

Cyber security is everyone's business.

Join Leading Experts on Cyber Security



Conference Guide

Monday, Sept. 29, 2025

8 a.m.-4 p.m.

This conference is a partnership between
the state of Nebraska and Southeast Community College

NEBRASKA
OFFICE OF THE CIO
Information Security Office

S Southeast
COMMUNITY COLLEGE

southeast.edu/ncsc

In today's world, we rely on technology and the Internet for a variety of transactions, communication and information – at home, in school and at the workplace. While we are familiar with the myriad of conveniences provided through Internet use, it is difficult to stay abreast of all the changes and the potential risks presented by the Internet. We are all “virtual neighbors” in cyberspace, and what we do, or don't do, can affect many others.

The Nebraska Cyber Security Conference will assist in raising our awareness of cyber security and help in protecting all of us in cyberspace. If we do our part individually, collectively we can have a tremendous positive impact on our state's cyber security.

This will be valuable time learning from skilled industry experts. The day will be filled with a variety of breakout sessions that will encompass different areas of information security and technology.

For more information, visit southeast.edu/ncsc.

Wi-Fi Login Information

Network: NUGuest

Username: September

Password: Innovate2025!

Keynote Speaker: Dan Lohrmann

Presidio®

Daniel J. Lohrmann is an internationally recognized cybersecurity leader, technologist, keynote speaker and author.

During his distinguished career, he has served global organizations in the public and private sectors in a variety of executive leadership roles. He has received numerous national awards, including CSO of the Year from SC Magazine, Public Official of the Year from Governing Magazine and Computerworld Premier 100 IT Leader.

Lohrmann is the Field CISO for the Public Sector at Presidio, a global digital services and solutions provider accelerating business transformation through secured technology modernization. He leads cybersecurity advisory services for public-sector clients, working with global CxOs and partners to provide best practices and solutions.

He previously served as CSO and Chief Strategist for Security Mentor, Inc., a security awareness and training company, and led Michigan government's cybersecurity and technology infrastructure teams from 2002 to 2014 in enterprise-wide CSO, CTO and CISO roles.

Lohrmann has advised senior leaders at the White House, the National Governors Association, the National Association of State CIOs, the U.S. Department of Homeland Security, federal, state and local government agencies, Fortune 500 companies, small businesses and nonprofit institutions.

He has more than 30 years of experience in the computer industry, beginning his career with the National Security Agency. He worked in England as a senior network engineer for Lockheed Martin (formerly Loral Aerospace) and as a technical director for ManTech International at a U.S./U.K. military facility.

Lohrmann is the co-author of *Cyber Mayday and the Day After: A Leader's Guide to Preparing, Managing, and Recovering from Inevitable Business Disruptions* (Wiley, 2021) with Australian cybersecurity expert Shamane Tan. He is also the author of *Virtual Integrity: Faithfully Navigating the Brave New Web* and *BYOD For You: The Guide to Bring Your Own Device to Work*.

He has delivered keynote addresses at security and technology conferences worldwide, from South Africa to Dubai and from Washington, D.C., to Moscow.

Lohrmann holds a master's degree in computer science from Johns Hopkins University in Baltimore and a bachelor's degree in computer science from Valparaiso University in Indiana. He is also a senior fellow at the Center for Digital Government.



Why Do Security Pros (and Team) Fail? And What Can You Do About It?

The standard security checklist is not enough. Uncover seven surprising problems sabotaging your program and learn tough solutions that will work for your team. Take a dive into the people side of cybersecurity.

