White Paper

Healthcare Security: Improving Network Defenses While Serving Patients

What You Will Learn

Safeguarding the privacy of patient information is critical for healthcare providers. However, Cisco has found that the industry's security executives appear to have less understanding of the threats facing their organizations than executives in other industries. They also tend not to use the best tools for meeting security challenges. In the Cisco 2014 Security Capabilities Benchmark Study, we found that:

- Chief information security officers (CISOs) in healthcare are more likely than security operations (SecOps) managers to believe that their security processes are optimal.
- Healthcare organizations do not implement as many strong security defenses as organizations in other industries.
- When healthcare organizations experience a breach, they may be more likely to implement a wider array of security defenses.

Maintaining Accessibility While Managing Security

First, do no harm. That's the often-quoted principal goal of medical professionals: doing what is best for patients and keeping them healthy. Nothing must get in the way of this objective, and that means keeping critical information systems immediately accessible and uncompromised.

Unfortunately, the need to maintain easy access to healthcare systems and data may be in conflict with the need to secure these systems from attack. For the Cisco 2014 Security Capabilities Benchmark Study, we surveyed CISOs and SecOps managers in several industries about their security resources and procedures. We discovered that healthcare organizations may not be deploying the same security defenses as those in other industries. For example, the heathcare organizations we surveyed are less likely to use vulnerability scanning, or they use it in fewer places than other industries do. This type of scanning is an effective tool for identifying vulnerabilities that the IT staff can patch or apply compensating controls to and thereby help prevent attacks.

As an industry, healthcare, like financial services, faces special challenges in protecting information systems from bad actors. U.S. regulatory requirements such as those under the Health Insurance Portability and Accountability Act (HIPAA) provide guidance for making sure that healthcare data is kept secure and confidential. Healthcare organizations and their security professionals are keenly aware of their responsibilities. However, as our survey shows, they may have less appreciation of security requirements. Regulatory compliance, while obviously important, does not equal strong security. But strong security measures can help enable compliance and at the same time help prevent an organization from suffering a potentially devastating cyberattack.

