CYBERCON VIII
CONFERENCE GUIDE

MAY 17-18, 2023 | WEST DES MOINES SHERATON

REGISTRATION DETAILS

REGISTER ONLINE: WWW.IACOMMUNICATIONSALL.ORG

Online registration allows the option to be invoiced or to pay online with a credit card.

COST:

- ICA Member: $265
- Non-Member: $365
- Student: $35

REGISTRATION CUT-OFF

Attendees: The cut-off to register as an attendee is **Monday, May 8th.** This provides us with a lead time for the completion of outsourced name badge printing, registration materials, and counts. Anyone registered after **May 8th** will receive a printed badge onsite and **an additional $40** will be added to the registration fees listed above.

CANCELLATION POLICY:

In the event that you need to cancel your attendee registration, the refund schedule will be enforced with the following dates listed below from the date of the cancellation request. All cancellations must be made via e-mail to Brittany@iacommunicationsall.com. Substitutions for conference attendees or exhibitor attendees will be accepted.

No refunds will be issued for Sponsorships.

- April 24, 2023 (and earlier) – 100% Refund
- April 25 - May 8, 2023 - 50% Refund
- May 9, 2023 (and after) - No Refunds Issued

ACCOMMODATIONS

ICA has a block of rooms at the Sheraton at a rate of $129 per night, plus tax. The room rate includes parking. Use this **reservation link** or call 515-223-1800 to reserve your room. The deadline to receive the room block rate is **April 25, 2023.**

CONSENT TO USE PHOTOGRAPHIC IMAGES:

Registration and attendance at, or participation in, ICA meetings and other activities constitutes an agreement by the registrant to ICA's use and distribution (both now and in the future) of the registrant or attendee's image or voice in photographs, video, electronic reproductions and audio of such.

2023 SPONSORS

All-Star SPONSORS

Diamond ALL-STARS

AUREON

FORVIS

Gold ALL-STARS

HunTel Engineering

Adtran

Calix

DENTONS

DAVIS BROWN

OlsenThielen CPAS AND ADVISORS

Silver ALL-STARS

FINLEY

Oak Hill Consulting, Inc.

ITCI

UHY Audit. Advisory. Tax. Consulting.

CNE

WEDNESDAY, MAY 17TH

12:30 - 1:00 PM | REGISTRATION AND VISIT SPONSOR TABLES

1:00 - 1:45 PM | OPENING GENERAL SESSION

Risk, Resilience and Purpose in Leadership
Colonel Todd "Riddler" Riddle
Colonel Todd "Riddler" Riddle is a combat decorated fighter pilot, former Air Force squadron commander, parachutist with the famous 82d Airborne, and former youth pastor. In addition to being a senior military leader, "Riddler" also served as a Secretary of Defense Executive Fellow with a Fortune 500 mobile technology company, learning to apply the agility of C-Suite decision making and innovation to the Department of Defense. Drawing from his 5 combat deployments and countless global exercises, Colonel Riddle speaks and consults nationally on organizational excellence, risk, resilience, purpose and leadership. Colonel Riddle and his family live near Washington D.C., while his current military duty at the Pentagon supports DoD efforts for software derived solutions to cryptological modernization.

1:50 - 2:40 PM | GENERAL SESSION

Cyber Threat Landscape, Cybersecurity and Infrastructure Security Agency (CISA)
Jim Hoflen, US Department of Homeland Security (DHS) / Cybersecurity & Infrastructure Security (CISA)
During Jim's presentation he will provide an introduction to the Cybersecurity and infrastructure on the Security Agency along with an overview of the current Cyber Threat Landscape seen at CISA. Jim will provide recommendations from CISA to protect your critical infrastructure along with at the State level, local, tribal and territorial (SLTT) governments.

