SI SCOTTSDALE INSTITUTE
COLLABORATION • EDUCATION • NETWORKING

INSIDE EDGE

Chief Information Security Officer Outlook 2016

Executive Summary

Healthcare's 'new normal' has many faces as it moves into a digital, value-based model, and surely one of them is the daily threat to the security of patient data. So much have CEOs and CIOs been kept awake at night worrying about cyber security that they created a new senior executive to absorb that headache: the chief information security officer or CISO. More than a full-time job, CISOs are tackling the fundamental tasks of integrating privacy and security, converting corporate culture to one of security and collaborating with other health systems nationally to track and fight cyber threats as preemptively as possible.

That's why we selected CISOs to feature in SI's traditional January Outlook issue. For our first CISO Outlook we interview some of the leading healthcare information security executives in the country. We hope you will sleep better tonight after reading this issue.

Meredith Phillips
Chief Information Privacy & Security Officer
Henry Ford Health System

Meredith Phillips is a veteran in a fairly new role—in her case, CIPSO, for chief information privacy and security officer—for Henry Ford Health System in Detroit. At Henry Ford for 13 years, she was chief privacy officer for eight years when the health system decided to combine that role in 2011 with the chief security officer job, traditionally focused more on the IT risk-management function.

Meredith Phillips, Chief Information Privacy & Security Officer, Henry Ford Health System

"Privacy is more behavioral, more policy oriented. It's about what you can and cannot do. Security is more on the technical side which ensures certain policies are followed," she says. "I love the question, 'What keeps you awake at night?' It's never a technical answer. Henry Ford has 23,000 employees who have been given access to secured information. Every day they have to make a judgment call. No level of technology is going to help them with that. The real question is 'How do we engage with those individuals?'" says Phillips.

"It's really a cultural shift for healthcare. We haven't been used to this in healthcare."

In 2016 BYOD will be a Henry Ford focus, especially with physicians who like to use their own devices like smartphones and tablets in a clinical setting. "It's always a delicate balance. How do you give them flexibility while securing data? How do we mobilize the enterprise and still protect privacy? In addition, the Internet of Things expands potential exposures to medical devices and BYOD, including laptops, iPads and iPhones." All must be examined to ensure risk for the organization is managed.

Second is data loss prevention. "The ability to store information in the cloud and go home" means the organization has to invest in technology to prevent data exfiltration. Phillips says she can never speak enough about data loss prevention. "How do we get ahead of it?"

Collaborating against attacks

Third on Henry Ford's list of security and privacy initiatives is beefing up security through cyber-threat sharing as a member of the National Health Information Sharing and Analysis Center (NH-ISAC, http://www.nhisac.org/), to which multiple healthcare organizations belong.

NH-ISAC is the nation's Healthcare and Public Health Information Sharing and Analysis Center, responsible for advancing all-hazards (physical and cyber) security national critical infrastructure resilience. NH-ISAC is recognized by the U.S. Dept. of Health and Human Services (HHS), the Health Sector-Coordinating Council (SCC), the U.S. Dept. of Homeland Security, the National Institute of Standards & Technology (NIST), Law Enforcement and the National Council of ISACs (NCI Directorate), representing all national critical infrastructures.

"If Henry Ford was being threatened by a foreign entity we'll share that information with other health systems through NH-ISAC, a society of security officers to protect our industry from cyber attacks. It helps us to be more proactive," she says.

Another area Henry Ford is focused on in 2016 is advanced threat detection. "We've gone through a period of asking, 'How do we react?' Our philosophy has changed to, 'How do we get ahead of the threat?" says Phillips. Henry Ford has planned out the strategy for a security operations center (SOC) that monitors all of the health system's data networks and enables staffers to quickly shut down a threat if the network comes under attack.

"We know technology is not foolproof. We want to expand the SOC to achieve greater visibility into our data center—'eyes on glass,'" she says. Amazingly, in a typical breach the cybercriminal is in a system for 204 days on average before the organization detects it. "So, one of our goals is to reduce that timeframe to the shortest timeframe possible."

