CYBER SECURITY SUMMIT
Security solutions through collaboration.™

2022 AGENDA

Public Sector Workshop

October 24, 2022
08:00

Welcome Kickoff / Operational Excellence

John Israel
Interim CISO, State of MN

Jeff Lubick
Regional Manager, CISCO Global Security Option

Welcome Kickoff

Join us for our Public Sector Welcome Kickoff with Interim CISO John Israel!

Operation Excellence

How do you consolidate, maximize your investment, streamline efficiencies in an underemployed space.

October 24, 2022
08:45

What Are The Challenges Most States and Local Government Face Today?

Joe Marshall
Sr. Strategist ICS/Threat Research, CISCO Talos

Lessons learned from defending Ukraine – and why it matters to you.

October 24, 2022
09:15

Enhancing Statewide Cybersecurity Programs - Building Collaboration and Support Networks

John Israel
Interim CISO, State of MN

Cybersecurity is a team sport – and we are all on the same team, yet competition keeps coming into play. Competition for cyber-aware employees, competition for funding, and competition to deflect the bad guys to someone else. Focusing on our collaboration and cooperation are our best defenses to raise the tide and work together to improve our posture and protect our critical resources. This session will look at opportunities to consider for the future as we build the workforce of tomorrow, build better collaboration channels, and engage the resources available to us today.

October 24, 2022
10:00

Strategy Break

October 24, 2022
10:15

Public Sector Cybersecurity: The State of the States, Local Governments, Tribes, and Territories

Emily Sochia
Manager, Maturity Services, Multi-State Information Sharing and Analysis Center (MS-ISAC)

This overview will provide critical observations from this year's Nationwide Cybersecurity Review (NCSR); an anonymous cybersecurity maturity self-assessment completed by thousands of SLTT governments and presented to Congress bi-annually. His presentation will include a brief on the threats and trends currently observed by the MS-ISAC and impacting SLTT governments, providing a summary threat landscape of the community. He will explore what the NCSR data can tell us about our risk reduction priorities considering increasing threats to SLTT, and help the audience consider how we can best leverage the NCSR to communicate those priorities to our law makers.

October 24, 2022
10:45

States Can Save the World. The All in Approach to Cybersecurity.

Shawn Riley
CIO, State of North Dakota

North Dakota is this amazing place that most people haven't been to yet. We have amazing things happening here, especially in the cybersecurity realm, stuff that is not happening anywhere else in America. North Dakota has redefined cyber security at the state government level. From comprehensive education Kindergarten through PHD to comprehensive defense for the executive branch, judicial branch, legislative branch, all K12, all Higher-Ed, all counties and all cities are just the start. Now crowning the first statewide High School Championships in Cyber security and leading a nationwide Join State Security Operations Center that covers over 60,000,000 people, North Dakota is solving the cyber problem defending against cyber-attacks is a round-the-clock job and having partnerships with other states to improves our ability to defend against these threats.

October 24, 2022
12:30

Insights into Vulnerability Management

Neal Dawson
Information Technology Security Manager, State of Minnesota

Nancy Skuta
Lead Information Security Analyst, ITSS, Threat and Vulnerability Management, Minnesota IT Services

The State of Minnesota will delve into its approach where it abandoned a cumbersome reports-based vulnerability ticketing system in favor of a relationships-based model where security analysts meet with responsible teams and start a conversation centered around risk-based actionable information and remediation. Hear how their unique approach to vulnerability management leverages both relationships and technology to yield better results than any previous methods.

October 24, 2022
13:20

CISA Grant Program

Chris Gabbard
Cyber Security Advisor – Region V, Office of Cybersecurity & Communications, Cybersecurity and Infrastructure Security Agency (CISA)

On September 16, 2022, the Department of Homeland Security (DHS) announced a first-of-its-kind cybersecurity grant program specifically for state, local, and territorial (SLT) governments across the country.
Funding from the State and Local Cybersecurity Grant Program (SLCGP) and the Tribal Cybersecurity Grant Program (TCGP) helps eligible entities address cybersecurity risks and threats to information systems owned or operated by—or on behalf of—state, local and territorial (SLTT) governments. Through two distinct Notice of Funding Opportunities (NOFO), SLCGP and TCGP combined will distribute $1 billion over four years to support projects throughout the performance period of up to four years. This session will provide and overview of the Program and how to connect within your state for funding.

October 24, 2022
14:10

Implementing Statewide Cyber Plans - State-level Perspectives

Peter Alsis
SOC Cyber Navigator, Minnesota IT Services

Shane Dwyer
CISO, State of Iowa

John Israel
Interim CISO, State of Minnesota

Shawn Riley
CIO, State of North Dakota

Ashley Podhradsky
VP, Research and Economic Development, Dakota State University

CISA's State and Local Cybersecurity Grant Program (SLCGP) creates new opportunities to fund cyber enhancements for SLTT government organizations nationwide and is delivered at the state level. State CIOs and CISOs are charged with leading efforts to build and implement statewide cybersecurity plans. Hear from multiple state resources directly on their plans to enact this program and build a whole-of-state approach to cybersecurity.

October 24, 2022
15:00

The Rear View Mirror

Chris Buse
SVP, Chief Information Security Officer, Old Republic Title

Since leaving the public sector former State of MN CISO reflects on lessons learned, the value of government buying power, MS-ISAC benefits, and more.

October 24, 2022
15:30

Networking Reception in EXPO

Women in Cyber - Technical Sessions

October 24, 2022
08:30

Welcome by WiCyS MN and Walking in Fire

Gretchen Block
CISO, SVP, United Health Care, Optum

Judy Hatchett
VP, CISO, Surescripts

Firewalking, a tradition that has been occurring for decades to test strength, courage, and faith where people watching become invested in the success of that person risking their health. There is a strong parallel between a firewalker and cyber security, and successful cybersecurity professionals know how to virtually walk in fire. Third-party risk continues to impact organizations. Teams are required to move to a 24/7 response and partner and support each other as we all walk through fire. As these threats continue to impact the world, we must act as firewalkers supporting each other, and do so with our Eyes Wide Open.

October 24, 2022
09:40

Goodbye Elevator Pitch. Hello Career Accelerator

Tissa Richards
Executive Coach, Tissa Richards

Telling Your Cybersecurity Story is critical if you're looking to rise in your career to the C-suite or to the boardroom, and surprisingly, this session recommends you need to stop sharing your elevator pitch and start talking about the value you deliver.

An elevator pitch only tells your audience what you do and how you do it. It ignores the most important pieces like why your work matters, and why YOU and only you can deliver the outcomes that matter most. Even more important: the internalization of your value and truly understanding what matters most if you want to overcome self-doubt and imposter syndrome. This is what is going to get you the compensation package you deserve; the bigger team; the global projects; the board visibility; the promotion and so much more.

Regardless of your level, you will learn how to stop speaking elevator pitch and start speaking business outcomes from cybersecurity tech founder, former CEO, and leadership expert, Tissa Richards. Tissa works with the worlds largest private and public companies and investment management firms, and their C-suite teams, to help them level up their leadership through actionable, pragmatic coaching to experience career- and company-transforming results.

Join Tissa to learn strategies for talking to revenue, brand impact, regulatory requirements, and more. This is just the beginning in communicating your so what with the world and being taken seriously as a key asset to the business.

October 24, 2022
10:30

Navigating Cyber as a Female Leader

Cindi Carter
Global CISO, Check Point Software Technologies, Ltd.

Sarah Engstrom
CISO & VP IT Security, Productivity & Privacy, CHS Inc.

Kristine Livingston
Sr. Manager, Security Operations and Incident Response, Sleep Number

Aimee Martin
Director, Information Security, Compliance and PMO, Vista Outdoor Inc.

Milinda Rambel Stone
Chief Information Security Officer, Bremer Bank

When women see others succeed in a career, they're more likely to choose it; and for women considering a career in cyber security, there's no shortage of inspiration.

Check Point Field CISO Cindi Carter is joined by four female leaders who are admired and respected in the field of cyber security, each sharing their unique journey, and whose contributions continue to help us create a better future.

October 24, 2022
11:30

Women in Cyber Luncheon

Julie Talbot-Hubbard
SVP, GM - Cyber Protection and Identity, Optiv

Nancy Brainerd
Senior Director, Deputy CISO, Medtronic

Lucia Milică
Resident CISO, Proofpoint

Jannell Mohn
CISO, RSM US

Beth Singer
Director of IT Compliance, CHS Inc.

Optiv is proud to be the Title Sponsor of CSS Women in Cyber Luncheon. Join Optiv's Julie Talbot-Hubbard and our panelists comprised of current Optiv partners and clients as we share stories, challenges, opportunities and perspective on how to be resilient in today's cyber business world.