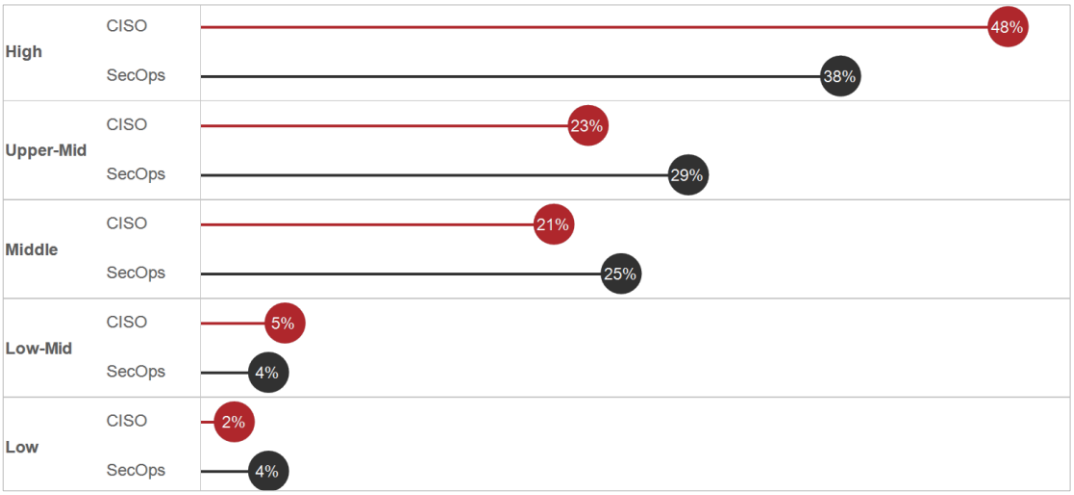
Major Findings

- CISOs in healthcare are more likely (64 percent) than SecOps managers (46 percent) to believe that their security processes help them anticipate and manage security issues proactively, rather than simpy react.
- Healthcare organizations are not implementing as full an array of strong security defenses as organizations in other industries. For example, 39 percent say they use vulnerability scanning as part of their threat defenses, while 49 percent of other organizations do.
- Healthcare organizations that have experienced a breach are more likely (67 percent) to perceive their security defenses as up to date. This confidence may be due to their having brought on additional defenses after the exposure. Just 51 percent of organizations that have not dealt with a public breach say their defenses are up to date.
- When healthcare organizations experience a breach, they may be more likely to implement a wider array of security defenses. For example, 61 percent are using virtual private networks (VPNs), compared with 38 percent that have not suffered a breach.
- Healthcare organizations are more likely (32 percent) than those in other industries (21 percent) to manage their security needs internally instead of outsourcing services such as monitoring, incident response, remediation, and auditing.

Healthcare CISOs More Optimistic than SecOps Managers

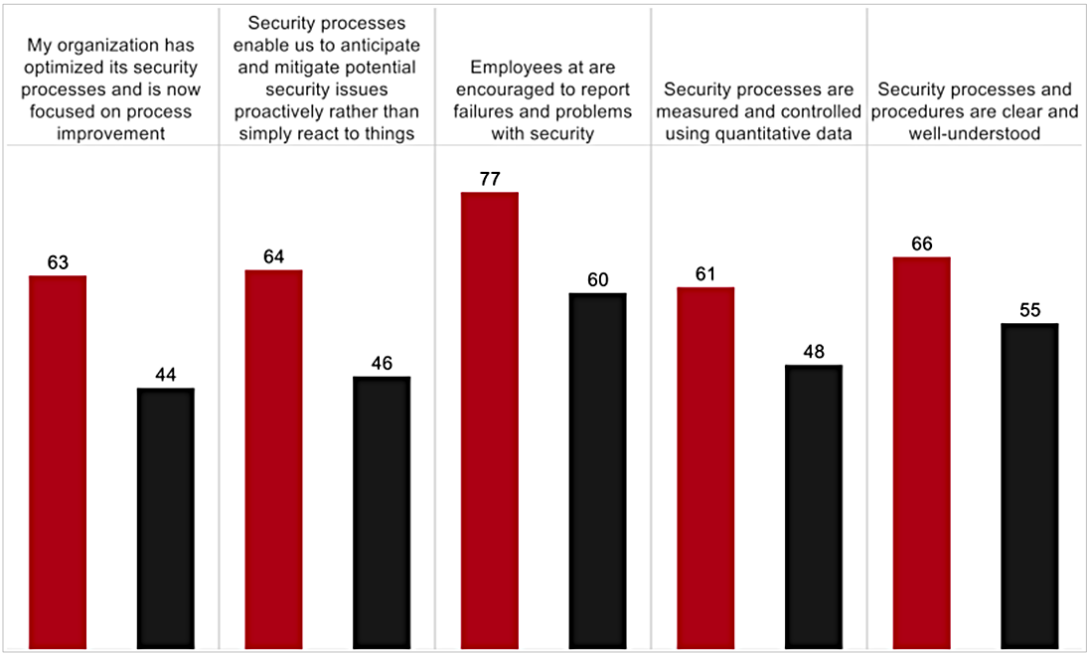
The Cisco Security Capabilities Benchmark Study shows that CISOs in all industries and regions tend to be more optimistic than their SecOps colleagues about their security measures. Those in healthcare organizations are no exception: CISOs in healthcare are more likely than SecOps managers to believe that their security processes are optimal (Figure 1). For example, using the CISOs' responses to our questions about their processes, we categorized 48 percent of their organizations as having a high level of security sophistication. But only 38 percent of SecOps managers gave responses that put their organizations at the same level.

Figure 1. Perception of Security Sophistication by Role



Although the difference is small, the gap between CISO and SecOps perceptions becomes more pronounced in their responses to specific questions that gauge attitudes toward security (Figure 2). For example, 63 percent of healthcare CISOs believe that their organization has successfully optimized security processes and now focuses on process improvement. Only 44 percent of SecOps managers believe they've optimized their processes.

