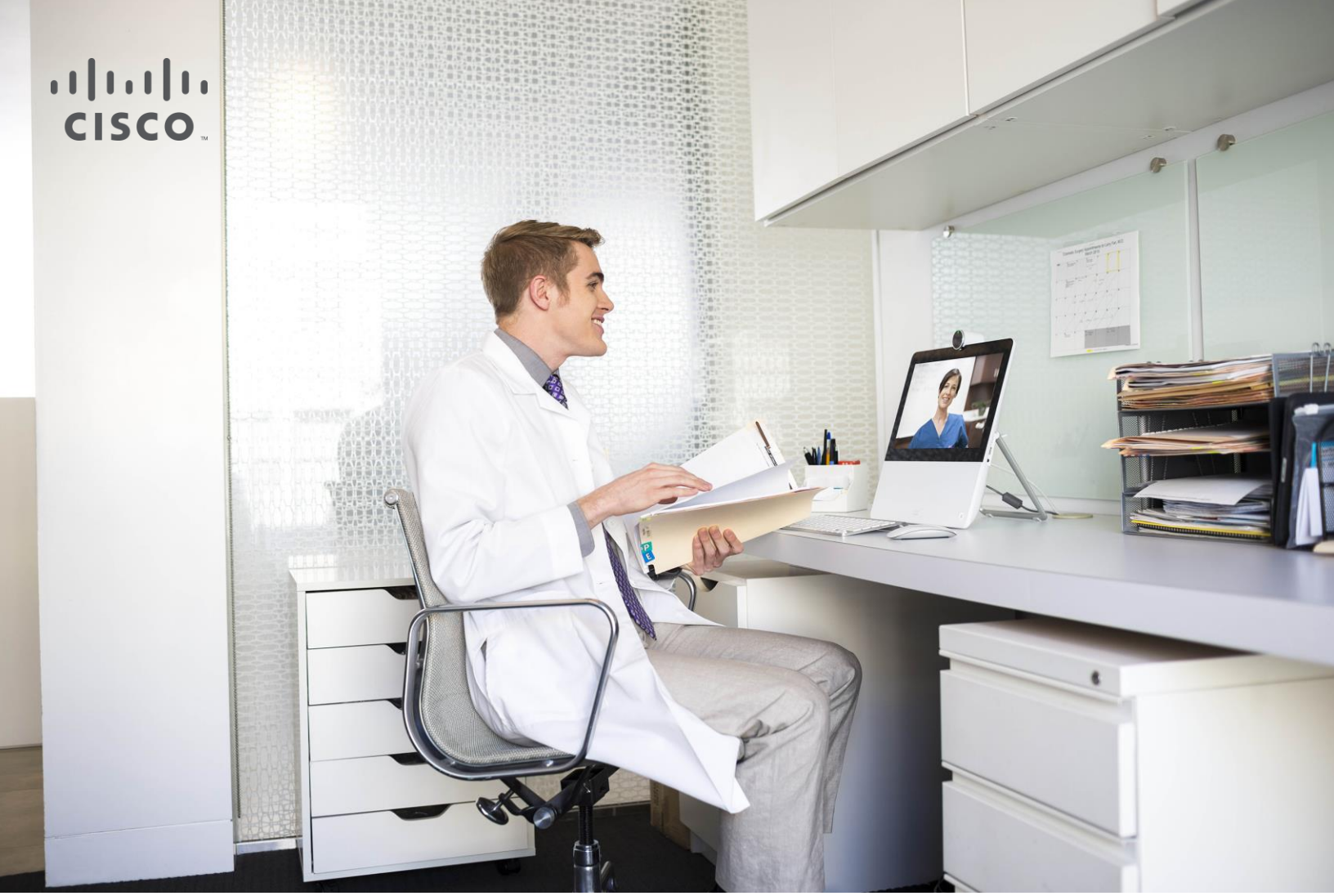


Security in Healthcare: Bolstering Connectivity and Protecting Patients

Connectivity and the Internet of Things (IoT) are pushing the boundaries of healthcare treatment. Medical professionals can access patient data and real-time health status in a way that can dramatically enhance their understanding of the progression of a disease and improve their response to patient health incidents. Medical equipment can automatically identify system failures and even generate maintenance tickets. Remote treatment allows doctors and patients to communicate remotely.