October 24, 2022
12:30

Empowering Women: A Look Into their Early/Mid Career

Lindsey Konerza
Security Engineer, University of Minnesota

Alexandra Bastian
Senior Information Security Risk Analyst, Bremer Bank

Mandie Grosskopf
Senior Consultant, Security Risk Advisors

Aanchal Manchanda
Senior Manager & HR Leader, Wipro Limited

As women look at making that early career decision or mid career transition, opportunities and challenges come into play both at the professional and personal level. This panel of women will be discussing what we face in the security industry as we join teams, embrace leadership opportunities, and make our mark to propel us forward.

October 24, 2022
13:30

Being a Better Ally in the Cyber Workplace

Karl Mattson
CISO, Noname Security

Kumar Dasani
VP, CISO, Digital River

Shayla Treadwell
Cybersecurity Executive, ECS

Ong Wang
Principal Security Analyst, Medtronic

How can allies of women in the workplace support growth and development as we navigate the challenges of industry? Please join us as we have a candid conversation around unconscious bias, creating opportunities of inclusiveness for all, and making a positive difference in the lives of women around us.

October 24, 2022
14:30

Learning the Dynamics of Leadership; Mindset, Culture & Behavior

Yolanda Hunte
Executive Assistant, Wipro

Stephanie Kasten
Senior IT Manager, Third Party and Compliance Risk Management, Medtronic

Rob Marti
Managing Director, Edgile

Sujatha Sadasivuni
Partner, Account Delivery Head, Wipro

The new landscape of leadership includes an increasing number of women leaders in Cybersecurity. We will help you understand how mindset, culture and behavior are interconnected in creating dynamic leaders. Join us in a engaging session that will trigger thoughts to help unlock your potential to becoming a better leader. You will learn what authentic leaders look like and how to push change in your role and organization. By attending you will recognize the factors in your personal life that contribute to creating a dynamic leader.

Join this session to learn and discuss:
- How has the leadership landscape changed over the years
- Understanding the factors that create a thriving culture in an organization
- What does NextGen leadership look like

October 24, 2022
15:30

Breaking Ceilings: A Journey to the Top

Tina Meeker
Sr. Director of Information Security, Sleep Number

Carolann Shields
Global CISO, 3M

Join this closing fireside chat to meet the new Global Chief Information Security Officer at 3M, Carolann Shields, moderated by Tina Meeker, Cyber Security Summit Program Chair and Sr. Director of Information Security at Sleep Number, to delve into Carolann's Journey to a Fortune 100 Global CISO as a female in the male-dominated cyber field, transformation from "Big 4" consulting to Industry, learn about her philosophy on security as a business enabler and driving cultural change within a global organization with many facets.

Technical Sessions

October 24, 2022
09:30

Enhancing SecOp Practices with MITRE

Chris Boehm
Technology Strategist, SentinelOne

MITRE Engenuity ATT&CK Evaluations emulations are constructed to mimic an adversary's known TTPs and are conducted in a controlled lab environment to determine each participating vendor's product efficacy. After this informative session, you will understand how to continuously tune your security strategy and leverage the connection between TTPs, adversary emulation plans, and real-world adversary groups.

October 24, 2022
09:30

Your CEO NEEDS to KNOW! Uber Breach and More! Cyber Tech translated to Business Strategy

Dan Wolfford
CISO, Blue Team Alpha

John Mess
VP of Business Development, Blue Team Alpha

Your CEO and leaders in your organization should probably be on the Cybersecurity train by now! With numerous attacks exfiltrating data and dollars, it has sure to hit all departments in all organizations by now. Whether it came from a super sophisticated spear phishing or whaling attack, or a simple text or phone call, it can all yield the same result.

We will look at some of the most recent well-known attacks, speak to the technical aspects, then translate that into how it will affect your business moving forward. Implementing a Cybersecurity program or plan is not a single software program, a single pen test, or just having a Cyber Liability policy to CYA… it is a multilayered approach that will require cooperation and sponsorship from your entire organization. What will you do next with your program?

October 24, 2022
09:30

How to Streamline Security Operations with Automation

Jay Spann
Security Automation Evangelist, Swimlane

The job of a security operations professional has never been more daunting. As organizational attack surfaces expand, the tools and environments required to protect them are becoming increasingly complex. Fortunately, there are tactics and technologies like low-code security automation that can help security-forward firms streamline and level up their SecOps processes. During this seminar we will show how you can: - Integrate and automate virtually any security tool in your security stack - Reduce manual effort drastically with easy-to-create workflows and playbooks - Create a system of record for your entire security organization - Improve key metrics like MTTD and MTTR without any additional hiring Join Swimlane experts as we explore how you can use low-code security automation to streamline and bolster your security operations.

October 24, 2022
10:30

Navigating Enterprise Security in a Post-Compromise Reality

Kanen Clement
Director, Specialist Sales Engineering, ExtraHop

Every organization gets compromised - it's how fast you detect and respond to an incident that counts. This is especially important when you look at trends like the overnight move to remote work, the rise in encrypted traffic and acceleration of cloud adoption, as well as the proliferation of enterprise IoT that have expanded the attack surface and complicated the job of security professionals. We'll explore those trends and the opportunity that lay ahead for security teams post-compromise to prevent an event that results in an outage or an incident from becoming a full-scale data breach.

October 24, 2022
10:30

Critical Success Factor #1: Injecting Security into your organization's DNA and Culture

Drew Koenig
Principal Security Architect, Federal Reserve of Minneapolis

The future of application security is here and it is called DevSecOps. Security can no longer be a "thing" you do at the end of a project and only if you have time. Security cannot be optional but integrated organically throughout the lifecycle from the start. Shifting security left is more than a process, it's a shift in culture, mindset, development practices and project management. This discussion will cover the foundational practices to help you get started in the new security journey.

October 24, 2022
10:30

The Role of Modern Asset Management in Cybersecurity

Lenny Zeltser
CISO, Axonius

The line between IT and Security is blurring. What was once a simple delineation between keeping information safe and providing the tools necessary to get work done is no longer clear. A foundational understanding of what devices, user accounts, and cloud services exist in organizations have jumped to the top of CISO's lists.

In this new enterprise, what role does asset management *(once a pure IT play)* play in cybersecurity? How can both the IT and Security teams benefit from a modern, cybersecurity-focused approach to asset management?

Join this session with Lenny Zeltser, CISO of Axonius to learn:
- How you can draw upon existing data sources to gather visibility into the state of your IT assets across data silos
- Which metrics you can gather based on your asset inventory to support IT and security initiatives
- Ways in which stakeholders throughout your organization can benefit from a modern approach to asset management

October 24, 2022
11:30

Network Luncheon Break

Join us for lunch and networking!

October 24, 2022
12:30

Panic Patching: Managing the Volume & Velocity of Alerts

Matt Ambroziak
Director of Security Solutions, Virsec Systems

Christian Trujillo
Senior Solutions Architect - Partner Ecosystem, Red Hat

Unpatched vulnerabilities are the most prominent attack vectors exploited by ransomware groups. Every time a new security patch is issued by a vendor, IT and Security teams must rush to deploy the patch across several server workloads. As the volume and velocity of patches increases, competing priorities place the IT Operations, SOC, and triage teams in constant high-pressure situations. This rushed, unplanned manual patching is disruptive to the business, error-prone, and overrides the planned release cycles. It also does not allow for proper patch testing and validation.

Join this session to learn how to build and implement a proactive vs. reactive patching strategy with the right technology, collaboration, and automation to solve this problem. You'll leave this session with a solution that will drive operational efficiency and improve morale and employee retention by allowing your experts to focus on more strategic security issues and improve your overall security posture.

October 24, 2022
12:30

The Data-First Approach; Managing the Tension Between Security and Productivity

Stephen Frethem
Senior Director of Sales Enablement, Varonis

Join me for a presentation covering risks and threats we're seeing across the industry, what security would look like if it started with data, and how to reduce your ransomware blast radius or the damage a compromised user can do.

October 24, 2022
12:30

Stay SaaSy my friends; Zero Trust in a Modern World

Brandon Potter
Chief Technology Officer, ProCircular

Zero Trust isn't a new concept. It's a universally recognized practice that has evolved over time to address challenges of the remote workforce and adoption of the "cloud" and modernized technology stacks.

Still, the gap in most implementations is that organizations rely heavily on Multi-Factor Authentication (MFA) to authenticate users and devices, inherently trusting all further activity. Today's threat actors combine older tactics and newer techniques to bypass these perimeter-focused zero trust implementations, wreak havoc as a trusted entity, and exfiltrate data undetected.