Figure 2. Percent of Security Professionals That Strongly Agree on Organizational Cultural Statements, by Role



The CISOs' higher level of confidence may stem from the fact that they work at a certain distance from day-to-day operations. SecOps managers are on the front lines, resolving major and minor security incidents every day. Healthcare CISOs may not realize that their security systems are subject to many small incidents, while SecOps managers spend hours responding to threats.

CISOs in healthcare are not often steeped in an information security background. Managers first and foremost, they rely on SecOps teams for the "detail" work of maintaining security. Even CISOs that come from technical

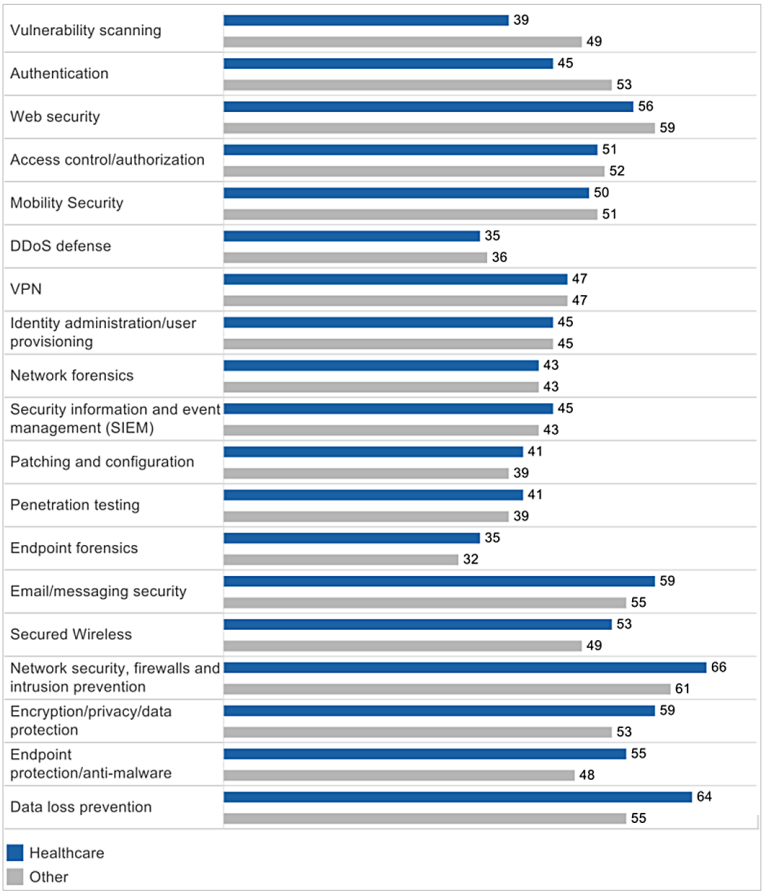
backgrounds are challenged to keep up with everything that happens on a day-to-day basis because they must manage executive responsibilities as well.

In addition, healthcare CISOs base most of their security decisions on data from internal surveys and high-level summaries, which may state that the organization's training scores are reasonable, and the list of devices they have deployed matches industry recommendations. They generally do not look deep enough to see how thoroughly controls are implemented, whether enough devices are being monitored, and whether the appropriate compensating controls are in place for devices that cannot have security controls implemented on them directly.

A Lack of the Strongest Defenses

Even though healthcare information is highly sensitive, healthcare organizations are not implementing as full an array of strong security defenses as organizations in other industries (Figure 3).

Figure 3. Percent of Organizations Using Various Threat Defenses



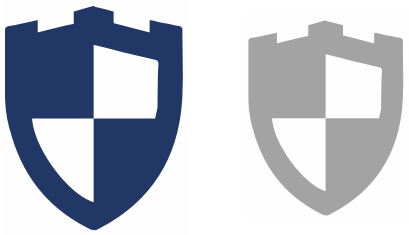
Judging from the study responses, healthcare organizations seem most concerned with protecting the network edge, rather than detecting threats already inside their networks.Their concern is that defenses such as vulnerability scanning or an instrusion prevention system (IPS) could delay or block access to critical patient-care systems. For example, radiology information systems typically do not have embedded antivirus or antimalware solutions. Scanning a multigigabyte image file would take a long time, and it could disrupt patient care by making the image library unavailable. Similar devices are not built to accept anything but the simplest type of inquiry (pings and requests, for example), so they could be knocked offline by vulnerability scanning. Consider a scenario where the devices in an operating room are scanned during an emergency surgery in the middle of the night and are taken offline. That is one of the major fears of IT in healthcare.