2:40 – 3:05 PM | BREAK WITH SPONSORS

3:05 – 4:30 PM BREAKOUT - TECHNICAL TRACK

Password Hygiene and Privileged Access Management (PAM)
Dawson Medin, Google/Mandiant
Organizations of all sizes and types require staff, staff require accounts, and accounts require passwords, which are meant to keep the accounts safe. On top of that, proper organizational security requires tiered groups of users such as guests, vendors, standard employees, help desk employees, C-Suite employees, IT/Security employees, break glass full admin accounts, service accounts, and more. With all those moving pieces, if passwords and privileged access management are not done properly from the start, it is difficult to be confident in the organization's security posture. This presentation will discuss these two topics from the perspective of an attacker, and what defenders should be considering when incorporating technical controls into their organization's network. This talk will be for both technical and non-technical individuals, and hopefully should create a few laughs along the way. **All names, organizations, and specifics, will be fictitious, non-revealing names for privacy purposes.**

3:05 – 3:40 PM BREAKOUT - NON-TECHNICAL TRACK

Executive Responsibilities in a Cyberthreat World
James Taylor, Vantage Point Solutions
Cybersecurity is critically important and carries grave consequences if disregarded or done improperly. For this reason, many organizations find cybersecurity intimidating. Even so, cybersecurity carries too much weight to justify guesswork; a strategic approach is necessary. In this presentation, Vantage Point Solutions will discuss cybersecurity strategy and many crucial security practices, as well as highlight the unique responsibilities of executive leadership in building and maintaining an effective cybersecurity program.

3:45 – 4:30 PM BREAKOUT - NON-TECHNICAL TRACK

Cyber Insurance "How to Utilize to Effectively Mitigate an Exposure?"
Luke Nelson, UHY Consulting
What does Cyber Insurance typically cover and not cover? What are the current pricing trends and what does the future hold? What are the challenges of filing claims and the process to collect payments? What else can you do to supplement Cyber insurance coverage? All of these questions affect your business and will be covered during this presentation.

4:30 – 5:30 PM | NETWORKING RECEPTION WITH SPONSORS

SPONSORED BY 大成DENTONS DAVIS BROWN

THURSDAY, MAY 18TH

7:30 - 8:15 AM | BREAKFAST SESSION

Cybersecurity for BEAD & Other Funding
Vantage Point Solutions
BEAD and other funding programs will begin requiring a cybersecurity plan. What do providers need to know? Vantage Point answers. This session will outline who the players are, from the White House, CISA, NIST to individual providers; what components are required as part of the plan; anticipated timelines on plan development and implementation; and up-to-the-minute information on other elements as they develop. Lastly, we'll also break down how individual broadband operators can realistically approach compliance with these plans, including cost and workforce considerations.

8:15 - 8:30 AM | COFFEE REFRESH WITH SPONSORS

8:30 - 9:15 AM | OPENING GENERAL SESSION

Update on Federal Cybersecurity Requirements
Jill Canfield, NTCA - the Rural Broadband Association
Congress and various federal agencies are paying close attention to the cybersecurity and resiliency of critical infrastructure, including telecommunications and broadband. This session will examine the cybersecurity laws and regulations telecom companies need to be aware of, including those attached to federal funding and grant programs.

9:20 - 10:00 AM BREAKOUT - TECHNICAL TRACK

Get These MFA Snakes Off This MFA Plane! Bypassing Multi-factor Authentication (MFA)
Brandon Potter, ProCircular, Inc.
Hackers have found multiple methods to bypass Multi-factor Authentication (MFA). While many organizations have enabled MFA across the enterprise, new risks arise every day. It's clear that pairing a user's password with a second factor of identification reduces the employee's and company's overall risk. However, incident response investigations from the past six months indicate that cybercriminals are combining older tactics and newer techniques to bypass common MFA implementations and achieve unauthorized access. Malicious hackers in the wild have designed and run specialized attacks to bypass an MFA-enabled account, navigate the network as a trusted entity, and exfiltrate data undetected. Methods such as OTP, fingerprint, push technologies, and hardware tokens all merit review. Join Brandon Potter, CTO at ProCircular, as he demonstrates the three most common MFA bypass techniques, breaks down the risks and defenses, and provides a punch list of quick wins to implement for immediate protection.

