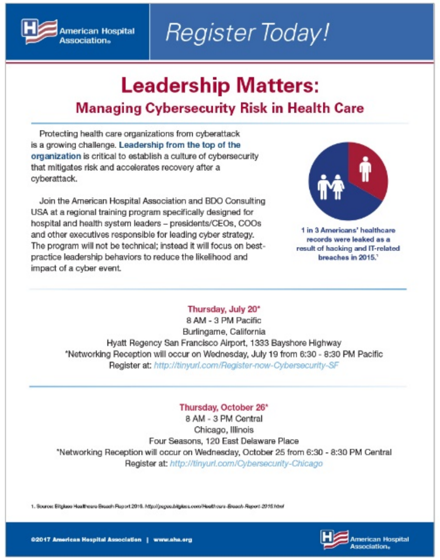
American Hospital
Association

BDO®

Medical Devices and Cyber Issues

JANUARY 23, 2018

AHA and Cybersecurity



American Hospital Association

Register Today!

Leadership Matters:

Managing Cybersecurity Risk in Health Care

Protecting health care organizations from cyberattack is a growing challenge. **Leadership from the top of the organization** is critical to establish a culture of cybersecurity that mitigates risk and accelerates recovery after a cyberattack.

Join the American Hospital Association and BDO Consulting USA at a regional training program specifically designed for hospital and health system leaders – presidents/CEOs, COOs and other executives responsible for leading cyber strategy. The program will not be technical; instead it will focus on best-practice leadership behaviors to reduce the likelihood and impact of a cyber event.

1 in 3 Americans' healthcare records were leaked as a result of hacking and IT-related breaches in 2015.[1]

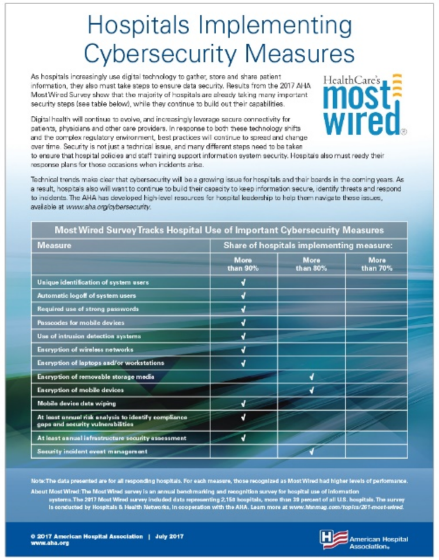
Thursday, July 20*
8 AM - 3 PM Pacific
Burlingame, California
Hyatt Regency San Francisco Airport, 1333 Bayshore Highway
*Networking Reception will occur on Wednesday, July 19 from 6:30 - 8:30 PM Pacific
Register at: *http://tinyurl.com/Register-now-Cybersecurity-SF*

Thursday, October 26*
8 AM - 3 PM Central
Chicago, Illinois
Four Seasons, 120 East Delaware Place
*Networking Reception will occur on Wednesday, October 25 from 6:30 - 8:30 PM Central
Register at: *http://tinyurl.com/Cybersecurity-Chicago*

[1] Source: Bitglass Healthcare Breach Report 2016. *http://pages.bitglass.com/Healthcare-Breach-Report-2016.html*

©2017 American Hospital Association | www.aha.org

American Hospital Association



Hospitals Implementing Cybersecurity Measures

HealthCare's most wired®

As hospitals increasingly use digital technology to gather, store and share patient information, they also must take steps to ensure data security. Results from the 2017 AHA Most Wired Survey show that the majority of hospitals are already taking many important security steps (see table below), while they continue to build out their capabilities.

Digital health will continue to evolve, and increasingly leverage secure connectivity for patients, physicians and other care providers. In response to both these technology shifts and the complex regulatory environment, best practices will continue to spread and change over time. Security is not just a technical issue, and many different steps need to be taken to ensure that hospital policies and staff training support information system security. Hospitals also must ready their response plans for those occasions when incidents arise.

Technical trends make clear that cybersecurity will be a growing issue for hospitals and their boards in the coming years. As a result, hospitals also will want to continue to build their capacity to keep information secure, identify threats and respond to incidents. The AHA has developed high-level resources for hospital leadership to help them navigate these issues, available at *www.aha.org/cybersecurity.*

Most Wired Survey Tracks Hospital Use of Important Cybersecurity Measures

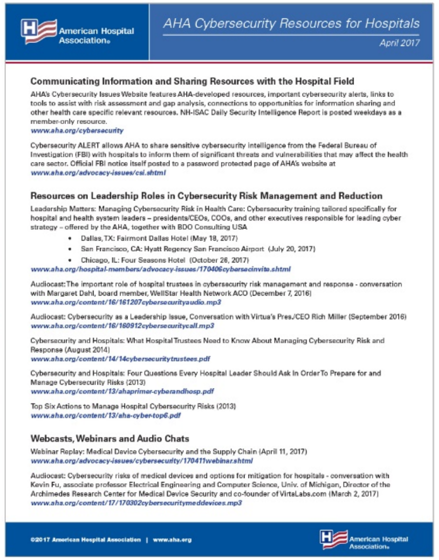
Measure	Share of hospitals implementing measure:		
	More than 90%	More than 80%	More than 70%
Unique identification of system users	✓		
Automatic logoff of system users	✓		
Required use of strong passwords	✓		
Passcodes for mobile devices	✓		
Use of intrusion detection systems	✓		
Encryption of wireless networks	✓		
Encryption of laptops and/or workstations	✓		
Encryption of removable storage media		✓	
Encryption of mobile devices		✓	
Mobile device data wiping	✓		
At least annual risk analysis to identify compliance gaps and security vulnerabilities	✓		
At least annual infrastructure security assessment	✓		
Security incident event management		✓	

Note: The data presented are for all responding hospitals. For each measure, those recognized as Most Wired had higher levels of performance.