To combat these challenges, healthcare organizations should consider solutions that segment networks. This measure could prevent attackers from gaining full access even if they breach a portion of the healthcare system. Having the appropriate network segmentation, authentication, and access control for people and devices is crucial, as are compensating controls. If organizations use a group of devices that cannot be scanned or have controls directly applied to them, they must be segregated behind gateway controls, isolating them from other network segments and traffic.

Perception of Up-to-Date Security Capabilities, Despite Few Defenses

Even though their security defenses are relatively weak, healthcare security professionals are more likely than their counterparts in other industries to believe their threat detection processes are optimal (Figure 4). Sixty-seven percent of healthcare respondents say their threat detection and blocking capabilities are kept up to date, compared with 56 percent of respondents in all other industries.

Figure 4. Percent of Organizations Saying Their Threat Detection and Blocking Capabilities Are Current



The reason for healthcare organizations' satisfaction levels with their security defenses probably lies in both the desire to speed care to patients, and the priority given to compliance with healthcare data privacy regulations, as opposed to security. These organizations may want to limit which systems they monitor for security breaches, so as not to overwhelm network resources and prevent healthcare professionals from accessing data for critical patient care needs.

Healthcare CISOs and SecOps managers are also tightly focused on compliance. Therefore, the acquisition of security defenses may not go beyond what is needed to "check the boxes" of compliance requirements. However, it's in the best interests of healthcare organizations to view security as an enabler of compliance—especially since compliance does not equal security.

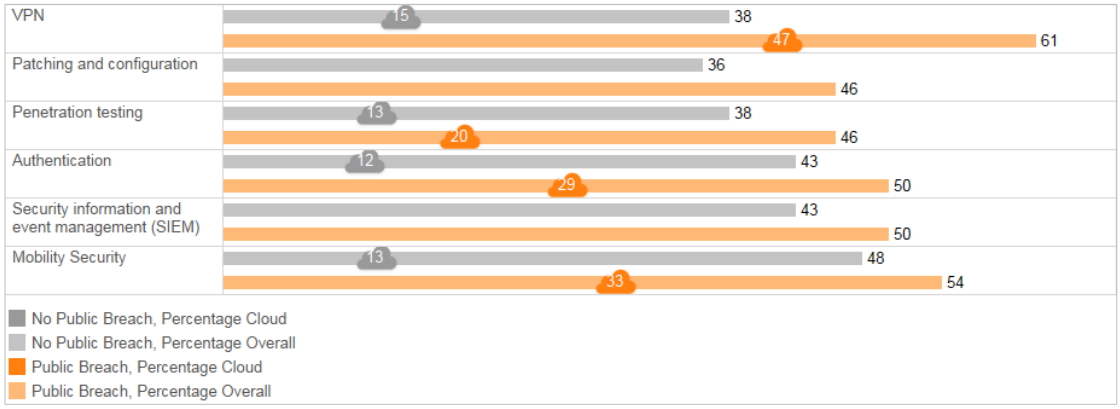
Breaches Deliver a Reality Check

Healthcare organizations that experience a public security breach are more likely to perceive their current security defenses as up to date, according to the study. Sixty-seven percent of organizations that suffered a public security breach say that their security infrastructure is up to date, while 26 percent say they're not equipped with the latest tools, and 7 percent say they replace security tools only when old ones no longer work or become obsolete.

However, perceptions are different among organizations that have *not* dealt with a public security breach: Of this group, only 51 percent believe their infrastructure is up to date, and 48 percent say they are not equipped with the latest tools.

