



# WEDNESDAY, MAY 13<sup>TH</sup>

## 1:00 PM | WELCOME

## 1:15 PM | GENERAL SESSION



**Law and Order TVU – Telco Victims Unit: True Stories of White-Hat Hacking Team**  
*Dan Burwitz, IT Security Staff, Vantage Point Solutions*

In the criminal justice system, technology-based offenses are considered especially heinous. In South Dakota, the dedicated Red-Team hackers who investigate these vicious felonies are members of an elite squad known as the Telco Victims Unit. These are their Stories. This session focuses on true-life findings from Vantage Point Cybersecurity Red-Team exercises. Don't miss your chance to hear firsthand all the unique new ways hackers are stealing your data through the eyes of a white-hat hacker. Dumpster diving, hiding in supply closets, stealing cars, and even leveraging data from the Equifax breach are just some of the techniques covered in this session.

## 2:00 PM | GENERAL SESSION



**State of Iowa Cybersecurity Journey**  
*Dan Powers, Security Operations Center & Networking Manager; Darwin Ten Haken, IT Infrastructure Architect; Calvin Moore, Security Engineer; Jesse Martinez, Cybersecurity Services Coordinator; State of Iowa, Office of the CIO Team Members*

The State of Iowa Office of the Chief Information Officer (OCIO) Information Security Division (ISD) has a vision to lead state government in protecting information technology resources and data. This session will cover the importance of the Center for Information Security (CIS) Top 20 critical

controls and highlight cybersecurity tools and how they are used in the Security Operations Center (SOC). Additionally, the critical nature of established partnerships and how those partnerships have helped with threat intelligence and information sharing will be discussed.

## 2:40 PM | NETWORKING BREAK – SMALL GROUP CHAT ROOMS WITH SPONSORS

Similar to visiting the sponsor display tables at an in-person conference, this break will allow attendees to visit directly with representatives from our sponsor companies. Attendees will access the breakout room of their choice through links posted to the ICA website. Company representatives will be in their breakout room, ready to visit with attendees, share about their products and services, and answer questions. Attendees can visit multiple sponsor breakout rooms during the break. Specific instructions will be shared during the Conference.

## 3:00 PM | BREAKOUT SESSION #1 - NON-TECHNICAL



**Should We Perform a Vulnerability Scan or Penetration Test?**  
*Steve Healey, Chief Technology Officer, Pratum*

Vulnerability scanning and penetration testing are different security activities. However, there are similarities, which lead to the confusion. In this presentation, we will compare these activities and highlight best practices. You will leave with a clearer understanding of why they are important, how they can impact your business, and when to perform them.

### 3:00 PM | BREAKOUT SESSION #2 - TECHNICAL



**Preventing a Cyber Pandemic with the Zero-Trust Network Security Model**  
*Jon Brown, Sr. Systems Engineer, CCI Systems*

This session will dive into the concept of exactly what the Zero-Trust-Design would look like and provide insights into how you can leverage this model to reduce your network's exposure to better secure network resources, regardless of where the user or resource resides. Don't miss your chance to get a look at the future tool-box of the network security engineer.

### 3:45 PM | BREAKOUT SESSION #1 - NON-TECHNICAL



**Data Breaches**  
*James Taylor, Sr. IT Security Consultant, Vantage Point Solutions*

Data is the most valuable commodity produced today. There are guidelines for handling certain types of sensitive data, but these rules do not exist in all industries. Even so, these rules

can't stop breaches entirely. We will walk through some of the largest breaches, how they occurred, and what could have prevented them from happening.

### 3:45 PM | BREAKOUT SESSION #2 - TECHNICAL



**Vulnerability Management Best Practices**  
*Dawson Medin, Security Engineer, ProCircular*

Vulnerability management is an integral part of any successful security program. With new threats and vulnerabilities released on a daily basis, proper vulnerability management can help reduce risk and secure your organization from the rapidly moving threat landscape. This session will share which best practices should be included in design, execution, and management of a successful vulnerability management program and how this can be used to achieve compliance with regulatory requirements and align with industry standards.

