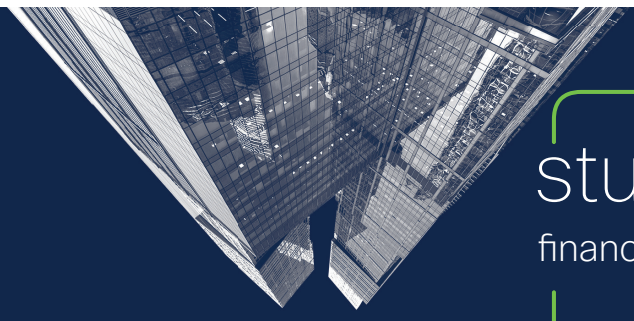
cisco SECURE

SECURITY

OUTCOMES



study
financial services

Introduction

What makes a successful cybersecurity program? Is there evidence that security investments achieve 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. This document is an offshoot of that study focusing exclusively on the financial services industry. Read on to discover how financial institutions compare to other organizations and what key factors contributed to the success of security programs like yours.

For the 2021 Security Outcomes Study, Cisco conducted a fully anonymous (source and respondent) survey of over 4,800 active IT, security, and privacy professionals from around the world. Of those participants, 589 represented firms in the financial services sector. An independent security research firm, the Cyentia Institute, provided analysis of the survey data and generated all results presented in this study.

Security Program Outcomes

We asked respondents about their organization's level of success across 11 high-level security outcomes organized under three main objectives: Enabling the Business, Managing Risk, and Operating Efficiently.[1] Our ultimate goal was to identify security practices that drive each of these outcomes, but let's not get ahead of ourselves. It's worth lingering here to see where the financial services industry excels and struggles with these various outcomes relative to other sectors.

[1] 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 programs' success.

Figure 1 shows the percentage of firms in the financial sector that say their security program is successfully achieving each respective outcome in our list.[2] So, 54.7% say they're meeting compliance regulations, 52.5% are gaining executives' confidence in the security program, and so on. The overall average rate of program success across all organizations and industries is 42%, which is why the entire figure pivots around that value marked by the vertical line. Outcomes with bars extending to the right of that line tend to be easier to achieve and those on the left are more difficult.

Figure 1: Reported success rates for various security outcomes in the financial services industry

Source: Cisco 2021 Security Outcomes Study

As with the main study, outcomes within the 'Managing Risk' objective generally show higher levels of success, those in 'Operating Efficiently' appear to be more of a struggle, and 'Enabling the Business' runs the gamut. That's where the similarities end, however, because security programs in the financial services sector report noticeably higher rates of success across every single outcome versus other industries.

Curious how we can make such an assertion? Great, you should be. Let's look back at subtle details in Figure 1 that will equip you to make your own determination about the relative success of the financial industry when it comes to security.

See that vertical white line in the middle of the 'Meeting compliance regs' bar? That's the overall average across all industries from the 2021 Security Outcomes Study. As stated before, the full length of the bar corresponds to the success rate for financial services. Thus, that horizontal line with the arrow pointing right shows the relative increase in reported success for that outcome (from ~48% overall to ~55% for the financial sector). For the last few outcomes, the vertical lines fall outside the bars, but the direction of the arrow still indicates that the financial sector is outperforming the overall average.

Overall, Figure 1 paints an impressive picture of security program success in the financial services industry. But could that picture be improved even more for your organization? Our data says yes. Head on to the next section to see what helped financial services firms take their security program performance to the next level.

[2] The "IR" in "Streamlining IR processes" stands for "Incident Response." "Peer" in "Obtaining peer buy-in" refers to non-security teams or divisions in the organization (e.g., IT, development).

Key Success Factors

In addition to the outcomes above, we asked study participants how well their organizations followed a set of 25 common security practices.[3] We then conducted multivariate analysis to measure which of these practices correlate most strongly with successfully achieving each objective. In other words, what factors contribute to successful security programs among financial services firms? Let's find out.

