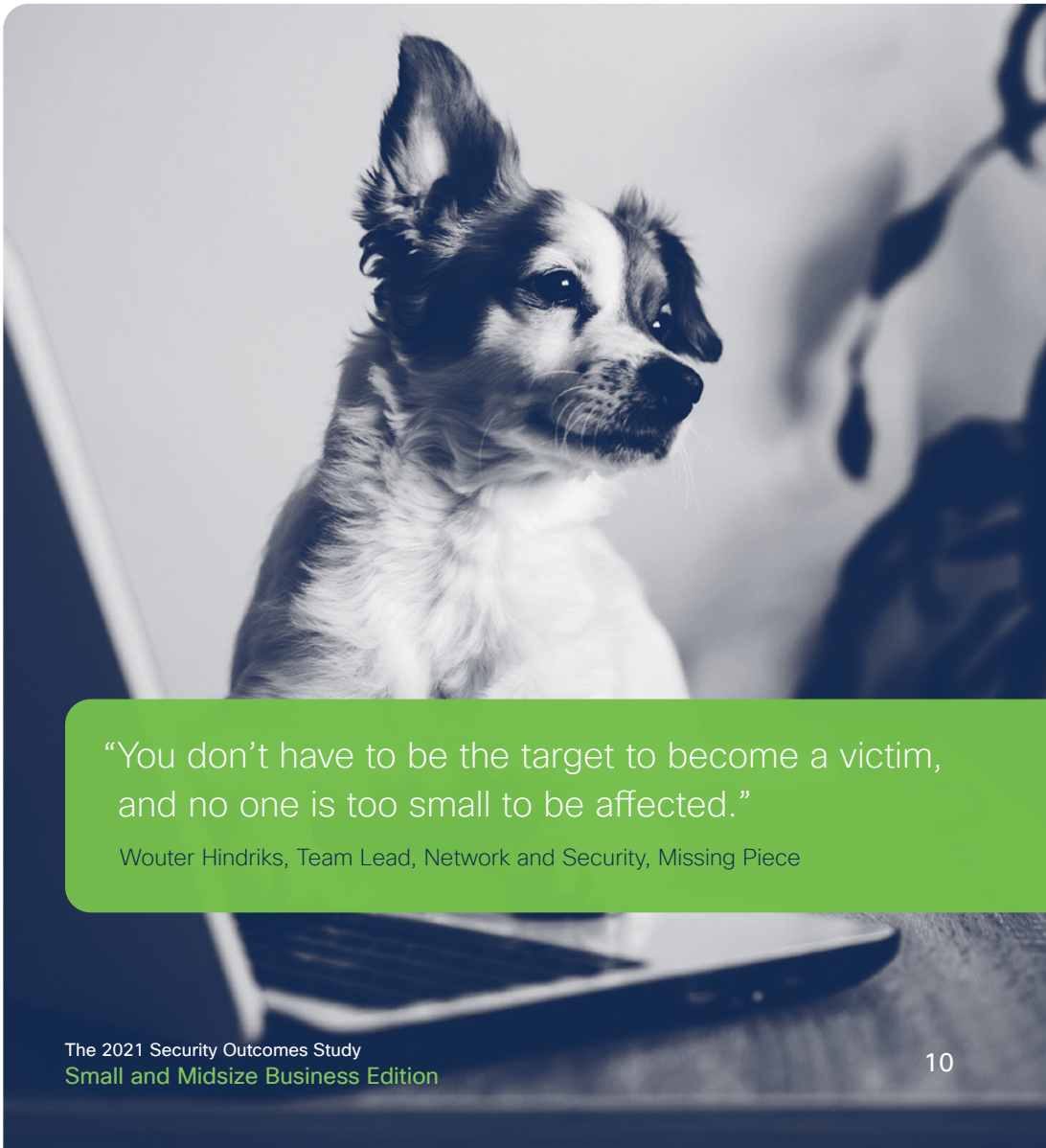
Security functions of all sizes appear most successful in meeting compliance regulations and gaining the confidence of executives. Minimizing unplanned work and obtaining buy-in from non-security peers, on the other hand, look to be more of a struggle.

[2] See the 2021 Security Outcomes Study: Appendix B: Full List of Security Outcomes for the full text for each outcome along with the explanation and example evidence given to respondents to guide the rating of their company's success.

In terms of company size comparisons, Figure 2 reveals generally higher success rates among larger organizations. We suspect this fits the expectations of many, since the resources available to pursue objectives often grow along with the size of the organization. But as the saying goes, more money means more problems, and that may explain why the differences among size groups aren't as large as some might expect.

That point brings us back to the 44% factoid mentioned above. SMBs actually outperform their bigger counterparts in terms of security keeping up with the business. This could reflect fewer degrees of separation between business and IT leaders in smaller companies. In some cases–tech startups, for example–those groups can be one and the same. And even when that's not the case, "less red tape" and "I know who to call" are often cited as enablers of getting things done in SMBs. Those same reasons also come into play when getting security things done to help the business.

Overall, we think SMBs should be encouraged by the results shown in Figure 2. Your smaller size doesn't prevent big wins when it comes to building successful approaches to security. We'll see what tips the data has for accomplishing that in the next section.



"You don't have to be the target to become a victim, and no one is too small to be affected."

Wouter Hindriks, Team Lead, Network and Security, Missing Piece

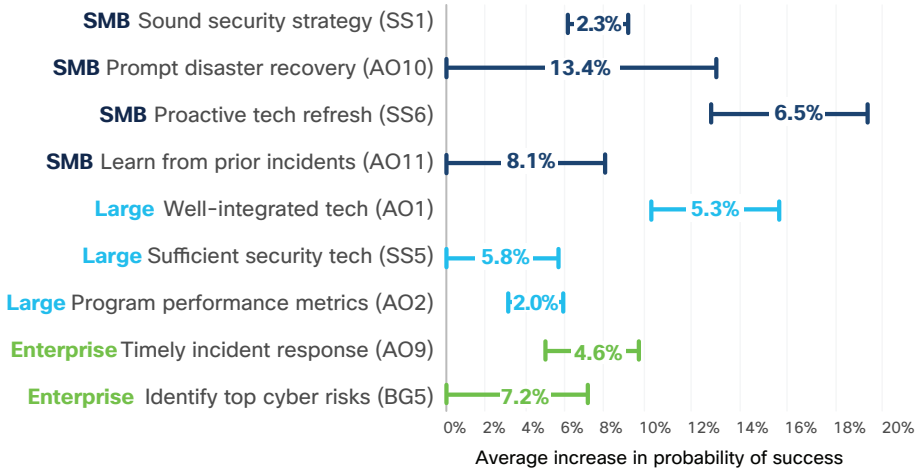
Overall Security Success Factors for SMBs

In addition to the 11 outcomes from Figure 2, we asked study participants how well their organizations followed a set of 25 common security practices.[3] We decided not to display implementation levels for all these practices because: 1) it makes for a really big chart, and 2) our focus is on outcomes in this study. But for those keeping score, the lead of larger firms over SMBs tends to be more pronounced among practices than for outcomes. That seems like bad news, but you could spin it like this: SMBs get more bang (successful outcomes) for their buck (investment in security practices).

