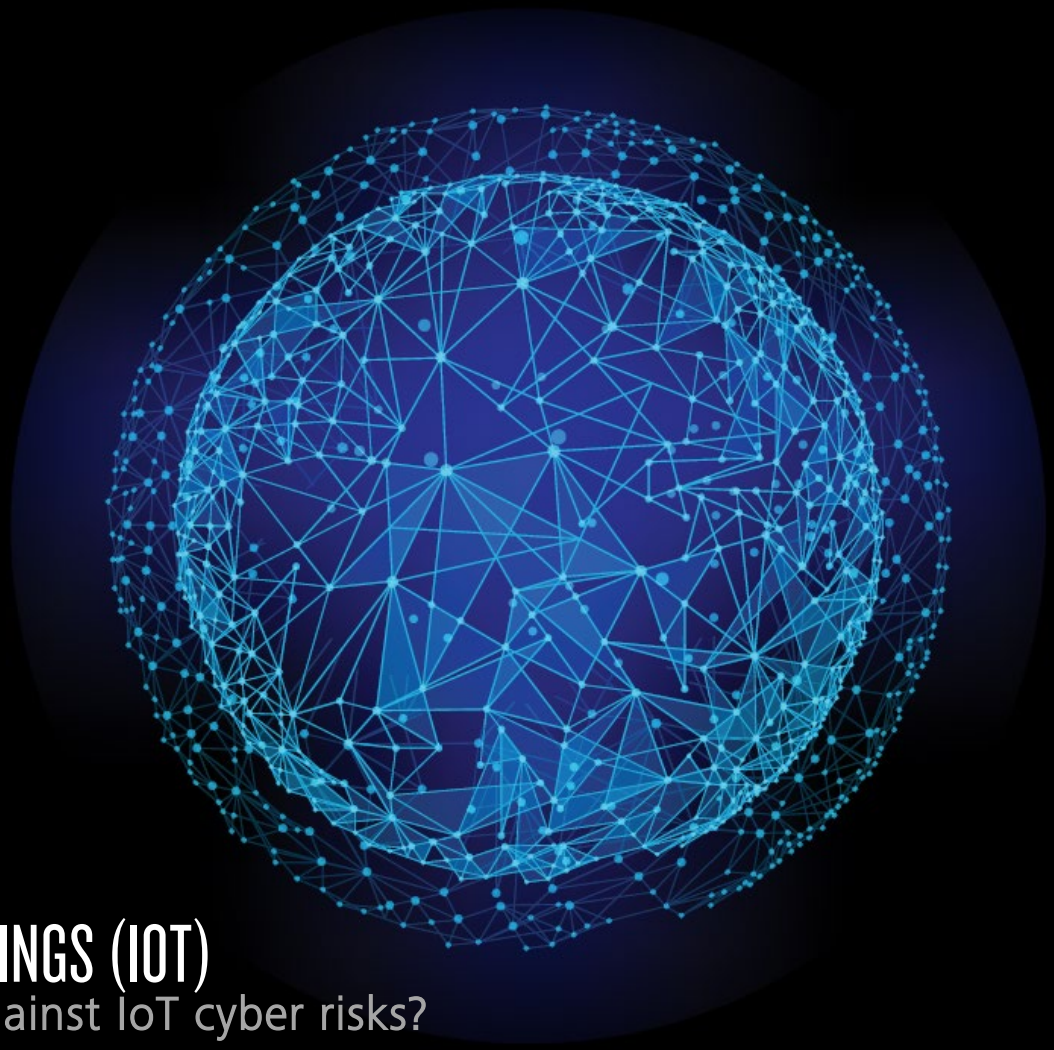
Deloitte.



SECURING THE INTERNET OF THINGS (IOT)

What can you do to protect against IoT cyber risks?

