SCOTTSDALE INSTITUTE
COLLABORATION • EDUCATION • NETWORKING

INSIDE EDGE

Cybersecurity: Building Resiliency

Introduction

It's no secret cybersecurity is at the top of the priority list for healthcare CIOs and other C-suite executives. One of the latest wakeup calls occurred in late June when the Petya computer virus attacked transcription-service provider Burlington, Mass.-based Nuance, a Scottsdale Institute Corporate Sponsor. Weeks later some health systems were still struggling to fix their physician transcription tools. As significant as the attack was—$2B Nuance derives half of its revenue from its healthcare and dictation business—it raised an even bigger specter: the security vulnerabilities of third-party and cloud-based software firms, which healthcare providers increasingly embrace to cut costs while keeping an innovative IT edge.

The Petya event followed on the heels of the WannaCry ransomware attack in mid-May which targeted computers running Microsoft Windows—including the UK's National Health Service—by encrypting their data and demanding ransom payments using Bitcoin.

Scottsdale Institute Conferences

Camelback Inn,
Scottsdale, AZ
April 25–27, 2018

April 10–12, 2019

The Internet of Things (IoT), the connection of proliferating devices ranging from cars, kitchen appliances, heart monitors and even pills—called "ingestible trackers"—to the Internet, is raising the security stakes exponentially. "And this is just the beginning," says Joe Kvedar, MD, VP of Connected Health at Partners HealthCare in Boston, and author of "The Internet of Healthy Things," a discussion of how connected health is likely to emerge as the platform for population health. http://theinternetofhealthythings.com/.

"Experts predict that by 2020, 26 billion everyday objects will be able to capture, receive and share data via a vast, interconnected global network linked together by inexpensive sensors, GPS and the cloud. Just around the corner, real-time biometric data will be automatically captured and used to learn more about the impact of lifestyle on disease and wellness, and ultimately change behavior for the better," he says.

What's a health system to do? Plenty, according to three 2017 SI Teleconferences tackling cybersecurity: from research firm ECRI (June 8), according to national health system Ascension Health (June 14) and by regional "high reliability healthcare organization" Texas Health Resources (Jan. 19). Highlights of those SI Teleconferences follow; complete audio and slides are available at https://scottsdaleinstitute.org/teleconferences/2017.asp.

Connected medical devices

"There's been a great change in the cybersecurity conversation with the evolution of medical devices from self-contained ones at the bedside to interoperable diagnostic and therapy devices that can exchange data with multiple information systems," says Rob Maliff, director of the applied solutions group at ECRI Institute, a nonprofit research organization focused on medical devices, drugs and procedures in Plymouth Meeting, Pa.

ECRI Institute
The Discipline of Science. The Integrity of Independence.

Rob Maliff, Director, Applied Solutions Group, ECRI

Today, each patient has an average of 17 devices connected to the bedside, and one in four of them connect to the network, he says. "As we create this Internet of connected things we become even more vulnerable to cyberattacks." That could mean increasing healthcare's investment in cybersecurity. The healthcare industry spends about 5 percent of IT budgets on cybersecurity compared to the financial industry's 15 percent.

What's different about healthcare, Maliff says, is that there are thousands of device manufacturers for whom "security has been an afterthought." Also, because healthcare is about life-critical functions, it is not as easy to manage or turn off these devices. Further, healthcare devices tend to have long useful lives of 10 years or more and it's not uncommon to find Windows XP still in use, which continues to be vulnerable to the WannaCry worm. Healthcare also presents a very large attack surface given patient and visitor access to areas with sensitive devices.

> *"The healthcare industry spends about 5 percent of IT budgets on cybersecurity compared to the financial industry's 15 percent."*