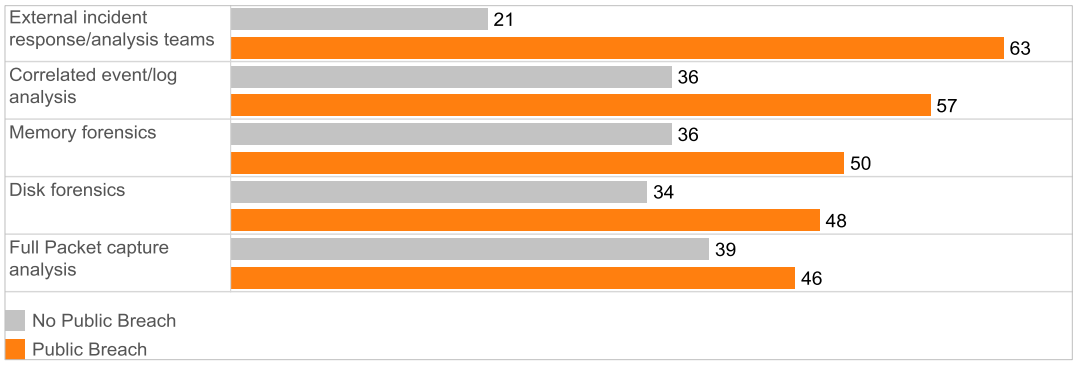
When healthcare organizations experience a public breach, they appear more likely to implement a wider array of security defenses (Figure 5). For example, 61 percent of healthcare organizations that have suffered a public breach are using VPNs, compared with 38 percent that have not suffered a breach. When asked about cloud-based security solutions, the organizations that have experienced public breaches are much more likely to adopt more threat defenses: 47 percent of those that have experienced a breach are using cloud VPN solutions, compared with just 15 percent of organizations that have had no public breaches.

Figure 5. Percent of Organizations Using Various Threat Defenses, Overall and Cloud-Based, by Public Breach Status



Healthcare organizations that have dealt with public security breaches are also more likely to rely on external response teams to resolve security issues (Figure 6). For example, of those that were the victim of public data breaches, 63 percent say they call on external incident response and analysis teams to analyze compromised systems. Only 21 percent of organizations that have not experienced a security breach do so. Also, 59 percent of organizations that have experienced a security breach rely on long-term fix development to eliminate the causes of security incidents. Only 31 percent of unbreached organizations do so.

Figure 6. Percent of Organizations Using Selected Processes to Analyze Compromised Systems, by Public Breach Status



It's encouraging that healthcare organizations tend to "see the light" after they suffer a public security breach, but it may take more than a security incident for them to strengthen their defenses. Although the healthcare industry's public breaches have resulted in the occasional costly lawsuit or fine, they tend not to suffer high damages—punishment that would serve as a deterrent to leaving personal healthcare information at risk of exposure.

In addition, the inflexibility of the healthcare market means that consumers can't instigate change. In industries such as retail, the theft of private data can cause customers to leave a vendor in droves. Most healthcare consumers can't easily shift to different providers or networks. They lack choice, and the cost is high. Therefore, the exposure of personal healthcare data, while no doubt frustrating, may not spur consumers to switch providers.

Healthcare More Likely to Handle Security Internally

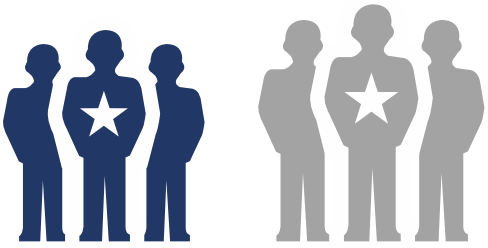
Compared with other industries that we surveyed, healthcare organizations are somewhat more likely to manage their security needs internally instead of outsourcing services such as monitoring and incident response. Thirty-two percent of healthcare organizations say they manage security functions such as incident response, remediation, and auditing internally. In all other industries only 21 percent do. The interest in managing security internally may be due to concerns about patient care and the impact of security tools on that care, the same concern that affects the perceptions of CISOs and SecOps managers about security defenses.

In addition, many university hospitals share or use many security functions supported by the university, such as network, monitoring, and audit. Therefore there may be conflicting interests, and the hospital may have relatively little control over how IT and information security is managed.

Healthcare Less Likely to Deal with Public Breaches

Healthcare organizations are less likely than others to have dealt with public security breaches: 43 percent say they've experienced such events, as opposed to 57 percent in other surveyed industries. They are also somewhat less likely to have internal security incident teams or executives directly accountable for the security function (Figure 7). Eighty-two percent of healthcare organizations say they have executives who are directly responsible for security; 92 percent in the other surveyed industries do.