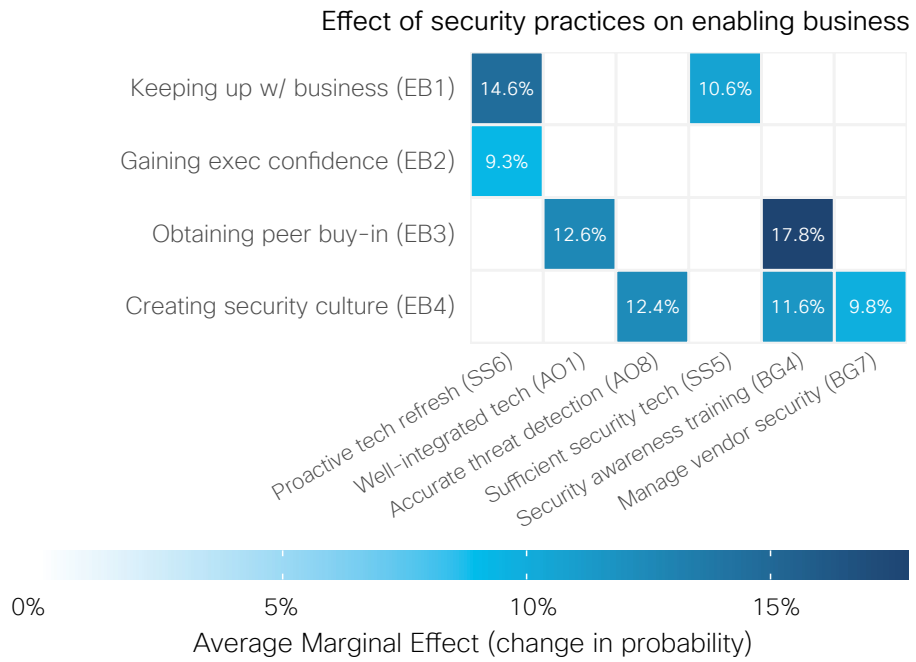
Figure Values

The values in Figures 2-4 denote the average increase in the likelihood of success for a given outcome when organizations report strong adherence to a certain practice. So, for example, the results find that a proactive tech refresh strategy increases the security program's chance of keeping up with the business by an average of 14.6% (top left square). Practice-outcome combinations with no shading or value indicate that our analysis did not find a statistically significant correlation.

Enabling the Business

As the label implies, this objective focuses on the security program'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 1 highlights several factors that measurably improve the ability of financial services firms to do just that.

Figure 2: Contribution of security practices to outcomes associated with enabling the business



Source: Cisco 2021 Security Outcomes Study

From these results, technology appears to be a major foundation for enabling the business in the financial services sector. Financial organizations are known for having generous IT and security budgets, and for utilizing advanced technologies ahead of other industries. It's no surprise, then, that many of them told us their security

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

technology resources were more than sufficient to support their mission. But we also saw a trend of financial firms continuing to invest in those technologies through proactive refreshes to maintain a best-of-breed, modern infrastructure. Our analysis shows that those investments are paying big dividends for the business.

Conversely, those who indicated that their organizations rarely upgrade infrastructure or only do so when things break showed significantly reduced rates of success. That might be why Figure 2 indicates that having a proactive technology refresh strategy also increases the confidence of executives. Reactive refreshes suggest something went wrong to force unplanned expenditures, and business leaders tend to frown on such surprises.

A well-integrated tech stack contributes to obtaining buy-in from the security program's IT and software development peers. Perhaps that's due to the requirements of a regulated industry where security integration is scrutinized to a greater degree.

At first glance, it may seem strange that accurate threat detection correlates with the creation of a positive security culture for the organization. But a security team that competently separates signal from noise and maintains situational awareness for the organization is a beautiful and inspiring thing to see. Plus, financial organizations place great importance on consumer trust, and quickly rooting out attempts by threat actors to undermine that trust sends a message that shapes the culture of security.

Financial organizations typically leverage a wide variety of third parties to deliver services to the market. Thus, managing third party risk is another cornerstone of consumer trust and that's probably why we see that ensuring the security of those third-party vendors is an important success factor for security culture in Figure 2.

Proving that success factors aren't all technical, security awareness training helps in obtaining buy-in from peers across the organization and in creating a strong security culture. This should provide ample encouragement to think of security awareness training as more than just a checkbox to satisfy security standards and regulators.