Volume 23, Number 5

Chairman
Donald C. Wegmiller, FACHE

Vice Chairman
Tom Sadvary, FACHE, former CEO, HonorHealth

Executive Director
Janet Guptill, FACHE

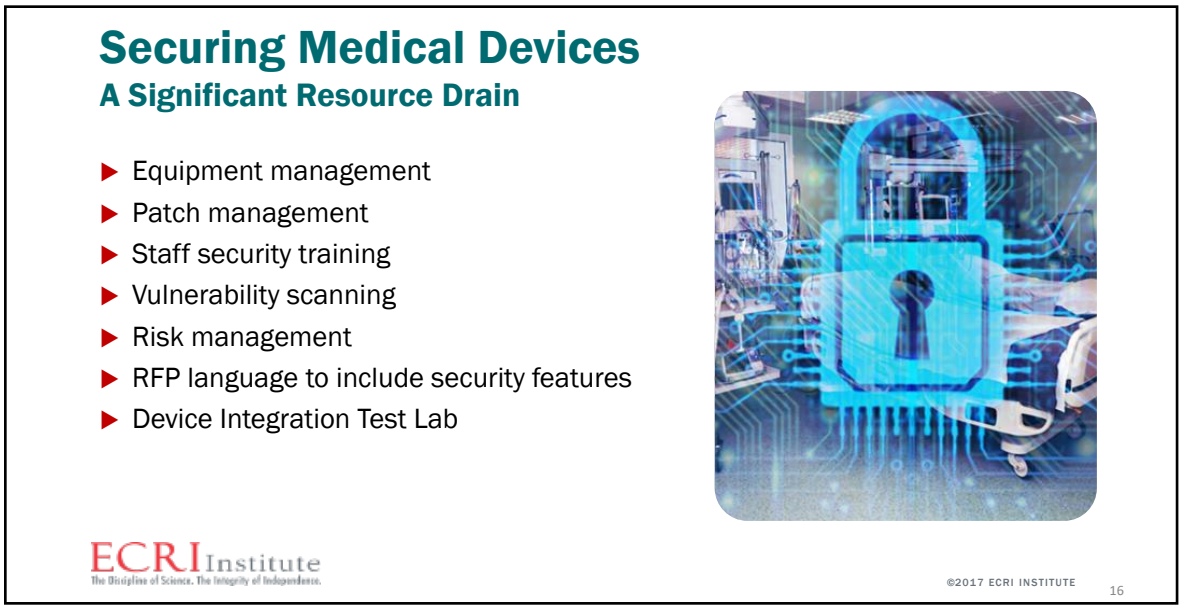
Editor
Chuck Appleby

Managing Editor
Jean Appleby

Membership Services Office:
7767 Elm Creek Blvd. N., Suite 208
Maple Grove, MN 55369

T. 763.710.7089
F. 763.432.5635
E. scottsdale@scottsdaleinstitute.org
w. www.scottsdaleinstitute.org

To secure medical devices, health systems should follow a seven-point framework.



Equipment management

"First, identify which devices are connected to the network," says Maliff, and then document their respective software versions, network configuration settings, IP addresses and Media Access Control (MAC) addresses. Next, prioritize these devices according to whether they hold personal health information (PHI) and life-critical functionality. "Ask, 'What happens if you cannot use this device?'" he says.

Patch management

"It's a myth that the FDA needs to approve a cybersecurity patch," says Maliff. "It's also a myth that customers need to put a device on a secure network. So, developing a policy for updating security patches via a safety committee is key."

PATCH MANAGEMENT DO'S & DON'TS FOR RANSOMWARE/WANNACRY

DO'S:

- Identify networked medical devices/servers/workstations that are operating on a Windows OS.
- Identify whether connected medical devices/device servers have gotten the relevant Microsoft Windows OS MS17-010 security patch.
- Consider running a vulnerability scan in your medical device networks to identify affected medical devices.
- Prioritize response on any connected Windows-OS-based medical device systems.
- If a malware infection is identified or suspected in a medical device:
  - If clinically acceptable, disconnect the medical device from the network and work with your internal IT and Clinical Engineering departments and the device manufacturer to contain the infection and to restore the system.
  - If any unencrypted patient data was involved, have risk management coordinate the response regarding the data breach, as per its obligation under HIPAA.

DON'TS:

- Don't overreact.
- Don't install unvalidated patches.
- Don't simply turn off or disconnect all networked medical devices that have Windows OS.

Source: ECRI

Staff security training

"This is Internet 101," says Maliff. "To avoid phishing scams don't open suspicious emails. Also, develop a policy for USBs, which can spread viruses and cause malfunctions." In 2015 ECRI identified USBs as a Top 10 Hazard. Block USB use if merited.

"Passwords matter!" he says, and the health systems should emphasize strong passwords and eliminating the use of stickies with passwords. Finally, decide if BYOD is a threat and develop a policy to manage it.

> *"What's different about healthcare is that there are thousands of device manufacturers for whom security has been an afterthought."*

Vulnerability scanning

IT uses standard network tools to scan IT assets for vulnerabilities, however, these are typically limited to known vulnerabilities—not Zero Day vulnerabilities. It is possible to scan some medical devices, but that task should be done during the day shift, when there's enough staff in case something goes wrong. It happens: One such scanning took out a hospital's telemetry unit.

Risk management

How do you incorporate medical devices under risk management? Governance of risk should involve physician and senior leadership, including the CISO, in developing a medical device security plan.