Join Brandon Potter, ProCircular's CTO, as he takes you on a journey through the past and present and finally into a future that embraces a "never trust, always verify" mentality for business-critical data and systems.
Analyze two real-world examples of common bypasses used in the wild, and fortify your zero-trust approach to meet the challenges of modernized, cloud-focused, and SaaS-based technology stacks.

October 24, 2022
13:30

Disrupting Nation State Hackers

Jake Iverson
Supervisory Special Agent, Cyber Program Coordinator, FBI

The FBI's cyber strategy is to impose risk and consequences on cyber adversaries and change the behavior of nation states who believe they can compromise U.S. networks, steal financial and intellectual property, and put critical infrastructure at risk without facing risk themselves. Join us for a discussion about the unique challenges of investigating and disrupting nation state hackers.

October 24, 2022
13:30

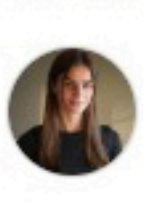
ITDR (Identity Threat Detection and Response): Making Sense of the Buzz

Brian Freedman
Global Solutions Engineering Manager, QOMPLEX

This session provides an overview of the current security problems in the identity landscape and how industry analysts refer to the new ITDR category. Explore how existing security tools such as PAM, MFA, IDP, etc. fit in the mix. Learn what you can do today and what to look for as a security practitioner to improve your organization's security posture as the threat of identity related attacks continues to rapidly expand year over year.

October 24, 2022
13:30

Breaking into Cyber: A Tale of Two Careers


Jessa Gegax
Information Security Testing Analyst, Surescripts

Will McCloskey
Threat Management Manager, Surescripts

Success in the cybersecurity realm is a journey, not a destination. The decisions security professionals make often tells a unique story that carves their career outcomes. Please join Jessa and Will as they talk about how they navigated the first years of their infosec path from distinguishing perspectives. Discover how frequently the choices we make can lead to unexpected opportunities that greatly influence one's professional life.

October 24, 2022
14:30

Armchair Cyberwarriors: The First 100 Days of Cybercriminal and Hacktivist Activities Related to the Russian War in Ukraine

Alexander Leslie
Associate Threat Intelligence Analyst, Recorded Future

Beginning on February 24, 2022, Recorded Future observed the rise—and, in some cases, downfall—of over 250 cybercriminal and hacktivist groups that became indirectly involved in the Russian war in Ukraine. This talk will cover the Conti and Trickbot leaks, the formation of the IT Army of Ukraine and Killnet, the operations of Anonymous and its allies, such as Distributed Denial of Secrets, AgainstTheWest, Network Battalion 65, GhostSec, and much more. Following the daily monitoring of approximately 100 active cybercriminal groups—with varying ideologies, motivations, nation-state allegiances, and hacktivist alliances—700,000 references in the Recorded Future Platform®, and regular threat actor engagements on dark web and special-access sources, this talk will document, summarize, and analyze the "armchair cyberwar" that took place over the first 100 days of the Russian war in Ukraine.

October 24, 2022
14:30

Not Your Average Bug Bounty: How an Email, a Shirt, and a Sticker Compromised a High Security Datacenter

Dalin McClellan
Senior Security Consultant, NetSPI

Earlier this year, the NetSPI social engineering team was tasked with attempting to gain physical access to a high security datacenter. With some small props to help them pose as a Pest Control company and significant background research, the team was successful.

But this assessment wasn't just about gaining unauthorized access. Hear Dalin McClellan share the story and the they lessons learned, including:

- The most sophisticated controls can quickly become irrelevant when they meet the real-world complexities of human interactions
- Humans are not the greatest vulnerability. Its vital to evaluate your security at the systemic level
- And more

October 24, 2022
14:30

Building Your Personal Brand: Navigating A Career in Cybersecurity With Three Unique Approaches

Zinet Kemal
Associate Cloud Security Engineer, Best Buy

Lee Ann Villella
Security Consultant, Proofpoint

Wendy Meadley
CEO, Next Phase Studio

With social media, podcast, blogs and other content creation, people who are looking to advance their career, find a job, network, or become a thought leader and present at conferences should be thinking about, and refining your personal brand.

How do you break into cybersecurity if you don't have a background? Many successful security practitioners and leaders come from different backgrounds and made a pivot into cyber.

This presentation will include three unique approaches on how to successfully network, build your brand, and how to stand out from the crowd.

Join this session to learn:

- Tools and tips on building your personal brand for a career in cybersecurity
- How to successfully network and find your next job in cyber
- Becoming a cybersecurity thought leader with your personal and business brand
- Advanced tips for building your LinkedIn profile with SEO, hashtags, with digital best practices
- Resource recommendations and how to use the Cyber Security Summit for building your network and career options

October 24, 2022
15:30

Networking Reception with Vendors

Join us for networking and meeting with our Vendors!

Healthcare & Med Device Seminar

October 24, 2022
09:30

Health Care & Medical Device Opening Remarks

Mary Diner
Information Security Director, Optum

Judd Larson
Medical Device Security, Medtronic

We built this agenda with the help of global healthcare cybersecurity experts and hope that you're looking forward to it as much as we are! We focused on the needs of Medical Device and Healthcare Infosec leaders and other professionals. The people who solve unique and challenging problems in healthcare cybersecurity space that other cybersecurity experts have nightmares over. We're keeping our Eyes Wide Open more than most ;-)

This one day special track includes presentations from infosec managers, regulators, medical device companies, and leading edge suppliers that address these unique challenges. Even the most seasoned professional will find a new angle or ....*something*.... to take back to their organizations and put into practice.

Minnesota - Home to the Medical Alley Association, strong support from the University of Minnesota (Technological Leadship Institute, Archimedes, and Medical School), large medical device companies, world leading healthcare delivery organizations, strong innovation pipeline and history of world-changing healthcare technology.

October 24, 2022
09:40

Frictionless & Secure Patient Care

Brian Kenyon
Chief Strategy Officer, Island.io

Healthcare and Care organizations spend significant time and capital in provisioning third-party care specialists access to web applications and critical systems. The process of sending physical hardware devices or asking care specialists to access via Virtual Desktop or Desktop as a Service offerings are costly, time-consuming and result in an unsatisfactory user experience. In this session learn how an Enterprise Browser can simplify access and security with your patient health information. In this talk we will discuss:
· Seamless onboard of care professionals
· Full control and visibility of all actions when accessing critical patient information
· Native and modern access and usage models

October 24, 2022
10:10

Approach to Segmenting Medical Devices

Stefan Boehme
Medical Device Security Specialist, Children's Healthcare of Atlanta

We've all heard the term "segmentation". We've all learned that it is an important piece to our security program, but what does it mean? How do you turn it from a talking point to a list of actionable items? Where do you start? What is the goal? How do you maintain it? Stefan Boehme, Medical Device Security Specialist, will share his story on how he guided the segmentation of wired connected medical devices at Children's Healthcare of Atlanta.

October 24, 2022
10:40

A Single Source of Truth in Healthcare Asset Management

Derek Loomis
Subject Matter Expert, Axonius

Modern hospitals now have 10 to 15 connected devices per patient bed. This increase in devices, along with strict regulations around cybersecurity and personal health information security, create more challenges for healthcare security teams. Enter: cybersecurity asset management. Cybersecurity asset management can help healthcare organizations easily get a comprehensive, up-to-date inventory of their complex environment — one single source of truth that all teams can work from.
Join this session led by IT security expert Derek Loomis to learn:
· A typical organization's various sources of truth — from HR, to network, to overall IT
· The challenges of maintaining a source of truth
· The value of all teams working from a single source of truth

October 24, 2022
11:10

Medical Device Software End of Life Planning

Judd Larson
Medical Device Security, Medtronic

Every medical device company has products running code not written by them. That software ranges from components like a small software bridge that enables Bluetooth connectivity to an entire Windows operating system that runs underneath our clinical applications. As that software ages, there are inevitably vulnerabilities that introduce new risks. If they doesn't control that software, how can we control these risks? This makes supporting our medical devices...tricky.

October 24, 2022
11:40

Strategy Break

October 24, 2022
12:45

Securing and Managing Connected Healthcare From Asset Inventory and Device Utilization to Zero Trust

Ben Stock
Director of Healthcare Product Management, Ordr

In the connected healthcare system, robots perform complex surgery, voice commands to Alexa devices are used as the nurse call button, and HVAC systems monitor air quality in surgery rooms. Telehealth and Telesitters are being used and will continue to be used across health systems to minimize patient movement and enable care.