Jigar Kadakia
Chief Information Security Officer & Chief Privacy Officer
Partners HealthCare

After more than a decade as a consultant, including at Deloitte, two years ago Jigar Kadakia arrived at Boston-based Partners HealthCare as CISO and Chief Privacy Officer (CPO). For 2016 he is focusing on "a few big-ticket items."

First is moving from a more reactive security program to a proactive one. That involves incorporating analytics into the IT-user environment to monitor user behavior, especially identifying fraudulent activity. "We perform a lot of event monitoring triggered by factors like bad IPO addresses or someone bringing a brand-new virus. When they hit your system it's possible to detect

Volume 22, Number 1

Chairman
Donald C. Wegmiller

Executive Director
Shelli Williamson

Editor
Chuck Appleby

Managing Editor
Jean Appleby

Membership Services Office:
7767 Elm Creek Blvd. N., St. 208
Maple Grove, MN 55369
T. 763.710.7089
F. 763.432.5635
E. scottsdale@scottsdaleinstitute.org
W. www.scottsdaleinstitute.org

them through their unique signatures and other identifiers," he says, adding that information-sharing groups like NH-ISAC play a critical role in this area.

Being proactive means scanning data and user behavior to detect such abnormalities. "While 99.9 percent of users might be safe, .001 percent could be someone who walked into the hospital undetectable. Analytics has to be able to detect that threat," Kidakia says.

PARTNERS® HEALTHCARE | FOUNDED BY BRIGHAM AND WOMEN'S HOSPITAL AND MASSACHUSETTS GENERAL HOSPITAL

Jigar Kadakia, Chief Information Security Officer & Chief Privacy Officer, Partners HealthCare

For example, a standard user typically works Monday through Friday, 8 to 5, logging in at about 8:30 and logging out at 5-ish. They go to seven systems. What happens if they come in early Saturday for a couple hours? The security staff would question that behavior and if necessary conduct a deeper analysis, ultimately talking to the supervisor or the individual. At the very least you're now aware of the work pattern," he says.

Documenting facetime

Second is to develop a long-term strategy for mobile devices, including BYOD and the expanding panoply of hospital devices. "We're addressing how to manage mobile in the context of our growing use of telehealth and telemedicine. The strategy is being developed and we're working on a number of options that fit with our culture and work with our patients. What is the strategy for documenting facetime, for example?" he says.

"We have to be patient-friendly and patient secure. The wave of the future is that physician/patient interaction is going to be different. Millennials don't go to the bank anymore. Ten years from now you'll have a doctor's visit on Facetime or take a picture of a rash and send it to the doctor. You may be monitoring vitals using a wearable. There's a lot of telehealth happening now which is changing most physician/patient interactions to remote ones so the physician can focus more time on sicker patients."

A third area is the continued focus on education, to make employees more aware of what they're doing. "People still fall into bad habits. They click on links they shouldn't, for example. This applies not only to the Partners environment but to their personal life as well," Kadakia says.

"The last line of defense is always the people and you need to find new and different ways to educate them. If you keep doing the same thing they'll become numb to it."

A fourth area, he says, "is talent, always. How do we create, acquire and maintain a top-notch security workforce? Cyber security skills are hot and from a limited pool. There's a high premium for the skillset. As a non-profit healthcare system we can't give employees stocks in an IPO. Google is the number two employer in our market; Partners is number one. To recruit people in the non-material generation you can appeal to a sense of gratitude, mission, giving back and social consciousness. For millennials, 17 to 35 years old who have grown up on iPhones, you look for new things. Technology for them is an enabler, not an efficiency tool."

Fernando Blanco
Chief Information Security Officer
CHRISTUS Health

You might say Fernando Blanco is the newest of the new. He has been chief information security officer at Irving, Texas-based CHRISTUS Health for only about three months, brought in to lead an initiative to consolidate the cybersecurity program at the Catholic health system.