9:20 - 10:00 AM BREAKOUT - NON-TECHNICAL TRACK

Defending Against Ransomware With A Layered Security Approach
Russ Ciezki, Heartland Business Systems
In this presentation, Heartland Business Systems IR Practice Manager, Russ Ciezki, will discuss the early stages of preventing ransomware including identifying the assets and data that are most vulnerable to attack, how to train your employees to recognize malicious social engineering tactics, staying up to date on updates and patches, and having a system in place to restore data in case of an attack. Additionally, Russ will cover what to do if you do become a victim of ransomware and the importance of having a plan in place to (prevent and) recover from a ransomware attack including backups, protection tools, and IR. Attendees will leave with knowledge of how to begin developing a security program to prevent and respond to ransomware at every level of the attack.

10:00 - 10:15 AM | BREAK WITH SPONSORS

10:15 - 10:45 AM BREAKOUT - TECHNICAL TRACK

Microsoft 365 – It Works! Now What??
Ryan Pieken, Oxen Technology
Microsoft 365 is a powerful platform, and an ever-evolving platform. With powerful tools, and constant changes, security is a moving target. Come to this session to learn about the latest best practices to secure your organizations Microsoft platform!

CONTINUED ON NEXT PAGE ▶

THURSDAY, MAY 18TH

10:50 - 11:45 AM BREAKOUT - TECHNICAL TRACK

Zero Trust Starts Here - The Prevention Layer Most Security Stacks are Missing
Corey Munson, PC Matic
The Department of Homeland Security endorses allowlisting as one of the most important security technologies that an organization can and should implement. So why do so few organizations implement application control/allowlisting? How does application control/allowlisting function as the foundation of any zero trust based security strategy? How are organizations addressing application control/allowlisting requirements - as specified in new Federal and State regulations & cybersecurity insurance underwriting standards?

10:15 - 11:00 AM BREAKOUT - NON-TECHNICAL

Navigating Cyber Threats and Uncertainty: An Example from a Rural Broadband IS
Curtis Thornberry, Panora Fiber
How well do we know our corporate and last mile networks? Are we confident that our company's assets are protected? Is our client and employee information secure? Are we vulnerable to attack and from where? These were questions we asked ourselves at Panora Fiber in the beginning of 2022. In an uncertain world, we were looking for some certainty across a rapidly changing threat landscape. While we felt confident about the things we were doing to identify, respond, and mitigate threats; we were much less certain about what we didn't know. To address this issue, we solicited quotes from several cyber security firms with the goal of conducting penetration tests and vulnerability scans on our networks. We then visited with each to discuss our ultimate goals. This talk will focus on how we worked to become more knowledgeable, how we navigated the testing process, what we learned, and how we are moving forward now that we know more than what we knew before.

11:00 - 11:45 AM BREAKOUT - NON-TECHNICAL

Understanding How Social Engineering is Crafted
Jordan Neal, Aureon Technology
This is a high level explaination (with some examples) of what social engineering is and how a bad actor performs reconnaissance to craft a seemingly complex attack. I'll cover where bad actors get the information they need to convince you or a team member to complete a desired action.

11:45 AM - 12:15 PM | LUNCH BUFFET

12:15 - 1:00 PM | CLOSING GENERAL SESSION

Securing the State of Iowa
Shane Dwyer, OCIO
Hear from Shane Dwyer, State of Iowa Chief Information Security Officer at OCIO to learn how to protect the users of the state of Iowa. OCIO offers an outreach program to help protect the state from attack. Learn about the iniatives OCIO is implementing to secure the state.

REGISTER ONLINE: WWW.IACOMMUNICATIONSALL.ORG