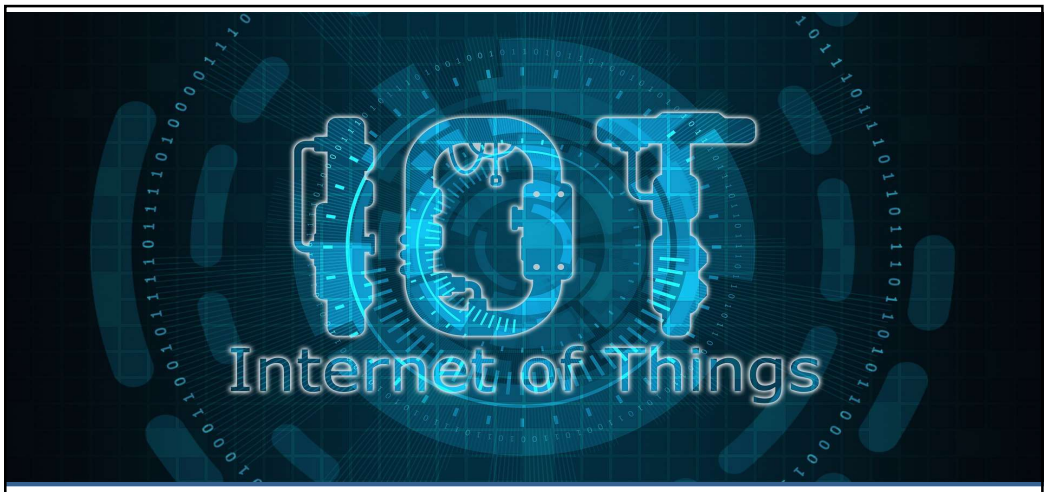


ROLE OF COMPLIANCE IN THE IoT WORLD

April 2021

Private and Confidential

KROLL

1

PRESENTERS

KROLL

Alan Brill, CISSP, CFE, CIPP/US, FAAFS
Senior Managing Director, Cyber Risk Practice, Kroll
Fellow of the Kroll Institute
Adjunct Professor, Texas A&M University School of Law

Yvette Gabrielian, ESQ., CIPP/US, CIPM
Senior Vice President, Cyber Risk Practice, Kroll

2

NOTICE

Any positions presented in this session are those of the panelists and are not necessarily the official position of Kroll.

This information is generic in nature and is believed to be accurate as of the date it was created. Before using this information, you should assure that it is appropriate for your particular circumstances.

This material is offered for educational purposes with the understanding that neither the authors nor Kroll or its affiliates are engaged in rendering legal, accounting or any other professional service through presentation of this material.

3

What is IoT?

4

WHAT IS IoT?

"The **Internet of things** (**IoT**) describes the network of physical objects—"**things**"—that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the **Internet**."

Source: Wikipedia

Source: NIST.org

5

IoT and HEALTHCARE

6

IoT and HEALTHCARE

INTERNET CONNECTIVITY has revolutionized the use of “smart” devices:

- Bedside devices from patient monitors to infusion pumps
- Laboratory devices such as autoanalyzers
- Digital imaging devices from x-rays to MRIs
- Home-based sensors from ICDs to EKGs
- Clinician access to patient records
- Patient access to laboratory results
- Monitoring of hospital equipment, including ultra-low temperature freezers for vaccine storage

Our objective today is to remind you of one vital concept:

7

You need to give specific thought to security and privacy before buying or installing that next IoT-ready device.

8

Regulatory Landscape

9

IoT LAWS AND COMPLIANCE FRAMEWORKS

STATE LEGISLATION

- CA
- OR

Primary requirements:

- Responsibility for manufacturers to build in security features
- Reasonable security features to protect information in the IoT device that collects, contains, stores, or transmits such information

FEDERAL

Proposed regulations addressing IoT devices:

- Cyber Shield Act
- Protecting Privacy in Our Homes Act
- Automatic Listening Exploitation Act

New federal law:

- Internet of Things Cybersecurity Improvement Act of 2020

INTERNATIONAL

- Australia
- Mexico
- Brazil
- China
- Malaysia
- EU

INTERNATIONAL IoT STANDARDS

OUR RECOMMENDATION

Pay attention to the proposed laws and regulations as they emerge to avoid being blindsided. Some will require actions on your part which may take time and resources to plan and prepare for.

10

FDA and Other Government Agencies are Warning Users About IoT Risks

"Medical devices are becoming increasingly connected, and connected devices have inherent risks, which make them vulnerable to security breaches. These breaches potentially impact the safety and effectiveness of the device and, if not remedied, may lead to patient harm"

Suzanne Schwartz, M.D.