7:30 a.m.	Check-in / Breakfast (provided)		Track	Room
8:15 a.m.	Opening Remarks from State of Nebraska Officials and Southeast Community College			Second Floor Banquet Hall
8:45 a.m.	Break			
9 p.m.	Keynote: Dan Lohrmann — Why Do Security Pros (and Team) Fail? And What Can You Do About It?			Auditorium
10 a.m.	Break			
10:15 a.m.	Breakout Sessions	Nelnet Cybersecurity: An Overview of Our Security Journey and What's Next, Ryan Regnier	   	Auditorium
		Over 9,000 Breaches: Powering Up Cybersecurity, Ross Coudeyras	   	Room A
		Insider Threats Aren't New. But Our Defenses Should Be., Mike Rider	  	Room B
11 a.m.	Break			
11:15 a.m.	Breakout Sessions	CISO Panel Discussion, Facilitated by Dan Lohrmann	 	Auditorium
		Command, Control, Automate: The Future of Endpoint Management, Ken Heller	 	Room B
Noon	Lunch (provided)			
1:15 p.m.	Breakout Sessions	The State of State Security: Cyber Threats, Resilience and Readiness, OCIO	 	Auditorium
		Leveling UP Vulnerability Disclosure: A Gamified Approach at the University of Nebraska, Phil Redfern & Raul Barrerras	 	Room A
2 p.m.	Break			
2:15 p.m.	Breakout Sessions	Shani the Zebra Knows More About Cybersecurity Than You, Karla Carter	   	Auditorium
		TTX: How Not To Crisis Your Crisis, Bruce Wray	 	Room A
3 p.m.	Break			
3:15 p.m.	Breakout Sessions	Cybersecurity in Higher Ed: CMMC Challenges and Smart Strategies, Judi Seguy		Auditorium
		Beyond the Firewall: Evolving Cyber Skills for the Age of AI and Automation, Ron Woerner	  	Room B



Education



End User



Management



Technical



Beyond the Firewall: Evolving Cyber Skills for the Age of AI and Automation

Ron Woerner, Forrester

As artificial intelligence, automation, and increasingly sophisticated threats reshape the cybersecurity landscape, the skills demanded of cyber professionals are evolving at an unprecedented pace. This interactive session explores the shift from traditional technical expertise to a broader mix of strategic thinking, adaptive learning, and interdisciplinary collaboration.

You'll examine the emerging competencies defining today's cybersecurity workforce—AI literacy, threat modeling, and risk communication—and how they complement core technical skills. The discussion will highlight ways to align cybersecurity initiatives with business goals, make informed decisions under uncertainty, and effectively engage diverse stakeholders.

Through practical examples and frameworks, attendees will learn how to build strategies for continuous upskilling at both the personal and organizational level. The session will also emphasize the value of mentorship, intentional development, and community involvement in fostering resilience. Whether you're a seasoned practitioner or just starting out, you'll gain insights to help you thrive in the future of cyber defense.



FORRESTER®

Ron Woerner is a nationally recognized cybersecurity leader, educator, and speaker with more than 20 years of experience in IT and security. He currently serves as a Senior Consultant at Forrester Research and as faculty at Bellevue University—an NSA Center of Academic Excellence—where he has helped shape cybersecurity programs and mentor the next generation of professionals.

Ron's TEDx talk, "Hackers Wanted," reframed hacking as a form of creative problem-solving, demonstrating his unique ability to connect technical expertise with human insight. He has presented at the RSA Conference 25 times and was named the Air Force Association's CyberPatriot Mentor of the Year.

Known for blending strategic vision with teaching excellence, Ron is deeply passionate about building people—not just systems. His commitment to empowering others makes him uniquely qualified to bridge technical and leadership skills in today's evolving cybersecurity landscape.



CISO Panel Discussion

Facilitated by Dan Lohrmann

Join us for an engaging panel featuring Chief Information Security Officers (CISOs) from leading regional organizations. This interactive session brings together top security executives to share their experiences, challenges, and strategies for navigating today's complex cybersecurity landscape.

Panelists will explore critical topics such as threat intelligence, incident response, regulatory compliance, zero trust architecture, and the evolving responsibilities of the CISO. Attendees will gain firsthand insight into how local leaders are addressing global threats and regional security concerns—and leave with actionable strategies to strengthen their own security posture.

Whether you're a seasoned professional or new to the field, this panel provides valuable perspectives on leadership, resilience, and the future of cybersecurity from those on the front lines.