Russell Jones, Ramsey Hajj, Louverture Jones, Thiago Alves
Deloitte & Touche LLP
June 16, 2020

INTRODUCING OUR SPEAKERS

Ramsey Hajj
Principal
Deloitte & Touche LLP
IoT & Industrial
Control Systems Leader
rhajj@deloitte.com

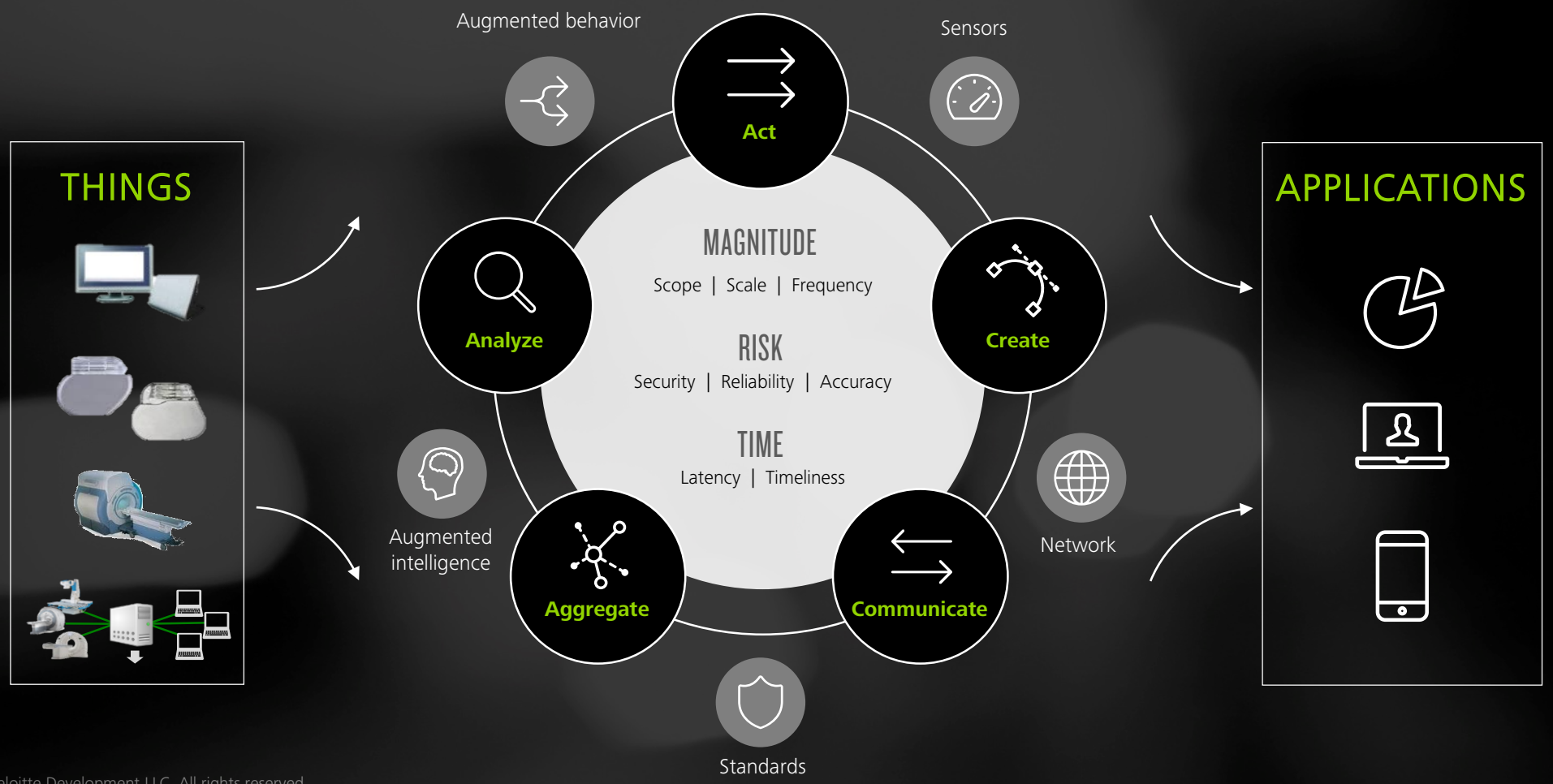
Russell Jones
Partner
Deloitte & Touche LLP
Medical Device
Safety & Security (MeDSS) Leader
rujones@deloitte.com

Louverture Lojo Jones
Senior Manager
Deloitte & Touche LLP
IoT Cyber Risk Leader
loujones@deloitte.com

Copyright © 2020 Deloitte Development LLC. All rights reserved.

MAKING SENSE OF THE BUZZWORDS: INTERNET OF THINGS?