These transformative hospital of the future initiatives vastly increase the stakes for healthcare cybersecurity. Connected medical devices can range widely, and often run outdated software even though they are a critical part of everyday operations and patient care. Unmanaged and unknown devices on the network create even more vulnerabilities, leaving hospitals open to ransomware and other malicious cyber-attacks.

Every conversation about the future of healthcare must include a strategy for securing medical technology. How can hospital leaders take responsibility now for determining what is connected to their networks and take the steps necessary to secure every IT, IoT and OT device on them?

Attend this session to learn about:

- Challenges securing connected devices
- Responsibilities and collaboration between HTM, IT and cybersecurity teams
- Security and operational use cases including asset inventory, risk identification, and device utilization
- Practical approaches to zero trust segmentation for security and cost avoidance

October 24, 2022
13:15

Security Resilience Program and Medical Devices

Debra Breummer
Senior Manager, Mayo Clinic

Building upon its medical device security program, Mayo Clinic will share its journey to develop and implement a proactive, ongoing asset "certification/validation" process spanning the life-cycle of an asset. The program measures cybersecurity risk empirically at the asset level, which is consolidated to a fleet view. The talk will focus on key deliverables: secure baseline requirements, certification program, asset drift, and risk measurement. This program enables vulnerable assets to be identified and risks to be assessed and quantified.

October 24, 2022
13:45

Crowdsourced Email Defense

Tonia Dudley
VP, CISO, Cofense

Phishing continues to be the preeminent approach attackers use to exploit an enterprise. Whether it's ransomware, or credential theft, falling for email and social media attacks continues to cost people and businesses millions of dollars in damages and lost information. Attackers are constantly changing tactics and tradecraft against unwitting humans. Fortunately, there are people equipped to recognize and report these threats to their security teams. Cofense is in the business of preparing humans to be a first-line of defense, and equipping those humans and security professionals with information and tools to recognize and even stay ahead of attackers. Tonia Dudley will be discussing how Cofense leverages crowdsourced email threat intelligence to proactively position detection and mitigation tools to stop attacks, and how your employees play a critical part in your enterprise defense.

October 24, 2022
14:15

Strategy Break

October 24, 2022
14:30

Highlights from the new FDA Premarket Cybersecurity Guidance: Impacts that Medical Device Manufacturers Need to Know

Michelle Jump
Chief Regulatory Strategist, MedSec Security Services

Matt Hazelett
Cybersecurity Policy Analyst, FDA

The FDA released a new premarket cybersecurity guidance, Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions Draft Guidance for Industry and Food and Drug Administration Staff, on April 8, 2022. This guidance is the follow-up draft from the 2018 draft premarket cybersecurity guidance and significantly expands on several key areas, such as threat modeling, security risk management, SBOM, security architecture documentation, and overall security lifecycle processes. The FDA has paid particular attention to aligning these expectations to existing quality system regulations. As such, some of these expectations are currently being requested as part of submissions. This presentation will review the notable expectations in the guidance and identify those elements that are currently recommended to be included in an FDA submission even though the guidance is still draft.

October 24, 2022
15:00

Essential Contract Provisions

Eran Kahana
Cybersecurity, AI and IP Attorney, Maslon LLP

Properly drafting data security language in a contract is essential for ensuring the data is protected from public exposure and misuse. All too often, however, parties opt for vague security provisions. Sometimes this is a result of the "drafting-by-momentum," a tendency that relies on what's been done before, by the organization, or other drafters. Other times it is just the result of carelessness. This session will highlight proper drafting considerations that can help effectively handle the various challenges organizations face in normal times and a pandemic environment.

October 24, 2022
15:30

Translating G-speak to C-speak

Andrew Bomett
VP, CISO, Boston Scientific

Getting quality time with executives and decision makers isn't easy in the fast-paced world we live in. It's gets even more challenging, when communicating technical details to business-oriented leaders. This session on Translating G-speak to C-speak aims to provide you with some tips and insights to help you in your next engagement with the C-suite. We will review the different audiences in that group, their communication styles, and ideas of how to tailor your message so that you can get your message across and get the desired outcome.

October 24, 2022
16:00

Networking

Join us for networking and socializing!

Industrial Cyber Security Track

October 24, 2022
08:00

Int'l Soc. of Automation: ISASecure Intro & Overview of ISA/IEC 62443 Solution Sets for Systems (3-1, 3-2, 3-3) and Components (4-1, 4-2)

Andre Ristaino
Managing Director, ISA

ISA is an ANSI accredited standards development organization (SDO) and the publisher of the international ISA/IEC 62443 cybersecurity standards for automation and control systems. These standards are now the de-facto standards for securing critical infrastructure in the USA and globally.

You will learn about the history of the standards and current status. In 2021 the IEC designated ISA/IEC 62443 as a 'technical horizontal' standard which will be discussed during Mr. Ristaino's presentation.

Mr. Ristaino oversees ISA consortiums including three related to cybersecurity: ISCI, LOGIIC, and ISAGCA. Consortium missions and activities will be presented along with other programs ISA oversees related to critical infrastructure cybersecurity including ISA's world-class training and education.

ISA offers many ways to participate in industry programs for advancing the state of control systems cybersecurity.

We strive to elevate OT cybersecurity from an art, to a science, to an engineering discipline.

October 24, 2022
09:00

Idaho National Labs (INL) Overview of Cybersecurity Research, ICS COP w/focus on Cyber-CHAMP©

Shane Stailey
Organizational Cybersecurity Development & Training Strategist, Idaho National Laboratory

Glenn Merrell
CAP, Owner & Freelance Consultant, Industrial Control System Security

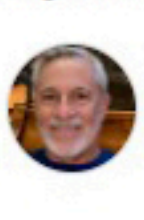
There is a pervasive talent deficit in the cybersecurity industry that prevents employers from being able to effectively fill their open positions and upskill existing employees to work in or maintain appropriate levels of cyber competency within their organizations. Without an understanding of those deficits, companies can struggle to efficiently plan, develop, and deploy effective security programs.

The Cyber-Competency Healthy and Maturity Progression (Cyber-CHAMP©) aims to help. The model provides a customized solution for businesses to:
· Understand their security program and personnel gaps
· Bring focus to closing current security gaps
· Align education and training needs to address security gaps in personnel competency
· Continually monitor and improve by having at the ready, cybersecurity workforce development visuals, metrics, and measurements

Cyber-CHAMP© provides several visual products, metrics, and measurements to help an organization build their current and target risk profiles and helps build a structure to examine competencies across an organization's workforce. It also offers recommendations and roadmaps for improvement across the organization to increase the organization's cybersecurity via improving the cyber cognizance and competency of individuals across the organization.

October 24, 2022
10:00

Cyber Ranges – For Gaining the Valuable Experience Needed now and Henceforward


Craig Cocciola
VP Cyber Range Operations, ABL Cyber Range and Academy

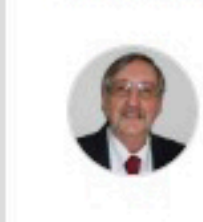
Susan Morris
SVP, Co-Owner, ABL Cyber Academy and Cyber Range

The job roles in both OT and IT Cybersecurity require the highest levels of competency and proficiency in situational awareness, critical thinking, and job role task specific actions. Cyber ranges provide great hands-on learning opportunities in many areas of cyber security, such as:
· INL's Consequence-driven Cyber-informed Engineering (CCE)
· ISA/IEC 62443 series of standards, developed by the ISA99 committee and adopted by the International Electrotechnical Commission (IEC)
· NIST Framework 800-82 Rev. 3 - Guide to Operational Technology (OT) Security
· NICE recommendation for the use of cyber ranges in cybersecurity education and training

Cyber ranges differ in terms of quality, price, and customization. New ranges pop up often, requiring due diligence to ensure you're choosing the correct one for your needs. The most valuable offer learners industry specific training relevant to the job role being performed. The range design must have:
· Learning experiences are consistently updated to meet threat actors' ever-changing APT strategies and tools
· Influence and persuasiveness, ensuring the learner chooses to invest the effort in acquiring new skills
· Use of digital twin technology to provide virtualized representations of real-world scenarios. (Not sure what this means?)
· Capability to map job role skills' development using the NICE Framework Mapping Tool
· Ability to meet the needs of the 16 Critical Infrastructure Sectors
· Dynamic learning for ongoing, rapid upskilling and verifiable transfer of skills to the job
· Actionable metrics and proficiency reporting to verify competency of industry standards
· Skills and tools to scan systems and devices for vulnerabilities, more efficient recognition, mitigation, and obstruction of attacks
· Nexus of multi-level learning for:
· New hires and all incumbent levels
· OT workforce pipeline to gain job role experience during critical OT/IT education at colleges, universities, and inside organizations
· Filling organizational job role skills gaps identified from, for example, Cyber-CHAMP©

October 24, 2022
11:00

International Society of Automation (ISA) Deeper Dive: Working Group 10 Details and new Technical Report Rollout


Glenn Merrell
Owner & Freelance Consultant, Industrial Control System Security

Shane Stailey
Organizational Cybersecurity Development & Training Strategist, Idaho National Laboratory

Problem Statement:
Non-control system professionals may feel application of the ANSI/ISA/IEC 62443 program and lifecycles are somewhat burdensome and/or confusing, certainly those with a discipline in Information Technology.