Command, Control, Automate: The Future of Endpoint Management

Ken Heller, Tanium

In an era when cyber threats evolve faster than traditional tools can respond, organizations need real-time visibility and control across every endpoint. This session explores how Tanium's autonomous endpoint management platform unifies IT operations and security to deliver instant insights, rapid response and operational resilience.



Ken Heller is a seasoned solution engineering leader with more than 20 years of experience shaping technical strategy and driving customer success across enterprise and public sector markets. He currently leads a national team of solution architects dedicated to delivering secure, scalable and mission-critical IT solutions.

Known for combining deep technical expertise with a consultative approach, Ken helps state and federal agencies modernize infrastructure, accelerate digital transformation, and implement autonomous endpoint management programs. His leadership focuses on reducing risk, optimizing operations, and ultimately creating better outcomes for the communities these agencies serve.



Cybersecurity in Higher Ed: CMMC Challenges and Smart Strategies

Judi Seguy, CampusGuard

Higher education institutions face unique cybersecurity challenges, especially as they navigate the evolving requirements of the Cybersecurity Maturity Model Certification. This presentation explores the intersection of CMMC compliance, the complexities of institutional assessments and the implementation of effective cybersecurity practices in academic environments.

We'll begin by examining the hurdles higher education institutions encounter during assessments, including decentralized IT environments, diverse data types and limited resources. Then we'll review the core components of CMMC and where the challenges are specific to colleges and universities.

The session will highlight real-world examples and lessons learned, offering practical strategies for aligning cybersecurity efforts with CMMC requirements. Attendees will gain insights into building a culture of security, streamlining assessment processes and leveraging existing frameworks to reduce risk and improve compliance.

Whether you're just beginning your CMMC journey or looking to refine your cybersecurity posture, this presentation will provide actionable guidance tailored to the higher education landscape.



Judi Seguy is a seasoned operations executive with more than 20 years of leadership experience in strategic planning, process optimization and organizational transformation. As Vice President of Operations, she drives cross-functional initiatives that improve efficiency, elevate performance and align operational goals with enterprise strategy.

Throughout her career across diverse industries, Judi has led large-scale change management efforts, implemented enterprise systems and built cultures of continuous improvement. She is especially passionate about cybersecurity, compliance and digital transformation in regulated environments, including higher education and government contracting.

Known for her collaborative leadership and sharp analytical insight, Judi is a trusted advisor to executive teams and a mentor to emerging leaders. Her approach blends a deep understanding of operational frameworks with a commitment to innovation, stakeholder engagement and integrity.



Insider Threats Aren't New. But Our Defenses Should Be.

Mike Rider, DTEX

In today's dynamic digital environment, the perimeter is gone — but the insider risk remains. As organizations accelerate adoption of AI tools and hybrid work continues to redefine where and how people operate, traditional methods of monitoring and mitigating insider threats are proving inadequate. Legacy user activity monitoring tools, while well-intentioned, are reactive, intrusive and often blind to the early indicators of risky behavior.

This session explores a modern approach to insider risk — one that prioritizes context, intent and proactive mitigation over surveillance. Drawing on lessons learned from engagements across federal and commercial sectors, we'll examine the behavioral patterns and digital exhaust that precede insider incidents — and how organizations can use this intelligence to shift left: detecting risk before it escalates to a threat.



Mike Rider is a senior counter-insider threat engineer at DTEX Systems with 24 years of experience in cybersecurity, 12 of which have been dedicated to U.S. government insider threat programs. He also completed a 20-year U.S. Navy career as a cryptologic warfare officer. Some of his noteworthy Department of Defense roles include positions at the White House Communications Agency, the National Security Agency, U.S. Strategic Command and Joint Special Operations Command, as well as technical roles at leading security vendors such as Forcepoint, Tanium and Menlo Security.



