Symantec

Cyber Security and Healthcare: An Evolving Understanding of Risk

Healthcare organizations and their supply chains are under attack—a review of 2017 and a look ahead.

AN ISTR EXECUTIVE SUMMARY FOR HEALTHCARE PROFESSIONALS

With cyber attacks becoming more purposeful, sophisticated, and costly, the healthcare industry is having to come to terms with its exposure to cyber risks. Considering this, Symantec examined the results of its 2018 Internet Security Threat Report (ISTR), and other relevant information published by third parties, to offer a detailed look into healthcare's current cyber security environment. The goal of this executive summary is to provide healthcare organizations with actionable information from select, reputable sources to help them identify, understand, and address cyber security risks.

Cyber Risks in Healthcare

The problem is not just that the number of breach incidents continues to grow about 10 percent each year. It's also the emergence of a new class of attacks, which has the potential to inflict great damage. In 2017, the industry was hit with several high-profile ransomware and malware attacks, which demonstrated both the vulnerabilities of healthcare organizations and their exposure to complex cyber risks.

Several factors shape healthcare's cyber risks:

- The industry's rapid adoption of digital systems
- The emergence of health data as a high-value target for cyber criminals—from sensitive patient data to confidential research and intellectual property
- The rise of healthcare organizations as high-profile targets for hacktivists and nation states
- The technical and organizational complexity of the industry, which makes it difficult to implement and maintain tight security controls

As threats continue to evolve, healthcare organizations—not just hospitals but all organizations in the healthcare supply chain—need to take steps now to identify and reduce their exposure.

Changing Healthcare Breach Trends

The healthcare industry clearly is in a time of transition, and that includes IT infrastructure and cyber security. A review of recent reports shows some important shifts in the traditional measures of cyber security: the number of breach incidents and the number of records breached.

Not all the news is bad. For example, according to a review of data collected by the Department of Health and Human Services' Office of Civil Rights, even as the number of reported breach incidents continues to increase at about 10 percent each year since 2010, the number of breached records has decreased by nearly 96 percent in recent years—from 113 million in 2015, a record-setting year due to several large or very large breaches, to 5.1 million in 2017.

But the pressure is not letting up. A global study by NetDiligence of cyber insurance claims in 2017 found that healthcare accounted for 18 percent of breaches across all sectors—tied for the lead with professional services—and that 63 percent of healthcare breaches were caused by criminal or malicious activity.

The numbers only tell part of the story, however. Last year also brought several high-profile ransomware incidents. At present, ransomware accounts for a small portion of all security incidents—10 percent, according to NetDiligence. But it represents a new kind of cyber risk: a targeted, well-orchestrated attack that, while limited in scope, can have a high impact along the healthcare supply chain.

In May 2017, the WannaCry ransomware outbreak provided an early indicator. This event affected mostly hospitals belonging to the National Health Service in the United Kingdom; only a few hospitals were affected elsewhere, including in the United States.

SamSam, which struck later in the year, was a different story. While most ransomware typically does not focus on specific organizations and is delivered via generic e-mails, SamSam exploited external-facing vulnerabilities or stolen credentials to penetrate targeted organizations—and used well-orchestrated execution to exert maximum pressure.

As these examples show, there are no easy answers when it comes to defending against and responding to ransomware. In general, the FBI does not advise giving in to ransom demands, and experience teaches us that systems are fully recovered in only half of the cases. But every situation is unique. The real lesson here is that ransomware is a significant challenge that healthcare organizations must meet head on.

More Trouble on the Horizon

Unfortunately, as outlined in the Symantec 2018 Internet Security Threat Report (ISTR), ransomware is just one of several emerging threat trends that dovetail directly with healthcare's weak spots:

- Software supply chain attacks. One effective method for penetrating an otherwise well-guarded network: Implant a piece of malware in an otherwise legitimate software package at its usual distribution location. The ISTR notes a 200 percent increase in this type of attack in 2017, including the Petya/NotPetya outbreak, which was introduced via a software supply chain attack and ended up affecting the global goods and services supply chain, including healthcare.
- Internet of Things (IoT) and industrial control system (ICS) attacks. Medical devices and industrial systems typically are not part of an organization's core IT infrastructure. But once they are on the network, they are exposed to a whole range of exploits. The ISTR notes a 600 percent increase of attacks on IoT devices, and a 29 percent increase in attacks involving ICS.
- Ransomware attacks. As noted, ransomware was a major issue in 2017. The ISTR notes a 46 percent increase in variants, but a decrease in total ransomware families. The profitability of ransomware led to a crowded market, lowering the average ransom cost (average demand was $522, about half of the year before) and signaling that ransomware is becoming a commodity. Going forward, we expect ransomware to continue playing a role in the healthcare industry, although cyber criminals are shifting their focus to coin mining as an alternative income source.
- Crypto-mining and crypto-jacking malware. The last quarter of 2017 saw a surge in these attacks, in which Bitcoin (and other crypto currency) 'miners' hijack an organization's processing power, often resulting in big hits on performance, if not system failure. This is clearly something that is very concerning in light of a hospital's need to reliably deliver 24x7 care.