With the preliminaries out of the way, we can now get to the fun part. We conducted multivariate analysis on the response data to measure which security practices correlate most strongly with successfully achieving each outcome. In other words, what are the key success factors for cybersecurity in SMBs? Let's first answer that question by focusing on overall success across all outcomes. We'll get to practices that drive specific outcomes for small and midsize businesses in the sections that follow.

Figure 3 identifies practices that, according to the data, offer the biggest boost for building a successful security program in each business segment. The starting point for each line marks the average success rate across all study participants. The endpoint of the line indicates how much more impact that factor has on success rates among companies in a particular segment.

Figure 3: Top security success differentiators for SMB, large, and enterprise segments



Source: Cisco 2021 Security Outcomes Study

So, for instance, organizations that report having a sound security strategy were on average 6.1% more likely to report a highly successful approach to security. A strong strategy among SMBs, by comparison, resulted in an average 8.4% lift to success rates, for a difference of 2.3%. Capabilities ensuring prompt disaster recovery didn't

[3] See Appendix C in the 2021 Security Outcomes Study for the full text and listing of these practices.

significantly contribute to overall success across all respondents, but made a big difference (+13.4% on average) for SMBs.[4] And so on.

Every reader will likely concoct their own recipe for SMB security success from the ingredients in Figure 3, and we encourage that very thing. For our part, we see three main themes reflected in the data: **focus, resilience,** and **modernization.** We'll take those in turn in the paragraphs that follow.

Focus is a critical component of any strategy—especially for SMBs, where prioritizing initiatives is paramount. Without it, companies lose sight of what matters most, cannot execute effectively, waste precious resources, and eventually lose their way. An 8.4% bump in success rates for SMBs with a solid strategy may not seem like much, but every little bit helps. The fact that it's on the list when 21 other practices showed no significant difference between SMBs and all respondents means it shouldn't be ignored. Plus, the nature of strategy is such that its indirect effects on other security practices may outweigh its direct effect.

> "My previous experiences with massive companies is they can be quite difficult, even arrogant, to work with if you're a small business. We haven't felt that with Cisco in the slightest. In fact, they've made specific efforts to help our small business remain competitive."
>
> Charl Tintinger, CTO at Gigaclear

IT and security functions have faced more than their fair share of challenges lately, which is probably why the 2021 RSA Conference (the largest security conference in the world) has chosen "Resilience" as its core theme. As stated in the explanation behind that choice, "*Cyber threats are relentless and our solutions must quickly recover from whatever adversity they throw at us.*" That's exactly what prompt disaster recovery capabilities are designed to do, and Figure 3 shows that they translate into big wins for SMB cybersecurity.

Why? Well, an independent study of more than 50,000 cyber loss events over a 10-year period may offer a clue.[5] The analysis found that while SMBs don't experience security incidents as often as their enterprise peers, the relative impact to their bottom line is much larger when they do occur. *"A $100B enterprise that experiences a typical cyber event ($292K) should expect a cost that represents 0.000003% of annual revenues. A mom and pop shop that brings in $100K per year, on the other hand, will likely lose one-quarter of their earnings ($24K) or more."* A swift recovery, therefore, becomes critical to business resiliency.

Applying learnings from prior security incidents in Figure 3 bridges the focus and resilience themes. No company, large or small, wants to suffer major breaches or disruptions, but the lessons gleaned from them can help turn lemons into lemonade. And these lessons don't need to be drawn only from your own experiences; what's happened to partners, peers, and other organizations can be instructive too.

[4] The 0% starting point shown here and in other similar charts indicates that the practice did not have a statistically significant effect on the probability of success across all respondents.

[5] Information Risk Insights Study 20/20 (Cyentia Institute)

Successful companies use these lessons to focus their security strategy, shore up defenses, and bolster recovery capabilities. Failure can be a good teacher, in business as well as in cybersecurity.

And that brings us to our third theme—modernization. It's true that the label 'proactive tech refresh' doesn't include the word 'modernization,' but the text presented to survey respondents gets at that theme. "*My organization has a proactive tech refresh strategy of frequent upgrades to best available IT and security technologies.*" Implementing that strategy will look different for every organization, ranging from traditional hardware and software refreshes to the continual upgrades provided through Software-as-a-Service (SaaS) solutions and Managed Service Providers (MSPs).

For many SMBs, those latter options (SaaS and MSPs) offer a cost-effective way of maintaining a modern tech stack. Scalability, agility, and efficiency are often cited as the drivers of cloud and SaaS migration, but Figure 3 makes the case for adding security to that list for SMBs. With that model, many critical security responsibilities like software updates, access control, threat monitoring, and incident response shift to the service provider, and are thus rolled into the recurring cost of the service.

Furthermore, we can connect this theme of modernization to that of resiliency in the wake of unexpected events. We asked study participants about how the COVID-19 pandemic and subsequent transition to remote work affected their organizations. Care to guess which practice stood out above all others among companies reporting minimal impact to operations and cyber risk posture? That's right—proactive tech refresh.

Bottom line: Modern cyber threats require modern cyber tech. That may sound cost-prohibitive for SMB budgets, but SaaS can offer a more attainable route to experiencing the security benefits of the latest technologies.

It's Good to Dream Big

Given the focus of this study on SMBs, we've thus far ignored key success factors for larger organizations. But SMBs aspiring to grow into those shoes might do well to consider what contributes to success for big companies.

Figure 3 reaffirms that the importance of having sufficient security technologies to support that strategy grows along with the business. So too does the need to ensure that those technologies integrate well together. Measuring security performance through metrics rounds out the list of differentiators for large companies.