Leveling UP Vulnerability Disclosure: A Gamified Approach at the University of Nebraska

Phil Redfern & Raul Barreras, University of Nebraska

Discover how the University of Nebraska has leveled up its Vulnerability Disclosure Program through gamification. This presentation will highlight the collaborative efforts between the university and independent security researchers to strengthen its security posture and recognize the contributions of experienced researchers. Attendees will gain insights into NU's innovative program model, built on the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency template, and learn effective strategies for engaging in remediation.



Phil Redfern is the director of security engineering at the University of Nebraska. Throughout his career, Redfern has led various enterprise IT initiatives and projects, successfully integrating risk-based cybersecurity across the university system. Highlights include a unified security model for edge networks, security baselines for endpoints, and the implementation of updated IT security policies and standards. He received his Bachelor of Fine Arts from the University of Nebraska-Lincoln and his Master of Science from the University of Nebraska at Omaha.



Raul Barreras is an information security professional with more than 20 years of experience in systems administration, development, teaching, information security leadership and hands-on penetration testing. In recent years, as cloud and application security manager at the University of Nebraska, he has focused on helping teams build secure and resilient software by promoting secure development practices and leveraging his broad technical and leadership background. Passionate about building communities of security-aware professionals, Barreras mentors developers and works to turn secure development from a checkbox into a habit.



Nelnet Cybersecurity: An Overview of Our Security Journey and What's Next

Ryan Regnier, Nelnet

We'll begin with an overview of Nelnet's cybersecurity team structure and how we partner with each business unit. Using specific examples and commentary, we'll explain how the teams perform their work. We'll also cover how AI is transforming our daily operations and where the field is heading in the coming years.



Ryan Regnier is the director of cybersecurity at Nelnet, where he leads the Protective Operations division. He oversees both defensive and offensive cybersecurity strategies, ensuring rapid threat detection and response across the organization's diverse technology landscape.



Over 9,000 Breaches: Powering Up Cybersecurity

Ross Coudeyras, Remesh

Join us for an insightful exploration of the 2025 Verizon Data Breach Investigations Report (DBIR). This session will clarify the crucial distinctions between breaches and incidents—and why this difference matters more than ever in today's digital landscape.

Together, we'll navigate the evolving web of cybersecurity threats, highlighting how breaches in particular compromise the integrity, confidentiality, and availability of critical systems. Drawing from real-world examples and the DBIR's comprehensive analysis, attendees will gain a clear understanding of the tactics cyber adversaries are using and the growing need for constant vigilance.

We'll also examine the timeline of incidents included in the report (November 2023–October 2024) to uncover key patterns, trends, and emerging threats. By exploring how the data is gathered and analyzed, participants will gain a nuanced perspective on the challenges of cybersecurity research and reporting.

Most importantly, this session provides practical guidance on where developers, engineers, and security professionals should focus their efforts to strengthen defenses, mitigate risks, and respond effectively to incidents.

By learning from the more than 10,000 breaches recorded in 2023 and embracing a proactive mindset, we can build resilience and confidence in facing tomorrow's threats.



 remesh

Ross Coudeyras brings more than 18 years of experience in software and technology and is a recognized authority in cybersecurity and data privacy. He currently leads Security and Compliance at Remesh, where he also serves as Data Protection Officer, ensuring the organization remains resilient against evolving cyber threats while meeting complex regulatory requirements.

Known for his practical approach, Ross bridges the gap between technical security measures and compliance demands. In addition to his industry role, he serves as an adjunct instructor at Doane University, where he prepares the next generation of cybersecurity professionals through hands-on, real-world learning.

Outside of work, Ross is a lifelong fan of Dune—reminding himself (and his students) that “fear is the mind-killer.”