About Most Wired: The Most Wired survey is an annual benchmarking and recognition survey for hospital use of information systems. The 2017 Most Wired survey included data representing 2,158 hospitals, more than 39 percent of all U.S. hospitals. The survey is conducted by Hospitals & Health Networks, in cooperation with the AHA. Learn more at *www.hhnmag.com/topics/261-most-wired.*

© 2017 American Hospital Association | July 2017
www.aha.org

American Hospital Association



American Hospital Association

AHA Cybersecurity Resources for Hospitals

April 2017

Communicating Information and Sharing Resources with the Hospital Field

AHA's Cybersecurity Issues Website features AHA-developed resources, important cybersecurity alerts, links to tools to assist with risk assessment and gap analysis, connections to opportunities for information sharing and other health care specific relevant resources. NH-ISAC Daily Security Intelligence Report is posted weekdays as a member-only resource.
www.aha.org/cybersecurity

Cybersecurity ALERT allows AHA to share sensitive cybersecurity intelligence from the Federal Bureau of Investigation (FBI) with hospitals to inform them of significant threats and vulnerabilities that may affect the health care sector. Official FBI notice itself posted to a password protected page of AHA's website at
www.aha.org/advocacy-issues/csi.shtml

Resources on Leadership Roles in Cybersecurity Risk Management and Reduction

Leadership Matters: Managing Cybersecurity Risk in Health Care: Cybersecurity training tailored specifically for hospital and health system leaders – presidents/CEOs, COOs, and other executives responsible for leading cyber strategy – offered by the AHA, together with BDO Consulting USA

- Dallas, TX: Fairmont Dallas Hotel (May 18, 2017)
- San Francisco, CA: Hyatt Regency San Francisco Airport (July 20, 2017)
- Chicago, IL: Four Seasons Hotel (October 26, 2017)

www.aha.org/hospital-members/advocacy-issues/170406cybersecinvite.shtml

Audiocast: The important role of hospital trustees in cybersecurity risk management and response - conversation with Margaret Dahl, board member, WellStar Health Network ACO (December 7, 2016)
www.aha.org/content/16/161207cybersecurityaudio.mp3

Audiocast: Cybersecurity as a Leadership Issue, Conversation with Virtua's Pres./CEO Rich Miller (September 2016)
www.aha.org/content/16/160912cybersecuritycall.mp3

Cybersecurity and Hospitals: What Hospital Trustees Need to Know About Managing Cybersecurity Risk and Response (August 2014)
www.aha.org/content/14/14cybersecuritytrustees.pdf

Cybersecurity and Hospitals: Four Questions Every Hospital Leader Should Ask In Order To Prepare for and Manage Cybersecurity Risks (2013)
www.aha.org/content/13/ahaprimer-cyberandhosp.pdf

Top Six Actions to Manage Hospital Cybersecurity Risks (2013)
www.aha.org/content/13/aha-cyber-top6.pdf

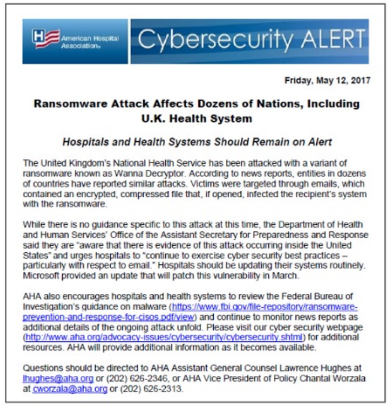
Webcasts, Webinars and Audio Chats

Webinar Replay: Medical Device Cybersecurity and the Supply Chain (April 11, 2017)
www.aha.org/advocacy-issues/cybersecurity/170411webinar.shtml

Audiocast: Cybersecurity risks of medical devices and options for mitigation for hospitals - conversation with Kevin Fu, associate professor Electrical Engineering and Computer Science, Univ. of Michigan, Director of the Archimedes Research Center for Medical Device Security and co-founder of VirtaLabs.com (March 2, 2017)
www.aha.org/content/17/170302cybersecuritymeddevices.mp3

©2017 American Hospital Association | www.aha.org

American Hospital Association



American Hospital Association

Cybersecurity ALERT

Friday, May 12, 2017

Ransomware Attack Affects Dozens of Nations, Including U.K. Health System

Hospitals and Health Systems Should Remain on Alert

The United Kingdom's National Health Service has been attacked with a variant of ransomware known as Wanna Decryptor. According to news reports, entities in dozens of countries have reported similar attacks. Victims were targeted through emails, which contained an encrypted, compressed file that, if opened, infected the recipient's system with the ransomware.

While there is no guidance specific to this attack at this time, the Department of Health and Human Services' Office of the Assistant Secretary for Preparedness and Response said they are "aware that there is evidence of this attack occurring inside the United States" and urges hospitals to "continue to exercise cyber security best practices – particularly with respect to email." Hospitals should be updating their systems routinely. Microsoft provided an update that will patch this vulnerability in March.

AHA also encourages hospitals and health systems to review the Federal Bureau of Investigation's guidance on malware (https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view) and continue to monitor news reports as additional details of the ongoing attack unfold. Please visit our cyber security webpage (http://www.aha.org/advocacy-issues/cybersecurity/cybersecurity.shtml) for additional resources. AHA will provide additional information as it becomes available.