Moving to enterprise-class organizations, we see that the timely identification of top cyber risks and swift incident response (IR) capabilities become critical. We suspect that's because the attention of threat actors, size of the attack surface, and frequency of incidents all tend to scale with the size and profile of the company. The transition from being a target of opportunity to a target of choice radically changes the game, and these practices will help even the score when you're ready to play at that level.

Achieving Specific Outcomes

Everybody wants better cybersecurity overall, but sometimes it's desirable or necessary to pursue specific outcomes. Perhaps you looked at the list of outcomes in Figure 2 and thought, "I wonder what factors would help us achieve *that* outcome?" If so, then the next sections are for you.

Because most readers of this report represent either small or midsize businesses, we've split out dedicated sections for each below. You're free to read our analysis and recommendations for both business segments, of course. We'll discuss success factors for small companies first, and then move to midsize businesses right after that.

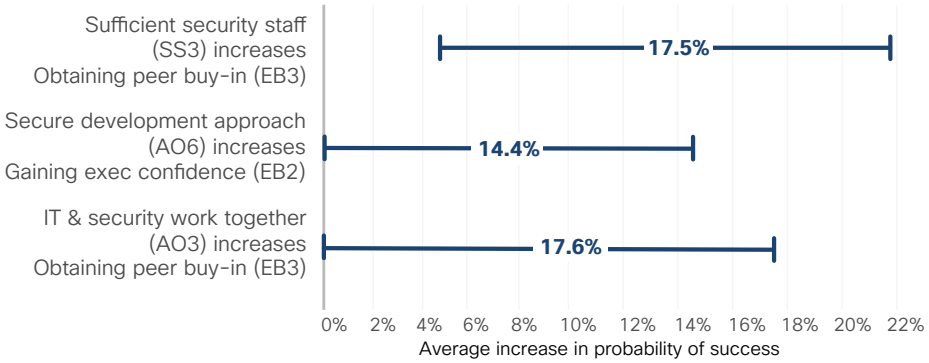
Key Success Factors for Small Businesses

We mentioned earlier that outcomes are organized into three categories: Enabling Business, Managing Risk, and Operating Efficiently. You'll find those same headings below, along with charts that identify security practices that correlate most strongly with small companies successfully achieving each objective. Keep in mind that our 2021 Security Outcomes Study Appendices give full text versions of all the shortened labels for practices and outcomes in the figures that follow.

Enabling Business

As the label implies, this objective focuses on security's mission of supporting and fostering business activities. The outcomes in this category recognize that security doesn't exist for security's sake; it serves the business. Figure 4 shows the top three differentiators for small companies successfully achieving outcomes under this objective. As a reminder, the starting point for each line marks the average success rate across all study participants. The endpoint of the line indicates how much more impact that factor has on success rates among small businesses.

Figure 4: Top three security differentiators for enabling small businesses



Source: Cisco 2021 Security Outcomes Study

The strongest practice-outcome correlation in this category is that having sufficient security staff results in improved buy-in for security from peers across the company. IT and security functions working collaboratively together also contributes substantially to that same outcome. Given that many small businesses don't have dedicated security personnel, that message might be rather unwelcome for some readers. But "sufficient" and "together" are the operative words here, not "dedicated." Quite a few companies participating in this study didn't have *dedicated* security staff, yet still reported successful approaches to security by having sufficient, collaborative personnel.

That said, there will inevitably come a time in the life of growing organizations when the security beanie of the person wearing many IT hats will begin to get a little snug. And when it's not swapped for a larger one, or those hats aren't donned equitably on multiple heads, it begins to impede the business. And Figure 4 suggests that one of the first areas that may become apparent is losing buy-in from other people or groups in the organization. Perhaps that's because IT can't support that new business initiative. Maybe it's because technology or security complications stifle productivity. Whatever the reason, these results emphasize the importance of adequate security talent (whether shared or dedicated) in serving the business and its mission.

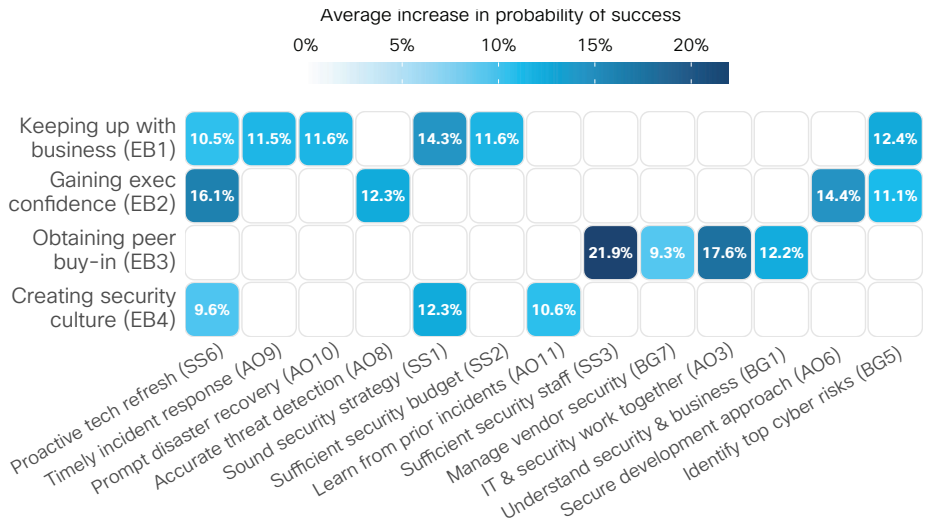
The other major difference maker from Figure 4 links secure software development practices with gaining the confidence of executives. Seems odd, but the answer to that riddle lies in the fact that software development firms were the largest industry represented among SMBs in this study. Thus, producing robust, secure code is intrinsically linked to the balance sheet of those companies (and probably executives' personal bank accounts).

But you don't have to be a software shop to put this principle into action. Any time security becomes essential to the business, it gains a higher profile at the top. Be ready to build solutions rather than obstacles.

That wraps up the top three security practice and outcome differentiators for enabling small businesses, but we suspect many will wish to see what other options are available to them. To that end, Figure 5 shows all practices that significantly correlate with any of the four outcomes under this objective. And as you can plainly see, the list of success factors is much longer than three.

The values in Figure 5 and those like it that follow denote the average increase in the likelihood of success for a given outcome when organizations report strong adherence to a certain practice. The shading corresponds to the strength of correlation between the practice and outcome. Combinations with no shading or value indicate that our analysis did not find a statistically significant correlation. That doesn't mean the practice isn't useful; it just means we found no convincing evidence that it leads to greater success for that outcome.

