SECURITY

OUTCOMES

study
healthcare sector
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 healthcare industry. Read on to discover how healthcare institutions compare to others 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, 281 represented firms in the healthcare sector. The Cyentia Institute provided independent 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. 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 healthcare industry struggles and excels with these security outcomes relative to other sectors.

1 See Appendix B in the 2021 Security Outcomes Study 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 healthcare sector that say their security program is successfully achieving each respective outcome in our list. So, 51.2% say they’re meeting compliance regulations, 49.1% are gaining executives’ confidence in the security program, and so on. The overall 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 more difficult.

**Figure 1:** Reported success rates for various security outcomes in the healthcare sector

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 healthcare sector report varied success rates that are rather hard to predict.

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 healthcare 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 healthcare institutions. Thus, that horizontal line with the arrow pointed right shows the relative increase in reported success for that outcome (from ~48% overall to 51.2% for the healthcare sector).

The other outcomes can be similarly read, but pay attention to the direction of the arrow. Scanning down Figure 1, the healthcare sector over-achieves in five outcomes, under-achieves in five, and runs about even in two. One of those two is a rating of the overall success of the security program. Thus, we can conclude that the healthcare sector generally appears to be on par with what we see across other industries with respect to overall security program success. But is it possible for your organization to do better than par? Our data says yes. Head on to the next section to see what helped healthcare institutions take their security program performance to the next level.
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. We then conducted multivariate statistical 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 organizations in the healthcare sector? 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 specific security 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 12.9% (top left square). Practice-outcome combinations with no shading or value indicate that our analysis did not find a statistically significant correlation — which doesn’t mean the practice is useless. It’s just not a key success factor according to the data.

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 2 highlights several factors that measurably improve the ability of healthcare security programs to do just that.

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

Proactive tech refresh plays a major role in all outcomes under the ‘enabling business’ objective for healthcare institutions. The value of modern, best-of-breed infrastructure cannot be understated. This was also a theme throughout the main

---

2 See Appendix C in the 2021 Security Outcomes Study for the full text and listing of these practices.
report, and if anything, the results are even stronger for healthcare. We can state this as a converse as well – those who let their infrastructure degrade and only update when things break showed significantly reduced rates of success in enabling the business.

We can also drill down further into the results. If you’re interested in fostering a security mindset throughout your organization, well-integrated tech goes hand-in-hand with those proactive tech refreshes. The inclusion of security awareness training serves as a reminder that successful security programs aren’t just about technology. Here we see that training significantly increases buy-in from peers across the organization. This should provide ample encouragement to think of security awareness training as more than just a checkbox to satisfy regulators.

It may be possible that we may be seeing some reverse correlation here. It’s difficult to know whether well-integrated tech begets well-integrated teams, or vice versa. It’s probably a bit of both.

Finally, automation and having specific vulnerability remediation deadlines help security keep up with the business. Those three often form the cornerstone of security operations and complete the well-known "people, process, technology" triad of security programs.

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.

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

<table>
<thead>
<tr>
<th>Effect of security practices on managing risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managing top risks (MR1)</td>
</tr>
<tr>
<td>Meeting compliance regs (MR2)</td>
</tr>
<tr>
<td>Avoiding major incidents (MR3)</td>
</tr>
<tr>
<td>Proactive tech refresh (SS6)</td>
</tr>
<tr>
<td>Timely incident response (AO9)</td>
</tr>
<tr>
<td>Prompt disaster recovery (AO10)</td>
</tr>
<tr>
<td>IT &amp; security work together (AO3)</td>
</tr>
<tr>
<td>Secure development approach (AO6)</td>
</tr>
</tbody>
</table>

Average Marginal Effect (change in probability)

Source: Cisco 2021 Security Outcomes Study
Proactive tech refresh pops up again as one of the top three factors for bolstering capabilities to manage the top cyber risks facing the organization. Adapting a popular adage, “You can’t teach old tech new threats.”

The practices of timely incident response and prompt disaster recovery go hand-in-hand here and serve as a good reminder that risk management isn’t just about preventing security events. It’s just as important to mitigate the impact of those events when they do occur. The association of disaster recovery with compliance struck us as odd at first, but considering how ransomware has crippled so many healthcare institutions, we suspect auditors might be scrutinizing these capabilities.

The last two factors listed in Figure 3 also seem related. When various tech teams work together, including during the software development lifecycle, healthcare institutions are better positioned to manage top risks and avoid major incidents. If that’s not a prescription for improving collaboration and cohesion across IT, security, and development teams, we don’t know what is.

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.

In this section, some of the same security practices appear again in helping businesses operate efficiently, while some newcomers appear as well. In particular, a proactive tech refresh strategy is the only practice that boosts success in all three major security program objectives (and 8 out of 11 outcomes). Taking a cue from evidence-based medicine, this makes a very compelling case for treatment.
Positively affecting four out of the 11 outcomes, focusing on improving technology integration seems like a well-justified decision too. This also syncs with experience: “Fragmented, legacy infrastructure leads to efficient operations,” said nobody ever.

The link between automation and retaining talent is interesting. We suspect organizations that implement this practice will free their security staff from mundane, soul-crushing tasks to focus on more challenging, rewarding work. Employees who have rewarding jobs are bound to stick around.

We’ll briefly skip the next three security practices for now (don’t worry - we’re coming back to them) to quickly address the right-most success factor, because we’ve seen it before too. We find it very intuitive that tech teams working together minimizes unplanned work and wasted effort.

That leaves us with the three newcomers in Figure 4, and they seem to fall in logical order. Establish a sound security strategy, obtain a budget sufficient to implement that strategy, and staff up accordingly to make it happen. Easier said than done, obviously, but it’s good to know there’s good evidence that getting basic building blocks like that in place actually does lead to better security outcomes.

“Because defending our network and data against malware, ransomware, phishing, and other threats may literally be a life-and-death matter, we needed a way to deliver maximum security with minimal impact to our operations and patient care.”

Lee Cullivan, Chief Information Security Officer, Boston Medical Center

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.

You can also learn more about Cisco’s solutions for healthcare cybersecurity on our website:, or by reading one of our many blogs:

• Healthcare Cybersecurity: What’s at Stake?
• Securing Internet-Connected Devices in the New Era of Healthcare
• Why Healthcare Providers Need Secure Telehealth Solutions
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