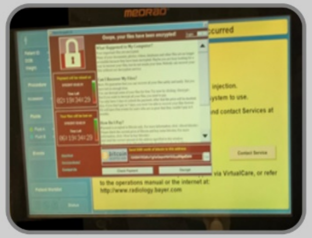
Questions should be directed to AHA Assistant General Counsel Lawrence Hughes at lhughes@aha.org or (202) 626-2346, or AHA Vice President of Policy Chantal Worzala at cworzala@aha.org or (202) 626-2313.

- Member education
- Coordination with federal government
- Policy

BDO

American Hospital Association®

Policy Approaches



Medical devices are a key vulnerability

Fraud and abuse laws stand in the way

Better balance of information sharing and security

Interaction with HIPAA

Workforce and resource challenges

BDO

American Hospital Association®

Role of the FDA

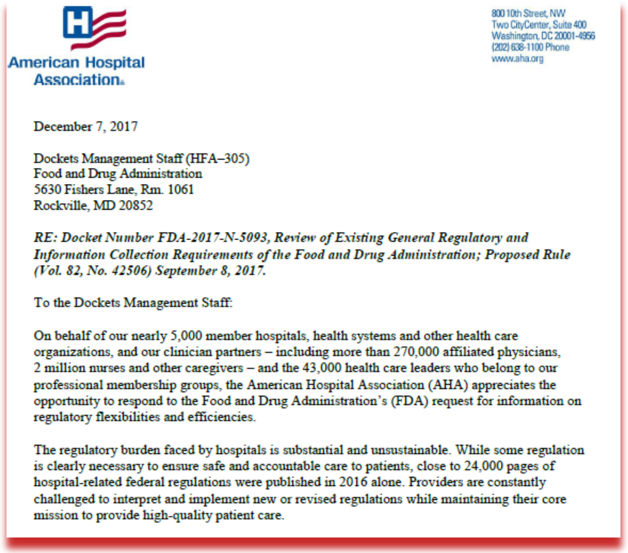
FDA Guidance and Roles

- Pre-market
- Post-market
- Assistance during attack

Recent AHA Recommendations

“The FDA must provide greater oversight of medical device manufacturers with respect to the security of their products. Manufacturers must be held accountable to proactively minimize risk and continue updating and patching devices as new intelligence and threats emerge.

“We recommend that the FDA proactive set clear, measurable expectations for manufacturers before incidents and play a more active role during cybersecurity attacks. This active role could include, for example, issuing guidance to manufacturers outlining the expectations for supporting their customers to secure their products.”



American Hospital Association

800 10th Street, NW
Two CityCenter, Suite 400
Washington, DC 20001-4956
(202) 638-1100 Phone
www.aha.org

December 7, 2017

Dockets Management Staff (HFA–305)
Food and Drug Administration
5630 Fishers Lane, Rm. 1061
Rockville, MD 20852

RE: Docket Number FDA-2017-N-5093, Review of Existing General Regulatory and Information Collection Requirements of the Food and Drug Administration; Proposed Rule (Vol. 82, No. 42506) September 8, 2017.

To the Dockets Management Staff:

On behalf of our nearly 5,000 member hospitals, health systems and other health care organizations, and our clinician partners – including more than 270,000 affiliated physicians, 2 million nurses and other caregivers – and the 43,000 health care leaders who belong to our professional membership groups, the American Hospital Association (AHA) appreciates the opportunity to respond to the Food and Drug Administration’s (FDA) request for information on regulatory flexibilities and efficiencies.

The regulatory burden faced by hospitals is substantial and unsustainable. While some regulation is clearly necessary to ensure safe and accountable care to patients, close to 24,000 pages of hospital-related federal regulations were published in 2016 alone. Providers are constantly challenged to interpret and implement new or revised regulations while maintaining their core mission to provide high-quality patient care.