Figure 5: Correlation of security practices and outcomes for enabling small businesses



Source: Cisco 2021 Security Outcomes Study

The first thing to note regarding Figure 5 is that each outcome has multiple ways in which security practices contribute to enabling business. That's good news because it suggests that small businesses can customize a route to success that suits their needs and capabilities.

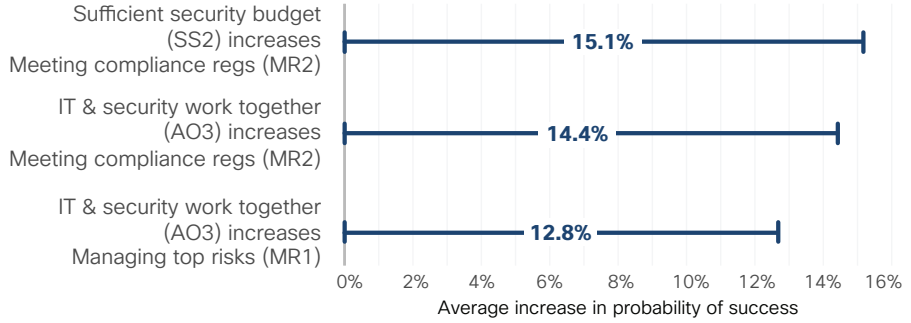
Beyond that, we again see the essential role that modern technology plays in building secure and successful small businesses. Keeping architecture and services current helps security serve the needs of the business, gains the confidence of executives, and promotes a stronger security culture. Wrapping that tech stack with a sound strategy and a strong understanding of the threats that seek to exploit it also nets wins on multiple fronts.

Feel free to spend as much time as you like with Figure 5. Charts like this offer a kind of "choose your own adventure" twist on security planning. We hope you'll use it to help get to where you want to go.

Managing Risk

Managing risk is what most people think of when asked about security'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 small companies manage cyber risk. Figure 6 highlights the practice-outcome combos that exhibit the strongest differentiators for small businesses when it comes to this objective.

Figure 6: Top three security differentiators for managing risk in small businesses

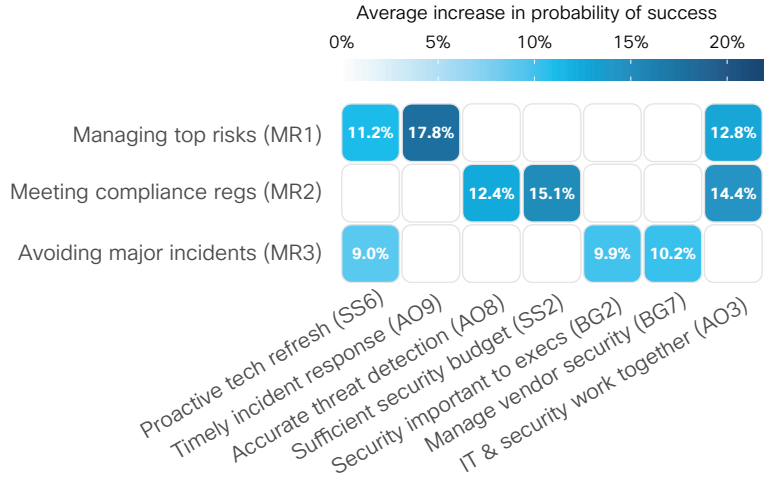


Source: Cisco 2021 Security Outcomes Study

Compliance has long been a driver for security adoption in organizations of all sizes. However, we've heard from clients and experts that it's becoming an even bigger issue for small businesses. As more standards emerge and regulations increase, the minimal requirements bar keeps getting notched up. And while most large organizations need to vault well over that bar, that's not always the case for smaller companies.

The data behind Figure 6 posits that budgets and collaboration increase the ability of small businesses in meeting their compliance obligations. The 'more budget, more compliant' association is hardly surprising, but it still might be a useful datapoint for leadership if resources are too scarce, yet regulatory pressures abound.

Figure 7: Correlation of security practices and outcomes for managing risk in small businesses



Source: Cisco 2021 Security Outcomes Study

As mentioned in the previous section, the concept of collaboration between IT and security functions can be sized up or down based on the company in question. For small businesses, this could go back to the person wearing multiple hats, of which IT and security are merely two. In that situation, this suggests that the person has sufficient time and training to do both things well. As companies grow, that could transition into two separate people who stay in close contact and consult one another on projects. However that looks, Figure 6 says keeping IT and security in close cahoots is a key differentiator for managing top cyber risks in small businesses.

Additional risk management practices that hold promise for small businesses can be found in Figure 7. Proactive tech refresh enters the picture once again, improving the chances of mitigating critical cyber risks and avoiding major incidents. Score another for the 'modern threats require modern tech' theme. We're probably seeing the benefits of SaaS again here. The vendor or MSP is fixing vulnerabilities, monitoring threats, responding to incidents, and so on as part of predictable, fixed costs.

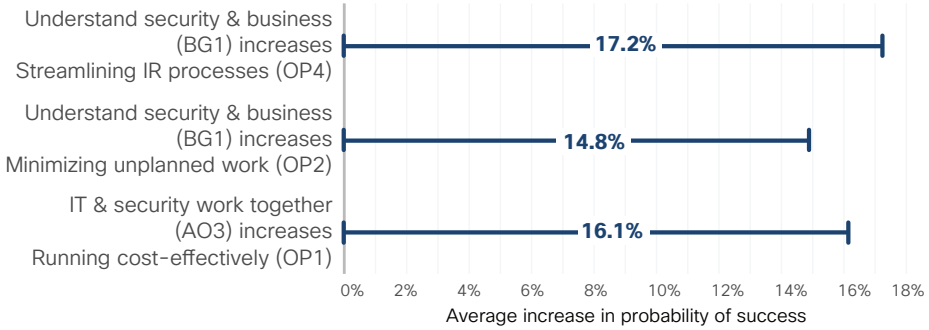
Speaking of responding to incidents, IR capabilities yield the highest correlation in Figure 7. Managing top risks isn't just about keeping bad things from happening; it's about minimizing their impact and maintaining resiliency when they do occur.

Supply chain security has received a lot of attention lately due to some high-profile breaches, so it's worth noting that managing the security of vendors contributes to avoiding major incidents. Small businesses form the building blocks of large supply chains, and research shows that they're more likely to be on the receiving end of cyber events propagating across those inter-organizational relationships.[6] Figure 7 gives evidence why risk-averse small businesses should evaluate the security of their key partners.

