Finding Remedies for Healthcare's Top 3 IT Security Headaches

With so much at stake to keep patients well and research humming while still maintaining financial integrity, healthcare organizations tend to have their hands full when it comes to cybersecurity.

HEADACHE #1

The highly regulated environment complicates compliance objectives.

HIPAA may be the most obvious compliance concern, but that's only the start for most healthcare organizations.

While HITECH put additional regulatory "teeth" into HIPAA security requirements in terms of penalties, its biggest impact has been accelerating the adoption of electronic medical records and expanding the scope of HIPAA to fully cover "business associates." Even with HITECH, the HIPAA Security Rules remain largely nonprescriptive, leaving healthcare organizations looking for guidance in how exactly to avoid costly breaches that result in fines from the Department of Health and Human Services or the Federal Trade Commission.

As a result, many healthcare organizations are increasingly dependent on frameworks like the Council on Cybersecurity's Top 20 Critical Security Controls and NIST 800-53 to guide their security practices. And since healthcare organizations also take credit cards to handle patient payment, they must comply with the Payment Card Industry Data Security Standards.

Overall, while healthcare may not be quite as regulated as, say, financial services, the industry is burdened by a complicated set of regulatory requirements. Furthermore, unlike financial institutions, where a fairly limited portion of an organization's data may be considered sensitive, sensitive data can be found on the vast majority of systems in healthcare. This limits the utility or practicality of network segmentation, expanding the scope of compliance efforts. Thus, many organizations find it difficult to not only keep continuous track of IT's state of affairs across all of these requirements, but to also maintain a trail of documentation that will satisfy all of the auditors and assessors connected with these regulations.

How Tenable can help: In addition to discovering and assessing 100 percent of an organization's physical, virtual, mobile, and cloud assets, Tenable continuously monitors the IT environment for compliance with configuration guidelines and controls relevant to healthcare auditors. Tenable's platform also incorporates an advanced analytics engine that combines sensor data with threat intelligence feeds, directory integration, and infrastructure connectors to provide comprehensive context for precise identification and efficient mitigation of security exposures and compliance violations. Delivered through a growing collection of dashboards and customizable reports, Tenable empowers security and IT personnel, auditors, and executives with the actionable information they need.

HEADACHE #2

Medical technology and mobility are advancing faster than security measures.

On one hand, HITECH has encouraged healthcare providers to adopt electronic records for the sake of efficiency. On the other, this transition has not always been met with commensurate security practices needed to effectively protect electronic health data.

This is just one example of how technological advancement in healthcare is outstripping IT security's ability to keep up. This trend rears its head elsewhere, as well. In many ways, healthcare IT is on the cutting edge of innovation. For example, mobility has been fully embraced by clinicians and healthcare executives to improve quality of care. Healthcare organizations are also broadly

embracing cloud services for a variety of clinical and non-clinical applications. And new internet-connected healthcare devices are making it easier for doctors to share data more quickly with one another when tracking patient health and collaborating on a patient's care.

Unfortunately, healthcare's security measures are not keeping up with the innovation. For example, in one report from a security ratings company, healthcare organizations ranked at the bottom behind retail, utilities, and financial verticals.[1] And healthcare experienced the largest growth in security incidents from 2013 to 2014.[2]

With all of those mobile devices and web-enabled medical devices floating around healthcare facilities, it is also not a surprise that nearly half of all incidents were the result of unprotected devices on healthcare networks.[3]

How Tenable can help: Tenable provides greater visibility into the entire IT environment, including managed and unmanaged mobile devices, such as tracking iPads that doctors are using, to ensure that they're not introducing vulnerabilities to the network. Similarly, since medical devices tend to be very fragile, Tenable's passive scanning technology can be used to find these devices and identify associated vulnerabilities and configuration issues without endangering patient safety by accidentally knocking them offline. This helps ensure the integrity of the devices and related patient data, while reducing the overall risk to an organization's network.

Additionally, Tenable's passive scanning technology helps prevent data loss by continuously analyzing data in motion and identifying sensitive data, such as patient identifiers, Social Security numbers, or credit card information. The technology provides deep packet inspection to continuously discover and track users, applications, cloud infrastructure, trust relationships, and vulnerabilities. It identifies a wide variety of file sharing and data-in-motion activity, which can be used to analyze insider activity, highlight inbound and outbound communications, and spot corporate policy violations.

HEADACHE #3

Criminals are monetizing cyberattacks against healthcare.

According to security researchers, stolen healthcare credentials are being sold on the black market for $10 each—about 10 to 20 times the value of credit card numbers.[4] As criminals increasingly monetize stolen healthcare data, the industry should anticipate a significant rise in cyberattacks.

Not only are health records of interest, but so, too, is personal data about patients and valuable repositories of medical research. A most recent example of how valuable this data is to attackers comes by way of the Chinese attack against Community Health Systems, which resulted in the personal data of 4.5 million patients being stolen.

How Tenable can help: As healthcare organizations monitor their IT environments, they must remain vigilant to ensure that the advanced, sneaky malware that is the hallmark of today's cybercriminal isn't lurking on the network. Tenable can help spot potential backdoors and footholds of crooks so that organizations can know if they've been compromised before they find out about a breach from the FBI knocking on the door. In those instances when healthcare organizations are targeted by capable and well-resourced

[1] "Health Care Lags Financial Sector in Security Effectiveness," eWeek, May 28, 2014

[2] "Health IT security lags behind retail industry," FierceHealthIT, May 28, 2014

[3] "Healthcare security stuck in Stone Age," Healthcare IT News, April 22, 2014

[4] "On black market, medical records far more valuable than credit cards," New York Post, Sept. 25, 2014

attackers, continuous monitoring enables faster breach detection. Being able to passively detect malware and suspicious network behavior are key components of continuous monitoring, which can result in the reduction of critical metrics like time to detection and time to containment.

Conclusion

Tenable's vulnerability and threat management platform enables healthcare organizations to clearly see their infrastructure, simplify the IT environment, and better protect the business. The platform enables continuous discovery, assessment, and reporting on every component of the network against a security policy. This gives healthcare organizations superior visibility into the risks to their business, so those risks can be measured and mitigated.

To enable continuous monitoring, Tenable provides a unique combination of detection, reporting, and pattern recognition, utilizing industry-recognized algorithms and models. Tenable sensors include vulnerability scanners, system agents, network sniffers, and log analyzers. These sensors discover 100 percent of healthcare infrastructure, regardless of whether it includes mobile, Software as a Service, Applications as a Service, Infrastructure as a Service or traditional on-premises hardware and virtualized applications—even sensitive (and otherwise "un-scannable") medical devices.

For healthcare organizations facing growing security threats, Tenable enhances day-to-day security operations capabilities, enabling resource-strapped healthcare organizations to meet multiple compliance demands, while simultaneously strengthening defenses. To accomplish this, Tenable integrates with and correlates data from existing security technologies, helping security teams orchestrate, optimize, and manage their defenses more efficiently. The Tenable platform also offers role-based administration and reporting. These are tied together with built-in security analytics and an expanding collection of dashboards. Ultimately, the total package delivers the insights that security operations and incident response teams need to respond faster and more effectively.