2015 HIMSS Cybersecurity Survey

Executive Summary

June 30, 2015

HIMSS
transforming health through IT

The breach of patient information, especially as it relates to cyber attacks, causes alarm throughout the healthcare industry. Indeed, over the last year, there have been high profile breaches at numerous healthcare organizations that have impacted millions of individuals. But, massive breaches are not just a problem facing the healthcare industry—all industries are targets and the cyber adversaries have become very sophisticated. For example, the high stakes of cyber-attacks were made very clear with the SONY attack and more recently reported breaches.[1]

The responses provided by the 297 individuals completing the 2015 HIMSS Cybersecurity Survey helps to gauge the awareness and readiness that healthcare organizations have in this era where significant security incidents are a regular occurrence. Respondents, each of whom have some level of responsibility for information security at their organizations, reported using an average of 11 different technologies to secure their environments and more than half indicated their organizations have hired a full-time professional, such as a Chief Information Security Officer (CISO), to manage the information security functions.

The majority of respondents (87 percent) also indicated that information security had increased as a business priority at their organizations over the past year, resulting in improvements to security posture, such as improvements to network security capabilities, endpoint protection, data loss prevention, disaster recovery and information technology (IT) continuity.

However, despite the protective technologies implemented at healthcare organizations, respondents reported an average level of confidence with their organization's ability to protect their IT infrastructure and data. Survey respondents were most confident their organizations could defend against a brute force attack[2] (**4.77**) and least confident their organizations could protect against a zero day attack (**3.82**)[3].

Indeed, two-thirds of respondents indicated their healthcare organizations had experienced a significant security incident in the recent past. And while the single largest source of a security incident was a negligent insider, 64 percent of respondents noted an incident at their organizations by

[1] Please see http://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation.
[2] Respondents were asked to rate their organization's ability to protect IT infrastructure and data against a number of types of compromises using a one to seven scale, where one is "not at all prepared" and seven is "fully prepared."
[3] For the purposes of this survey, a zero day attack was defined as the exploitation of vulnerabilities not known to the software vendor/manufacturer.

an external actor, such as an online scam artist, hacker, or through social engineering. Furthermore, while the majority of respondents noted that security incidents were detected within 24 hours, approximately 20 percent of these security incidents ultimately resulted in the loss of patient, financial or operational data.

Additionally, respondents noted that today's security tools are not going to be sufficient to protect the industry against the types of security threats their organizations expect to face in the future. Indeed, respondents were widely likely to indicate that more innovative and advanced tools are required to secure their environments in the future. Furthermore, they indicated that healthcare organizations must operate from a perspective which presumes their organization's perimeter has already been breached. Moreover, more than half of respondents (59 percent) indicated agreement with the statement "cross-sector cyber threat information sharing is beneficial to my organization."

Finally, respondents reported being highly concerned about the prospect of a future attack against their organizations. They were most likely to be concerned about phishing attacks, negligent insiders and advanced persistent threat (APT) attacks.

Other key survey results included the following:

Security Tools and Technologies: Healthcare organizations continue to rely on technologies such as anti-virus software, firewalls and data encryption to secure their IT environments. Respondents were much less likely to report their organizations used multi-factor digital identity (where digital identity is used for authentication), dynamic biometric technologies and dark web research.

Assessment of Network Defense and IT Security Capabilities: Respondents were most likely to report the use of risk assessments and vulnerability scans to assess their organization's security. Only 12 percent reported their organization conducted a mock cyber defense exercise.

Motivators for Improving Information Security Environments: The top motivators for improving information security environments included results of risk assessments and concerns about phishing attacks and viruses/malware.

Detecting Security Incidents: The majority of respondents indicated that security incidents at their healthcare organizations were identified by an internal resource, such as an internal security team. Only 17 percent of respondents indicated that security incidents were identified by an external source, such as a patient whose information was compromised or a law enforcement agency.

Sources for cyber threat intelligence: Nearly 60 percent of respondents reported getting information about cyber threat intelligence from their peers (i.e., word of mouth). Third party vendor threat intelligence feeds (49 percent) and US Computer Emergency Readiness Team (CERT) alerts were also fairly widely used (45 percent).

Investigating Security Incidents: More than half of respondents reported that an external organization, such as a vendor/consultant or law enforcement agency, was brought in to investigate their security incidents. However, nearly half reported their healthcare organizations addressed the security incidents solely through an internal investigation.

Barriers to Mitigating Security Events: While respondents were most likely to indicate that lack of staffing and lack of financial resources were key barriers, 42 percent also indicated that there were too many emerging and new threats to keep track of.

External threat actors: Two-thirds of respondents reported a high degree of concern related to external threat actors. In comparison, 42 percent of respondents reported a high degree of concern in regard to insider threat actors.

For More Information

Joyce Lofstrom
Senior Director, Corporate Communications
HIMSS
312/915-9237
jlofstrom@himss.org