Shani the Zebra Knows More About Cybersecurity Than You

Karla Carter, Bellevue University

What can a foal, a crocodile and a dusty river crossing teach us about digital risk management? More than most security frameworks, it turns out. This session leverages one of nature's most compelling cybersecurity metaphors — the African migration — to reframe enterprise risk management through the lens of survival. Following Shani the zebra and her vulnerable newborn through a perilous journey, we'll examine how predators exploit every transition point, mirroring the attack vectors that compromise digital ecosystems. Drawing from behavioral ecology and threat intelligence, this presentation maps the NIST Risk Management Framework to migration survival patterns: asset management as herd dynamics, vulnerability assessment as environmental scanning, incident response as predator evasion, and legacy system integration through the lens of warthogs — ugly but resilient. Through this unconventional framework, attendees will develop practical strategies for risk visualization, stakeholder communication and security program optimization. The session includes actionable deliverables: a field guide for mapping organizational “predator patterns,” threat classification cards and assessment templates designed for immediate implementation. Participants will learn to apply biological risk models to cybersecurity program design, develop enhanced risk communication strategies using natural metaphors, and create visual frameworks for executive reporting that actually resonate. Come for the metaphor. Stay for the methodology. Leave with tools that work in both the Serengeti and the SOC.



Karla Carter is an Associate Professor of Cybersecurity in the College of Science and Technology at Bellevue University, in Bellevue, NE. Drawing on degrees in psychology, history and cybersecurity, and more years than she should admit to of information technology experience, she teaches undergraduate and graduate courses in cybersecurity operations, social engineering, human factors, security awareness, white-collar crime, information warfare, and technology ethics. Additionally, she serves on the IEEE Nebraska Section Executive Committee and ACM Committee on Professional Ethics. Curious, intense and irreverent, Carter lives by the question, “what if...?” and has a low tolerance for the phrase “because that’s the way we’ve always done it.” Ask her about her growing (and glowing!) uranium glass collection!



The State of State Security: Cyber Threats, Resilience, and Readiness

As state and local governments face mounting pressure from increasingly sophisticated threats, understanding the true state of cybersecurity in the public sector has never been more critical.

This timely presentation will examine the evolving threat landscape targeting state governments. We'll explore recent high-profile incidents, common vulnerabilities across public infrastructures, funding and staffing challenges, and how agencies are adapting their strategies to stay ahead.

Attendees will gain a comprehensive overview of state-level resilience efforts—from legislative actions to incident response frameworks—and discover how public-private collaboration is shaping the future of state security.

Whether you work in government, support the public sector, or simply want to understand how the security of civic systems impacts broader national resilience, this session is not to be missed.



TTX: How Not To Crisis Your Crisis

Bruce Wray, Wray Law TCP

The truism “When Not If” has these corollary: crises will happen, crises are unavoidable, and crises are part of business. An organization’s preparation and response are all that you can control.

This interactive discussion will focus on Practicing Your Crisis before you Crisis Your Crisis. We will explore how other crisis training approaches preparation and how your organization can adopt and implement Table Top Exercises to avoid common pitfalls that businesses face when the unthinkable, but inevitable, occurs



Bruce thrives where the Law intersects with Technology, Cybersecurity and Privacy. He leverages a Master's in Computer Science focused on Information Assurance, a CISSP, more than a decade working in IT, and now more than a decade providing legal guidance to global corporations, in order to enable organizations to manage their TCP risks.

Bruce operates a boutique legal practice, Wray Law TCP, and is the Director of the Innovation and Entrepreneurship Legal Clinic at Creighton School of Law. He serves on the boards of both NebraskaCERT and ISC2 Omaha/Lincoln Local Chapter, the latter as President.

Bruce is a frequent presenter with local information security organizations, including ISACA, NECERT and ISC2 Omaha/Lincoln Local Chapter, and will be speaking this October at the ISC2 Security Congress 2025 in Nashville.