But this connectivity comes at a price. More devices and more communication increase the opportunities for attackers to breach defenses. On the one hand, the healthcare industry has been resistant to changes because it fears that interfering with critical systems could harm patients. On the other hand, not investing in security may not only affect patient healthcare if systems are disrupted but also injure patients' well-being if their private records are stolen. To mitigate these problems:

- The industry must take a more proactive approach to security to protect itself against growing threats such as ransomware.
- Healthcare organizations should better define and protect critical business assets and implement compensating controls for those systems that they cannot directly secure.

Major Findings

In this paper, Cisco experts analyze IT security capabilities in the healthcare industry, using data from the Cisco Security Capabilities Benchmark Study.[1] We found that:

- Healthcare security professionals appear to be losing confidence about the strength of their security defenses. In 2015, only 47 percent of healthcare professionals said they believe their security infrastructure was up to date and constantly upgraded, compared with 58 percent in 2014.
- Budget constraints were the most likely barrier to adopting advanced security processes and technology. However, in 2015, healthcare organizations showed a greater use of outsourcing than they did in 2014. This increase may help them strengthen security defenses at affordable costs.
- Breaches may influence security improvements. Fifty-one percent of healthcare organizations said they dealt with public scrutiny following a breach. Of those, 49 percent said they increased spending on security defense technologies after the breach.
- In 2015, more healthcare organizations have an executive in charge of security. There was also an increase in the number of executives that have metrics in place to assess security. These numbers suggest that organizations in this industry are taking more active measures to address threats.

Greater Connectivity Demands Stronger Defense

Breakthroughs in technology enabled by the IoT show great promise for the healthcare industry. These include home devices that can monitor critical health indicators and deliver alerts to healthcare professionals. But with greater connectivity, healthcare organizations must address risks such as exposure to malware and ransomware.

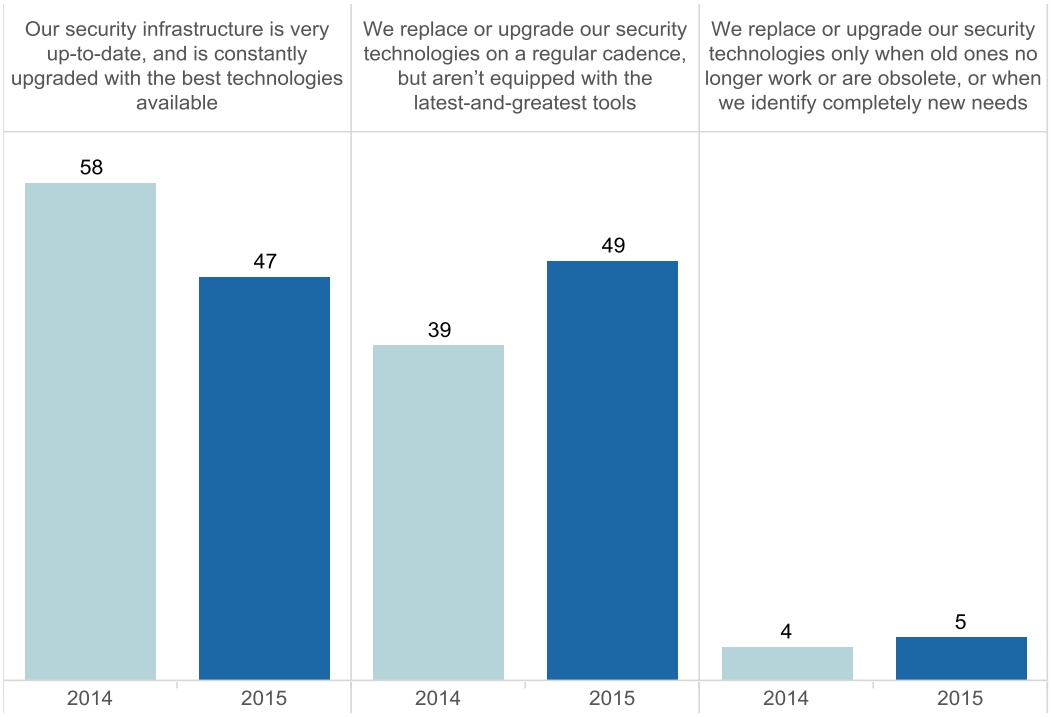
This risk played out in recent attacks using the SamSam ransomware, as reported in the Cisco Talos security blog.[2] Attackers are targeting healthcare facilities and demand that they pay a ransom to ensure continued access to their own data. Healthcare data is not easy to re-create, and its loss could put patient care at risk. These organizations may feel compelled to pay the ransom to avoid further disruption in patient care.