Dissertation:
Extreme Risk injected into your IACS Security Lifecycle may not be hackers, but rather from the absence of cognizance, knowledge, and recognition training of the risks inherent in the IACS/ICS.
Without proper focused training of the physical vulnerabilities that can endanger or restrict control system functions, a control system cannot be properly secured. Techniques and methods of securing control systems that do not address field device, instrumentation, and measurement, such as vibration, temperature, and pressure, leave significant vulnerability open to exploit.
The upcoming ANSI/ISA TR62443-1-4 Program, Lifecycles and Use Cases proposes a deeper review of the application of ANSI/ISA/IEC 62443 explaining its program's, its lifecycle's, and reference application examples through various use cases.

This Technical Report explains why a properly designed, instituted, deployed, and practiced security management system is critical to the success of securing control system functions.

In addition to identifying differences in risk between ITandOT cybersecurity, an outline overview of the upcoming Standard series Technical Report; TR62443-1-4 Program, Lifecycle and Use Cases will be presented covering this in-development Technical Report, progressing toward release in early 2023.

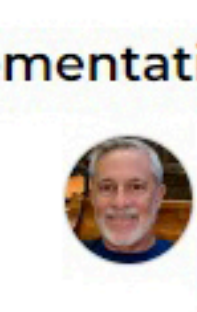
October 24, 2022
11:50

Strategy Break

October 24, 2022
13:00

ABL Virtual Cyber Range Implementation Details

Susan Morris
SVP, Co-Owner, ABL Cyber Academy and Cyber Range


Craig Cocciola
VP Cyber Range Operations, ABL Cyber Range and Academy

Each organization, college, and university requires an implementation plan unique to their sector, OT or IT systems, and current state of cyber OT and/or IT workforce competence.

The foundational tenet of a range implementation plan is the alignment of supporting organizations who interconnect for success assurance.
This session will discuss three basic steps common for a range implementation across industries and sectors. They include:
Step 1: Preparation
Step 2: Initial deployment
Step 3: Ongoing maintenance and update training content

Subordinate steps will change based on the organization's and/or educational institution's current and desired state of skills offerings and workforce development strategies and paths.

A Cyber Range may be out of reach for many small- and medium-sized businesses. ABL has implemented a Virtual Cyber Range configurable to most IT scenarios and now growing into OT Cybersecurity for Critical Infrastructure. This subscriber service is a flexible model enabling customized content creation.

October 24, 2022
14:00

State of the Art IoT Cybersecurity

Joel Hollenbeck
Office of the CTO, Head of Engineering, Check Point Software Technologies, Ltd.

This session will discuss where cyber security efforts are at today, what needs to be done to improve cyber security efforts and improve how cyber security efforts are applied to the world of IoT. Everything from Industrial Control Systems to SmartWatches represent nuanced and unique infrastructure diversity challenges that make the application and development of tool sets, and control of said cyber security environments different from those in traditional IT environments.

October 24, 2022
15:00

Securing IT and OT Convergence is a Team Sport

Bryan Gillson
Head of Vertical Market Sales, Ordr Inc.

For decades, manufacturing, utility operations, and transportation have relied on operational technology (OT systems) for daily functions. These systems have stood apart from the traditional IT and IoT structure, and placed reliability, production output and safety as foremost. Two forces are upsetting the status quo – the drive towards digital transformation and the ever-aggressive attacks on security that can bring operations to a halt.

In this session, Bryan Gillson, Head of Vertical Strategy at Ordr, discusses the considerations for a secure path towards digital transformation. Connected devices now span IT, IoT and OT, and increase the risk landscape. At the same time, IT and security teams may have differing priorities from OT leaders. Bryan will share considerations for a security strategy to protect the converged environment, and tactics to align IT, IoT and OT teams.

October 24, 2022
16:00

Dunwoody Presentation: New Cybersecurity Initiatives

E.J. Daigle
Dean of Robotics & Manufacturing, Dunwoody College of Technology

Julie McFadden
Director of Computer Technology Programs, Dunwoody College of Technology

Cybersecurity, compliance, and risk have become pressing issues across the world. Lack of shared norms, rampant cybercrime, uneven knowledge and competency, and the threat landscape of connected devices create pressing challenges for the future. This session will discuss Dunwoody College of Technology's expertise, and programs in both Information Technology (IT) and Operational Technology (OT) and delve into its New Cybersecurity Initiatives, highlighting the recent partnership between Dunwoody's computer and industrial automation programs to bridge the gap between IT and OT cybersecurity. The session will include a demonstration of Dunwoody's newest educational asset, the Process Controls & Instrumentation Lab, that provides students and educators the opportunity to play out real-world scenarios, preparing the next generation of cybersecurity graduates and practitioners for immediate impact across industries and critical infrastructure.

October 24, 2022
16:30

Networking

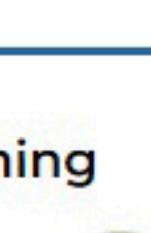
Join us for networking and socialization!

Small Business Seminar

October 25, 2022
13:00

Cyber and Small Business Opening

David Notch
CISO, Castlelake L.P.


Brian McDonald
District Director, SBA

Lyle Wright
Associate State Director, MnSBDC

Perception vs. Reality

"We're too small to be a target."

"This company has bigger issues."

"Defending against cyber-attacks costs too much."

"I'll worry about it when it happens."

These sentiments and more are often heard when discussing the impact of cyber security risks to small businesses. This session will dive briefly into the facts and help set the stage for the rest of the afternoon's sessions about ways to address the situation and dispel these perceptions.

Small business owners often think they are too small to be targeted for cyber-attacks or that defending against such attack's costs too much. Little do they know those beliefs are exactly what make them an enticing target. This session will set the stage for the remainder of the afternoon's sessions and explain why it's important to be proactive about defending their companies from attack.

Essential Small Business Resources

Cyberattacks are a growing threat to the U.S. economy. Small businesses are attractive targets because they have information that cybercriminals want, and they typically lack the security infrastructure of larger businesses. This welcome session will provide information about no-cost programs available from the U.S. Small Business Administration to support businesses. You will also learn about resources available from other federal agencies and organizations that will start you on a path to becoming more cyber savvy.

America's SBDC North Star Cybersecurity Program

The ASBDC North Star Cybersecurity Program provides a baseline to promote cybersecurity awareness to small businesses nationwide through the SBDC network. No matter where the small business is in the US, there is a SBDC center to provide guidance for effective cyber/data hygiene. Attendees will learn about an ASBDC website with additional cyber resources they can begin using immediately. Attendees will have access to the 'Cybersecurity Consultation Guide' to let them begin a casual, non-technical review of basic cybersecurity awareness for their own business.

October 25, 2022
13:30

CISA & DHS Resources for Small Businesses

Karissa Zamora
Intelligence Officer, Department of Homeland Security

Chris Gabbard
Cyber Security Advisor Region V, Office of Cybersecurity & Communications, Cybersecurity and Infrastructure Security Agency (CISA)

DHS Intelligence and Analysis Threat Assessment

Karissa Zamora, Intelligence & Analysis, DHS

Nontechnical Actions To Enhance Cybersecurity Posture

Chris Gabbard, CISA

This presentation will provide an overview of the Department of Homeland Security and Cybersecurity and Infrastructure Security Agency (CISA), including the services that can be provided. This session will cover information on current cyber threats provided by DHS Intelligence & Analysis. It will also provide simple nontechnical actions that small businesses can perform to enhance an organizations' cybersecurity posture and no cost resources you can take advantage of.

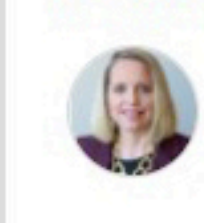
October 25, 2022
14:30

Strategy Break

Meet with others to network and socialize.