EDUCATION

10:15 a.m. Session

Nelnet Cybersecurity: An Overview of Our Security Journey and What's Next, *Ryan Regnier*

Over 9,000 Breaches: Powering Up Cybersecurity, *Ross Coudeyras*

Insider Threats Aren't New. But Our Defenses Should Be., *Mike Rider*

2:15 p.m. Session

Shani the Zebra Knows More About Cybersecurity Than You, *Karla Carter*

3:15 p.m. Session

Beyond the Firewall: Evolving Cyber Skills for the Age of AI and Automation, *Ron Woerner*



END USER

10:15 a.m. Session

Nelnet Cybersecurity: An Overview of Our Security Journey and What's Next, *Ryan Regnier*

Over 9,000 Breaches: Powering Up Cybersecurity, *Ross Coudeyras*

2:15 p.m. Session

Shani the Zebra Knows More About Cybersecurity Than You, *Karla Carter*

3:15 p.m. Session

Beyond the Firewall: Evolving Cyber Skills for the Age of AI and Automation, *Ron Woerner*



MANAGEMENT

10:15 a.m. Session

Nelnet Cybersecurity: An Overview of Our Security Journey and What's Next, *Ryan Regnier*

Over 9,000 Breaches: Powering Up Cybersecurity, *Ross Coudeyras*

Insider Threats Aren't New. But Our Defenses Should Be., *Mike Rider*

11:15 a.m. Session

Command, Control, Automate: The Future of Endpoint Management, *Ken Heller*

1:15 p.m. Session

Leveling UP Vulnerability Disclosure: A Gamified Approach at the University of Nebraska, *Phil Redfern & Raul Barrerras*

2:15 p.m. Session

Shani the Zebra Knows More About Cybersecurity Than You, *Karla Carter*

TTX: How Not To Crisis Your Crisis, *Bruce Wray*

3:15 p.m. Session

Cybersecurity in Higher Ed: CMMC Challenges and Smart Strategies, *Judi Seguy*

Beyond the Firewall: Evolving Cyber Skills for the Age of AI and Automation, *Ron Woerner*



TECHNICAL

10:15 a.m. Session

Nelnet Cybersecurity: An Overview of Our Security Journey and What's Next, *Ryan Regnier*