High-profile attacks in the past year brought more attention to the vulnerabilities of this industry. Not surprisingly, there was a decline in how confident these organizations feel. In 2015, only 47 percent of healthcare professionals said they believe their security infrastructure is up to date and constantly upgraded, compared with 58 percent in 2014 (see Figure 1).

[1] For more information about this study and the other white papers in this series, see the final pages of this document.

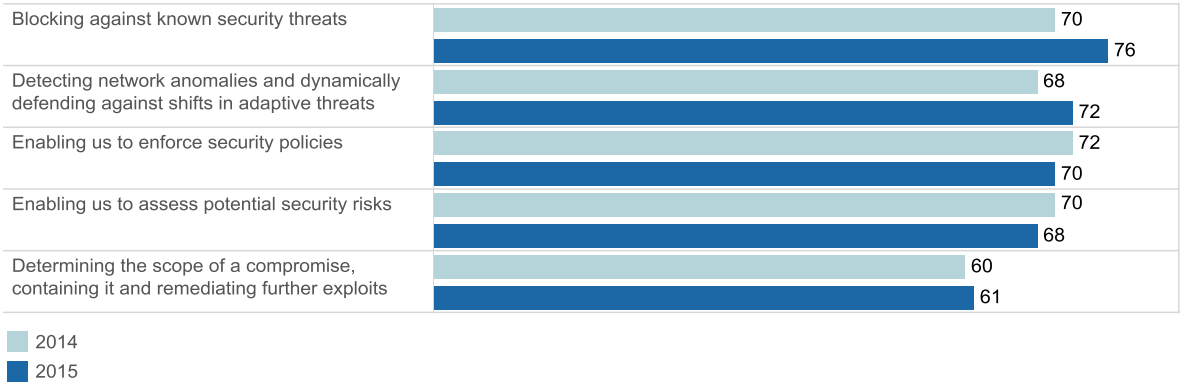
[2] "SamSam: The Doctor Will See You, After He Pays the Ransom," Cisco Talos Security blog, March 23, 2016: http://blog.talosintel.com/2016/03/samsam-ransomware.html

Figure 1. Healthcare Organizations' Perception of their Security Infrastructure



Healthcare professionals' perceptions of the effectiveness of their existing tools remained stable (Figure 2). For example, in 2014, 68 percent said their tools were effective in detecting anomalies and defending against shifts in adaptive threats, and 72 percent said so in 2015.