October 25, 2022
15:00

Panel > Cyber Risk and the Small Business Owner: What you Need to Know


Milinda Rambel Stone
CISO, Bremer Bank

Muhammad Khokhar
Deputy CISO, Bremer Bank

Kristin Hines
AVP, Loss Prevention Services Manager, Bremer Bank

Jarrod Hutchinson
Business Solutions Market Leader, Bremer Bank

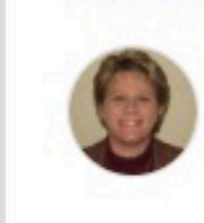
Joel Quam
Commercial Insurance Advisor, Bremer Bank

Financial fraud is now a common reality in the world of cyber security. It is prevalent in the small & medium sized business space and new scams only continue to transpire.
Join Bremer Bank as we discuss fraud techniques you need to be aware of. We will also focus on no to low-cost take-aways to secure your company that you can immediately implement for additional safety and protection.
Topics to cover:

- Business owners need to challenge vendors. Are they secure/how?
- Why do SMB owners need to think differently? And defensively?
- Use of modern technology. Faster payments and money movement. How is your business being protected?
- Why is it in your best interest to be your own advocate for secure transactions?
- Should you be asking/demanding secure tech for your business transactions?
- What do we need to think about when handling confidential documents?
- The Basics....what do we need to understand as small business owners?

October 25, 2022
15:45

Securely and Responsibly Disposing of your IT Equipment


Rebecca Duvick
Business Development Manager, PCs for People

Even electronics recycling vendors can present a threat to small business owners, who must take steps to safely dispose for their outdated IT equipment.

We'll explore the current standard in data sanitization and considerations for selecting a vendor to recycle your IT assets, as well as the opportunity for your organization to improve your   Environment, Social, Governance score through your equipment disposition.

October 25, 2022
16:00

Breaches and how to Manage Them

Aaron Campbell
FBI Computer Scientist, FBI

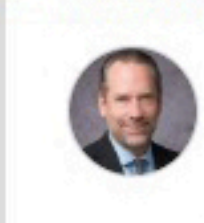
Benjamin Canine
CIO, Lorenz Bus Service

Eileen Manning
CEO, The Event Group / Cyber Security Summit

This session will kick off hearing a few recent real-life experiences of small business attacks and their impact. The FBI will then discuss recommendations for dealing with an attack after it has occurred. This will include resources and strategies to help you prioritize your response, giving you the best opportunity for recovery.

October 25, 2022
16:30

What to Look for in IT and Security Service Providers


David Notch
CISO, Castlelake L.P.

You've worked hard to build your company. You wouldn't consider walking out the door at night without locking up or giving the combination of the safe to just anyone. You need to make sure you take the same precautions with your cyber security. When you bring in a company to build, maintain and secure your infrastructure what questions should you be asking?

What certifications should they have? Is there a Better Business Bureau equivalent for cyber security providers? How do I know to ask what I don't know?

October 25, 2022
17:00

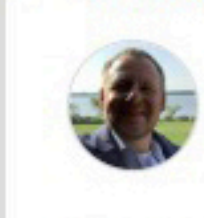
Networking

Meet with others to network and socialize.

Full Summit Agenda - Tuesday

October 25, 2022
07:15

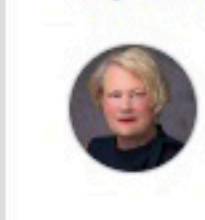
Student Career Breakfast with the CISO of the State of Minnesota


John Israel
Interim CISO, State of MN

Meet the Deputy CISO for the State of Minnesota, John Israel as he presents sage advice and career-shaping insights for newer and future
cyber security professionals.

October 25, 2022
08:00

Welcome to the 2022 Twelfth Annual Cyber Security Summit > The 2022 Theme is Eyes Wide Open!


Eileen Manning
CEO, The Event Group / Cyber Security Summit

Judy Hatchett
VP, CISO, Surescripts

Jeffrey Norem
Deputy CISO, Freddie Mac

Eileen Manning, Executive Producer and Founding Partner of the Cyber Security Summit and the 2022 Summit Co-Chairs, Judy Hatchett VP, CISO, Surescripts and Jeff Norem Deputy CISO, Freddie Mac, will officially kick-off this year's summit sharing why you need Eyes Wide Open!

October 25, 2022
08:30

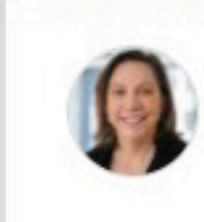
Stronger Together: Lessons from 21 Years of Intelligence Integration

Andrew Borene
Associate Vice President for Research, National Intelligence University

Andrew Borene will discuss insights from his role at the National Intelligence University and set the stage for our morning keynote speaker, Beth Sanner. Ms. Sanner is an innovator, change agent, and c-suite level leader with more than three decades of experience in national security who has briefed the President of the United States on Cyber for several years.

October 25, 2022
09:00

Adversaries Turning to Cyber as Weapon of Choice


Beth Sanner
Former Deputy Director of National Intelligence

Growing global competition and conflict, amplified by Russias invasion of Ukraine, are shifting the threat environment for nations and the private sector alike. Many of our adversaries are using, sponsoring, or planning to use cyber attacks on Western companies and critical infrastructure for a variety of reasons, including moneymaking, stealing intellectual property, revenge, and potential war. As a result, companies in every sector need to be prepared for a larger range of threats than ever before. But there is some good news. The US government and it's Allies are focusing on these challenges more than ever before and partnering with private sector firms to more quickly understand and address cyber threats.

October 25, 2022
09:30

What if The Browser Was Designed for The Enterprise?

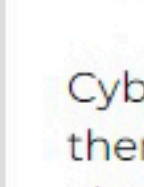
Michael Fey
Co-Founder, CEO, Island.io

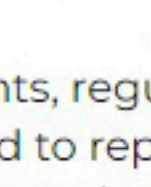
The application enterprises use the most is the browser. In fact, it has become our primary work environment, but the browser we most often use was built for consumers. So, we have surrounded it with an endless, complex and expensive stack that overwhelms your security teams and interrupts end users. But what if the browser was designed for the enterprise? What could that do for security, productivity and work itself? Join this session to discover how an enterprise browser can:

- Protect critical SaaS and internal web applications
- Streamline and secure third-party contractor access and BYOD strategies
- Free you from the cost and poor user experience of VDI and DaaS solutions
- Give you last-mile control to protect users' activity with critical applications and underlying data
- Deliver it all in a familiar, Chromium-based application

October 25, 2022
10:00

Here Be Dragons - Navigating An Ocean of Security Frameworks


Tony Sager
Senior Vice President & Chief Evangelist, Center for Internet Security


Thomas Sager
Associate Cybersecurity Engineer, Center for Internet Security

Cybersecurity frameworks, requirements, regulations, and standards must be wonderful, because we have so many of them. But enterprises today often need to report to several of them, each with its own focus, language, level of abstraction, and assessment/audit approach. Cross-mapping among them has become a way of life for many enterprises, and has led to a sea of mappings that include commercial services, vendor tools, volunteer donated, hand-crafted one-offs, and everything else you can imagine. While some of this is inevitable, we believe the creators of such frameworks need to simplify this problem for adopters.

At the Center for Internet Security (CIS), we're doing our part by creating and openly sharing authoritative and vetted cross-mappings from our products and services (like the CIS Benchmarks and Controls) into the ocean of similar schemes. We'll describe how we go about creating, validating, and sharing these – as well as our thoughts on how to make this simpler and more valuable for everyone.

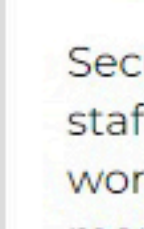
October 25, 2022
10:30

Break & Expo

Meet with solution providers in the Expo Hall while enjoying a networking break

October 25, 2022
11:00

Adjust your Cybersecurity Approach to Today's Rapidly Changing Macro-Environment


Ross Rosenzeig
Sr. Director of Engineering, BlackBerry

Security has become a board level topic for many organizations and we know the balance of budget, technology and staff continues to challenge IT. Industry reporting, including a recent ISSA report, shows over 50% of increased workload, over 25% of staff burnout and over 90% report cyber skill set shortage within their business and in the market. Combine these challenges with increased threat dynamics and risk profiles that cover both external and internal threat actors we need to look at our security approach and practices in context around how, with who and with what we stay secure.

October 25, 2022
11:45

Lunch Buffet & Expo

Lunch & Networking

October 25, 2022
11:45

VIP Lunch > Invite Only > Why CSOs and CISOs are Critical in the Boardroom / And How to Accelerate Your Way to a Board Director Role.

Tissa Richards
Executive Coach, Tissa Richards

If you've ever thought, "There's no place on a corporate board for someone with my background," You are wrong.

88% of boards view cybersecurity as a business risk, according to Gartner. Addressing cyber risk must start at the top: in the boardroom. The time is now for CSOs and CISOs to take a seat at the table. Boards are identifying and bringing on more directors than ever before with technology and security expertise, strategizing how to protect brand reputation, revenue, continuity and resilience.