"CISOs with Catholic health systems are all in about the same early stage," he says. "The 2015 high-profile hacking in healthcare was a wakeup call. But it seems to be a healthcare-industry alert. Cyber security was neglected until now."

CHRISTUS has significantly increased its investment in cybersecurity from last year, with the objective of building a resilient organization. The strategy will focus on five major priorities for 2016. The first is strengthening basic security strategies—"basic blocking and tackling:"

- Vulnerability management;
- Patching (strengthening of perimeters);
- Perimeter Protection (firewalls).

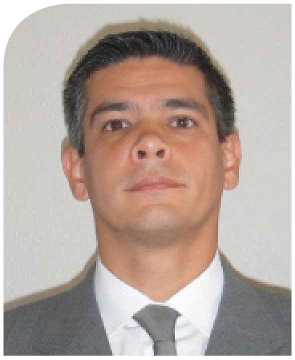
"This is not new. Everybody does it. However, we can never neglect the foundation," Blanco says.

The remaining security priorities are more consistent with new trends in the industry:

- The cloud;
- Mobility;
- Big data;
- User education.

Tension

"There's a tension between IT and security," he says. "To support the business IT wants to be cheaper, better and faster, factors that often conflict with security. The cloud is a perfect example. The cloud's accessibility to any device allows great business flexibility. Using the cloud allows health systems expanding into the community, for example, to quickly open many new clinics in a short time.



Fernando Blanco, Chief Information Security Officer, CHRISTUS Health

From a security standpoint that same speed and flexibility pays a price, however.

"The cloud does not exist," says Blanco. "Your data is stored on some server. Where is the server? Who is managing this server? How much is insurance and liability? Do we want a multi-tenant server or an independent one? Do I have my own database within this server or am I sharing it with another hospital?"

There is no alternative. "This is a trend that nobody can stop. There will be cloud services in every health system. The question is can we do this in a controlled way? The leadership team needs to decide what kind of information the organization wants in the cloud. Patient information? Financial information? With mergers and acquisitions that include cloud services you need to ask, 'Are we ok with this?'" he says.

Mobile matures

Mobility is another challenge because it involves providing associates with access to information systems from their own devices. "In the infancy of mobile technologies in healthcare we didn't have the tools to segment information for security purposes. Now we have apps installed in mobile devices to split or segment the personal information from business information. In the past if the device got lost or the person left the company, if you decided to wipe the corporate information from the device you could erase the personal information as well," says Blanco.

Big data is a big test in 2016. "We have a business intelligence (BI) program that allows us valuable analysis of data out of the data warehouse. The key is transforming that data into information and then, once that's done, figuring out how to exchange this information in a secure way," he says.

Leadership must decide whether or not to outsource the big-data function to outside firms, many of which excel at distilling usable information from stored data. However, says Blanco, "to do that you give them access to the data warehouse. There's a tension. Business versus security. We have a responsibility to maintain security and privacy for patients. That's the work we're going to be doing this coming year."

Finally, the "wrapper" around all these elements is user education. "As health systems we have a lot of self-inflicted damage. There are a lot of phishing attacks and the clicking rate is very high at CHRISTUS, 3 percent to 5 percent of my users, which is still lower than the rest of healthcare. We're going to invest a lot in user education in the next year."

Conclusion

It's clear from our first CISO Outlook that 2016 will be a pivotal year for security and privacy in healthcare. A confluence of factors promises to put the healthcare CISO in the spotlight: an expanding digital footprint, increased mobility and BYOD, big data and the need for employee and patient engagement all dramatically increase the all-ready high stakes. Healthcare CISOs are looking beyond this year, of course, presenting three-to-five-year plans to CEOs and COOs, which validates the top-down focus on security and privacy. The jury's still out on whether they'll sleep better at night.