Figure 2. Healthcare Organizations Believe Their Security Tools Are Highly Effective



Penetration Testing Believed to Improve Security Effectiveness

As the security landscape undergoes seismic changes, healthcare organizations realize that they must improve their infrastructure in order to keep pace with attackers. The adoption of tools such as penetration testing indicates that more organizations are giving priority to a stronger infrastructure. In fact, those that perform penetration testing

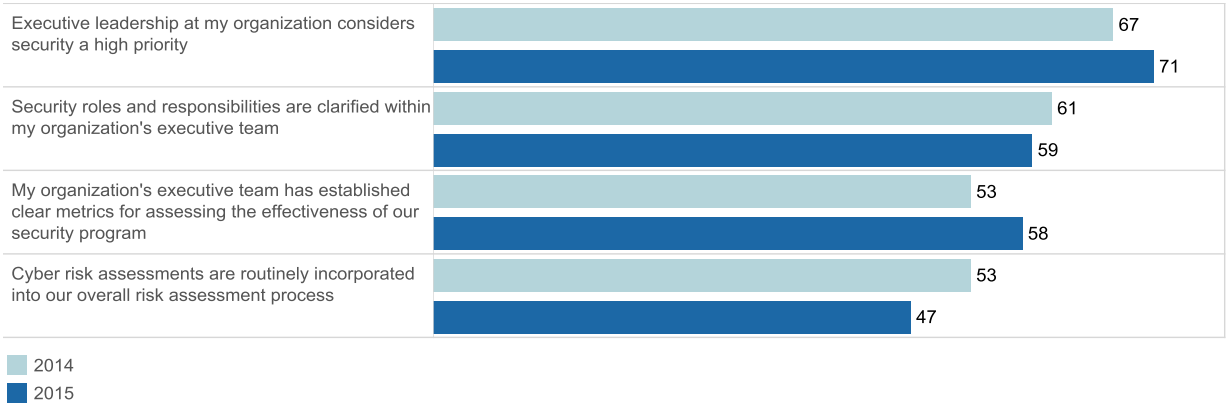
are more likely to agree that their security tools are highly effective. For example, 91 percent of healthcare organizations that conduct penetration testing said their tools were effective in blocking known security threats. On the other hand, only 70 percent of those that do not conduct penetration testing believe their tools are effective (Figure 3). However, Cisco experts believe that organizations that do not conduct any penetration testing cannot know with certainty that their tools are truly effective. Respondents may be overconfident.

Figure 3. Percentage of Healthcare Organizations That Believe They Are Effective in Various Security Functions

Another important factor in keeping pace with security threats is the support from executives. On this metric, healthcare organizations show improvement: In 2015: 91 percent of organizations reported having an executive accountable and responsible for security, an increase from 82 percent in 2014.

In addition, 58 percent said that in 2015, their organization's executive team has established clear metrics for assessing the effectiveness of security, up from 53 percent in 2014 (Figure 4). In 2015, 71 percent said their leadership considered security a high priority, compared with 67 percent in 2014.

Figure 4. Percentage of Healthcare Organizations That Agree with Various Statements Regarding Security



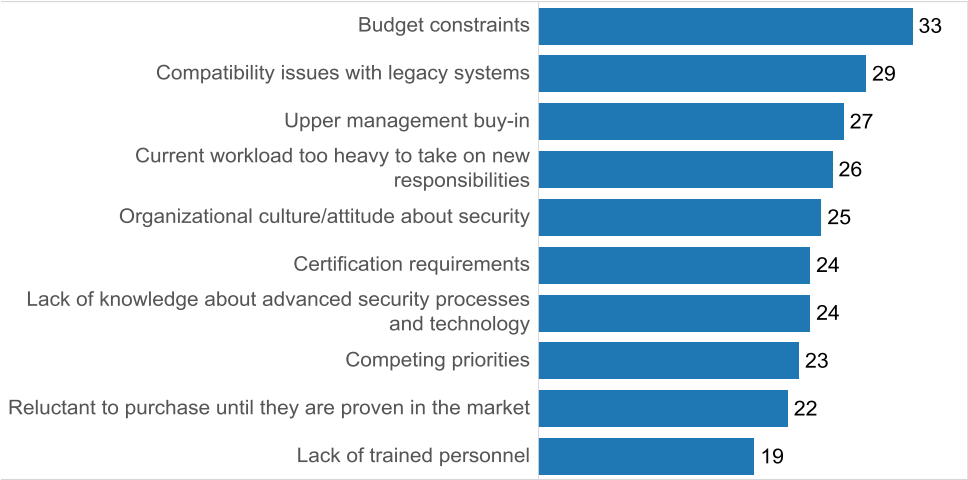
Budget Constraints Are a Barrier to Security Improvements

