SCOTTSDALE INSTITUTE
COLLABORATION • EDUCATION • NETWORKING

INSIDE EDGE

Security and Data Protection

Introduction

The headline of a March 20 article in *The Washington Post* said it all: "2015 is already the year of the health-care hack—and it's only going to get worse." The article noted some dire figures: "Data about more than 120 million people has been compromised in more than 1,100 separate breaches at organizations handling protected health data since 2009." It cited the recent breaches at Anthem and Premera and quoted a cybersecurity expert that this was only the beginning.

Healthcare data is a target because that's where the money is. Personal healthcare data has significantly more resale value in black markets than financial data because it is more comprehensive, can be used for fraudulent medical charges and has a longer life than credit-card information, which issues new cards frequently. While payment-card information currently sells on the Internet for $1 to $3 per name, healthcare information sells for $50 to $60 per name.

The Washington Post article asserted that the industry and government are failing to do enough to protect healthcare consumers' assets, partly because HIPAA lacks specificity and there is "no culture of using ironclad security." Legacy systems from vendors slow to invest in security technology are a major factor in why healthcare, once again, is years behind other industries in IT in this area.

Scottsdale Institute Conferences

Fall Forum 2015
Oct. 29-30, 2015
Seton Healthcare Family
Austin, Texas

Spring Conference 2016
April 20-22, 2016
Scottsdale, AZ

Intermountain's tactical array

Of the IT risks facing healthcare systems, cyber breaches are number one, says Karl West, chief information security officer (CISO) and assistant VP information systems, Salt Lake City-based Intermountain Healthcare, with 22 hospitals and a health-insurance plan covering Utah and southeast Idaho. Beyond the "standard response strategy" of tools and techniques to prevent, detect and meet cyber threats, he outlines several discrete strategies perhaps not on every health system's radar.

1. COMPLETE DATA AND APPLICATION INVENTORY

While inventorying software applications has been hit or miss in the past, today it's absolutely a must to carefully review and identify all software apps and data and to include factors like geolocation and access, West says. For example, is the data/app accessible from mobile devices? From outside the enterprise? Understanding location is critical for physical security.

2. AUTHENTICATION

It's imperative to authenticate software users based on data classification and data categorization: Is it Critical, High, Medium or Low Risk? Intermountain classifies data as level 1, 2, 3 or 4. These levels differentiate public, proprietary, Internal only and Classified data sets.

3. BREACH RESPONSE STRATEGY

"We asked the question, 'What would we do if someone breached our cyber security?'" says West, in order to formulate a response strategy. As a result, Intermountain will conduct two exercises this year to "test the playbook." A security playbook documents critical processes and procedures to create order during a chaotic situation. It organizes and prescribes a consistent

response and all activities required to resolve a security incident.

4. SECURITY OPERATIONS CENTER

Two years ago Intermountain began planning a cyber-security operations center and reviewed outsourcing and service-provider options for that purpose. In the end the organization chose to develop its own center. Up and running today with 14 staffers, six days a week, 14 hours a day, the center uses sophisticated tools to monitor all network access from outside the state of Utah and the U.S.

Karl West, AVP, Information Systems, Intermountain Healthcare

The center also monitors "total volume of requests and size-based access," meaning, West says, "We note the volume of data a user is transferring, and we note how many times a day an individual user is making requests. With that data we can use anomaly-detection software that can identify patterns according to category or user role. If the size or volume of transfers and requests are inconsistent for the user's role we can immediately block the request. We've used off-the-shelf software, but have had to do some log-in data correlation and—following compromise of a database account—added database-monitoring tools to determine who is accessing it 24/7. We also change database passwords every 90 days."

5. DATA-LOSS PREVENTION

Intermountain also implemented a data-loss prevention strategy based on ranking of data risk on a scale of 1 through 4, with 2 and above as high enough risk to require monitoring of network, web, intranet, servers and PCs.

"If people are storing data inappropriately or moving it to a PC or mobile device without authorization, we investigate, asking, 'Why did you do this and move it to a non-approved Intermountain device?' At Intermountain, we open and inspect all SSL traffic such as Google and Yahoo," says West.

6. DEDICATED SECURITY STAFF

Intermountain has gathered a large staff enterprise-wide dedicated to data security and protection. A 45-person privacy & compliance team tackles the issue of appropriate use of information; a 50-person security team covers protection of information. Another 20 to 30 people focus on data security at individual facilities, and on any given day an additional 50 to 100 people can spend up to 20 percent of their time on cyber-security.