Over 9,000 Breaches: Powering Up Cybersecurity, *Ross Coudeyras*

Insider Threats Aren't New. But Our Defenses Should Be., *Mike Rider*

11:15 a.m. Session

Command, Control, Automate: The Future of Endpoint Management, *Ken Heller*

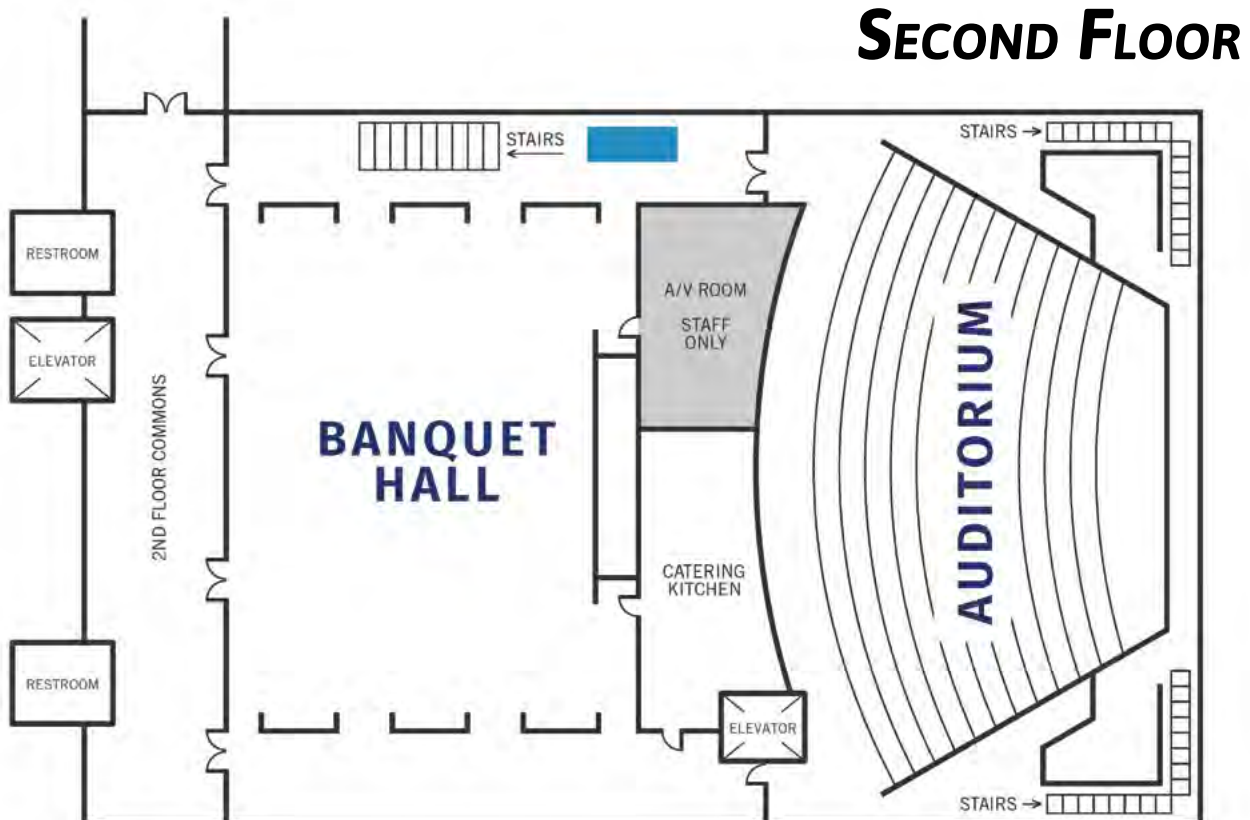
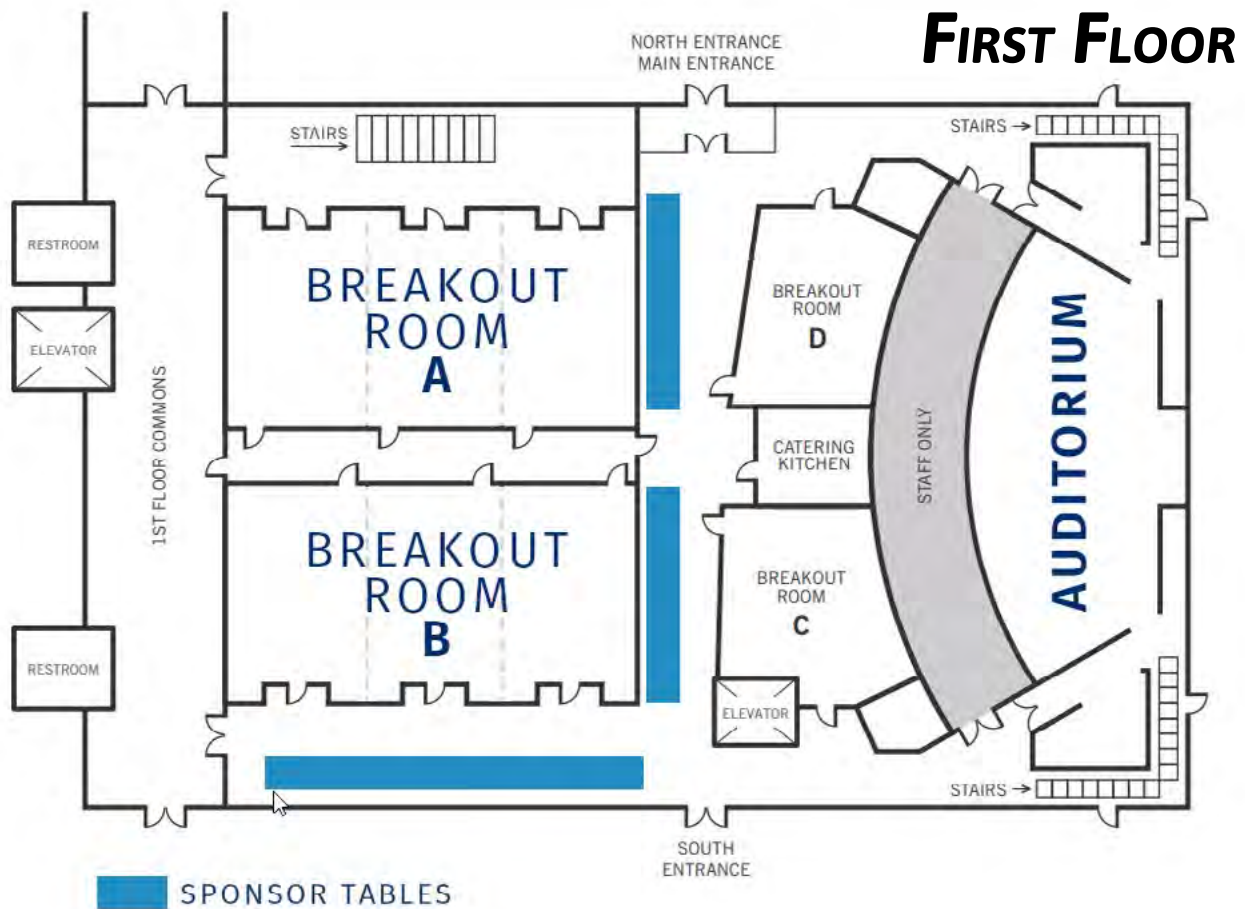
1:15 p.m. Session