### 4:30 PM | VIRTUAL HAPPY HOUR AND NETWORKING

Grab your beverage of choice and then connect with other attendees in small video chat groups.

# 2020 SPONSORS



Diamond  
ALL-STAR



Gold  
ALL-STARS



Bronze  
ALL-STARS



## PRESENTING



## GOLD



## CONFERENCE APP SPONSOR

## SILVER



# THURSDAY, MAY 14<sup>TH</sup>

## 8:30 AM | GENERAL SESSION



**Cybersecurity Risk Analysis**  
*Tim Fawcett, Director of Cyber Security Consulting, C.H. Guernsey & Company*

Tim will be discussing how post WWI French military strategy provides lessons for securing our systems and networks. IT departments in today's organizations are tasked with many job functions, of which, cybersecurity is only one. IT professionals are trying to protect against new and expanding threats with few resources. Much like the French prior to WWII, who took a defensive posture using the most sophisticated technology of the day to compensate for the lack of available manpower, organizations today are relying heavily on technology to protect against cyber threats. Though not a perfect analogy, there are some interesting lessons related to understanding new threats and technology. We will also be discussing risk and controls as it relates to IT and other topics.

## 9:20 AM | BREAKOUT SESSION #1 - NON-TECHNICAL



**State of Cyber Attacks – The Human Element**  
*Jessica Richter, Director, BKD CPAs & Advisors*

Cyber attacks have become more sophisticated. However, the attacks are focusing more on the human aspect than technical. The majority of successful attacks are through phishing schemes in which payment are redirected from legitimate sources to malicious user accounts. We will discuss these tactics amongst others. As well as steps to mitigate the risks.

## 9:20 AM | BREAKOUT SESSION #2 - TECHNICAL



**Mobile Threats & Data Access**  
*James Taylor, Sr. IT Security Consultant, Vantage Point Solutions*

Many companies today allow access to corporate or business networks from smart phones and mobile devices. The sheer amount of data stored on mobile devices creates a huge challenge for device administrators. Containing and controlling the amount of data, dealing with untethered access across file systems, and deciding and maintaining

what data is accessible by which applications proves to be a daunting task. These issues coupled with social engineering can lead to the greatest exposure and data loss. We will walk through mobile threats and the techniques that you can use to protect your users and data.

## 10:05 AM | COFFEE BREAK WITH SPONSORS

Another chance to meet with sponsors in small group breakout rooms. Specific instructions will be shared during the Conference.

## 10:20 AM | BREAKOUT SESSION #1 - NON-TECHNICAL



**Vendor Requirements From a Cybersecurity Perspective and Third Party Risk Management**  
*Ben Hall, Information Security Consultant, Pratum*

Organizations relying on outside vendors to provide and perform services opens up the organization to new risk potential. In this presentation, we will go over the steps necessary to properly evaluate the information security controls for a vendor and develop a plan to mitigate possible risks. We will also discuss how to continue to evaluate vendors on an ongoing basis.

## 10:20 AM | BREAKOUT SESSION #2 - TECHNICAL



**Cybersecurity – Hacks, Tips & Tools**  
*Blake Griffin, President, CNE & CNE IT Solutions*

Everyone has been to presentations discussing cyber threats and best practices. This presentation will include live demonstrations of these hacks. Tips to avoid these hacks and the tools that can be used to combat them will also be discussed.

## 11:05 AM | GENERAL SESSION



**Partnering for Success: Confronting Today's Cybersecurity Challenges**  
*David Cotton, Chief Technology Officer & Chief Information Officer, Aureon*

In this session, we will discuss cybersecurity challenges in today's mixed-generational equipment environment. Attendees will gain insight on common threats and vectors of attack, while also learning about effective frameworks for risk assessment, identification, mitigation and mediation.

## 11:45 AM | CLOSING REMARKS