Operating Efficiently

Beyond enabling business and managing risk, the ability to operate efficiently often sets great IT programs apart from the good ones. This last set of outcomes addresses cost-effectiveness, executing strategy, talent management, and incident response processes. Important stuff, especially for small businesses.

Figure 8: Top three security differentiators for operating efficiently in small businesses



Source: Cisco 2021 Security Outcomes Study

Figure 8 brings us back to the notion that security and the business share an integral relationship in small companies. According to our analysis, understanding how security initiatives support business imperatives streamlines incident response and

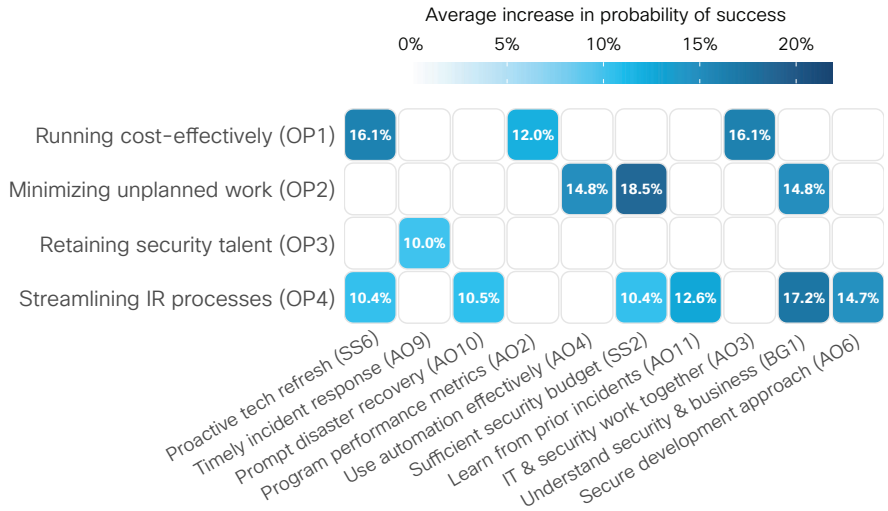
[6] Ripples Across the Risk Surface (RiskRecon, Cyentia Institute)

minimizes unplanned work. This presents an opportunity to make standard security training more personal and impactful. IT staff should know how the business works and how their responsibilities fit into its mission.

And that brings us back to IT and security working together. If it seems like the conversation keeps getting pulled back in this direction, you're absolutely right. It's the only practice that makes the top three differentiators for each of the major security objectives in this small business section. Regardless of how many people comprise IT and security functions, frictions and factions between them create inefficiencies. Teamwork fosters cost efficiency—especially in a small company.

As we've done in prior sections, Figure 9 broadens the list of data-backed security practices in this category beyond the top three differentiators for small businesses. Sufficient security budget, proactive tech refresh, and ensuring staff understand security in the context of the business are all multi-outcome benefactors.

Figure 9: Correlation of security practices and outcomes for operating efficiently in small businesses



Source: Cisco 2021 Security Outcomes Study

Proactive tech refresh is a familiar success factor by this point. Figure 9 links it to cost-effective security approaches and streamlined incident response. Yes, modernizing your tech stack comes at a cost, whether hardware, software, or SaaS. But we see evidence here that the investment helps pay for itself through other benefits. A poor response to major security incidents can blow an IT budget faster than just about anything else.

Pursuant to that topic, sufficient security budgets and minimizing unplanned work notch the strongest correlation. Companies that have the resources they need don't have to constantly abandon or alter plans, allowing them to get things done.

Small Businesses

Cisco Small Business Security Resource Center

Cisco Small Business Free Trials and Promotions

Cisco Designed Secure Remote Work Offer

For the full text for each outcome and security practice, along with the explanation and example evidence given to respondents to guide the rating of their programs' success, see: **Appendix B and C of the 2021 Security Outcomes Study.**

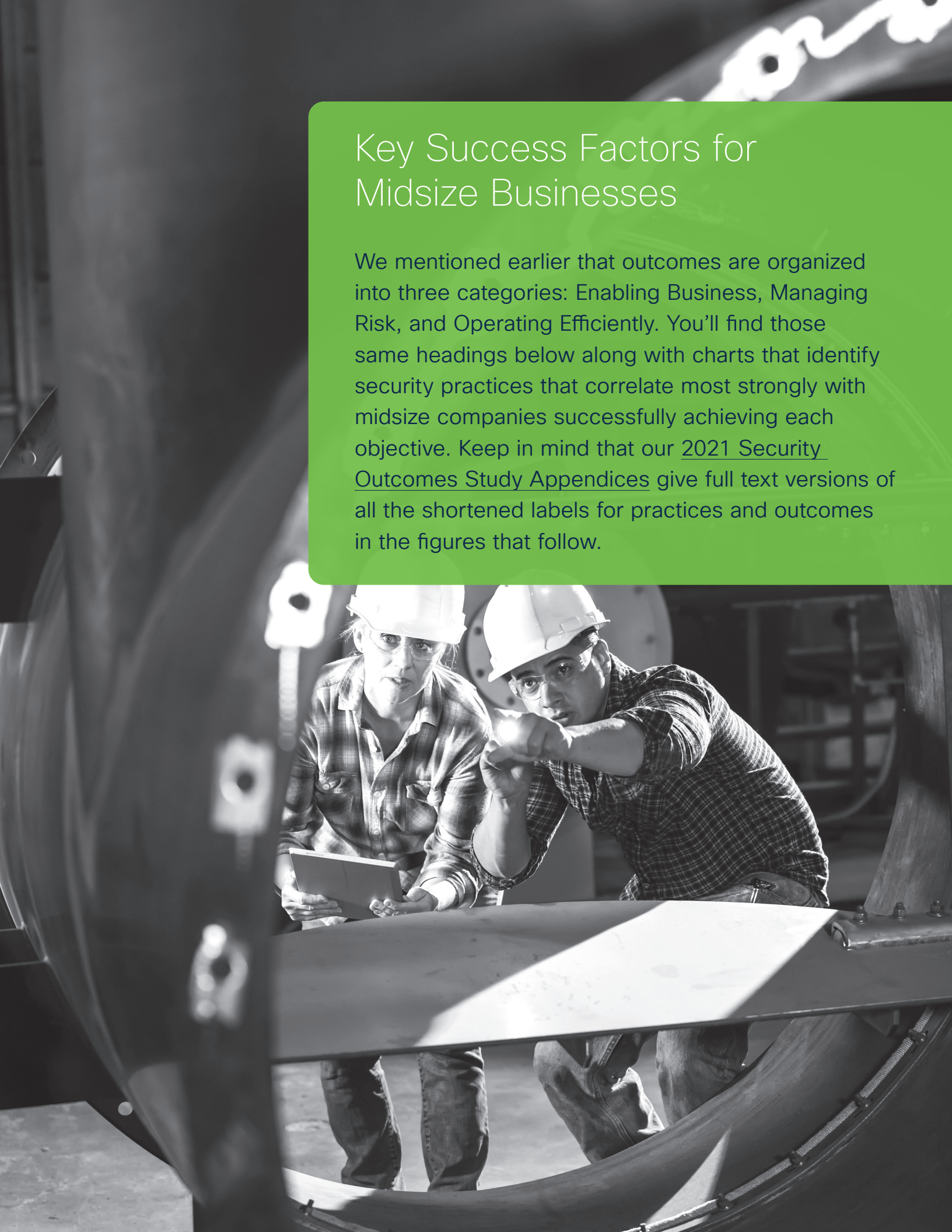
"Have you ever tried to resolve a technical issue and felt you were getting a sales pitch instead of an answer? I've often experienced that with other vendors, but Cisco and SVA act as partners who have Strenge's best interests in mind."