American Hospital Association

Laura Hars

Senior Manager, Cyber
BDO Advisory Services

Overview

- Introduction to medical device risk
- What can go wrong?
- Compliance

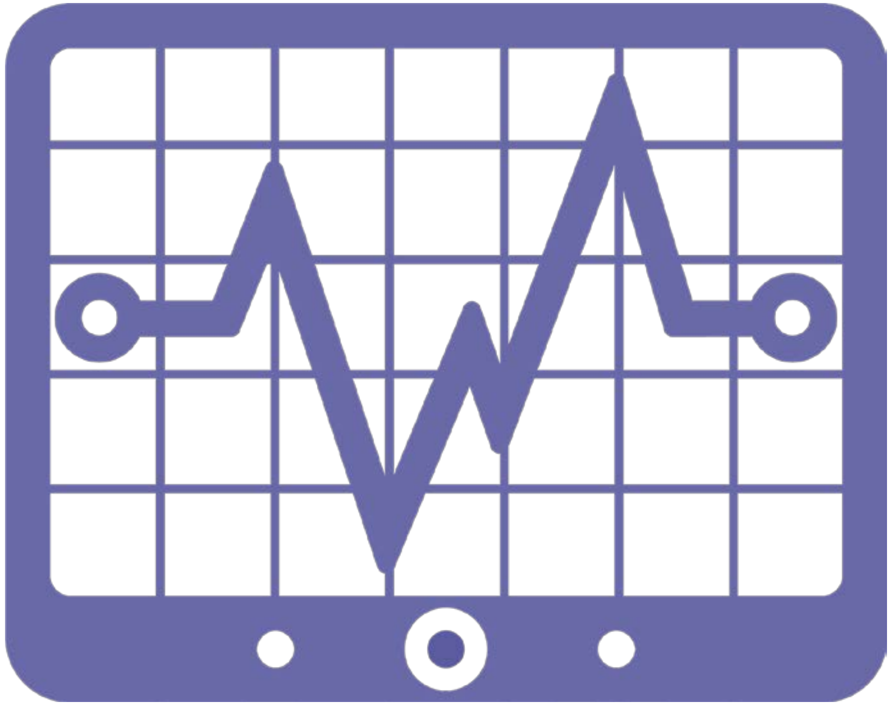
American Hospital Association

BDO

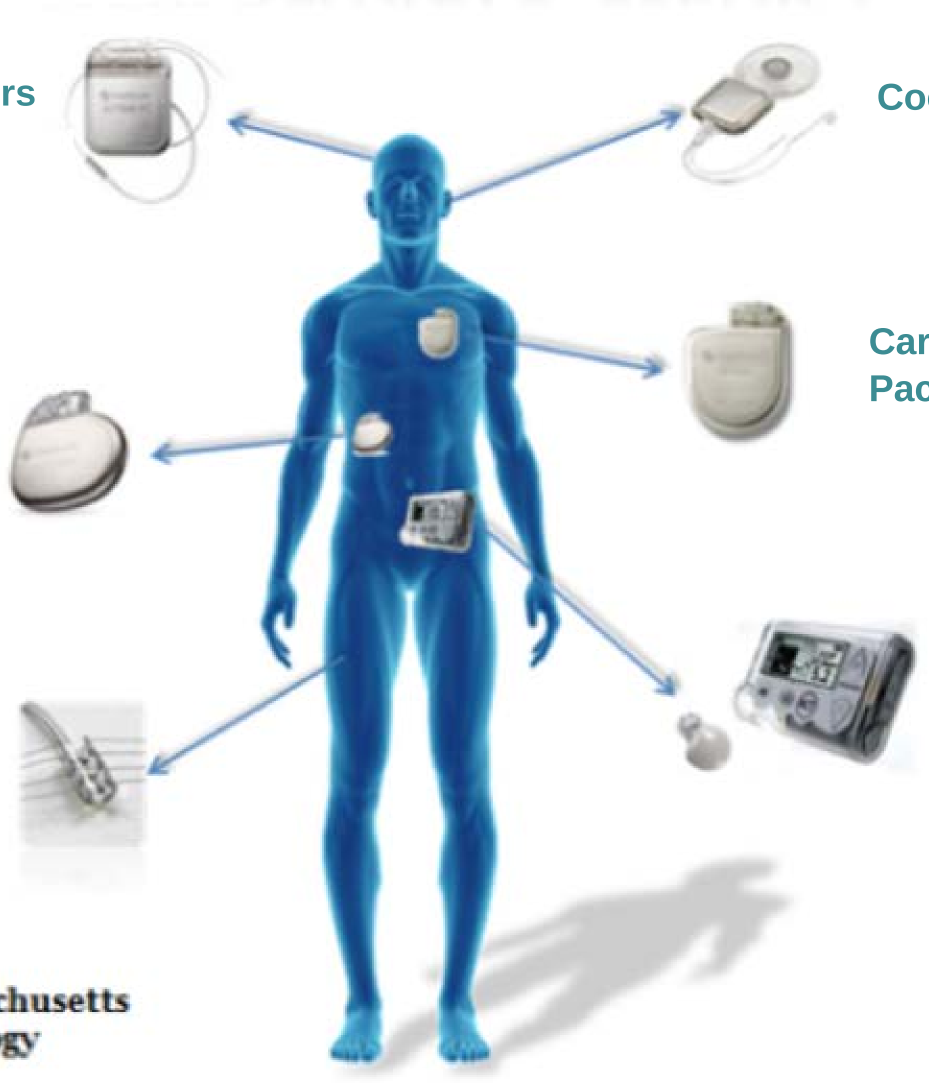
Overview

Medical Devices

- What Are They?
- What Types?



