THE CONFERENCE BOARD

Cybersecurity for Essential Services SEMINAR

Healthcare | Energy | Law Enforcement | Emergency Management

December 4, 2019
The Conference Board
Conference Center
New York, NY

www.conferenceboard.org/cybersecurityevent

Wednesday, December 4, 2019

8:00 – 9:00 am
Seminar Registration/Breakfast

9:00 – 9:15 am

Welcome and Introduction

In this introduction, we lay out the structure and goals of the seminar, including as overview the current state of cybersecurity for essential services.

9:15 – 10:00 am

Ransomware attacks: Lessons learned in detecting, preventing, and responding to attacks

There are now 50 families of ransomware, and they are becoming more sophisticated. While recent media attention has drawn more attention to it, understanding what healthcare organizations must do to prevent and respond to ransomware is not widely understood. In this in-depth discussion, learn how:

- Vulnerabilities are exploited and what protections can be implemented to mitigate exposure
- Automation, and cyber protection systems can detect attacks quickly to protect records from becoming encrypted
- Organizations must respond to an attack to ensure operational resiliency and regulatory compliance

Larry Karl, Section Chief of Cyber Engagement and Intelligence, **FBI**

10:00 – 10:30 am
Networking Break

10:30 – 11:15 am

Bolstering your cybersecurity defenses: The importance of incidence training, simulation, and risk management

Cybersecurity is a key component of any organization's risk management strategy. And because the scope of the risk often paralyzes staff, the most effective response is to train your staff appropriately. Build strategic initiatives to:

- Move toward a more proactive risk management strategy to cybersecurity through better training opportunities
- Build more robust partnerships with both internal and external experts to manage cyber risks
- Lessons learned from Grid Ex, the largest emergency management exercise for utilities in North America, with more than 6,500 participants, representing 450 organizations

Keith Butler, SVP, Global Risk Management and Insurance, Chief Risk Officer, **Duke Energy**

11:15 am – 12:00 pm

Case Study: Mayo Clinic

Best practices in defending against phishing emails: What healthcare teams need to know

One of the most prevalent security breaches healthcare organizations experience is through phishing emails. However, with proper training and due diligence, this is also one of the easier attacks to prevent. Learn how the Mayo Clinic:

- Developed internal campaigns to ensure all staff become more aware of phishing attacks
- Created resiliency in the system to limit harm and lost data
- Improved from a 50% to 5% fail rate over the last 4 years
- Achieved higher success rates by publishing score cards

JoEllen Frain, Senior Manager – Risk Management, **Mayo Clinic**

12:00 – 1:00 pm
Lunch

1:00 – 1:45 pm

Case Study: Catholic Health Services of Long Island (CHS)

A "Risk Based" Approach to Incident and Threat Management strategies for critical operational organizations.

"With the evolution of cybersecurity over the last decade, it's easy to forget what security really is; the art of dealing with risk."

CHS is a critical part of the health care system in the areas they serve. And, as a key component to the health care system, they are proactive in their cyber management practices to combat cyber-attackers. Take advantage of this important discussion to understand:

- How CHS developed their cyber security program
- How CHS incorporates it into their larger risk management strategy
- How CHS responds to all threats, but specifically cyber threats
- Some lessons learned following cyber incident
- The importance of NIST standards for healthcare cybersecurity

Tim Swope, Chief Information Security Officer, **Catholic Health Services of Long Island**

1:45 – 2:30 pm

Cyber prevent and detect: How New York City's Cyber Command is securing its smart city essential services

New York City's cyber command leads the city's cyber defense efforts and incorporates more than 100 agencies and offices "to prevent, detect, respond, and recover from cyber threats." With everything from water security to transportation to elections, NYC Cyber Command must manage the cyber risk for all essential services. Understand how you can:

- Protect smart city technology to enhance your cyber defenses
- Ensure essential services have robust risk management to detect and respond to cyber threats in real time
- Create an action plan to keep services operational even during a cyber attack

Mike Krygier, Deputy CISO, Urban Technology, **City of New York Cyber Command**

2:30 – 3:00 pm
Networking Break

3 00 – 3:45 pm

IoMT: Building robust security protocols in an increasingly connected world

Connected medical devices operate on a different model from an enterprise system. These devices are subject to the same security risks as other enterprise components, plus they present some additional cyberattack targets driven by the devices' criticality and high-risk profile. Device security isn't easy to bolt on to a product. It really needs to be baked into the design. Moreover, the security hardening is not a simple or a quick process. For example, patching, testing and integrating these devices into the enterprise IT ecosystem is much more difficult.

Learn how traditional and emerging cyber security concerns and threats impact the security and privacy of medical information and medical devices. Understand the challenges and solutions currently being developed to make connected medical devices more secure, such as:

Secure by design initiatives with more robust security standards

- Innovative solutions unique to connected medical devices
- The challenges of securing patient-centered devices
- The role recently proposed legislation could have on device makers
- Guiding principles of Secure-by-Design and how they apply to medical devices and the entire ecosystem of patient-related data

Charles Popper, Program Director, CIO Business Council, Leader, Digital Transformation Institute, **The Conference Board**

3:45 – 4:30 pm

Proactive Cyber Management: Effective strategies for building the business case for a robust cybersecurity program

Despite an increase in cyberattacks, including cyber-terrorism, organizations continue to fall behind in the ability to thwart attacks. All organizations have experienced increases in cyber-attacks, and not just data breaches. And while awareness is a necessary response, your first requirement is ensuring your defenses are in place to detect and respond automatically. Determine how to best secure your organization by:

- Bolting security features onto your organization's strategic enterprise wide initiatives
- Demonstrating that cybersecurity impacts your organization's ability to exist
- Demonstrating that the infrastructure costs saves money relative to the cost of lost data

Mikhail Falkovich, Director IT, **Con Edison**
Larry Clinton, President, **Internet Security Alliance**

4:30 pm

Closing remarks

REGISTRATION INFORMATION

Online www.conferenceboard.org/cybersecurityevent
Email customer.service@conferenceboard.org
Phone 212.339.0345
8:30 am –5:30 pm ET, Monday – Friday

Pricing:	
Members	**$500**
Non–Members	**$600**

Fees do not include hotel accommodations.

Location

The Conference Board Conference Center
845 Third Avenue (Between 51st and 52nd)
New York, NY 10022
Tel: (212) 339-0345

Cancellation Policy

Full refund until three weeks before the meeting. $500 administration fee up to two weeks before the meeting. No refund after two weeks before the meeting. Confirmed registrants who fail to attend and do not cancel prior to the meeting will be charged the entire registration fee.

Team Discounts per Person

For a team of three or more registering from the same company at the same time, take $300 off each person's registration. One discount per registration. Multiple discounts may not be combined.

Program subject to change. August 2019