Learn proven strategies to launch your board journey or expand your existing board portfolio from a repeat cybersecurity tech founder, former CEO, and leadership expert, Tissa Richards. Tissa works with the world's largest private and public companies and investment management firms to diversify their boards by successfully identifying critical board candidates.

In this keynote, you'll learn how to:

· Translate your operational experience into a compelling board story
· Talk about security in a way that resonates with non-technical board members
· Create a crisp, concise, and effective narrative about your career successes
· Get started on your journey with the right board materials
· Leverage your network to identify board opportunities and scale your search

And, more important than anything, you'll discover how to communicate your value in a way that is memorable and clear – allowing you to be the first to come to mind when opportunities arise.

October 25, 2022
13:15

Technology Alone Cannot Solve our Greatest Cybersecurity Challenges. How to Effectively Leverage Technology to Maximize the Value of Human Creativity, Experience, and Ingenuity.

Cody Chamberlain
Head of Product, NetSPI

Cody Wass
Vice President of Services, NetSPI

Technology cannot solve our greatest cybersecurity challenges. At least not on it's own. All too often in the cybersecurity industry, we view technology as the 'silver bullet' against today's threat actors. But at the end of the day, it's the combination of people and technology that will solve the greatest challenges we face. In this session, Cody Wass and Cody Chamberlain from Netspi will take a deep dive into the intersection of technology and talent and why both are necessary to combat the world's greatest adversaries. Attendees will explore:
· Where tech-only and human-only solutions fall short
· Technology's role in overcoming the cybersecurity talent / skills shortage
· How to effectively leverage technology to maximize the value of human creativity, experience, and ingenuity
· Real stories and examples from our penetration testing team

October 25, 2022
13:45

Fireside Chat with CISA

Mike Kearn
VP, Business Information Security Officer, U.S. Bank

Nitin Natarajan
Deputy Director, CISA

Join CISA Deputy Director Natarajan and U.S. Bank BISO Mike Kearn as they discuss CISA updates and how our audience can be part of the cyber solution.

October 25, 2022
15:10

BREAKOUT ROOM 1 > BLOOMINGTON > Translating Risks to Business Terms: Conveying Complex Risk Topics in Simple Business Language

John Valente
Security Consultant

Ivan Fong
Executive Vice President, General Counsel and Secretary, Medtronic

Todd Hartman
Executive Vice President, Best Buy

Melissa Krasnow
Partner, VLP Law Group

A board of directors has many duties, but its first is to protect shareholder assets. The protection of assets includes the management of Business Risk, including Cyber Security Risks. The panel will discuss how best to responsible present Cyber Security Risks to the Board of Directors in business terms that relate to protecting the organizations assets. As well as preparing company specific actions being taken again current media coverage of Cyber Security issues.

October 25, 2022
15:10

BREAKOUT ROOM 2 > ATRIUM 4 > Ukraine and the Three Bears (Not A Fairytale)

Mike Kearn
VP, Business Information Security Officer, U.S. Bank

This talk will walk through how offensive cyber operations performed by Russia's three intelligence units directly supported the invasion of Ukraine in early 2022. We will discuss each of the three units, their missions, past notable attacks, and the operations they completed in support of the invasion. All information presented will be open source and unclassified.

Attendees will take away:

- An understanding of the FSB, SVR and GRU within Russia's intelligence apparatus
- Familiarity of the tradecraft leveraged by FSB. SVR and GRU based upon open sources
- Comprehension of how each of these agencies supports the larger nation state objectives for Russia

October 25, 2022
15:10

BREAKOUT ROOM 3 > ATRIUM 6 > Adapting your Strategy to a Higher Degree of Risk Tolerance

Eli Davis
Information Security Architect, Vista Outdoor Inc.

This talk will be focused on personal observations, experiences, and lessons learned from seeing a company transform it's security posture from that of a defense contractor to a consumer goods manufacturer. Subtopics include team culture, learning to embrace risk instead of avoiding it, overhauling your entire tech stack, and steering the work culture over multiple years. The talk will be primarily non-technical, directed toward management, and from the perspective of boots-on-the-ground Information Security Engineers and individual contributors.

October 25, 2022
16:00

BREAKOUT ROOM 1 > BLOOMINGTON > How Kindness Builds Effective Security Operations

Nathan Caldwell
Managed Awareness Evangelist, Arctic Wolf

Cybersecurity professionals are responsible for keeping companies secure but security should never end with technology. Only those who also focus on effectively leading people with kindness will be able evolve their cybersecurity from a technology safety net into a mesh network of cyber-wise diligent defenders who understand how to protect themselves and their organization.

Kindness is the key to helping people:

- Understand WHY they must care
- Understand HOW to proactively identify risks and take measures to ensure their organization is powerfully secure
- Increase motivation while reducing stress
- Develop into trustworthy teammates

October 25, 2022
16:00

BREAKOUT ROOM 2 > ATRIUM 4 > Identity Governance Transformation Partnership: A Case Study with Edgile & Sleep Number

Mercy Schroeder
Director, Business Development, Edgile

Devan Koss
Director of Information Security GRC, Sleep Number

Josh Oldham
Senior Engineering Manager - Datacenter Infrastructure and Identity Engineering, Sleep Number

Becky Sandberg
Director, Edgile

Join Sleep Number's Information Security and Identity Leaders along with Edgile's Identity expert to learn about their ongoing journey to transform and modernize Sleep Number's identity program and practices. This session will feature an overview of the initiative, unique challenges faced, advice on pitfalls to avoid and how to keep your teams engaged. If you are thinking about investing in an Identity Modernization initiative, this is a must attend!

Attendees will take away:
· The decision point that led Sleep Number to choose to invest in a new identity platform
· The Identity Governance platform and Integrator(s) selection process
· Unexpected challenges that were overcome/pitfalls to avoid
· Best practices on deploying a modern cloud Identity solution
· How the teams at Sleep Number and Edgile collaborated successfully on this initiative
· The benefits already realized and future benefits to come
· Q&A

October 25, 2022
16:00

BREAKOUT ROOM 3 > ATRIUM 6 > Executive Level Cybersecurity Report Cards

Kathy Washenberger
Executive Director of Information Security GRC, Deluxe Coporation

All of us are familiar with the concept of report cards. Like many, "bad" grades aren't easy to accept. Couple that with a bit of healthy competition among the strongest Type A personalities at a company, and the results are amazing! I'm excited to share the incredible success I've had in using this commonly known technique to drive action around some of the most difficult-to-solve cybersecurity problems.

October 25, 2022
16:45

Expo Reception

Join us for refreshments and networking!

October 25, 2022
17:30

Visionary Leadership Awards > VIP Reception

Invite only: Private Networking Session for Visionary Leadership Award Nominees and Invited Guests.

October 25, 2022
18:00

Visionary Leadership Awards Ceremony

Chris Buse
CISO, Old Republic Title

Jennifer Cichoski
Enterprise Sales, Virsec

Betty Elliott
Senior VP, CISO, Freddie Mac

Naomi Hospodarsky
Security & Compliance Analyst, Minnesota Supercomputing Institute

Laura Johnson
Enterprise Endpoint Manager, Minnesota IT Services

Chip Laingen
Executive Director, Defense Alliance

Alyssa Maki
IT/InfoSec Analyst, Kimley-Horn and Associates

William Rankin
Director of Governance and Compliance, ECS

Nadia Rizk
Director of Technology Audit & Data Analytics, Target Corporation

Prasenjit Saha
Executive Vice President and Global Cyber Security Business Head, L&T Infotech

Terry Seiple
Senior Information Security and Cloud Architect, State of Minnesota

Natascha Shawver
Information Security Architect, University of Minnesota

Join us for the 2022 Visionary Leadership Awards Presentation.

October 25, 2022
18:00

Visionary Leadership Awards Dinner

Join us for the 2022 Visionary Leadership Awards Dinner preceding the Awards Ceremony

October 25, 2022
20:00

Cyber Warrior Tribute Program at the Visionary Leadership Awards

Domenick Allen
Musician

Legendary rock musician, Domenick Allen (formerly of "Foreigner") will perform for the Cyber Warrior Tribute portion of the Visionary Leadership Awards Banquet.

Full Summit Agenda - Wednesday

October 26, 2022
07:00

Have you ever Considered a Career with the FBI? > Onsite Only

Brenda Kane
Recruiter, FBI

Colleen Peña
Cyber Special Agent, FBI

Join us early for this not to miss breakfast. Featuring representatives from the Federal Bureau of Investigation who will be on hand to speak about the application process, IT, Cyber and Tech Careers in the FBI.