Identify existing vulnerabilities based on clinical value versus security risks and develop compensating controls to minimize risk such as blocking commonly used communication ports. And, consider the adoption of ANSI/AAMI/IEC 80001-1:2010, which is a standard for healthcare facilities incorporating medical devices into their networks.

RFP language to include security features

"Many hospitals and health systems are challenged by this requirement, but they need to push security to the front of the decision-making process," asserts Maliff. "Make sure the language stipulates to NOT buy any device using Windows XP, which has known vulnerabilities!" Also, require the MDS2, or Manufacturer Disclosure Statement for Medical Device Security and the VA Directive 6550 for Pre-procurement Assessment. "Make sure you have the right to require full testing," he says.

Device Integration Test Lab

"Not everyone can do this," says Maliff, because it's costly. However, large health systems should have the lab capability to conduct engineering tests and validate every patch and update prior to release.

Cybersecurity in Ascension

"Cyber resilience" is the term used by Duane Hopkins, director of security operations, cyber response and investigation for Ascension Information Services, to help lead Ascension Health into a dynamic culture of cyber security. "The traditional approach has been to be reactive, looking at one-to-one connections and removing the affected machine from the network. Becoming cyber resilient means becoming proactive by tracking attackers and unwanted activity, searching for the indicators of attack and

ASCENSION HEALTH

Duane Hopkins, Director of Security Operations, Cyber Response & Investigation, Ascension Health

remediating the problem as fast as possible with as little impact as possible. Automation is key. Without automation you can't surface data great enough to make decisions," he says.

Cyber-threat intelligence is the foundation for cyber resilience. Hopkins breaks threat intelligence into four areas:

Cut the noise. "There's a lot of noise coming into the healthcare environment from lots of data feeds. It's hard to cut down to actionable data. The goal of automation is to focus on the threats that can have a major impact on your enterprise."

Build the knowledge. "How do we build a threat-actor profile? It's the ability to break down malware into understandable categories. Threat reports provide information on threat actors targeting specific industries, geographies and enterprise types, as well as on their tactics, techniques and procedures (TTPs)."

Identify. "Threat diagnostics identifies an organization's threat profile, highlighting the threat sources actively targeting their assets and associated tactical and strategic implications."

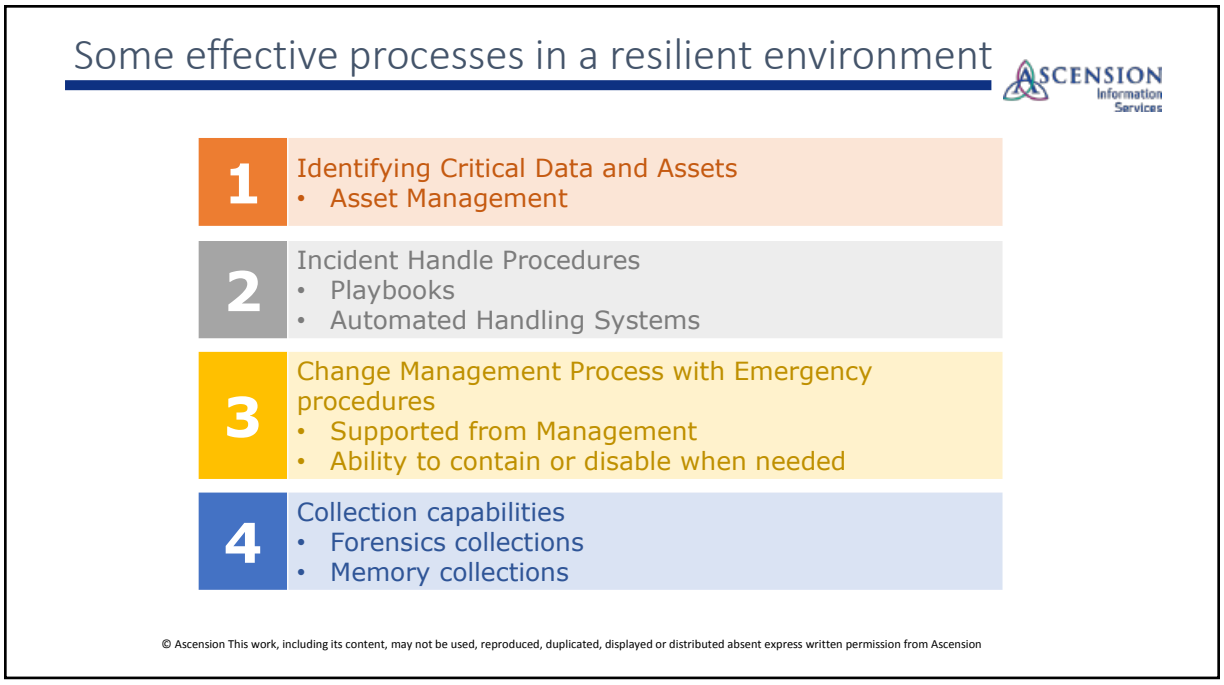
Measure risk. "It's about understanding the unknown and being able to shift or deftly slide away from the attacker so they'll go somewhere else. It's taking the noise and distilling down to knowledge that's actionable and intelligible to our environment." This component prioritizes risks to a given enterprise and identifies appropriate policies, process improvements and technologies in order to manage security.