> *"If people are storing data inappropriately or moving it to a PC or mobile device without authorization, we investigate."*

While the security team reports to West and the privacy team reports to Compliance, many meetings are combined

Volume 21, Number 3

Chairman
Donald C. Wegmiller

Executive Director
Shelli Williamson

Editor
Chuck Appleby

Managing Editor,
Jean Appleby

Membership Services Office:
1660 Highway 100 South, Suite 306
Minneapolis, MN 55416
T. 952.545.5880
F. 952.545.6116
E. scottsdale@scottsdaleinstitute.org
W. www.scottsdaleinstitute.org

ADVISORS

Vishal Agrawal, MD, Harris Healthcare Solutions
Mark Barner, Ascension
David Bensema, MD, Baptist Health
Joe Boyce, MD, Mosaic Life Care
George Conklin, CHRISTUS Health
Julie Creamer, Northwestern Medicine
John Delano, INTEGRIS Health
Darren Dworkin, Cedars-Sinai Health System
Robert Eardley, Houston Methodist
Lois Elia, Advocate Health Care
Tom Giella, Korn/Ferry
Devin Gross, Emmi Solutions
Todd Hollowell, Impact Advisors
Marianne James, Cincinnati Children's Hospital Medical Center
John Kocon, Catholic Health Initiatives
Gilad Kuperman, MD, NewYork-Presbyterian Hospital
Brent Lang, Vocera
Randy Lipps, Omnicell, Inc.
Jonathan Manis, Sutter Health
Mitch Morris, MD, Deloitte Consulting LLP & Deloitte & Touche, LLP
Mike Neal, Cerner
Patrick O'Hare, Spectrum Health
Rich Pollack, VCU Health System
Dale Sanders, Health Catalyst
Marcus Shipley, Trinity Health
Brent Snyder, Adventist Health System
Alan Soderblom, Adventist Health
Bill Spooner, Independent HIT Advisor
Cindy Spurr, Partners HealthCare System, Inc.
Jim Veline, Avera
Scott Weingarten, MD, Cedars-Sinai Health System

to address strategy and questions like who is allowed access to a medical record. "Is it appropriate for a physician to have access to a record in a location if that physician is 200 or 400 miles away? We have telehealth," for rural areas of Utah, says West, which raises the complexity of protecting data. HIPAA requires minimum necessary access, which means that a nurse who works only in OBGYN has restricted access to other parts of the medical record.

7. SCAN THE WEB

Intermountain also looks for data threats to its corporate identity, monitoring the web for its brand and logo. The health system owns 200 registered domains. "We look for PHI, then call and get websites shut down to protect Intermountain data," he says.

Comes down to integrity

Arlington-based Texas Health Resources (THR), a 24-hospital system serving north-central Texas, views security and data protection as a grass-roots issue. "Our philosophy," says Ed Marx, THR's former CIO, "is that we've made an implicit promise to patients to do everything possible to be good stewards of their care. We've made this our issue."

Ed Marx, former CIO, Texas Health Resources

In addition to conducting "all the old stuff" like audits and penetration testing, he says, "the single biggest issue is the decision each employee makes" to protect the privacy and confidentiality of patient data. An employee answering a phone or clicking on a link that allows even modest access to personal health information makes the organization vulnerable. "It's about personal integrity," Marx says.

Although THR has 25 IT staff involved in data security, each of its 24,000 employees is responsible for security. "We're good at the perimeter stuff, we're current with technology. I could pontificate with you all day about layers of security, all the firewalls and testing. But at the end of the day, the individual person is accountable."

That doesn't mean THR is passive about personal accountability. "We've really focused on the individual person and what their role is. We focus on all the staff, continually educating them and making sure they understand all the factors. That's our biggest risk."

Transparency about audits

Once a year every associate must watch a video series featuring vignettes about security breaches; each person then gets tested—with 90 percent of the 24,000 employees passing. THR also periodically sends out reminders to employees about security issues. A third-party firm conducts penetration tests that include phone calls requesting unwarranted credentials and emails attempting to extract private information. If an employee fails to comply with protocols in responding to these 'intrusions,' THR's security function records the findings and targets that person with special education and training.

> *"At the end of the day, the individual person is accountable."*

Security is a board-level issue. For the past three years an audit committee of THR's board that includes directors and board members has governed security strategy. "We're very transparent about findings from security audits. I don't know how many organizations do that," says Marx. Audits consist of two layers: One, a traditional audit function that conducts multiple audits per year and reports to the compliance officer; Two, a third-party audit by a firm that changes every year. "If we always went with the same firm it would be subject to biases."

