NINTH ANNUAL LEADERSHIP EVENT

CYBER SECURITY SUMMIT

Security solutions through collaboration.™

Pushing the CYBER SECURITY Envelope

CYBER SECURITY SUMMIT 2019

October 28–30, 2019 | Minneapolis, MN

FEATURED SPONSORS

TECHNOLOGICAL LEADERSHIP INSTITUTE

TARGET

UNISYS | Securing Your Tomorrow™

protocol46 cybersecurity

VERACODE

cisco

CYBERARK

MICRO FOCUS

MINNESOTA IT SERVICES

TECHNOLOGICAL LEADERSHIP INSTITUTE

The Master's Degree for

Security Technology Leaders

tli.umn.edu

Become a Security Leader & Shape Tomorrow's Future.

Acquire the skills necessary to prevent, protect and respond to today's security demands with an **M.S. in Security Technologies (MSST)** from the University of Minnesota's Technological Leadership Institute (TLI). Our proven curriculum, renowned faculty and alumni network will provide you with the expertise to lead. The numbers speak for themselves: Cybersecurity professionals are in peak demand across all industries to respond to evolving threats, prevent breaches and protect assets and private data.

>2.9M

Unfilled Cyber Security Jobs Across the Globe

Source: ISC^2

$2T

Estimated Cost of Cyber Crime in 2019

Source: Junpier Research

32%

Expected Job Growth Into 2028

Source: Bureau of Labor Statistics

Attend an information session to learn how MSST can transform your career:

Nov. 20 & Dec. 9 at 5:30 p.m.

Contact TLI admissions (tli-info@umn.edu or 612-624-5747) for details.

Thank You Sponsors + Exhibitors

Founding Partner

TECHNOLOGICAL LEADERSHIP INSTITUTE

Presenting Sponsor

TARGET

Printing Sponsor

UNISYS | Securing Your Tomorrow™

Platinum Sponsors

protocol46 cybersecurity

VERACODE

Diamond Sponsors

cisco

CYBERARK

MICRO FOCUS

Student Breakfast Sponsor

MINNESOTA IT SERVICES

Healthcare and Med Device

Host

MASLON

Sponsors

medcrypt

ARMIS

Small to Mid-size Businesses

Sponsors

BRIGGS

WELLS FARGO

Supporters

SBA U.S. Small Business Administration

AMERICA'S SBDC MINNESOTA

SCORE

Gold Sponsors

A10

CWT

FRSECURE

KPMG

KUDELSKI SECURITY

NaviLogic

netskope

proofpoint.

TEKsystems

Silver Sponsors

ATOMIC data.

Attivo NETWORKS

BACKBONE

Centrify ZERO TRUST PRIVILEGE

ControlCase

DIRSEC

Drexel UNIVERSITY

Fidelis Cybersecurity

Microsoft

ProcessBolt

RAPID7

RASMUSSEN COLLEGE

Secureworks

Synack

TANIUM

TIFFIN UNIVERSITY

VECTRA

VERODIN NOW PART OF FIREEYE

WHITE OAK SECURITY

Bronze Sponsors

Metropolitan State University

Symantec.