Managing Risk

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

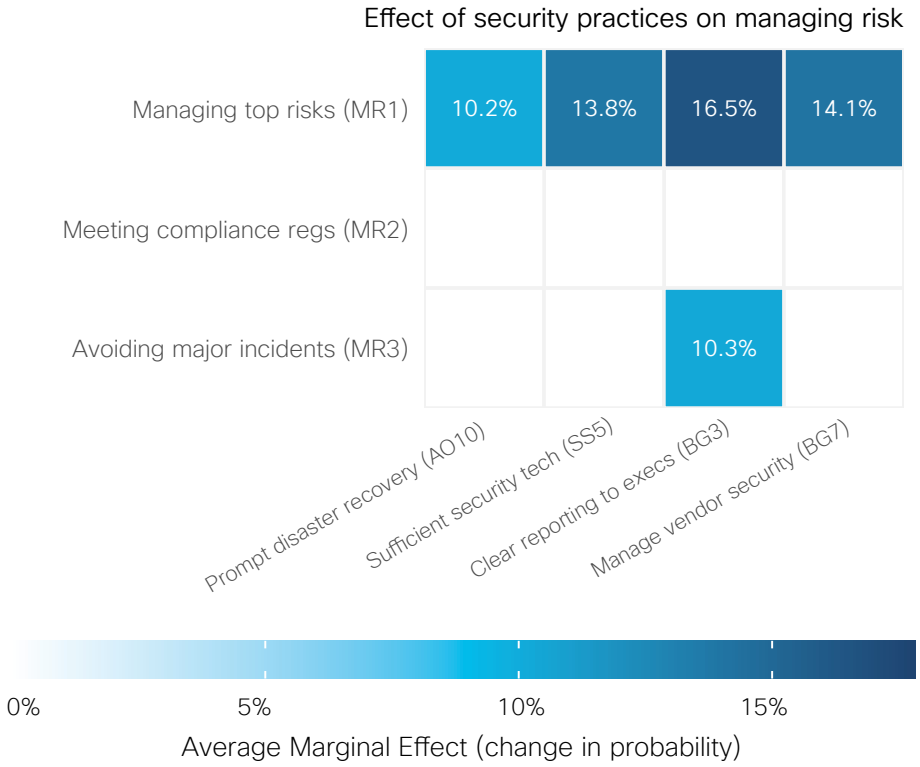
Overall, the list of practices in Figure 3 that significantly improve the chances of financial firms managing risk successfully is surprisingly short. Furthermore, no practices correlate with a higher likelihood of meeting compliance regulations, and only one links to avoiding major incidents. Before deeming your entire security program a lost cause, let's consider what the data might be telling us here.

It's worth noting that statistics likely plays a part in what we see in Figure 3. Because financial institutions generally rate higher than other industries for both successful security outcomes and adherence to best practices, it makes it harder to establish significant differentiators.

Think of it like this: If you measure height in the general population, professional basketball players would literally stand high above the average, and height would be a major factor in identifying good players. But if you did that same test among just pro basketball players, their relatively small height differences may not be a factor at all.

We see a similar effect here with financial organizations having security programs that are stronger and more successful than average.

Figure 3: Contribution of security practices to outcomes associated with managing risk



Source: Cisco 2021 Security Outcomes Study

Beyond statistics, there are other explanations for low correlation between risk management practices and outcomes among financial firms. Cyber-related risk represents the fastest-growing operational risk as digitization of financial services continues. Regulations generally provide guidance but are not prescriptive about how to address cyber risk. Approaches vary among financial institutions due in part to their own assessment of risk and compliance. However, the predominance of cyber risk in financial services indicates that the clear connection of security practices to the managing top risks outcome in Figure 3 would also contribute to an FI's ability to remaining compliant.

However, considering the predominance of cyber risk in financial services, it can be inferred that the clear connection of security practices to the 'managing top risks' outcome in Figure 3 would also contribute to an organization's ability to remain compliant. The fact that the data finds no single practice that correlates with the outcome of meeting compliance regulations likely reflects the diversity of approaches to compliance across the industry and also within particular institutions.

Looking specifically at the practices that drive the successful management of top risks, it's no surprise to see prompt disaster recovery among those listed in Figure 3. IT failures are increasingly THE top operational risk for financial firms. The financial services industry is critical to healthy economies, and ensuring the resiliency of those services is job #1.

Having sufficient security technology shows up again as a major success factor for managing risk. Financial institutions are afflicted by constant threats from all sides, and fending them off is much easier with the right tools.

The heightened risk and regulatory pressures on financial services demand greater boardroom visibility and responsibility. That's almost certainly why the practice of clear security reporting to corporate leadership pops up as the strongest contributor to managing risk – and the only significant factor for avoiding major incidents and losses. Without this, the security program is less likely to have the funding and support it needs, and less likely to mitigate the fallout when incidents do occur.