As in many industries, cost is a deterrent to implementing security measures. Budget constraints were named by 33 percent of respondents as the top barrier to adopting advanced security processes and technology. Other main

reasons, as seen on Figure 5, were compatibility issues with legacy systems (29 percent) and the lack of upper management buy-in (27 percent). Expenditures for patient care systems tend to trump all other budget line items in healthcare facilities. For example, hospital administrators are probably more likely to devote funds for imaging machines that can help detect cancer instead of using those funds for security technology.

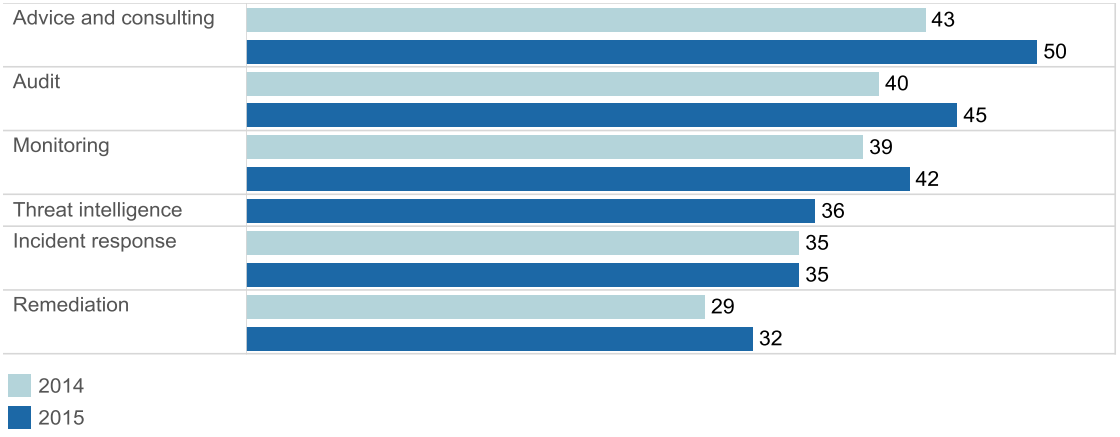
However, as more attackers target healthcare organizations for profit, executives should recognize that protecting patient data and ensuring that networks stay functional is just as important for patient well-being.

Figure 5. Barriers to Adoption of Advanced Security in Healthcare Organizations



Outsourcing security services offers a path for healthcare organizations to strengthen security while keeping expenses in check. In 2015, healthcare organizations appear to have moderately increased their outsourcing of security services in several areas, including auditing, advice and consulting, and remediation (Figure 6). Continued outsourcing could lead to further improvement of security defenses.

Figure 6. Percentage of Healthcare Organizations That Outsource Various Security Services



