



**ATTN: ICA MEMBERS
BUY ONE, GET ONE
1/2 OFF
REGISTRATION**
look inside for details

APRIL 24-25, 2018

Prairie Meadows Conference Center
ALTOONA, IOWA



The number of cyber-attacks increase daily. They are becoming more sophisticated, and experiencing a breach is not an if, but when. How quickly can you detect, respond, and recover before the cost of repair and damage control puts you in the red?

SESSIONS



Learn how to mitigate that risk, develop procedures and policies in case of a breach and hear from security experts on best practices for employee training at the ICA CyberCon III. Roll up your sleeves for this one! Day one will include Crises Scenario roundtables where you and your tablemates will work through response plans for different types of attacks.

Hotel Reservations: ICA has a block of rooms at Prairie Meadows at the rate of \$124 + tax per night. Call **(800) 325-9015** or **(515) 957-3000** by April 3, 2018 to reserve your room. Be sure to ask for the ICA rate.

DEPARTMENT OF HOMELAND SECURITY CYBER RESOURCES OVERVIEW

Geoffrey Jenista, Office of Cybersecurity & Communication Stakeholder Engagement and Cyber Infrastructure Resilience

Mr. Jenista serves as Cyber Security Advisor, Region VII, for the Stakeholder Engagement and Cyber Infrastructure Resilience Division of the Office of Cybersecurity and Communications (CS&C) National Protection and Programs Directorate (NPPD). He supports the Department of Homeland Security (DHS) mission of strengthening the security and resilience of the nation's critical infrastructure. His program coordinates cyber preparedness, risk mitigation and incident response, and provides cyber security resources, including assessments, to the nation's sixteen critical infrastructure sectors and state, local, tribal, and territorial government entities.

CRISIS SCENARIO ROUNDTABLE EXERCISE

One of the best ways to prepare for a cyber security incident is to run a cyber incident scenario. We've assembled an expert team and selected two scenarios to demonstrate how you are your team might act in response to a cyber incident. These hands-on cyber exercises will help you improve your incident response plans by clearly identifying roles and responsibilities, clarify decision-making responsibilities, ensure a strong understanding of protocols and requirements, and build the capacity to successfully respond to and recover from a significant cyber event.

SELECTING A CYBER VENDOR

Jack Schroeder, Aureon

As cyberattacks and threats continue to be on the rise and in news headlines there's no better time than now to assess your strategy for selecting and qualifying the right cyber vendors. This session will provide tips and insights to help you navigate through the vendor selection process when considering cloud-based applications or other IT services that could impact your data security efforts.

NETWORK SECURITY

Mykola Konrad, Ribbon Communications

Cyberattacks on communications infrastructure- specifically DDoS, TDoS and toll fraud on unified communications – both on enterprise and service provider networks. The types of attacks, the affects of the attack and how to prevent or identify.

CYBER INSURANCE FOR YOUR BUSINESS CHOOSE WISLEY

Mark Densmore, Densmore Insurance

Every business has a weakness. What is yours? We will dive deeper into those weaknesses to help focus on the pandemic-like cyber threats that are impacting our business world with more intensity than every before. We will answer the following questions: Where will my business be most impacted by a loss? What does NIST say are the 5 most important guidelines we must follow? What role does the FTC play in your business? What are the real and most common costs from a cyber event? Do I need insurance and what is the difference between a 1st, 2nd and 3rd party policies? Where do I turn when I have a loss without insurance or my policy denies part or all of my claim?

GAINING DEEPER VISIBILITY INTO YOUR BUSINESS WITH SIEM

Steve Healey, Pratum

Security information and event management (SIEM) provides visibility into the never- ending flow of data through your business. This presentation provides an overview of SIEM and the ways SIEM integrates into an environment to assist with compliance, multi-factor authentication, mobile device management, and advanced persistent threat identification. You will learn ways to achieve a deeper understanding of your business through proper device configuration and tuning. And, we will discuss how SIEM can play a key role in breach investigations and forensic analysis.

DEVELOPING AND CONDUCTING A TABLE TOP EXERCISE

Vicky McKim, Aureon

Nearly two-thirds of businesses do not have an emergency plan in place for responding to disasters such as hurricanes, floods, or cyberattacks according to an Ad Council survey. One such way to help your business be prepared is to conduct table top exercises. Join Vicky McKim, Aureon's Manager of Enterprise Business Continuity, as she covers:

- The different types of exercises for crisis planning and their value.
- The types of preparation you want to make for each exercise.
- How to track and monitor findings for resolution in your plans.
- Incorporating exercises into your risk management and business continuity program.