Internet of Things refers to a world of intelligent, connected devices and supporting infrastructure that can help drive innovative medical treatment, patient outcomes, physical sensors, and business operations.



 Copyright © 2020 Deloitte Development LLC. All rights reserved.

: POLL QUESTION :

I ENJOY WORKING FROM HOME

A) Yes

B) No

C) Occasionally

D) Not applicable / No opinion

 Copyright © 2020 Deloitte Development LLC. All rights reserved.

MEDTECH/DIAGNOSTICS IS ADVANCING AT AN EXPONENTIAL RATE

Highly connected and increasingly smart medical technologies and devices enabled by interoperable data will help form the core of tomorrow's health ecosystem. Today's MedTech is already transforming how health care is provided…

Supercomputers that can diagnose lung cancer *at a low error rate*

Mobile health platforms *integrating data from biometric sensors*

Artificial Intelligence (AI)-powered clinical decision support systems *that improve accuracy and reduce costly, invasive tests and ineffective treatments*

Advanced cognitive analytics and predictive modeling *that promote prevention, early detection, and targeted treatment*

Affordable, commercially available sensors *that monitor and capture individual, population, and environmental data*

5 building blocks of exponential technological progress

Increased Computing Power | Augmented Data Storage Capacity | Hardware Miniaturization | Improved Network Connectivity | Advanced Software Capabilities

… and technology improvements will drive further disruption sooner than we expect

Continuous monitoring and ***real-time data collection in a highly connected environment of bio-sensors***

Aggregation of limitless amounts of data *and across an array of inter-connected sources with open and secure access*

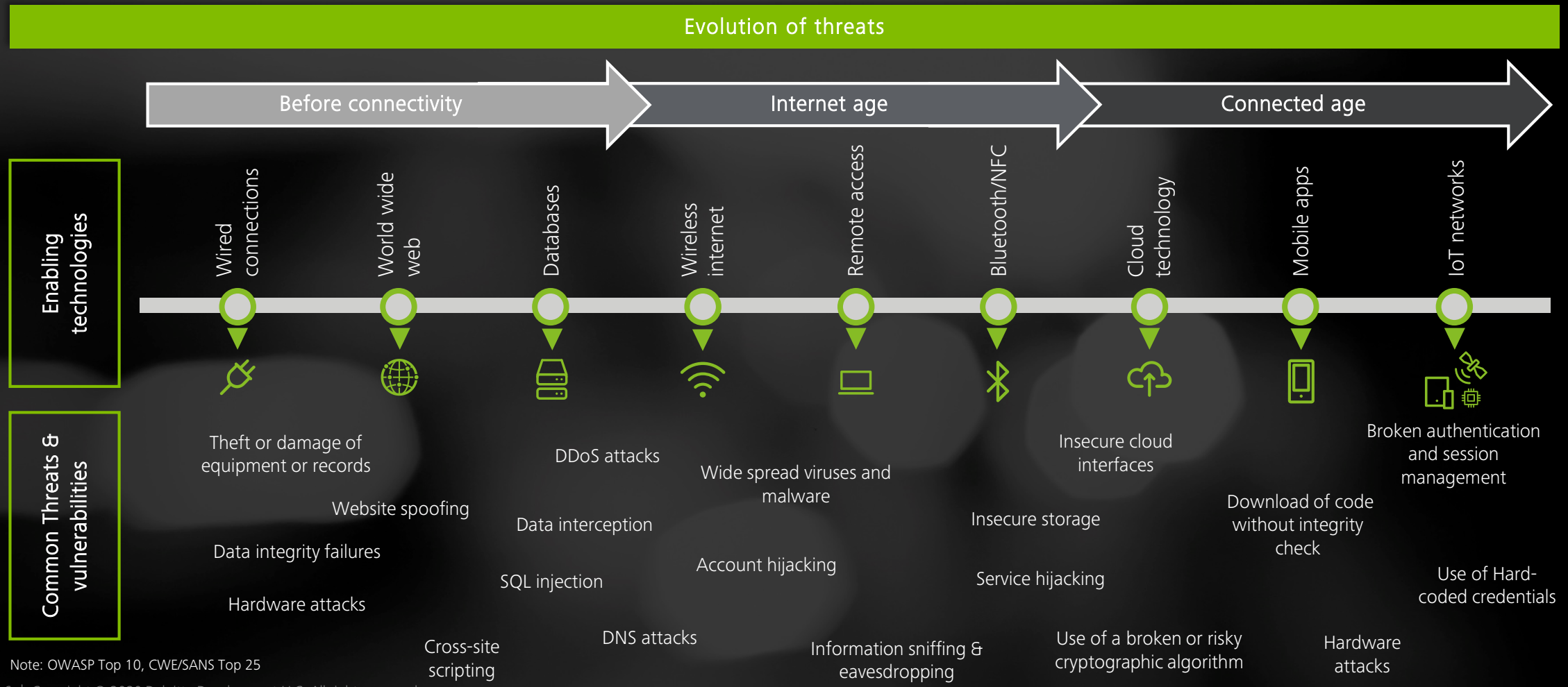
Application of advanced cognitive technologies to ***analyze infinite number of parameters and provide insights in real-time***