FDA Center for Devices and Radiological Health

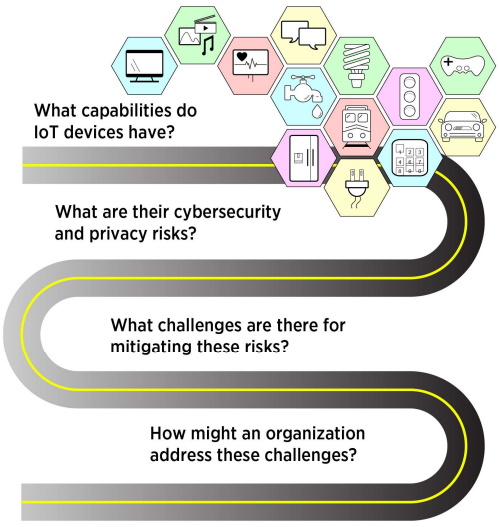
11

Healthcare IoT Risks

12

HEALTHCARE IoT RISKS

- Risks include:
  - ✓Unauthorized Access to Data/Device Software
  - ✓Compromise Integrity of Data
  - ✓Affect Device Performance
  - ✓Shutdown Device
  - ✓Device Takeover
  - ✓Modify or Prevent Alarms/Warnings



Source: NIST

13

Role of Compliance in Healthcare IoT

THE VITAL ROLE OF COMPLIANCE IN HEALTHCARE IoT

- Experience indicates that IoT-related problems represent a very real risk to healthcare institutions and that devices with significant risk are finding their way into actual use.
- Why a particular failures occurred varies between cases, but somewhere, when it came to security, someone dropped the ball.
- Problems occur when appropriate standards do not exist or are not followed.
- *Assuring that appropriate standards are in place and that those standards are being implemented is an important role of compliance officers and compliance departments.*
- The real question is: ***What should the rules be for IoT security?***

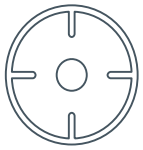
Credit: Wikipedia Commons

A COMPLIANCE OFFICER'S GUIDE TO ASSURING REASONABLE SECURITY OVER THE INTERNET OF THINGS

Understand different categories of IoT devices

- **CATEGORY 1: devices that the institution installed as part of its technology. These are the "official" IoT devices - organization knows it's there and that it's doing work that organization knows about.**
- **CATEGORY 2: devices owned or used by or for the institution that the institution does not know are there. Devices where there is no official recognition that they have an IoT component.**
- **CATEGORY 3: devices that get connected to institution's networks but are not owned or operated on behalf of the institution.**

IDENTIFY



Does your organization know what IoT devices are attached to its networks?

- ❑ You MUST know what is connected to your network. If you don't expect to be surprised in a way that you will not like.
- ❑ Develop an inventory of what you know you own.
- ❑ Verify the inventory.
  - ❑ Use technology to identify what is connected to your company network, both hard-wired and wireless. You can identify devices through unique MAC addresses.
  - ❑ Remember that not all devices are obviously medical. For example, the Ultra Low Temperature (ULT) freezers you may be using for clinical supplies like the Pfizer-BioNTech COVID-19 vaccine. Same is true for some air cleaning devices.
  - ❑ Use in-person inspection to identify owned resources that could be, but currently aren't connected to the network.
- ❑ Lock down the network to prevent unexpected devices to be connected.
- ❑ Do not allow these devices to be connected to your "guest" network to bypass controls on the company network.

17

ANALYZE

Does your organization understand how to analyze the security of an IoT device?

- Can the software and firmware be updated/patched?
- Can those updates/patches be done reliably and securely?
- Does the device provide appropriate limitations on who can access it and what they can do?
- Is the device designed to safeguard data that is received, transmitted, generated, or stored?
- Does the device manufacturer stand behind its product?
- Was the device designed with security reviews of its components (hardware and software)?
- Is there assurance that the device is genuine not counterfeit?

18

WHAT ARE YOU GOING TO DO ABOUT PERSONALLY OWNED IoT DEVICES?

KROLL

Have you considered what rules you should have for connection of personally owned/controlled IoT devices to your visitor network?

- Some devices use a lot of bandwidth.
- Some devices are often associated with activities that could take time – such as devices that can stream movies.
- Should you have a separate guest network for staff and for patients/visitors?
- Should you have rules on bandwidth usage?

19

THE ROLE OF THE COMPLIANCE OFFICER

KROLL

- Depending upon circumstances, the role of the compliance officer may range from identifying an urgent need to create policies and procedures relating to IoT to assurance of compliance with company rules to an urgent need to review devices already in use.
- At a minimum, we think that you should be using the CIS Top 20 Controls as a guide for establishing minimum reasonable security practices for your organization , including security related to IoT devices.
- Help to assure that IoT security is documented from policies through compliance reviews.
- However, IoT is an area of interest to lawmakers and regulators globally. Therefore, it is reasonable to assume that applicable laws and regulations will change overtime and every organization has a responsibility to monitor and adjust is standards, policies and procedures to maintain compliance.

20

IN CONCLUSION

- ✓ **IoT devices in healthcare are a real and current problem.**
- ✓ **They are likely in your organizations now, whether you know it or not.**
- ✓ **It is virtually inevitable that they will be the subject of laws/regulations.**
- ✓ **You need to assure that there are policies, that they are implemented and that they remain current as technology, laws and regulations evolve.**
- ✓ **Without compliance oversight, we believe that IoT will represent a greater risk to healthcare organizations than is the case with compliance's involvement.**

21

For more information, please contact:

Yvette Gabrielian, ESQ., CIPP/US, CIPM
Senior Vice President, Cyber Risk Practice, Kroll
yvette.gabrielian@kroll.com

Alan Brill, CISSP, CFE, CIPP/US, FAAFS
Senior Managing Director, Cyber Risk Practice, Kroll
abrill@kroll.com

22