SI **SCOTTSDALE INSTITUTE**

COLLABORATION • EDUCATION • NETWORKING

BOARD OF DIRECTORS

STANLEY R. NELSON
Founder & Chairman Emeritus (1993–2012)

Executive Committee

Don Wegmiller, Chairman

Shelli Williamson, Executive Director

David Classen, MD, Associate Professor of Medicine, University of Utah, CMIO, Pascal Metrics

Tom Sadvary, CEO, HonorHealth

Board Members

David Campbell, David Campbell and Associates

Stephen C. Hanson, FACHE, CEO, Baptist Health

Steve Heck, Chairman, MedSys Group

Laura Kaiser, EVP & COO, Intermountain Healthcare

M. Michael Shabot, MD, EVP, Chief Clinical Officer, Memorial Hermann Healthcare System

Bruce Smith, SVP & CIO, Advocate Health Care

Joseph R. Swedish, FACHE, President & CEO, Anthem

Anthony Tersigni, CEO, Ascension Alliance

Scott Weingarten, MD, SVP & Chief Clinical Transformation Officer, Cedars-Sinai Health System

Nicholas Wolter, MD, CEO, Billings Clinic

COLLABORATION • EDUCATION • NETWORKING

MEMBER ORGANIZATIONS

Adventist Health, Roseville, CA

Adventist Health System, Altamonte Springs, FL

Advocate Health Care, Oak Brook, IL

Ascension, St. Louis, MO

AtlantiCare, Egg Harbor Township, NJ

Avera, Sioux Falls, SD

Banner Health, Phoenix, AZ

Baptist Health, Louisville, KY

BayCare Health System, Clearwater, FL

Baystate Health, Springfield, MA

Beaumont Health, Southfield, MI

Billings Clinic, Billings, MT

Catholic Health Initiatives, Englewood, CO

Cedars-Sinai Health System, Los Angeles, CA

Centura Health, Englewood, CO

Children's Hospitals and Clinics of Minnesota, Minneapolis, MN

CHRISTUS Health, Irving, TX

Cincinnati Children's Hospital Medical Center, Cincinnati, OH

Eastern Maine Healthcare Systems, Brewer, ME

Emory Healthcare, Atlanta, GA

Henry Ford Health System, Detroit, MI

HonorHealth, Scottsdale, AZ

Houston Methodist, Houston, TX

Indiana University Health, Indianapolis, IN

INTEGRIS Health, Oklahoma City, OK

Intermountain Healthcare, Salt Lake City, UT

Memorial Health System, Springfield, IL

Memorial Hermann Health System, Houston, TX

Memorial Sloan Kettering Cancer Center, New York, NY

Mercy Health, Cincinnati, OH

Mosaic Life Care, St. Joseph, MO

Munson Healthcare, Traverse City, MI

NewYork-Presbyterian Healthcare System, New York, NY

Northwestern Medicine, Chicago, IL

OSF HealthCare System, Peoria, IL

Partners HealthCare System, Inc., Boston, MA

Sharp HealthCare, San Diego, CA

Spectrum Health, Grand Rapids, MI

Sutter Health, Sacramento, CA

Tampa General Hospital, Tampa, FL

Texas Health Resources, Arlington, TX

The University of Texas MD Anderson Cancer Center, Houston, TX

Trinity Health, Livonia, MI

UCLA Health, Los Angeles, CA

UK HealthCare, Lexington, KY

University Hospitals, Cleveland, OH

University of Virginia Health System, Charlottesville, VA

Virginia Commonwealth University Health System, Richmond, VA

Virginia Mason Health System, Seattle, WA

CORPORATE SPONSORS

Cerner

IBM Watson Health

NantHealth

HealthCatalyst
ignite change

Deloitte.

vocera

KORN FERRY

Omnicell®

emmi®
Expertly Designed to Drive Results

Impact advisors

STRATEGIC PARTNER

KLAS®
ACCURATE. HONEST. IMPARTIAL.

January, 2016