Frank Bettenworth, CIO, Strenge GmbH & Co. KG

Photos courtesy of Strenge GmbH & Co. KG

Key Success Factors for Midsize Businesses

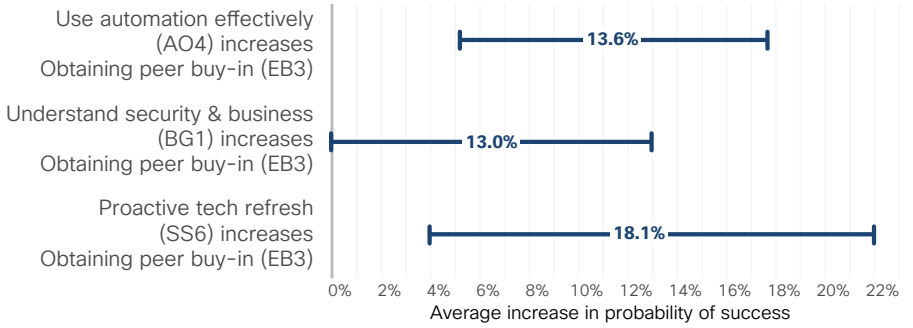
We mentioned earlier that outcomes are organized into three categories: Enabling Business, Managing Risk, and Operating Efficiently. You'll find those same headings below along with charts that identify security practices that correlate most strongly with midsize companies successfully achieving each objective. Keep in mind that our 2021 Security Outcomes Study Appendices give full text versions of all the shortened labels for practices and outcomes in the figures that follow.



Enabling Business

As the label implies, this objective focuses on security's mission of supporting and fostering business activities. The outcomes in this category recognize that security doesn't exist for security's sake; it serves the business. Figure 10 shows the top three differentiators for midsize companies achieving outcomes under this objective. As a reminder, the starting point for each line marks the average success rate across all study participants. The endpoint of the line indicates how much more impact that factor has on success rates among midsize businesses.

Figure 10: Top three security differentiators for enabling business in midsize companies



Source: Cisco 2021 Security Outcomes Study

Given that all three of the top security differentiators for enabling business in midsize organizations tie to the outcome of obtaining peer buy-in, we should clarify what that entails. Example evidence given to survey respondents to help them evaluate this outcome includes: 1) IT enlisting other groups to build a cooperative defense, 2) strong cross-organizational communication, and 3) a fair sense of "give and take" among coworkers for the greater good. Conversely, a culture of inter-group complaints and contention is a sign of struggling to meet this goal.

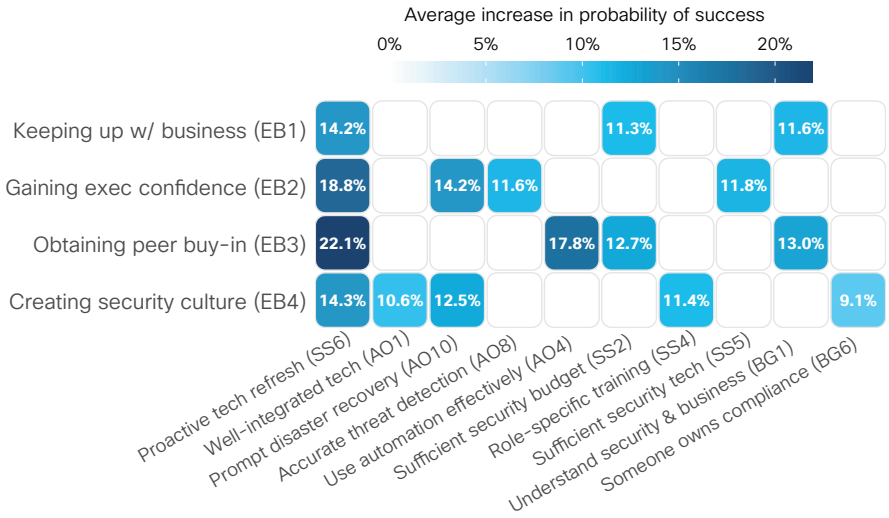
With that context, the link between automation and obtaining peer buy-in established by Figure 10 makes more sense. As midsize businesses grow and mature, IT processes become increasingly interwoven throughout multiple groups. Streamlining those processes through automation helps ensure things don't bottleneck or break somewhere in the middle of it all, and that everyone can keep doing what they need to do instead of stopping to troubleshoot.

The data also reinforces the concept that security and the business share an integral relationship in midsize companies. A better understanding of security's role in the larger mission improves buy-in from peers across the company and helps security initiatives keep pace with evolving business imperatives (see Figure 11). We think this presents an opportunity to make standard (and often dull) security training more personal and impactful. IT staff should know how the business works and how their responsibilities fit into its mission.

Last but not least, Figure 10 highlights the essential role that modern technology plays in building secure and successful midsize businesses. Keeping technology current (often through SaaS, MSPs, etc.) helps foster buy-in from peers and, as you'll see from Figure 11, serves the needs of the business, gains the confidence of executives, and promotes a stronger security culture. That's an impressive list of accomplishments if you ask us.