Wireless Implantable Medical Devices



Deep Brain Neurostimulators

Cochlear Implants

Cardiac Defibrillators/
Pacemakers

Gastric Stimulators

Insulin Pumps

Foot Drop Implants

Image Credit: Massachusetts
Institute of Technology

Medical Devices & Compliance

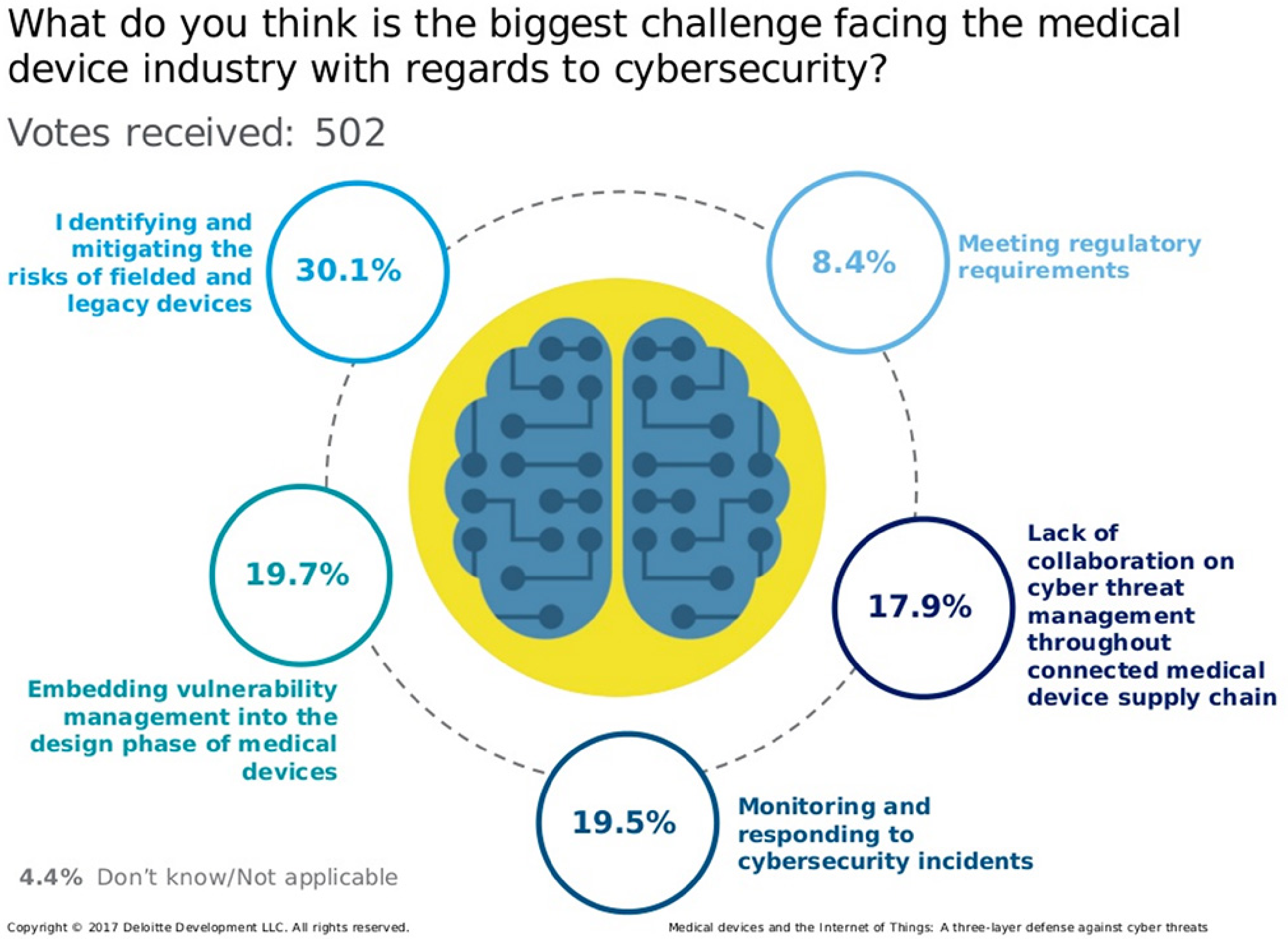
Cybersecurity & Medical Devices

Medical device manufacturers must comply with federal regulations. Part of those regulations, called quality system regulations (QSRs), requires that medical device manufacturers address all risks, including cybersecurity risk. The pre- and post-market cybersecurity guidance provide recommendations for meeting QSRs.

American Hospital Association

BDO

Biggest Challenges of Securing Medical Devices



What do you think is the biggest challenge facing the medical device industry with regards to cybersecurity?

Votes received: 502

30.1% Identifying and mitigating the risks of fielded and legacy devices

8.4% Meeting regulatory requirements

19.7% Embedding vulnerability management into the design phase of medical devices

17.9% Lack of collaboration on cyber threat management throughout connected medical device supply chain

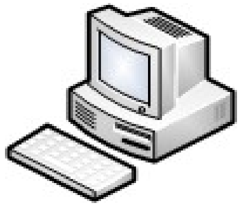
19.5% Monitoring and responding to cybersecurity incidents

4.4% Don't know/Not applicable

Medical devices and the Internet of Things: A three-layer defense against cyber threats

Medical Devices & Systems: How do they differ?

Differences in Impact of Failure



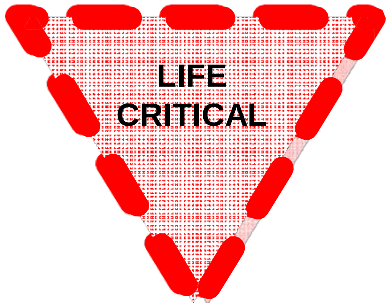
INFORMATION TECHNOLOGY

MISSION CRITICAL

Security (i.e., data confidentiality, integrity or availability) compromise can

- ✓ *have serious financial impact*
- ✓ *have serious operational impact*
- ✓ *have serious reputation & legal impact*

MEDICAL TECHNOLOGY



LIFE CRITICAL

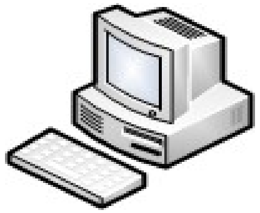
*Security compromise **of Medical Devices** can result in death or serious injury*

American Hospital Association

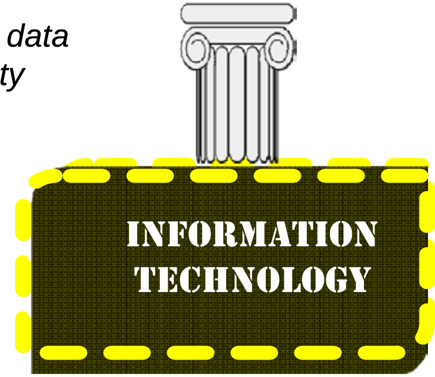
BDO

Medical Devices & Systems: Who Has Responsibility?

