Level 3 COMMUNICATIONS

Connecting and Protecting the Networked World℠

# COMPLIANCE DOES NOT EQUAL SECURITY

## 3 EMERGING SECURITY THEMES IN HEALTHCARE

## INTRODUCTION

Security is a serious issue for healthcare providers — and one that won't resolve itself. With close to 100 million healthcare records compromised between January and June at a high cost of $363 per record, IBM labeled 2015 the "year of the healthcare security breach."

Ninety-six percent of industry IT security experts feel vulnerable to a data breach, and 63 percent report having suffered one. Despite these concerns, 69 percent feel that meeting compliance requirements is "very" or "extremely" effective in safeguarding sensitive data.

Is that confidence misplaced?

## THE SHORTCOMINGS OF COMPLIANCE

The security and privacy rules outlined in HIPAA established national security standards to protect electronically held and transferred healthcare information. Rolled out alongside meaningful use stipulations, these standards were a critical step in the fight to protect highly confidential digitized information from unauthorized access.

Cyber threats and the security landscape evolve rapidly, and industry standards cannot keep pace. As more communications are run over networks and more care-critical applications are virtualized in centralized data centers, ensuring security and uptime will become more important. Providers must protect not only data, but also the continuity of care and the availability and performance of digital tools.

End points are expanding and growing ever more complex. New approaches in healthcare, telemedicine, at-home care and mobile health will only increase over the next decade. These developments will amplify current complexities, making end-to-end security even more critical.

## **THE BIGGEST THREATS TO** HEALTHCARE SECURITY

Healthcare professionals should concern themselves with three major threats today:

1. **Vulnerable Connected Devices**

   The number of connected devices in healthcare is growing exponentially, and industry forecasters predict the market for these devices will reach $163.24 billion by 2020. This is a welcome development in that it is helping to revolutionize our healthcare industry — but more devices also mean more end points and, subsequently, a greater threat of potential criminal interference along the way.

   Cyber criminals can exploit these devices and scan for open ports to find ways to infiltrate networks. Once inside, they can plant malware, Trojan horse attacks and viruses capable of causing untold damage. While the threat to data is recognized, the impact such attacks can have on connected devices is less commonly understood. And everyone involved with a healthcare organization needs to appreciate this danger.

   If a dialysis machine is connected to the internet, for example, then it is vulnerable to malware — and the consequences of such an event could be deadly. To avert such catastrophes, healthcare organizations must educate all employees and consistently scan the edges of their own infrastructure for weaknesses.

2. **Distributed Denial-of-Service (DDoS) Attacks**

   Imagine an ER doctor consulting with a neurologist as he or she treats a stroke patient. The two are talking via a telemedicine connection when the network suddenly goes down and communication channels close. The result could be devastating, and DDoS attacks can create this kind of situation.

   A distributed denial-of-service (DDoS) attack is one of the most prevalent types of security threats today, with a 40 percent increase in DDoS attacks in the second half of 2015 — and they don't require a high level of technical knowledge to pull off. A DDoS attack consists of an attempt to make a machine or network resource unavailable to its intended users by flooding it with access requests from thousands of unique IP addresses.

   This type of attack is particularly worrisome for healthcare organizations whose care-critical applications and communications rely on uptime and network performance. In early 2016, for instance, a large acute care provider called us after experiencing a DDoS attack that nearly took down its entire IT organization. We were able to identify the threat and mitigate it, but this is just one of countless examples where healthcare organizations are targeted by DDoS attacks and left with no or limited access to care-critical tools and information. As more care-critical applications are virtualized, these attacks will become increasingly devastating.

3. **Phishing Scams**

   Thus far, more than 36 percent of security breaches suffered by U.S. healthcare organizations in 2016 were phishing attacks. Because they target one of the most labor-intensive industries, healthcare phishing attacks, in particular, require immediate attention and action.

   A phishing attack involves an attempt by criminals to acquire sensitive information — from usernames and passwords to credit card details and Social Security numbers — by masquerading as a trustworthy entity. Employees, administrators and IT departments need to collaborate as a team to prevent such attacks and ensure that confidential patient information is protected.

   To do so, organizations must carefully determine who will be provided with access to data sets and systems on the network. Clearance should be restricted, and access codes should never be shared. Creating a proper framework for data access is the best way to help IT professionals identify unusual activity.

   Security threats are so prevalent today that it is not a matter of whether an attack will occur, but when. Healthcare organizations must make security a top priority and invest in digital tools that are iterative to help prioritize resources and address the most pressing threats.

With 73 percent of U.S. healthcare organizations suffering incidents related to third-party vendors, it's critical to research and vet all potential providers thoroughly. This requires selecting best-of-breed players with a global view of the healthcare security landscape capable of delivering comprehensive security solutions, secure-but-mobile end points, protected patient data and network continuity. There is simply too much at stake for organizations to sit on the sidelines and maintain simple compliance.

## **ABOUT** THE AUTHOR

**Karin Ratchinsky, the director of healthcare vertical strategy at Level 3 Communications, is highly motivated, competitive and collaborative. At Level 3 Communications, Karin has been instrumental in accelerating sales, generating and deploying effective market strategies, and growing brand equity within the company's healthcare vertical ecosystem.**

## ABOUT LEVEL 3

We operate and take end-to-end responsibility for network solutions that connect you to the world. We put customers first and take ownership of reliability and security across our broad portfolio.

**1.877.4LEVEL3 | INFO@LEVEL3.COM**
**LEVEL3.COM**