Cyber resilience starts with an *external assessment*: Do we understand our environment where the attacker lies? *Proactive intelligence* enables a health system to make intelligent business decisions—do we sidestep or go hunt for the attacker? It means gathering cyber intelligence from controls and technology to give you the visibility of the threat. *Awareness* involves the organization's ability to use intelligence to respond to the attacker.

Driving the resilient approach means integrating and infusing it into your organization's culture. This includes the "human firewall" strategy involving social engineering like user training around trust, phishing and human-error gaps. It also involves building cybersecurity into policies for contracting, SLAs, third-party relationships, patching auditing and investigation. Driving the resilient approach also means developing internal partnerships with legal, compliance, risk, human resources, IT and public relations—and external partnerships with cyber insurance providers, external forensics providers, information-sharing associations like NH-ISAC and HITRUST, law enforcement and any data-breach providers.

Building a resilient cybersecurity process, according to Hopkins, involves understanding the need for enhanced threat detection and prioritized incident investigation:

1. **Trigger & escalate:** Starts the gathering process of the security event. "Do we need full, partial or day-to-day response?"
2. **Triage:** Starts the forensic process and collection of data. "Triage narrows the scope and gives us fast response around data."
3. **Analyze:** Understanding of who, what, where and start the why. "Who's attacking us? What are their tactics? What's the extent of damage?"
4. **Quarantine:** Tactics and procedures for containment. "Pause at that point to collect an image via memory or disc collection. Otherwise you can't get into the investigation."
5. **Investigation:** Digs deep into the process of who, what, where, why, when and how. "All critical information is at your fingertips."
6. **Mitigation:** Builds on the information to establish a mitigation strategy and cleanup of the security incident.
7. **Lessons learned:** "No resilient cybersecurity plan is complete until lessons learned, which are key to continuous improvement."



High Reliability at THR

Ron Mehring, VP technology & security at Texas Health Resources, describes how an integrated health system can develop "a rational, well-integrated cybersecurity program focused on quality and high reliability." He cites Texas Health's principles of a high reliability organization as:

Texas Health Resources®
Healing Hands. Caring Hearts.℠

Ron Mehring, VP Technology & Security, Texas Health Resources

- A preoccupation with failure;
- A reluctance to simplify interpretations;
- A sensitivity to operations;
- A commitment to resilience; and,
- A deference to expertise.

"I came out of aviation," says Mehring, and that framework is embedded in every facet of aviation-industry operations. "These principles, which are essentially about managing the unexpected, are very common sense but very hard to implement in practice."

Texas Health has applied quality-management-system and system-engineering practices to cybersecurity, which helps ensure that cybersecurity is programmatically integrated into the healthcare delivery environment in an actionable and meaningful way. "It's more about the principles of quality," he says. "Most healthcare-delivery organizations set up robust quality management processes. It's important that cybersecurity programs lean into workflow and become part of everyday work."

Cybersecurity encompasses several components—governance, risk management, control architecture & engineering and performance management & monitoring. While all components are important, Mehring focuses on Texas Health's strategy for control architecture & engineering as a way to embed performance management into cybersecurity. Under that framework, high-reliability security designs are heavily influenced by:

> *"It's important that cybersecurity programs lean into workflow and become part of everyday work."*

- Risk appetite;
- Risk scenarios and threat models;
- Need to control robustness needs and tradeoffs; and,
- Performance monitoring.

> *"These high reliability principles, essentially about managing the unexpected, are common sense but very hard to implement in practice."*

'Good enough'

Critical to this technical-sounding strategy is an almost subjective decision-making process, a judgment-call element, that balances the two extremes of robustness. "Every control has to have a robustness: how strong or how weak are you going to make controls," he says. "A robustness requirement is the level of security needed within a security control for it to be considered 'good enough.'

Robustness requirements are applied to "in place" and "proposed" control standards to form a security architecture baseline.