A Path to Greater Maturity

Given the growing spectrum of risks and resulting impact or harm, healthcare organizations need to think in new ways about cyber security. First, they need to see cyber security not as a compliance exercise but as an independent activity with its own priorities and timelines. In the same vein, they must recognize that cyber security is not just the responsibility of IT, but of the whole organization.

Here are key characteristics of an organization with a mature approach to cyber security:

- Executive board members, who understand cyber risks and how they might affect the business of healthcare, establish a culture of security and provide sufficient budget and staff to enable execution.

- Hospital administrators take responsibility for cyber security, both tactically (for example, by including cyber requirements in contracts) and strategically (for example, by preparing for possible supply chain disruption).
- Clinical staff members recognize their role in cyber security and contribute to the discussion, providing insight and finding a balance between care delivery and security controls—including during security incident response when critical decisions affecting patient care need to be made.

Healthcare is more than just a large and complex industry. It is part of our nation's critical infrastructure—one that is increasingly in the crosshairs of cyber adversaries. Given these stakes, the industry's traditional reliance on new and better point solutions is not enough. What's needed is a holistic, layered, and multistakeholder approach to protecting these vital assets. The goal is not to treat each risk as a one-off problem, but to integrate solutions into a cohesive whole, from the on-premise network to the cloud to the endpoint … and everything in between.

For the details, download the
Symantec 2018 Internet Security Threat Report (ISTR)
https://go.symantec.com/ISTR

Resources

Additional information on key issues.

HHS OCR Breach Data Analysis

Here are key findings from a review of data collected by the Department of Health and Human Services' Office of Civil Rights (data based on reporting of breaches affecting more than 500 individuals):

- 'Hacking/IT incident' is now the single largest category of breach events, at 41 percent, and accounts for 68 percent of breached records.
- Although the number of breach incidents continues to increase by about 10 percent each year since 2010, the number of breached records actually has decreased by nearly 96 percent over the last three years—from 113 million in 2015, when there were several large or very large breaches, to 5.1 million in 2017.
- Healthcare providers account for 80 percent of breach incidents, far more than health plans or business associates, and almost 90 percent of breached records.

NetDiligence Study

Here are key findings from the global study by NetDiligence of 2017 cyber insurance claims:

- Healthcare accounted for 18 percent of breaches across all sectors, tied for the most with professional services.
- Healthcare accounted for 28 percent of breach costs, due to higher than average per-record costs.
- Criminal or malicious activity caused approximately 63 percent of healthcare breaches.
- Hacking was the most common cause of loss in healthcare (20 percent), with an average breach cost of $2.4 million.
- Ransomware accounted for 10 percent of the costs, with an average cost-per-incident of $76,000.

WannaCry

According to a report from U.K. Health and Social Services, WannaCry hit 81 of the 236 National Health Service hospital trusts, and 595 of 7,545 general practices, affecting about 1,000 pieces of equipment and requiring the cancelation of approximately 20,000 procedures and appointments.

Petya/NotPetya

Here are two examples of how Petya/NotPetya hit the healthcare supply chain:

- Merck Pharmaceuticals reported infections of its production, formulation, and packaging systems, as well as R&D and other operations. This impacted drug and vaccine availability, and the company reported a $310 million revenue impact for the fiscal year. Also noteworthy: The duration of events exceeded six months; the company stated in December 2017 that it was 'mostly recovered.'
- Several of Nuance Communications' hosted transcription services were affected for several weeks, impacting customers and resulting in a $92 million revenue impact for the company's fiscal year.

SamSam Ransomware

Here are two examples of how SamSam played out:

- Hancock Health (Greenfield, IN): The attacker used compromised credentials of a backup system hardware vendor to first penetrate a backup site, and then the main data center. The hospital paid the ransom (approximately $55,000) and took four days of downtime to get 1,400 computers back online.
- Erie County Medical Center (Buffalo, NY): The hospital did not reveal how it was attacked—and it did not pay the ransom. Instead, the center converted to manual processes, and relied on the state's Health Information Exchange to access basic patient data. It took 12 days to restore limited system access and six weeks to fully recovery at an estimated cost of $10 million.

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure.

Likewise, a global community of more than 50 million people and families rely on Symantec's Norton and LifeLock product suites to protect their digital lives at home and across their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats.

Symantec Corporation
World Headquarters
350 Ellis Street
Mountain View, CA 94043
United Stated of America

+1 650 527–8000
+1 800 721–3934

For specific country offices and contact numbers, please visit our website. For product information in the U.S., call toll-free 1 (800) 745 6054.

Symantec.com