TrustedSec

WIPFLI

Conference Producer

the EVENT GROUP incorporated

Supporters

AAMI

BCPA

CSAMN Minnesota Chapter

FINANCE & COMMERCE

H-ISAC HEALTH-ISAC

ISACA

(ISC)² CHAPTER TWIN CITIES AREA

ISSA MINNESOTA CHAPTER

MDMA

MEDICAL ALLEY ASSOCIATION

mhta

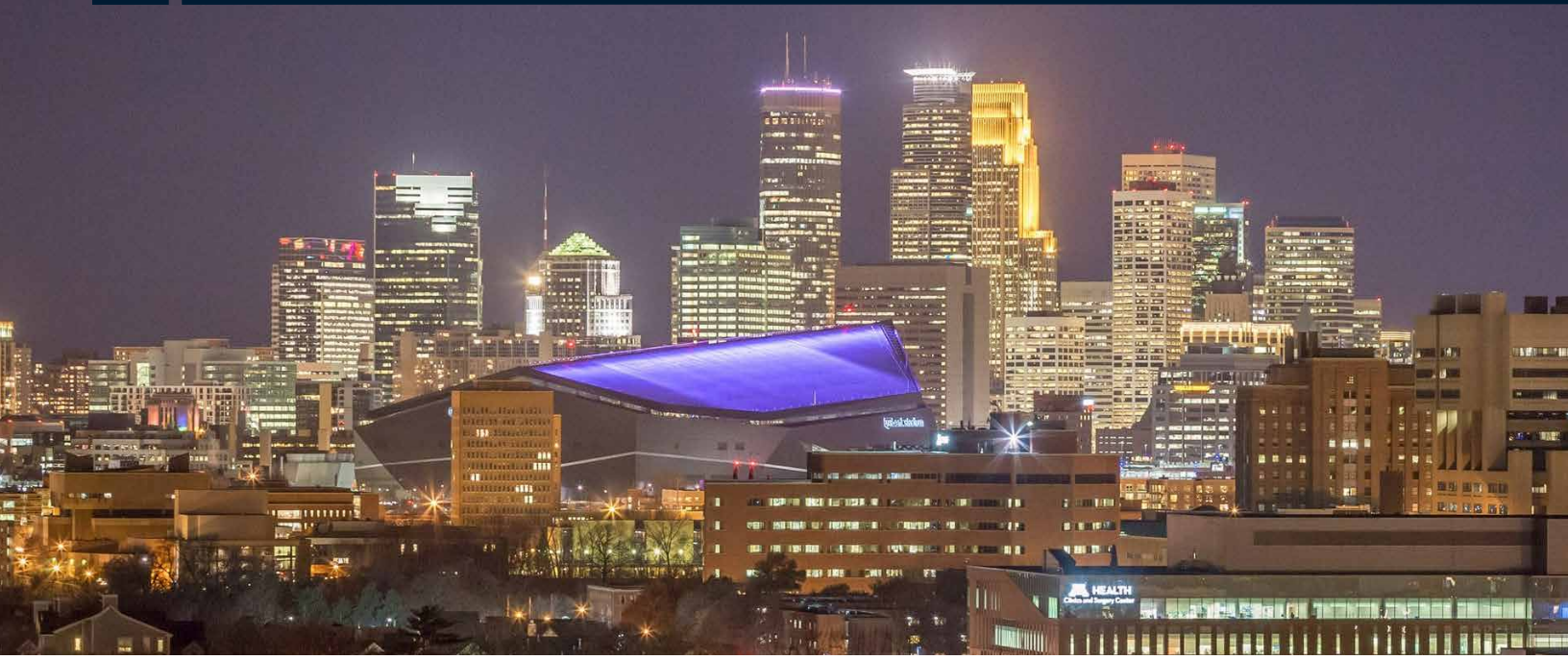
MINNESOTA LAWYER

as of 10.22.19

Maximize Your Exposure in 2020

The 2019 Cyber Security Summit would not have been possible without the efforts, commitment and expertise of all who were involved. Sign up to sponsor Cyber Security Summit 2020 today and receive a 10% discount through December 31, 2019.
For more information, contact our sponsorship sales consultants:

Companies (A-M) – Jennifer Churchill	763-548-1306	jennifer.churchill@eventshows.com
Companies (N-Z) – Stephen Burk	763-548-1303	stephen.burk@eventshows.com



Welcome to our Ninth Annual Cyber Security Summit

The Cyber Security Summit brings together people with different viewpoints on the cybersecurity problem to hear from experts, learn about trends and discuss actionable solutions.

Tim Crothers

2019 Co-Chair
Cyber Security Summit

Catharine Trebnick

2019 Co-Chair
Cyber Security Summit

Stefanie Horvath

2019 Program Chair
Cyber Security Summit

Eileen Manning

Executive Producer
Cyber Security Summit

Thank you for joining us for our 2019 Summit. We're delighted to see old friends and welcome new ones. Summit content evolves as fast as the attack vectors that confront us. We address the offensive onslaught head-on. Our theme is Pushing the Cyber Security Envelope. It speaks to embracing the challenge to do more than just respond to attacks. Now and for the future, we need to strive to get ahead of attacks.