- Control robustness should be focused on adding friction to attacker operations and reducing friction within business and clinical operations.
- Higher levels of robustness have the potential to increase cost or complexity.
- A robustness level that cannot be met by a specific control may create robustness requirements in other controls. (compensating controls)

> *"Ultimately, it's about rhythm. Cybersecurity requires a continuous feedback loop, a continuous cycle."*

A simple example: No Password to Password Required to Two-Factor Authentication. The process requires trade-off decisions that must have stakeholder input and be data-driven.

Says Mehring: "Ultimately, it's about rhythm. Cybersecurity requires a continuous feedback loop, a continuous cycle."

Conclusion

As evidenced by our experts from ECRI, Ascension Health and Texas Health Resources, cybersecurity is achieving a maturity and discipline at some leading health systems previously unseen. For more detailed content related to these innovative cybersecurity programs and frameworks, check out their respective SI Teleconferences: ECRI (June 8), Ascension Health (June 14) and Texas Health Resources (Jan. 19) at https://scottsdaleinstitute.org/teleconferences/2017.asp.

Join the continuing cybersecurity discussion. Register for **Scottsdale Institute's 2017 CISO Fall Summit: Best Practice Standards in Cybersecurity Risk Management**. Sponsored by Deloitte Wednesday, October 18, 2017 – Thursday, October 19, 2017, Chicago

And, don't miss our next *Inside Edge* report on "Population Health: Redesigning Care" coming in September.

RELATED RESOURCES

Check out these downloadable ECRI resources:

Ransomware Attacks: How to Protect Your Medical Device Systems
https://www.ecri.org/components/HDJournal/Pages/Ransomware-Attacks-How-to-Protect-Your-Systems.aspx

The Petya Ransomware Attack and Medical Device Systems at
https://www.ecri.org/components/HDJournal/Pages/Ransomware-Attack-Petya.aspx

Check out another 2017 SI Teleconference on Cybersecurity at
https://scottsdaleinstitute.org/teleconferences/2017.asp

March 18: (Cynergis Tek)

SCOTTSDALE INSTITUTE

COLLABORATION • EDUCATION • NETWORKING

BOARD OF DIRECTORS

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

Executive Committee

Don Wegmiller, FACHE, Chairman

Tom Sadvary, FACHE, Vice Chairman, CEO, HonorHealth

Janet Guptill, FACHE, Executive Director

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

Board Members

David Campbell, David Campbell and Associates

Stephen C. Hanson, FACHE, former CEO, Baptist Health

Steve Heck, Chairman, MedSys Group

Laura Kaiser, President & CEO, SSM Health

Wright L. Lassiter III, President & CEO, Henry Ford Health System

Patrick O'Hare, SVP Facilities & CIO, Spectrum Health

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

Bruce Smith, former 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, former CEO, Billings Clinic

COLLABORATION • EDUCATION • NETWORKING

MEMBER ORGANIZATIONS

Adventist Health, Roseville, CA

Adventist Health System, Altamonte Springs, FL

Advocate Health Care, Oak Brook, IL

AMITA Health, Arlington Heights, 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

IU 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

Methodist Le Bonheur Healthcare, Memphis, TN

Mosaic Life Care, St. Joseph, MO

Munson Healthcare, Traverse City, MI

NewYork-Presbyterian, New York, NY

Northwestern Medicine, Chicago, IL

OSF HealthCare System, Peoria, IL

Partners HealthCare System, Inc., Boston, MA

Rush University Medical Center, Chicago, IL

Sentara Healthcare, Norfolk, VA

Sharp HealthCare, San Diego, CA

Spectrum Health, Grand Rapids, MI

Sutter Health, Sacramento, CA

Tampa General Hospital, Tampa, FL

Texas Health Resources, Arlington, TX

Trinity Health, Livonia, MI

UCLA Health, Los Angeles, CA

UK HealthCare, Lexington, KY

University Hospitals, Cleveland, OH

University of Chicago Medicine, Chicago, IL

University of Virginia Health System, Charlottesville, VA

Virginia Commonwealth University Health, Richmond, VA

Virginia Mason Health System, Seattle, WA

CORPORATE SPONSORS

HEARST HEALTH
fdb · zynxhealth · mcg · homecare homebase · MEDHOK

Omnicell · NUANCE · OPTUM · HealthCatalyst ignite change

IBM Watson Health · emmi Expertly Designed to Drive Results

KORN FERRY · Cerner

Deloitte. · Epic · Impact advisors

STRATEGIC PARTNERS

C-SUITE Resources · KLAS ACCURATE. HONEST. IMPARTIAL.

August, 2017