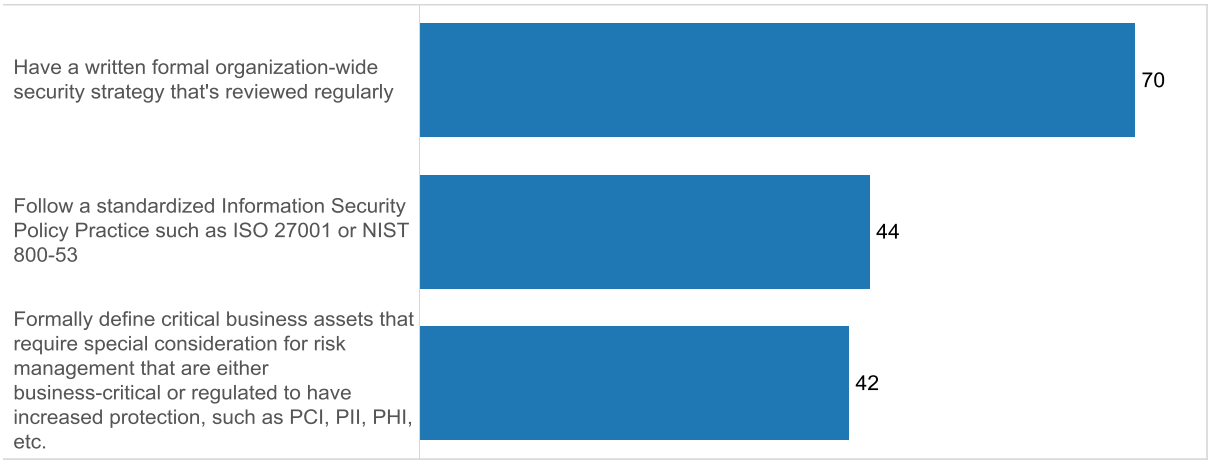
Greater Need to Define Critical Assets

Building stronger security requires a deeper focus on policies and processes—not just technology. In this area, healthcare organizations have room for improvement. For example, less than half of the organizations reported formally defining critical business assets that require special consideration for risk management (Figure 7). This is

of concern, because it suggests there is little segmentation of data. It is important to identify and isolate critical assets to keep them secure in the event of attacks, especially those that involve ransomware.

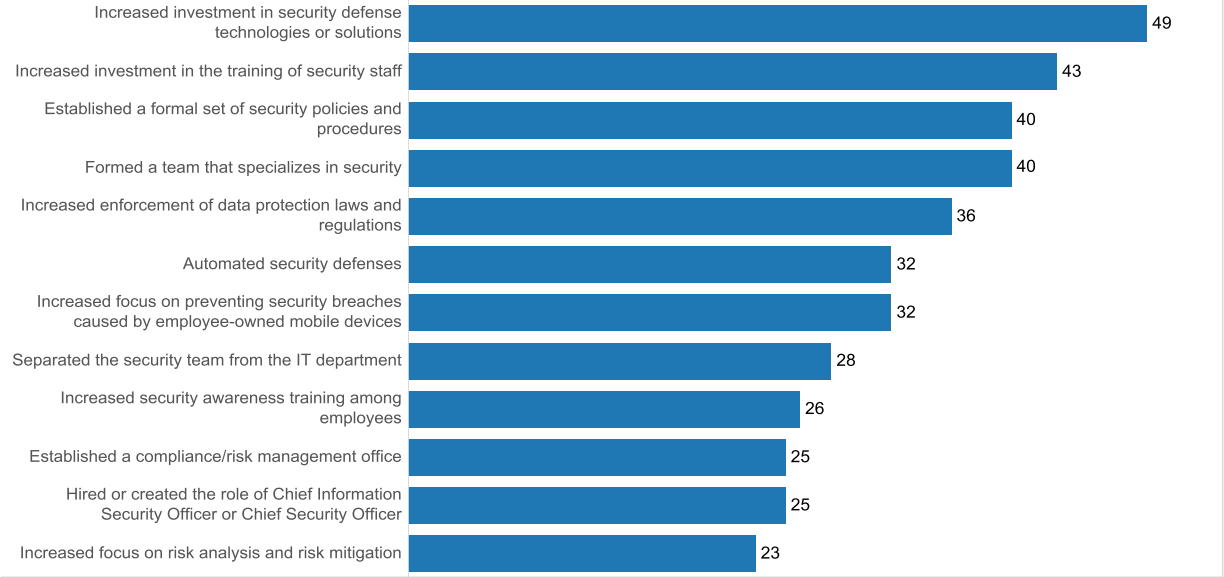
Another worrisome figure is that only 70 percent of healthcare organizations reported using formal written policies (Figure 7). Cisco experts believe this number is too low for effective security, considering that most healthcare organizations take credit card payments. Regulatory compliance requires written security policies of those organizations that do accept credit cards. Cisco experts also note that these policies must be detailed, enforceable, and auditable.