THR also has a chief information security officer (CISO), Ron Mehring, with dual reporting to CIO Marx and THR's chief compliance officer. "We don't want security to be too cozy with any single department," he says.

Vendors need to step up

"We're fortunate to have built a robust security program," says John Delano, CIO at INTEGRIS Health, an Oklahoma City-based health system with 9 hospitals serving the Oklahoma market. "It takes money and resources," he says, and INTEGRIS has been able to dedicate FTEs to develop security programs, incidence response and perform risk assessments.

"That said, our IT vendors are not much help. They create a lot of holes for us. We're continually unable to patch to current, security-enhanced versions of software applications," says Delano. For example, INTEGRIS can't upgrade either Internet Explorer or Java software because that would cause a number of INTEGRIS apps to crash. "Healthcare vendors can't keep up. I can't load the latest security patches because I'll bring down clinical applications," he says, adding, "Patching in and of itself is bad enough. Now we've created a hole."

INTEGRIS

John Delano, CIO, INTEGRIS Health

The situation often forces CIO Delano to make difficult decisions, "choosing an old version of an application because you have to keep care going" or risking breakdowns of clinical applications as a result of introducing new technology. "We do risk assessments of any new technology, however, often the vendor lacks security focus and a willingness to fix any vulnerabilities we find. It's scary."

As the number of digital devices and network connections grow, the threat becomes more insidious daily.

Even the air conditioning

For example, the recent and highly-publicized cyber-security breach at Target was the result of an HVAC [heating, ventilating, air conditioning] vendor. "Now, air conditioning units are plugged into the network. It was a vulnerability in an AC-monitoring application that allowed hackers to enter the network," Delano says. "We get a lot of resistance around doing risk assessments, 'Oh, it's just an air conditioner.' But it's a node on the network. Those nodes are regularly expanding, especially with Blue Tooth wireless."

Home health poses an interesting dilemma. For example, for INTEGRIS to get reimbursed for a patient using a CPAP machine for sleep apnea requires 30 days of compliance data. Today those machines are transmitting the data wirelessly. "It's the proliferation of data, the Internet of Things. Everything is gathering data. Today, your healthcare data is worth more than financial data."

At this point, Delano says, the only approach is vendor-by-vendor. "Part of it is the lack of standards in healthcare. You can point to HIPAA as a loose standard. Another example, cross-site script errors are a known vulnerability. Why wouldn't any vendor make sure they have corrected it? Any 12-year-old can download instructions on how to exploit it. Vendors don't have enough stakes in the game. If any data gets breached, it's our brand that takes the hit."

> *"Healthcare vendors can't keep up. I can't load the latest security patches because I'll bring down clinical applications."*

Conclusion: All it takes is a single device

On one level the struggle for security and data protection is like trying to keep the tail from not only wagging the dog but destroying it. An event at Intermountain last summer offers a glimpse of the kind of random event that keeps executives like West awake at night.

The organization lost a digital device from a load of 24 such devices in transit from a facility to a doctor's office to a car to a truck and finally a warehouse. The device was missing for nine days. "This particular division had a lot of records," recalls Intermountain's West. Staff searched every step of the path including the trailer carrying the devices. "The ninth day we found that asset where we suspected all along: in the transmission dock, behind the cage. The person working there was dead certain it wasn't there. There was a lot of relief."

Says INTEGRIS CIO Delano: "It's a constant battle that takes a lot of time and resources to feel good about a security program. We've just encrypted hard drives but now we've got mobile phones. They're now an endpoint that could tunnel into our network. They're all out there collecting data. It's a nightmare problem."

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, EVP, Operations, System Strategy and Growth, Oakwood Healthcare, Inc.

Stephen C. Hanson, FACHE, CEO, Baptist Health

Steve Heck, President, MedSys Group

Stan Hupfeld, Past President & CEO, INTEGRIS Health, Inc.

Scott Parker, President Emeritus, Intermountain Health Care

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, WellPoint

Anthony Tersigni, CEO, Ascension Alliance

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 Healthcare System, Houston, TX

Metro Health, Wyoming, MI

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

SSM Health, St. Louis, MO

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 Medical Center, Seattle, WA

CORPORATE SPONSORS

Cerner · CSC · Deloitte. · HARRIS Healthcare Solutions · vocera · HealthCatalyst ignite change · KORN FERRY · Omnicell · Microsoft · emmi SOLUTIONS · Impact advisors

STRATEGIC PARTNER

KLAS ACCURATE. HONEST. IMPARTIAL.