Integrated monitoring, data access and AI technology to provide ***personalized insights on-the-go***

 Copyright © 2020 Deloitte Development LLC. All rights reserved.

THE EVOLUTION OF THREATS TO MEDICAL DEVICES

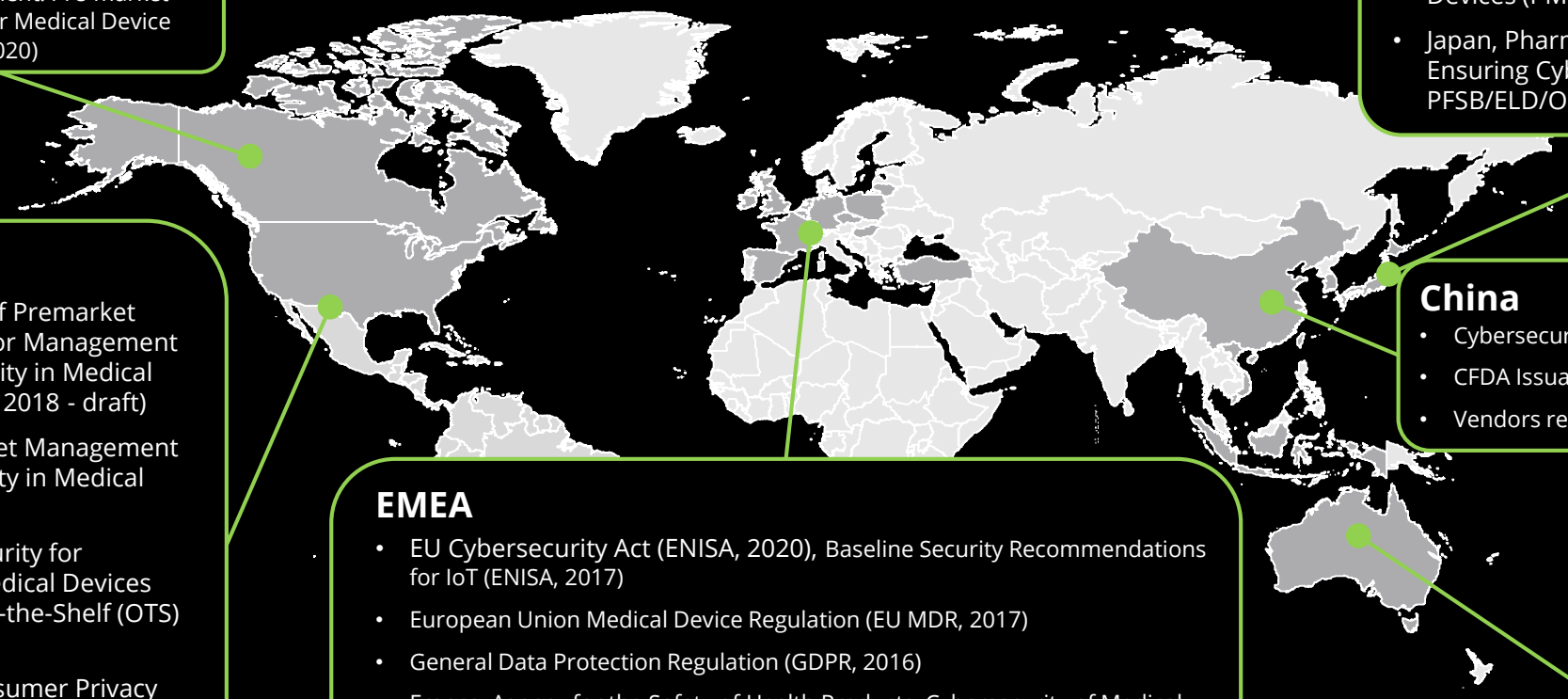
As connected device technology advances, the number of medical devices exposed to malicious threats increases, resulting in an increased risk to customer safety and information security.