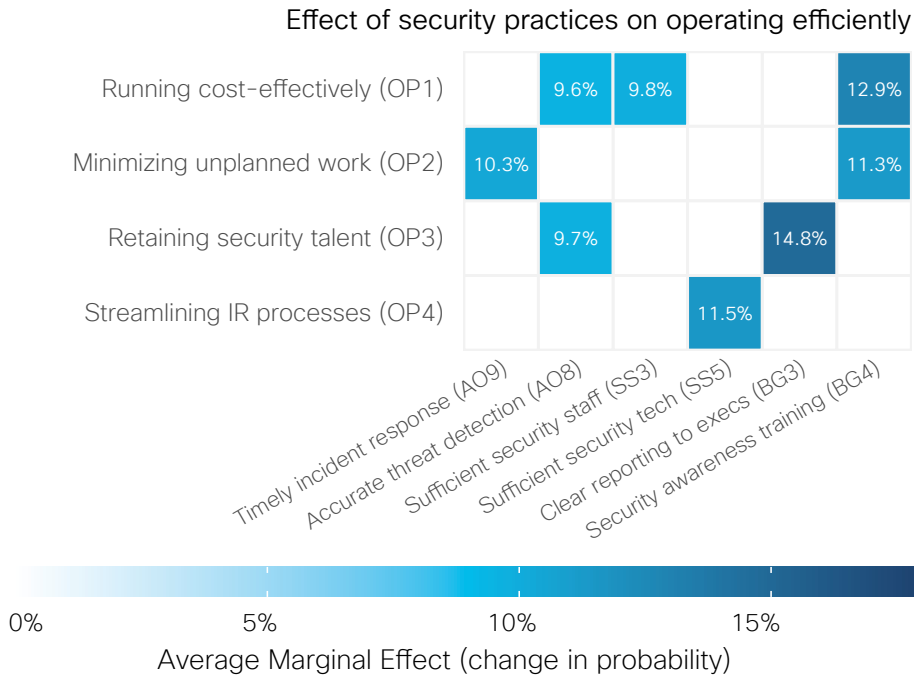
Last but not least, managing the security of vendors makes another appearance. This reinforces our earlier comments about financial firms relying on large networks of third-party service providers in order to deliver value to customers. Managing third-party risk well is a key differentiator for security success across the financial sector.

Operating Efficiently

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

Factors that pop for **running a cost-effective security program** include accurate threat detection, sufficient security staff, and security awareness training. The amount of wasted time and effort associated with chasing down endless false-positives is likely why threat detection features here. The latter two practices are a good reminder that effective security programs rest on the shoulders of the people who carry out the mission. Without them–or when they're not adequately enabled–operations quickly lose efficiency.

Figure 4: Contribution of security practices to outcomes associated with operating efficiently



Source: Cisco 2021 Security Outcomes Study

Minimizing unplanned work means a program is able to execute its strategy without major deviations or delays. It appears that a security-aware workforce along with solid incident response capabilities help the program stay on target. When employees understand that security is part of their job no matter where they sit in the organization, they're less likely to engage in behaviors that create work for the security team. And even though we're trained that security incidents aren't a matter of 'if' but 'when,' their occurrence still throws a wrench into daily operations. Planning for that eventuality and handling it smoothly lessens the size and disruptiveness of that wrench.

The connection between clear reporting to execs and **talent retention** is interesting. We've already established that good security reporting instills confidence in executives, so it's not much of a leap to assume that those good vibes translate to better funding and support for security programs to use in attracting and retaining talent.

Surveys of security operations analysts often show high levels of job dissatisfaction and burnout. Reasons offered for this trend often tie back to the repetitive and mundane nature of common tasks like triaging security alerts. The presence of accurate threat detection in Figure 4 as a key success factor for retaining talent hints at higher satisfaction among security analysts who don't have to spend all their time chasing down false-positives.

If you're keeping score, having security technologies that sufficiently enable the security program to carry out its mission is the only practice that contributes to all three high-level objectives. That's significant and triples down on the message that investing in the right tools yields strong ROI for the organization, and per Figure 4, for **streamlining incident response processes** in particular.

About Cisco Secure

At Cisco, we empower the security community with the reliability and confidence that they're safe from threats now and in the future with the Cisco Secure portfolio and Cisco SecureX platform. We help 100 percent of Fortune 100 companies protect what's now and what's next with the most comprehensive, integrated cybersecurity platform on the planet. Learn more about how we simplify experiences, accelerate success, and protect futures at cisco.com/go/secure.

Get inspired by the latest security success stories shared by Cisco customers: https://www.cisco.com/go/secompanies.

You can also learn more about Cisco's security solutions for financial services on our website, or by reading one of our many blogs:

- Bolstering Cyber Resilience in the Financial Services Industry: Part One
- Bolstering Cyber Resilience in the Financial Services Industry: Part Two
- Cisco's Connected Experiences: Secure your Financial Institutions

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

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

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Published December 2020 FSIRPT_12_2020

cisco SECURE

The Cisco Security Outcomes Study

We invite you to read the global Security Outcomes Study, engage with interactive data, and view short videos with some of the key findings at: cisco.com/go/SecurityOutcomes.

Also check out our Security Outcomes Study blog series and follow the conversation on social channels using #SecurityOutcomes

CISCO

SECURE

The bridge to possible