THE 2018 PHISHING TRIP

Scott Kaylor, NISC

Many businesses and people hide behind the illusion that these cyber criminals are becoming more sophisticated with time and creating exploits never seen before by man. However, sophisticated attacks are only used if the crime is not one of the 76% of breaches that were resulted by someone's lost or stolen credentials (Traina, 2016). This belief provides the perfect smoke screen for cyber criminals to keep their true exploit under wraps. By the public misdiagnosing the true weakest link in a business' security infrastructure, cyber criminals have free reign to keep leveraging the vulnerability of a business' culture for future attacks. Without the culture being corrected, the people within the company change, but the weakness does not. The goal of our 2018 Phishing Trip is to give participants the knowledge they need to better educate their employees about password security and phishing awareness. To achieve this goal, we will discuss the inner workings of a password from its creation to the storage in a company's database. By showing my password on the big screen, I aim to expose the password sharing taboo that is plaguing the world of IT. We will dissect emails to determine what is real, and identify key factors within an email that can blow the door

off the hinges of even the finest of "cyber wizardry". All of this information is pointless if we cannot relate it back to employees in the work place. We will end our trip with industry proven insight into implementing a positive security awareness culture within a business. At the end of the day, when the clock strikes 5:00 pm, a business is only as secure as its most vulnerable employee. This is not your average family fishing trip. Packed with passwords, emails, hacking attempts, and one pretty pony... this will be one phishing trip you will not want to miss!

PASSWORDS, PASSWORDS, AND MORE PASSWORDS!

Ryan Pieken, Oxen Technology

We all know authentication is important, so everything has a password. How do we keep track of all these passwords and keep them secure at the same time. In this session we will learn about how to manage passwords and advancements in authentication, like 2-factor authentication (2FA). Having a plan and policy for identity management are crucial to being able to secure your business from cybersecurity breaches. Come to learn how your business can improve its security posture through good password management practices.

BRING A GUEST

ICA Members
BUY ONE
GET ONE
1/2 OFF
your registration fee

Because cyber threats affect companies big and small we want to collaborate with our neighbors and introduce them to the companies we're working with for cyber insurance solutions, crisis management, and employee training. We encourage you to invite your clients and community partners to attend the conference. ICA members will receive a buy one get one 1/2 off your registration fee for the conference. You may take advantage of the pricing for both employees and your customers.

AGENDA

2018 ALL-STAR SPONSORS

TUESDAY, APRIL 24TH

- 12:30 PM Registration
- 1:15 PM Department of Homeland Security Cyber Resources Overview
Geoffrey Jenista, Department of Homeland Security
- 2:15 PM Break
- 2:30 PM Crisis Scenario Demonstration
- 3:00 PM Cyber Crisis Roundtable Exercises
- 4:30 PM Roundtable Reporting
- 5:15 PM Networking Reception
- 6:30 PM Dinner—on your own

WEDNESDAY, APRIL 25TH

- 8:00 AM Breakfast/Registration
- 8:45 AM Selecting a Cyber Vendor
Jack Schroeder, Aureon
- 9:45 AM **Concurrent Sessions**
- Cyber Insurance for Your Business Choose Wisely
Mark Densmore, Densmore Insurance
 - Network Security
Mykola Konrad, Ribbon Communications
 - The 2018 Phishing Trip
Scott Kaylor, NISC
- 10:45 AM **Concurrent Sessions**
- Gaining Deeper Visibility into Your Business with SIEM
Steve Healey, Pratum
 - Developing and Conducting a Table Top Exercise
Vicky McKim, Aureon
 - Passwords, Passwords and More Passwords!
Ryan Pieken, Oxen Technology
- 11:45 AM Conclusion—Lunch with Sponsors
- 1:00 PM End of Day

AUREONTM

BKD^{LLP}
CPAs & Advisors

FINLEY
ENGINEERING

HunTel
Engineering

ITCI



CYBERCON III SPONSORS

densmore
INSURANCE STRATEGIES, INC.

gmvw
CONSULTING

ribbon

TORUSTM
TECHNOLOGIES

csb
community state bank

Hotel Reservations: ICA has a block of rooms at Prairie Meadows at the rate of \$124 + tax per night. Call (800) 325-9015 or (515) 957-3000 by April 3, 2018 to reserve your room. Be sure to ask for the ICA rate.