Leveling UP Vulnerability Disclosure: A Gamified Approach at the University of Nebraska, *Phil Redfern & Raul Barrerras*

2:15 p.m. Session

Shani the Zebra Knows More About Cybersecurity Than You, *Karla Carter*

TTX: How Not To Crisis Your Crisis, *Bruce Wray*



Continental Breakfast

Breakfast Frittata Casserole

Assorted Danish

Mini & Medium Donuts

Mini Muffins

Mini Bagels & Cream Cheese

Market Fresh Seasonal Fruit

Lunch

Fried Chicken

Penne Rigatte Pomodoro

**Oven Roasted Rosemary
Potatoes**

Chef's Vegetable Mix

Premier Salad

Broccoli & Bacon Pasta Salad

Macaroni

**Sour Dough & Wheat Berry
Rolls Assorted Cookies**

Assorted Pepsi Products

Available All Day

Assorted Pepsi products, Ice Tea, Water, Coffee

**For those who have special dietary requests,
please talk to staff for options.**














Meals are prepared in a shared kitchen.

Catering provided exclusively by: Premier Catering

SPONSORS



Agenda

10:00 a.m.	Breakout Sessions	Cyber Tatanka Panel , Tim Pospisil, Dustin Thorne and Dana Turner	   	Auditorium
		Impact of Open Source Intelligence of Offensive Security and Investigative Practices , Md Rashedul Hasan	   	Room A
		Network Threat Hunting and You! Two-Hour Workshop (Part 1) , John Strand	 	Room B
		When the Whole World is Watching - Enduring Security , Robert Palmer	  	Room D

Additional Breakout Session



When the Whole World is Watching - Enduring Security

Robert Palmer, Mandiant, Now Partner of Google Cloud

Experience Level: Beginner, Intermediate

Robert Palmer is the Director of Mandiant-Google Cloud's "Incident Response and Proactive Services" teams, providing services to state, local government, higher education, and federal agencies. Robert has been with Mandiant for eight years, specializing in Incident Response. Prior to joining the Mandiant team, Robert was provided the opportunity to hold roles specific to incident response, cyber threat hunting and malware reverse engineering. Robert additionally has a background with the 1st Marine Special Operations as a team level combat communicator. Robert's time with Mandiant affords him the opportunity to lead incident response efforts against the most complex and impactful cyber security threats across the globe. Leading a team of dedicated Incident Response consultants, Roberts' team is regularly on the forefront of compromises conducted by advanced, nation-funded threat actor organizations, developing methodologies for detection, investigation, and eradication and facilitating a stronger cyber security posture for his clients.



Education



End User



Management



Technical