Note: OWASP Top 10, CWE/SANS Top 25

 Copyright © 2020 Deloitte Development LLC. All rights reserved.

GLOBAL REGULATIONS DRIVING MEDICAL DEVICE SECURITY



Canada

- Guidance Document: Pre-market Requirements for Medical Device Cybersecurity (2020)

Japan

- Guidance for Ensuring Cybersecurity in Medical Devices (PMDA, 2018)
- Japan, Pharmaceutical and Medical Device Agency, Ensuring Cybersecurity of Medical Device: PFSB/ELD/OMDE Notification No. 0428-1

Americas

- FDA Content of Premarket Submissions for Management of Cyber Security in Medical Devices (2014, 2018 - draft)
- FDA Postmarket Management of Cybersecurity in Medical Devices (2016)
- FDA Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software
- California Consumer Privacy Act (CCPA)
- Association for the Advancement of Medical Instrumentation; AAMI TIR57

China

- Cybersecurity Law (2016)
- CFDA Issuance (2017)
- Vendors required to register with CFDA (2018)

EMEA

- EU Cybersecurity Act (ENISA, 2020), Baseline Security Recommendations for IoT (ENISA, 2017)
- European Union Medical Device Regulation (EU MDR, 2017)
- General Data Protection Regulation (GDPR, 2016)
- France, Agency for the Safety of Health Products, Cybersecurity of Medical Devices integrating software during their lifecycle
- German Institute for Drugs and Medical Devices (BfArM), Cyber Security Requirements for Network-Connected Medical Devices

Australia

- Australian regulatory guidelines for medical devices (TGA, 2018)

International Medical Device Regulators Forum, Draft IMDRF Principles and Practices for Medical Device Cybersecurity

 Copyright © 2020 Deloitte Development LLC. All rights reserved.

: POLL QUESTION :

HOW DO YOU VIEW IOT WITH RESPECT TO YOUR COMPANY'S FUTURE?