Information Technology vs Clinical/Biomedical Engineering



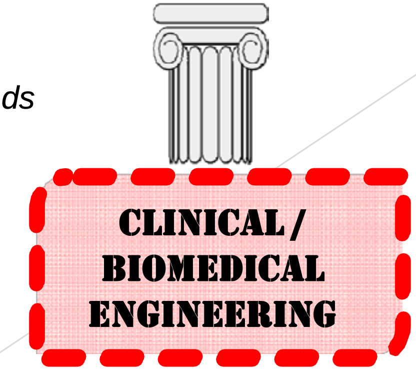
IT knows data security



INFORMATION TECHNOLOGY

BUT …
IT generally has limited knowledge of type, number and vulnerabilities associated with medical devices

CE knows number/location of medical devices & misunderstands criticality, lifecycle, and supportability issues



CLINICAL / BIOMEDICAL ENGINEERING

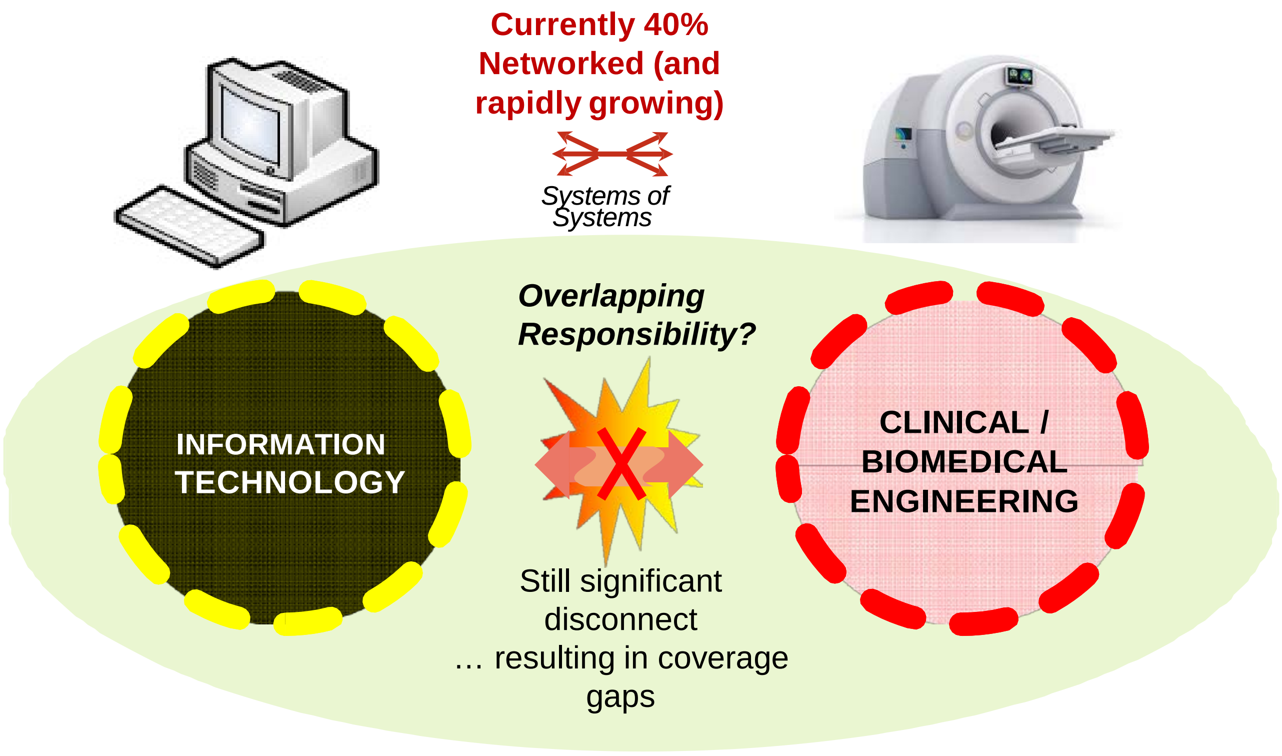
BUT …
CE generally has limited knowledge of data security issues

American Hospital Association

BDO

Medical Devices & Systems: Shared Responsibility

Degree of Integrated Support



Currently 40% Networked (and rapidly growing)

Systems of Systems

Overlapping Responsibility?

INFORMATION TECHNOLOGY

CLINICAL / BIOMEDICAL ENGINEERING

Still significant disconnect
… resulting in coverage gaps

American Hospital Association

BDO

Case Study – Medical Device Concerns at a Large Healthcare Provider Network

During a cybersecurity assessment the following concerns were noted:

- The IT department estimated the number of devices on the network to be approximately 61,000 based on the current asset inventory
- A scan of the network revealed slightly over 98,000 devices
- Through interviews with clinical personnel and examinations of manual inventories, it was determined that approximately 35,000 of the 98,000 devices were medical devices (infusion pumps, pacemakers etc.)
- The Clinical Engineering department maintained an inventory of device manufacturers and serial numbers of the devices but not their network address
- Although the IT department had to be contacted to enable the connectivity of the device on the hospital network, they also did not keep any inventory or notation of the devices network address

Solution:

The issue of tracking medical devices was solved by creating a business process that involved both departments using the IT Service Desk tool to track and record the purchase and registration of the devices on the network