October 26, 2022
07:00

Learn about Women In Cybersecurity (WiCyS) Minnesota Chapter

Judy Hatchett
VP, CISO, Surescripts

Tina Meeker
Sr. Director of Information Security, Sleep Number

Marie Igtanloc
District Sales Manager, MINK, CyberArk

Start your morning with WiCyS MN. The WiCyS Minnesota chapter was launched in 2019. Learn all about WiCyS MN, events planned throughout the year and how to get involved.

The Women in Cybersecurity Minnesota (WiCyS MN) is a regional affiliate that covers these geographic areas: Minnesota with outreach into Wisconsin, Iowa, North and South Dakota. As a WiCyS Affiliate, we will undertake activities to promote recruitment, retention, and advancement of women in cybersecurity.

October 26, 2022
08:00

2022 Cyber Security Summit Intern Showcase

Jeffrey Peal
Information Security Officer, Clinician Nexus

Aynura Berdyyeva
Cyber Summit Coordinator, Cyber Security Summit

Sherwin Bothello
Cyber Summit Coordinator/Product Security Engineer II, Security Summit/Medtronic

Joseph Mathias
Cyber Summit Coordinator, Cyber Security Summit

As the Cyber workforce faces challenges, here at the Summit we started a unique internship program that is giving soon-to-graduate and recently graduated students a jumpstart on their careers. Hear firsthand from some of our executive coordinators on their background, Summit experiences, skill sets, and how you can hire them. Additionally, the Summit offers an ongoing scholarship program and is seeking corporate support.

October 26, 2022
08:30

Narrowing the Gap - A Unilateral Understanding of Engineering and Network Security

Joe Weiss
Managing Partner, Applied Control Solutions

Critical infrastructures are heavily reliant on industrial control systems. Industrial Control systems consist of engineering devices "owned and managed" by engineering departments. Ethernet networks are "owned" by Information Technology and/or Information Security. As the nation's threats continue to evolve it is critical that these two teams learn to coexist and work together to ensure the safety and security of our critical infrastructures. These two teams have different tools, skillsets and priorities. Applying inappropriate network cyber security technologies have impacted the operation of the devices exacerbating the culture divide. Technology has been demonstrated that can provide a more secure approach to control system devices that can help overcome the cultural divide.

October 26, 2022
09:00

The Intersection of Privacy and Security: How you can use Existing Security Tools to Build an Adaptive Privacy Program

Jerrod Montoya
Principal, Truvantis

Privacy and security were historically two separate disciplines. Over the years, the two have grown closer together. As the landscape of privacy regulations continues to evolve, the most recent comprehensive privacy laws continue to close that gap even more. With this convergence, there's opportunity to blend what are known as best security practices and incorporate them into best privacy practices.

In this presentation, you will hear about upcoming legal changes in privacy with an emphasis on US privacy laws, how these laws converge with best security practices, and how you can use security practices to make privacy programs more resilient to frequent changes in the law. Whether you are responsible for privacy or just a resource to a privacy group in your organization, this presentation will leave you with actionable steps to get your program on the right track.

Hear expert advice on how you can develop and maintain a risk-based program designed to evolve with changing regulatory, threat landscape and business requirements.

October 26, 2022
09:30

"Cyber Risk Economics". We Can Be Better.

Jeffrey Norem
Deputy CISO, Freddie Mac

Andrew Herbert
Information Security Analyst - Risk Quantification, Freddie Mac

Corey Tower
Sr. Risk Manager, Freddie Mac

In this session we will give an overview of cyber risk quantification, specifically focused on our experience using the FAIR methodology in multiple organizational risk programs. We will discuss the benefits and use cases for CRQ and how it can be used to advance the common qualitative approaches used today like heatmaps with ordinal scales, maturity models and weighted number approaches. Lean tips for how to get started with a risk quantification program and some of the challenges you can expect along the way.

October 26, 2022
10:15

Networking and Break

October 26, 2022
10:45

Third-Party Risk: Evolving and Tailoring your Approach to Address this top Attack Vector for your Organization

Gretchen Block
CISO, SVP, United Health Care, Optum

Cyber-attacks continue to disrupt critical supply chain and business partners, impacting key business processes. Hackers are targeting larger enterprises through their smaller, less-sophisticated partners and subcontractors as attack vectors into their larger clients' networks. To manage this risk, it is important to build an organization wide Supplier Risk Management Program that oversees the risk and ensures the appropriate capabilities are in place to respond and recover rapidly from potential attacks. As the threat landscape continues to shift, it is crucial for the Supplier Risk Management program to evolve and tailor approach commensurate with advancing risk.

October 26, 2022
11:15

Cyber Incidents Happen - Who Is To Blame?

Ben Corll
CISO Americas, Zscaler

In this session, we'll look at some of the common attack scenarios for cyber incidents as well as the common controls that security teams have used to minimize harm or threat. Attendees will then learn about the 4 core tenets of zero trust architecture and what the future of security and computing could look like with zero trust implemented.

October 26, 2022
11:45

Lunch Buffet & Expo

Join us for our Lunch Buffet!

October 26, 2022
13:00

Solving the Unsolvable With Crowdsourced Security

Justin Beachler
Director of Trust and Security, Bugcrowd

Crowdsourced security has evolved from its roots in bug bounty, moving into the mainstream for numerous use cases (including penetration testing and attack surface management) to help solve problems that other approaches can't. In this session you'll learn about the drivers for and value of modern crowdsourced security, how to adopt and operationalize it gracefully and at scale, and why "crowd fear" is a red herring.

October 26, 2022
13:30

Humans are Vital for Cybersecurity

Sean Costigan
Director and Co-Founder, George C. Marshall European Center for Security Studies

Dinos Kerigan-Kyrou
Lead for Cybersecurity, Joint Command & Staff Course, Abertay University

Rois Ni Thuama
Head of Cyber Governance, Red Sift

Are you to blame for your organization's failures in cybersecurity? Even if you are, this panel is for you. While not offering forgiveness, we are going to discuss the many changes in thinking and practice required to do "human factors" well in today's information environment. While it's easy to instill a blame culture, which is often reinforced through cybersecurity training, it is much harder to build resilence and help people become the backbone of secure organizations. This panel will address practical ways to combine education with technology and look to new trends to see what they might portend for us all.

October 26, 2022
14:15

Hindsight is 20/20

Jeremy Treadwell
COO, Treadwell Agency

"Hindsight is 20/20" is usually what most cyber leaders say after falling victim to an attack. As we all know, cybercrime is on the rise, and Cybersecurity Ventures estimates the annual economic toll to be approximately $6 trillion; by 2025.

Every organization has a cyber approach to ensure compliance with regulatory requirements, and most companies analyze attack vectors to strengthen critical that requires defense. Frequently these activities happen after an attack.

However, how do we look to the horizon to determine the future security needs of our systems, data, and information assets?

Foresight has a role in cybersecurity. It requires a long-term view of cyber risks, which requires organizations to adopt a strategic and proactive approach to managing them. In this talk, we will discuss practices that leverage scenario planning designed to help your organization develop robust strategies for building security-first cultures utilizing foresight.

Key Takeaways:

- Understand the art of foresight and how to see change
- Critical methodologies to leverage scenario planning with foresight
- Best ways to build cyber strategies of the future that drive security-driven cultures.

October 26, 2022
15:00

Authorization: The New Frontier of Identity-First Security for Data

Rich Dandliker
Chief Strategist, Veza

As organizations seek to continue down the zero trust journey by establishing effective, secure management of resources in the cloud and on-prem, authentication (i.e., who are you) and authorization (i.e., what can you do) are both mission-critical. To maximize workforce productivity, organizations need to provide streamlined, frictionless, user-friendly access to enterprise applications, data stores, and other resources. And to deliver secure, seamless digital experiences to customers —while protecting their privacy—companies need to provide a consistent access experience that makes sure customer data stays in the right hands. Hear from Rich Dandliker, Chief Strategist at Veza, about how organizations should be making the shift to identity-first security for data via the power of authorization.

October 26, 2022
15:30

Ready Set RUN – the New Offense is a Collective Defense!

Teri Williams
Brigadier General, Vice Director of Operations (CYBER), National Guard Bureau

America doesn't play defense very well when it comes to cyber security! A great defense is a collective defense. Brigadier General Williams will share her efforts in a holistic approach to cyber resiliency!

October 26, 2022
16:15

Summit Wrap Up and Take Away

Judy Hatchett
VP, CISO, Surescripts

Jeffrey Norem
Deputy CISO, Freddie Mac

Join Judy and Jeff as they review Summit highlights, share key take aways, and help define your call to action items to take back to your organization.