Figure 7. Percentage of Healthcare Organizations with Formal Policies for Risk Management



The impetus behind some process improvements–or the purchase of new security technologies–may be public breaches that expose the weaknesses in healthcare defenses. In 2015, 51 percent of healthcare organizations said they dealt with public scrutiny following a breach. Of those, 49 percent of organizations stated they increased spending in security defense technologies after a breach, and 43 percent said they increased training for security staff (Figure 8). However, it is important to note that simply purchasing new tools does not automatically improve defenses. The tools need to be deployed with strong processes and qualified people. They must be part of an integrated threat defense strategy to protect all devices and networks, and they must be maintained and monitored around the clock.

Figure 8. Percentage of Healthcare Organizations Reporting Improvements After a Public Breach



Conclusion: Closer Attention to Threat Defenses and Critical Data

As connected services become more commonplace in healthcare, more opportunities exist for bad actors to exploit weaknesses in the industry's security defenses. There is certainly evidence that attackers have focused their attention on healthcare.

Healthcare professionals argue that investing in technology that directly affects patient care takes precedence over investments in security. However, they are becoming more aware that security can indeed have an impact on preserving patient well-being. If healthcare professionals believe in the maxim "Do no harm," then that philosophy should extend to the security of patient data.

Healthcare security professionals should:

- Recognize the value of an integrated threat defense, which relies on security tools working together to present a holistic view of the organization. Individual tools cannot provide this view.
- Pay closer attention to identifying and segmenting critical data and systems. Those systems should be isolated from other parts of the network, and their security reinforced. For sensitive systems that are difficult to secure, organizations should implement compensating controls to minimize the risk of breaches.
- Explore the value of outsourced services to provide the security tools and processes that budget constraints may not allow for in-house.

Learn More

To learn about Cisco's comprehensive advanced threat protection portfolio of products and solutions, visit www.cisco.com/go/security.

About the Cisco 2015 Security Capabilities Benchmark Study

The Cisco 2015 Security Capabilities Benchmark Study examines defenders across three dimensions: resources, capabilities, and sophistication. The study includes organizations across several industries in 12 countries. In total, we surveyed more than 2400 security professionals, including chief information security officers (CISOs) and security operations (SecOps) managers. We surveyed professionals in the following countries: Australia, Brazil, China, France, Germany, India, Italy, Japan, Mexico, Russia, the United Kingdom, and the United States. The countries in the survey were selected for their economic significance and geographic diversity.

To read findings from the broader Cisco Security Capabilities Benchmark Study, get the Cisco 2016 Annual Security Report at www.cisco.com/go/asr2016.

About This Series

A team of industry and country experts at Cisco analyzed the Cisco 2015 Security Capabilities Benchmark Study. They offer focused insight on the security landscape in 10 countries and four industries (financial services, healthcare, telecommunications, and transportation). The white papers in this series highlight the security landscape and challenges that organizations face in cybersecurity. This process helped to contextualize the findings of the study and bring focus to the relevant topics for each country and industry we analyzed.

About Cisco

Cisco is building truly effective security solutions that are integrated, automated, open and simple to use. Drawing on unparalleled network presence as well as the industry's broadest and deepest technology and talent, Cisco delivers ultimate visibility and responsiveness to detect more threats and remediate them faster. By calling on Cisco Security, companies are poised to securely take advantage of a new world of digital business opportunities.

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

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**