Figure 7. Percent of Organizations with an Executive Directly Responsible for Security



Executive Engagement and Security Controls Most Likely to Predict Security Sophistication

As part of its study, Cisco segmented organizations by their level of security sophistication. We based our categories on the respondents' answers to questions about security processes. The categories ranged from "low sophistication" (processes are ad hoc and unpredictable) to "high sophistication" (processes are optimized and the focus is on improving them). Forty-three percent of the healthcare organizations surveyed were classified as having a high level of security sophistication.

The top influencers of security sophistication among healthcare organizations are executive engagement and security control systems. Those in 82 percent of highly sophisticated organizations agree that security roles and responsibilities are clarified within their executive teams, compared with 49 percent in less sophisticated organizations. And 80 percent of those in highly sophisticated organizations say that they have good systems for verifying that security incidents have occurred, compared with only 37 percent in less sophisticated organizations.

Cisco's analysis of security sophistication has highlighted the hallmarks of the best-prepared healthcare institutions. These characteristics provide signposts for any organization that seeks to upgrade its stance on security. They are:

- Good systems for verifying that a security incident has actually occurred.
- Cyber risk assessments that are routinely incorporated into overall risk-assessment processes.
- Standardized incident response practices such as those outlined in documents from the Internet Engineering Task Force (RFC 2350), the International Organization for Standardization and International Electrotechnical Commission (ISO/IEC 27035:2011), and U.S. Computer Emergency Readiness Team (US-CERT).
- Security roles and responsibilities clarified within the executive team.
- Experience in managing public scrutiny after a security breach.
- Effective processes for interpreting and prioritizing incoming incident reports and understanding them relative to each other and to trends.

Conclusion: Healthcare Requires Sophisticated Threat Protection

As we recommend in the Cisco 2014 Security Capabilities Benchmark Study, healthcare organizations should:

- Realistically understand the risks they face.
- Continually assess the quality of their security defenses.
- Segment and control network traffic in such a way that security is optimized while information remains readily available to healthcare professionals.

To improve the sophistication and reliability of their security defenses, healthcare organizations should consider continuous threat detection. Such a system not only monitors the inside of networks (not just the edge), but also detects and mitigates threats to make sure that if attackers gain entry to critical systems, their impact is limited. A threat-centric and operationalized approach to security can reduce complexity and fragmentation, while providing superior visibility and continuous control.

Through a combination of technology and services, defenders can employ the mindset of an attacker to develop and implement protections across the extended network and the entire attack continuum – before, during, and after an attack.

Learn More

To read findings from the broader Cisco Security Capabilities Benchmark Study, download the Cisco 2015 Annual Security Report at www.cisco.com/go/asr2015.

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

About Cisco

Cisco delivers intelligent cybersecurity for the real world, providing one of the industry's most comprehensive advanced threat protection portfolios of solutions across the broadest set of attack vectors. Cisco's threat-centric and operationalized approach to security reduces complexity and fragmentation while providing superior visibility, consistent control, and advanced threat protection before, during, and after an attack.

Threat researchers from the Collective Security Intelligence (CSI) ecosystem bring together, under a single umbrella, the industry's leading threat intelligence, using telemetry obtained from the vast footprint of devices and sensors, public and private feeds, and the open source community at Cisco.

This amounts to a daily ingestion of billions of web requests and millions of emails, malware samples, and network intrusions. Our sophisticated infrastructure and systems consume this telemetry, enabling machine-learning systems and researchers to track threats across networks, data centers, endpoints, mobile devices, virtual systems, web, email, and from the cloud to identify root causes and scope outbreaks. The resulting intelligence is translated into real-time protections for our products and services offerings that are immediately delivered globally to Cisco customers.

The CSI ecosystem is composed of multiple groups with distinct charters: Talos, Security and Trust Organization, Active Threat Analytics, and Security Research and Operations.

To learn more about Cisco's threat-centric approach to security, visit www.cisco.com/go/security.

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.**