The values in Figure 11 and those like it that follow denote the average increase in the likelihood of success for a given outcome when organizations report strong adherence to a certain practice. The shading corresponds to the strength of correlation between the practice and outcome. Combinations with no shading or value indicate that our analysis did not find a statistically significant correlation. That doesn't mean the practice isn't useful; it just means we found no convincing evidence that it leads to greater success for that outcome.

Figure 11: Correlation of security practices and outcomes for enabling business in midsize companies



Source: Cisco 2021 Security Outcomes Study

That wraps up the top three security practice and outcome differentiators for enabling midsize businesses, but we suspect many will wish to see what other options are available to them. To that end, Figure 11 shows all practices that significantly correlate with any of the four outcomes under this objective. And as you can plainly see, the list of success factors is much longer than three.

The first thing to note regarding Figure 11 is that each outcome has multiple ways in which security practices contribute to enabling business. That's good news because it suggests that midsize businesses can customize a route to success that suits their needs and capabilities.

As for specific success factors from Figure 11, companies with prompt disaster recovery capabilities report greater confidence from executives and a better overall culture of security. Reassurance that the business will survive—perhaps even thrive—in the face of major adverse events eases concerns at the top and fosters shared purpose at all levels.

Sufficient budgets help IT keep up with the changing security needs of the business. They also earn buy-in from peers, probably because IT isn't borrowing resources from other departments or being a recurring roadblock to progress. Not every midsize company has a dedicated security budget, so this message might be

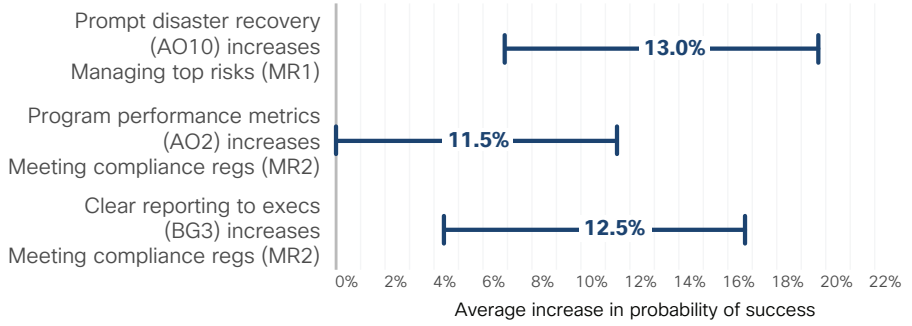
rather unwelcome for some readers. But “sufficient” is the operative word here, not “dedicated” or “unlimited.” This might be a good datapoint to put in front of leadership if resources are scarce, yet the business needs to move fast.

Feel free to spend as much time as you like with Figure 11. Charts like this offer a kind of “choose your own adventure” twist on security planning. We hope you’ll use it to help get to where you want to go.

Managing Risk

Managing risk is what most people think of when asked about security’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 midsize companies manage cyber risk. Figure 12 highlights the practice-outcome combos that exhibit the strongest differentiators for midsize businesses when it comes to this objective.

Figure 12: Top three security differentiators for managing risk in midsize companies



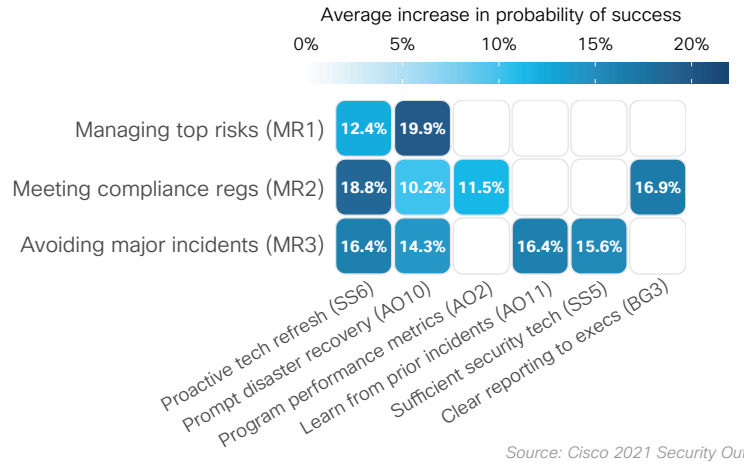
Source: Cisco 2021 Security Outcomes Study

It’s not surprising to see the topic of resilience assert itself once again here among the strongest differentiators for managing top cyber risks and, per Figure 13, avoiding major security incidents too. By most accounts, midsize businesses face a growing threat from ransomware and other disruptive security events. Maintaining robust capabilities to recover quickly from such incidents and minimize impact to the business is imperative for managing today’s top cyber risks.

The two remaining differentiators from Figure 12 share common themes of communication and compliance. While performance metrics and executive reporting don’t typically tick any boxes on the compliance requirements checklist, companies that track and report useful metrics are likely better positioned to offer evidence to auditors about the status of regulated security controls. The NIST Cybersecurity Framework (though not a regulatory standard) offers this advice: “*Organizations are encouraged to clearly identify and know why [metrics] are important and how they will contribute to the overall management of cybersecurity risk.*”

Additional risk management practices that hold promise for midsize businesses can be found in Figure 13. Proactive tech refresh enters the picture once again, improving the chances of achieving all three outcomes under the umbrella of managing risk. Keeping hardware and software current puts organizations on better footing to face whatever threat actors or fate throw their way. Score another for the ‘modern threats require modern tech’ theme. We’re probably seeing the benefits of SaaS again here. The vendor or MSP is fixing vulnerabilities, monitoring threats, responding to incidents, and so on at a manageable cost.

Figure 13: Correlation of security practices and outcomes for managing risk in midsize companies



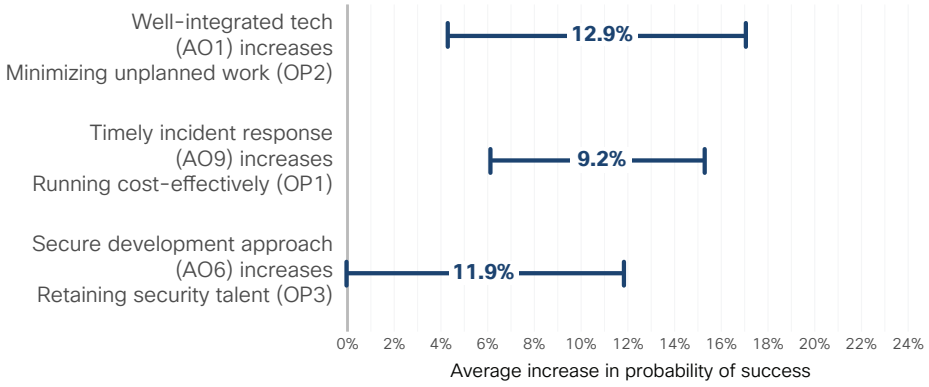
Source: Cisco 2021 Security Outcomes Study

The connection between learning from prior incidents and avoiding future ones borders on tautology. But that's exactly what the practice is designed to do, and the fact that Figure 13 says it works provides good justification for making the effort to actually do it. Focusing first on tackling security problems that have affected your organization and its peers is a savvy way to maximize risk reduction while minimizing cost. Then you can broaden the scope of risk remediation from there. If you don't know your history, you're bound to repeat it.