American Hospital Association

BDO

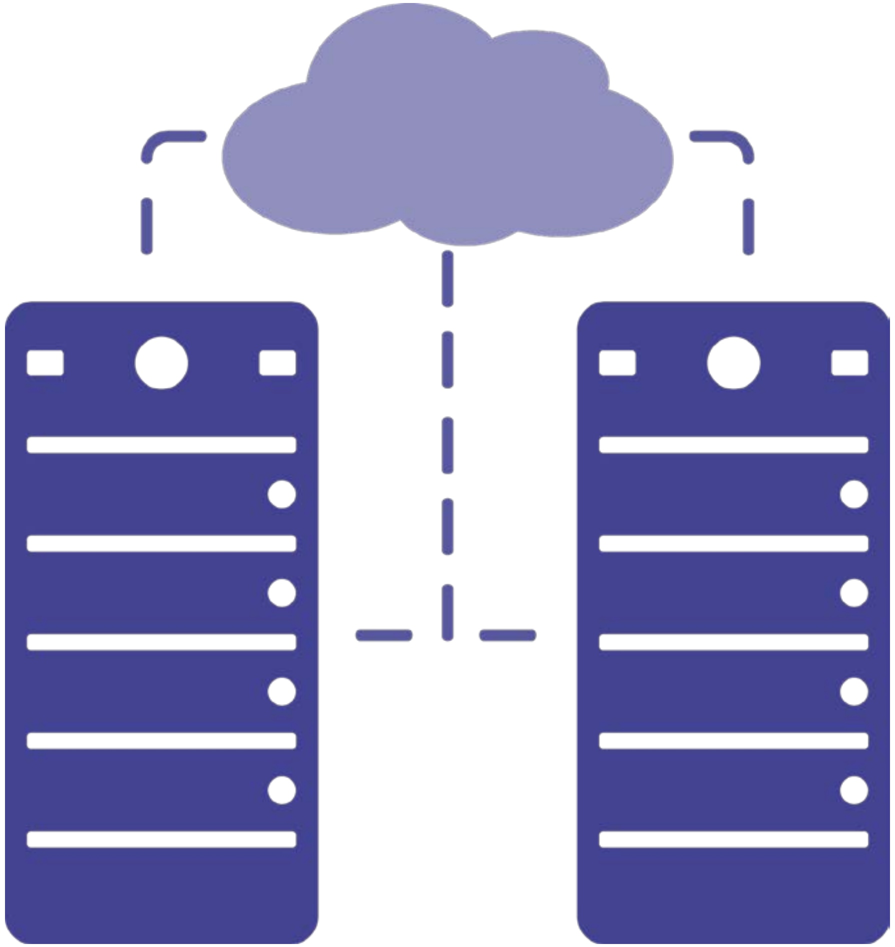
FDA Guidance on Responsibility – Manufacturers vs Providers

Cyber Risk

The FDA does not conduct premarket testing for medical products. Testing is the responsibility of the medical product manufacturer.

The medical device manufacturer is responsible for the validation of all software design changes, including computer software changes to address cybersecurity vulnerabilities.

“Cybersecurity routine updates and patches,” are generally considered to be a type of device enhancement for which the FDA does not require advance notification or reporting under 21 CFR part 806.



American Hospital Association

BDO

Managing the Risk of Medical Devices Through Process and Planning

Change Management Process Must Include Risk Assessment

Medical device manufacturers can always update a medical device for cybersecurity. In fact, the FDA does not typically need to review changes made to medical devices solely to strengthen cybersecurity.

The FDA recognizes that Health care Delivery Organizations (HDOs) are responsible for implementing devices on their networks and may need to patch or change devices and/or supporting infrastructure to reduce security risks. Recognizing that changes require risk assessment, the FDA recommends working closely with medical device manufacturers to communicate changes that are necessary.

Controlled Versus Uncontrolled Risk

?

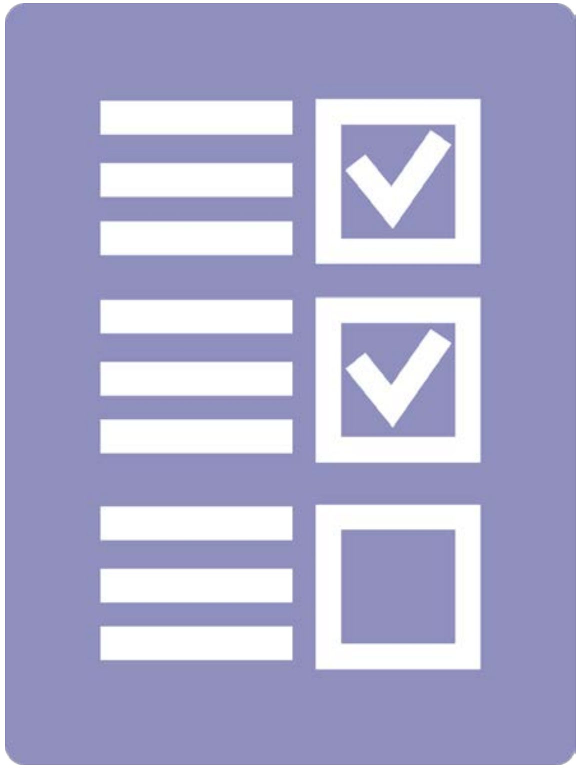
CONTROLLED

?