A) MY COMPANY HASN'T THOUGHT ABOUT IOT YET

B) MY COMPANY IS EXPERIMENTING AND TRYING TO UNDERSTAND IF AND WHERE IOT FITS FOR US

C) MY COMPANY IS BETTING BIG ON IOT AND VIEWS IT AS AN INSTRUMENTAL PART OF OUR FUTURE

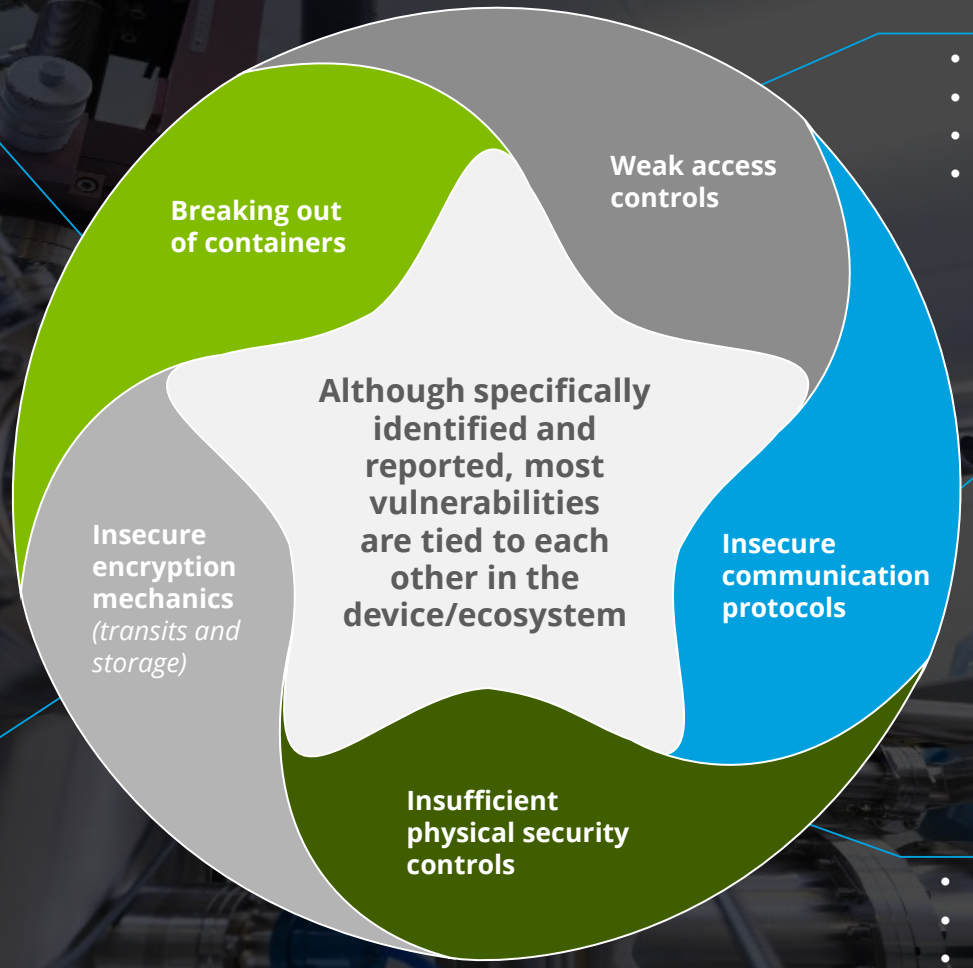
D) NOT APPLICABLE / UNKNOWN

 Copyright © 2020 Deloitte Development LLC. All rights reserved.

TOP SECURITY FLAWS OBSERVED IN THE FIELD

Below is an unofficial list of the top 5 security flaws observed from over 50+ recent connected medical device security assessment engagements

- Bypass of kiosk mode
- Virtual machine breakout
- Software to infrastructure



- Plaintext credentials
- Hardcoded credentials
- Weak password policies
- Passing of credentials

- Radio frequency
- Denial of service / availability
- Capture of patient Data

- No encryption
- Proprietary encryption

- Disassembly
- Debugging interfaces
- Unprotected storage media

 Copyright © 2020 Deloitte Development LLC. All rights reserved.

NOT ALL DOOM AND GLOOM: WHAT THE INDUSTRY IS DOING WELL

Building product security programs

Many device manufacturers have foundational to mature product security programs aligned to regulatory requirements and customer expectations

Shifting security left

Rather than reactive product security practices, device manufacturers are beginning to take a security-by-design approach to new product development

Integration of third party services

Device manufacturers are beginning to offer integration of third party security services/products (e.g., antivirus) in order to fulfill the requirements of their customers

Moving away from legacy

With more devices moving on to supported operating systems, this shift enables device manufacturers to utilize the latest vendor security capabilities (if desired)

Embracing security research

Security researchers have become a driving force across the industry and device manufacturers have begun to utilize and appreciate their feedback by establishing relationships and programs to facilitate information sharing (i.e., coordinated vulnerability disclosure)

 Copyright © 2020 Deloitte Development LLC. All rights reserved.

"A combination of factors is dramatically reshaping OT security. More Internet connected industrial automation devices, and the convergence of OT and IT infrastructures, in addition to a shortage of security skills, means that accurate evaluation and mitigation of security risks is increasingly challenging."

Department of Homeland Security's Industrial Control System Cyber Emergency Response Team (ICS-CERT)

 Copyright © 2020 Deloitte Development LLC. All rights reserved.

TOP CHALLENGES IN SECURITY INDUSTRIAL CONTROL SYSTEMS (ICS)

Below are challenges from a cybersecurity standpoint in security industrial control systems, especially with the emergence of smart factories

The ever-increasing attack surface

- Increase in the amount and complexity of automation system, tools, as well as communication channels in the OT landscape.
- Emergence of communication channels for monitoring between previously independent objects.
- Expanded opportunities for criminals to plan and execute attacks.