Operating Efficiently

Beyond enabling business and managing risk, the ability to operate efficiently often sets great IT programs apart from the good ones. This last set of outcomes addresses cost-effectiveness, executing strategy, talent management, and incident response processes. Important stuff, especially for midsize businesses.

Figure 14: Top three security differentiators for operating efficiently in midsize companies



Source: Cisco 2021 Security Outcomes Study

As companies grow, their IT ecosystem tends to become more complex and fragmented. As a result, "I remember when this used to be so easy" is a common complaint accompanying the growing pains of midsize businesses. And those complaints only intensify as trends like remote work further fragment the ecosystem.

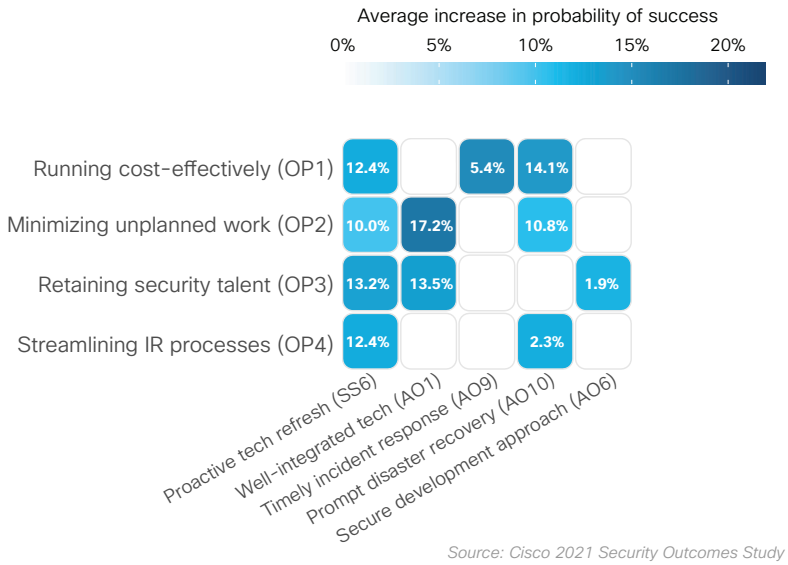
Integration eases those pains by enabling information technologies to work as a seamless and secure unit, effectively minimizing unplanned work. People are free to focus on important projects rather than mundane tasks, and begin to shower IT personnel with praises of thanksgiving. (Okay, that last part may be overdoing it, but the rest is spot on.)

A huge amount of money can be wasted very quickly in the "fog of war" that often surrounds security incidents. A recent study found that poor incident response more than doubles the median cost of major cyber events.[7] Ensuring an IR plan is in place, tested, and practiced helps make for more cost-effective IT and security operations.

And that brings us to the third practice-outcome pairing in Figure 14, which suggests a secure approach to software development helps retain security talent. That's a bit of a head scratcher, but recall that software shops are the most common industry among respondents to this study. In that light, this correlation makes more sense. Good talent recognizes good practice.

As we've done in prior sections, Figure 15 broadens the list of data-backed security practices beyond the top three differentiators. For the sake of consistency, let's start with proactive tech refresh. Have you noticed that this practice correlates with every single outcome we measured for midsize businesses, including the four shown here? Yes, modernizing your tech stack can come at a cost, whether hardware, software, or SaaS. But this presents compelling evidence that the investment will pay for itself through many other benefits. Poor operational efficiency is far more costly in the long run than periodic IT refreshes.

Figure 15: Top three security differentiators for operating efficiently in midsize companies



Source: Cisco 2021 Security Outcomes Study

[7] Information Risk Insights Study 20/20 - Xtreme, Cyentia Institute. https://www.cyentia.com/wp-content/uploads/IRIS2020-Xtreme.pdf

We mentioned technology integration with respect to Figure 14, but Figure 15 also connects it to retaining security expertise and experience. Nobody enjoys fighting IT fragmentation—especially in midsize businesses where the expectation is less red tape and legacy tech.

Let's give one last nod to the importance of resilience in midsize companies. Prompt disaster recovery correlates with three out of four outcomes associated with this objective. And so it should. It's hard to operate efficiently when prolonged periods of disruption bring everything to a halt.

"SMBs should look to Cisco for IT assistance. There is a notion out there that they are only focusing on larger enterprises, but nowadays there are many solutions and programs tailored to smaller companies as well."

Gustavo Guida, Head of Marketing, Cheetah

Resources for Successful Security in Midsize Businesses

The Cybersecurity Playbook for Midsize Companies

Cisco Free Trials for Midsize Businesses

Secure Remote Work for Midsize Businesses

For the full text for each outcome and security practice, along with the explanation and example evidence given to respondents to guide the rating of their programs' success, see: **Appendix B and C of the 2021 Security Outcomes Study.**

About Cisco Secure

Whether your organization is large or small, chances are security has become more complex over the years. More threats leads to more point products, which can further complicate investigation and response.

For several years, Cisco has been on a mission to simplify security. With the launch of our Cisco SecureX platform, we have brought greater visibility and automation to streamline and strengthen threat defense. SecureX integrates both Cisco and third-party technologies, enabling various security and IT products (and teams) to work together for more comprehensive protection. By automating common security functions, SecureX helps teams do more with less and focus on more strategic initiatives.

Customers can benefit from our integrated SecureX platform whether they have one or many Cisco Secure technologies – creating an advantage for organizations of any size. Since it's a cloud-native platform, SecureX allows you to easily add on new technologies and functionality as your needs evolve.

Learn how our **security portfolio** and **integrated platform** can help protect you from what's now and what's next.

Get started with a **free trial**.

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 April 2021 SMB_04_2021

cisco SECURE

CISCO

SECURE

The bridge to possible