UNCONTROLLED

Threat x Vulnerability x Consequence = Risk

Steps to Cybersecurity for Internet of Things - Medical Devices

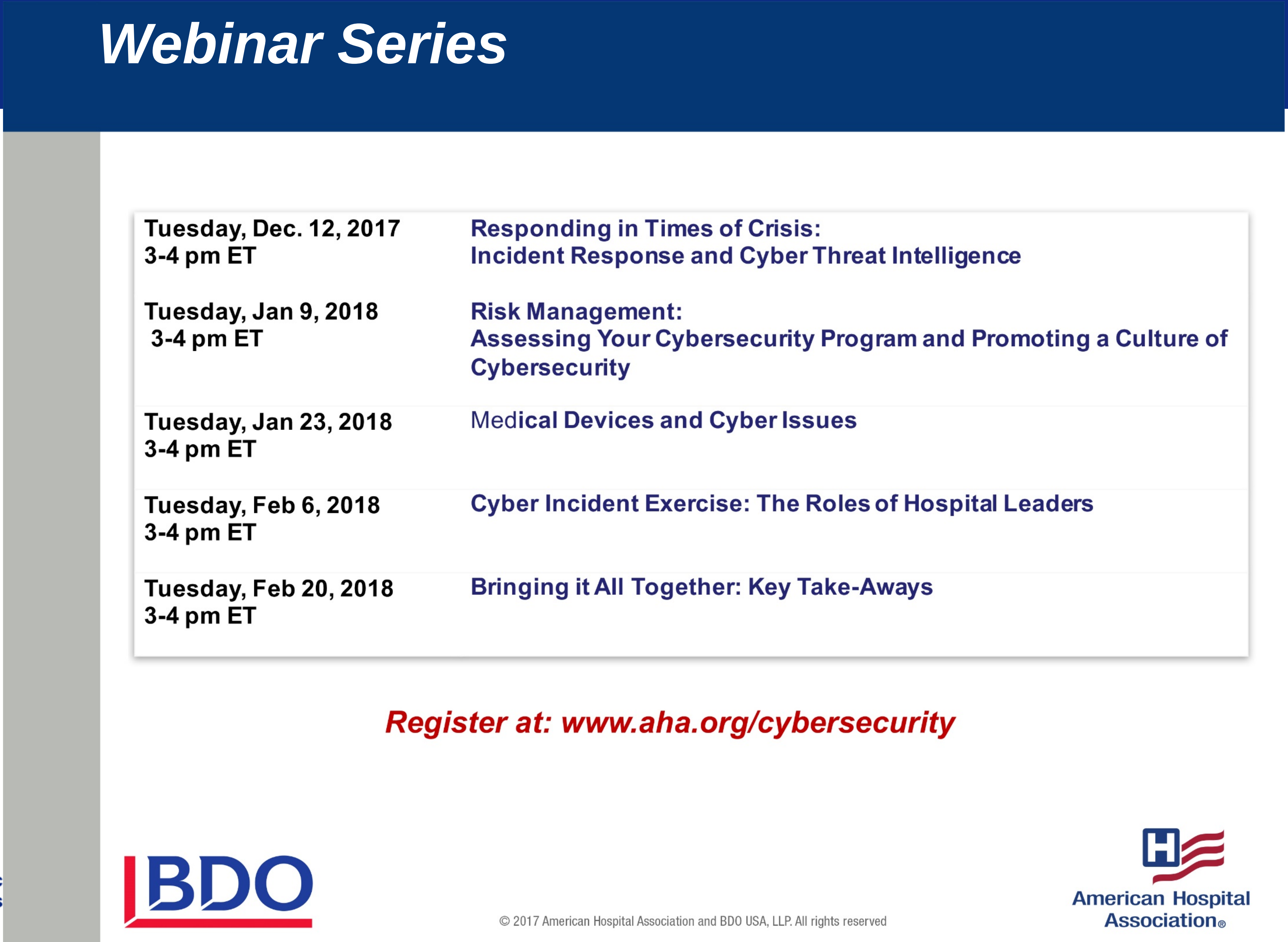


1. Categorize existing devices based on risk
2. Implement a clinical risk management framework
3. Ensure your organization follows basic security hygiene
4. Include security requirements in new device contracts or requests for proposals
5. Apply a zero trust networking architecture

American Hospital Association

BDO

Questions?



Webinar Series

Tuesday, Dec. 12, 2017 3-4 pm ET	**Responding in Times of Crisis: Incident Response and Cyber Threat Intelligence**
Tuesday, Jan 9, 2018 3-4 pm ET	**Risk Management: Assessing Your Cybersecurity Program and Promoting a Culture of Cybersecurity**
Tuesday, Jan 23, 2018 3-4 pm ET	Medi**cal Devices and Cyber Issues**
Tuesday, Feb 6, 2018 3-4 pm ET	**Cyber Incident Exercise: The Roles of Hospital Leaders**
Tuesday, Feb 20, 2018 3-4 pm ET	**Bringing it All Together: Key Take-Aways**

Register at: www.aha.org/cybersecurity

Contact Information

Laura Hars

Senior Manager
Cybersecurity
BDO Advisory Services
Direct: +1 732 734-3059
Mobile: +1 973 903-0453
Email: Lhars@bdo.com

About BDO Advisory

BDO Consulting, a division of BDO USA, LLP, provides clients with Financial Advisory, Business Advisory and Technology Services in the U.S. and around the world, leveraging BDO's global network of more than 67,000 professionals. Having a depth of industry expertise, we provide rapid, strategic guidance in the most challenging of environments to achieve exceptional client service.

BDO is the brand name for BDO USA, LLP, a U.S. professional services firm providing assurance, tax, advisory and consulting services to a wide range of publicly traded and privately held companies. For more than 100 years, BDO has provided quality service through the active involvement of experienced and committed professionals. The firm serves clients through more than 60 offices and over 500 independent alliance firm locations nationwide. As an independent Member Firm of BDO International Limited, BDO serves multi-national clients through a global network of 1,400 offices across 158 countries.

BDO USA, LLP, a Delaware limited liability partnership, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. BDO is the brand name for the BDO network and for each of the BDO Member Firms. For more information please visit: www.bdo.com.

Material discussed is meant to provide general information and should not be acted on without professional advice tailored to your firm's individual needs.