The growing interest of cybercriminals in industrial enterprise

- A decrease in profitability and increase in risks from cyberattacks aimed at traditional victims is pushing criminals to search for new targets in OT.
- There is a significant increase in activities engaged in the research and development of techniques to implement espionage and terrorist attacks aimed at industrial enterprises.

The underestimation of general threat levels

- Lack of public access to information about information security issues within industrial enterprises results in the denial of objective reality and underestimation of threat levels.

The misunderstanding of threat specifics and the suboptimal choice of mitigation options

- Industrial cybersecurity often lacks sufficient understanding of threats and is mislead by high profile incidents.
- As a result, security products protect better from artificial scenarios than from real world day-to-day threats. Hence, leaving industrial enterprises vulnerable to attacks.

 Copyright © 2020 Deloitte Development LLC. All rights reserved.

: POLL QUESTION :

OUR CURRENT SECURITY, AUDIT, AND/OR RISK MANAGEMENT PROGRAM CONSIDERS IOT RISKS

A) Yes

B) No

C) Not applicable

 Copyright © 2020 Deloitte Development LLC. All rights reserved.

ALIGNMENT BETWEEN BUSINESS, OT, AND IT

A common challenge is an organization's Chief Information Security Officer (CISO) being given overall responsibility for security covering both IT and OT. Misalignment between the business, IT, and security occurs.

Safe and secure ICS/OT Ecosystem

Governance and leadership

- **ICS/OT security operating committee**
  - Operations leadership
  - Legal leadership
  - R&D leadership
- **ICS/OT security leadership council**
  - Privacy leadership
  - IT security leadership
  - Regulatory compliance leadership
- **Governance**
  - + Program framework
  - + Governance model
  - + ICS/OT Security policies

Operating components

Security risk management
- Asset inventory and identification
- ICS/OT security risk assessment
- Third party security risk management
- Buildout of controls framework

Security event incident handling
- Threat intelligence through active monitoring
- Patch and vulnerability management
- Security event handling
- Security incident handling

Security education and training
- Security awareness—personal and shared responsibilities
- Secure configuration management
- Secure software development lifecycle (SSDLC)

Program monitoring
- Key performance indicators
- Program audit framework - self, peer and audit function assessments
- Program assessment framework

Foundational components

Planning → Analysis → Design → Remediation and build → Test → Continuous program monitoring → Maintain → End-of-life

- Central document repository
- Infrastructure and security components
- Change control
- Industry and organizational context

Security by Design

Outcomes

- Formal governance program established to cover both IT and OT stakeholders
- Mechanisms and processes developed to allow for communication and secure data exchange
- Business-centric representation in the governance structure allowed the IT and OT teams to collaborate where practical and enable the business in a secure fashion
- Standards-based architecture adopted and used to drive transformation and remediation efforts

 Copyright © 2020 Deloitte Development LLC. All rights reserved.

INDUSTRIAL IOT (IIOT) USE CASES

Use cases

- Real-time equipment monitoring, visual analytics, in-line quality testing
- Tracking sensors to dynamically adjust schedules
- Predictive maintenance, augmented reality (AR) to assist maintenance personnel, sensor-enabled asset monitoring
- Automated guided vehicles, automated conveyance to confirm continuous material flow

Considerations

- Apply defense-in-depth strategies: Detect, plot, and translate the cyber threat landscape.
- Perform cyber compromise assessments, security evaluations of new technologies, and threat modeling and simulation exercises.
- Employ application whitelisting, source code review, and file integrity monitoring to reduce the risk of malicious code being installed and executed.
- Continuously assess entry points, motivation, and vehicles to execute an attack to enable the organization's technical teams to build operational response capabilities.

 Copyright © 2020 Deloitte Development LLC. All rights reserved.

CYBER IOT STUDIO DEMONSTRATION

: POLL QUESTION :

HAS YOUR ORGANIZATION EXPERIENCED ANY CYBER INCIDENTS OR BREACHES IN THE LAST 12 MONTHS?

A) Yes

B) No

C) Not sure / unknown

D) Not applicable

 Copyright © 2020 Deloitte Development LLC. All rights reserved.

Q&A

 Copyright © 2020 Deloitte Development LLC. All rights reserved.

Deloitte.

This document contains general information only and Deloitte is not, by means of this document, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This document is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this document.

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2020 Deloitte Development LLC. All rights reserved.