This Summit has been fortunate to attract world cyber security thought leaders as speakers to share insider insights on the timeliest issues. We're thankful that so many luminaries invest their commitment to promote this Minnesota innovation hub. These leaders who serve in top posts in business, government and academics graciously help us recruit yet others to present emerging issues to you.

This ninth Summit again reflects a forward look at the state of cyber security. New this year are half-day sessions -- Women in Cyber Security, plus 16 Technical Tracks on Monday, Oct. 28, along with the third annual Healthcare and Medical Device Cyber Security event. There also are special sessions tailored to Small- and Mid-Size Business, students, CISOs, legislators, international attendees and more.

In the main two-day Summit, we present dynamic Keynote Speakers and a power-packed line-up of other specialized speakers and panels. To foster engagement and greatly simplified networking, we introduce a newly expanded version of Roundtable Discussions as part of Lunch Encounters on Tuesday, Oct. 29. Each Roundtable will display one of nine discussion topics and Moderators will be present to lead conversations. Enjoy lunch at a table with your chosen topic. We believe you will find this valuable.

Recognizing cyber security professionals is a Summit tradition. More of our peers became eligible for Visionary Leadership Awards last year since we opened categories representing additional vulnerability fronts. Cyber security people often work apart from others, supporting operational security, alone and unrecognized. It's fitting that we acknowledge their contributions here. We will award a field of eight deserving individuals and a special one-time award. If you haven't already signed up to attend this worthy event on Tuesday, Oct. 29, there are still a few seats available. Check at the registration table for information.

We bring Cyber Security Summit to you with the beneficial help of our Think Tank and vital support from our sponsors. Please visit our valued vendors to discover the resources available.

Please visit our sponsors and exhibitors, without their support the cost to provide this Summit registration would be tripled. By agreeing to have your badge scanned on-site at the Summit, you are agreeing to have your contact details provided to the sponsors who interacted with the attendee. The contact details will be used by said sponsors to follow up on such interactions.

Contents

Questions?

Find help from staff at the registration desk in the front of the expo hall.

Network: **cyber security summit**
Password: **css2019!**

Highlights

Continuing Education Credits

Summit participation fulfills up to 24 hours of continuing education credits, depending on organization and sessions you participate in.

Networking

Build relationships with delegates from around the U. S. and at least 8 countries throughout the world. Networking is even easier now. See Lunch Encounter Roundtable Discussions section, below.

Expo Reception

Join us Tuesday for cocktails and appetizers in the EXPO area and network with fellow attendees, industry thought leaders and our solution strategy partners.

Lunch Encounter Roundtable Discussions

Lunch tables are designated for specific topics and Moderators will be present to help move the discussions forward. A great way to join peers, share ideas and engage in low-key networking. Bring business cards to share and plan for an easy way to enhance your visit to Cyber Security Summit 2019.

Visionary Leadership Awards Dinner & Gala

Join us on Tuesday, Oct. 29 at 6:00 p.m. to help us recognize peers for their diligent performance and achievement of our high industry standards when we acknowledge some unsung heroes. If you don't have tickets yet, a remaining few are available. Check at the desk at your earliest opportunity.

Security Solutions Interviews

During the Summit, you may notice Keynotes and other experts being interviewed. After the Summit, podcasts of these interviews will be available at **cybersecuritysummit.org/2019-videos** to view and share with others in your organization. Video interviews are a way to gain more knowledge from the Summit.

2020 VIP All Access Pass Giveaway

Want a chance to win a free All-Access VIP Pass to Cyber Security Summit 2020? If you post real time comments about this Summit on Twitter, Facebook or LinkedIn you will be entered in the drawing. Blog on two sites for two chances to win! Blog on all three social media sites for three chances to win! Winner will be announced on Wednesday afternoon at the conclusion of this year's Summit. Good luck!

Post your comments about the Summit at **#cybersummitMN**

/cyber-security-summit /cssummit /cs_summit

SUMMIT CO-CHAIRS

Tim Crothers
Target

Catharine Trebnick
Dougherty & Company LLC

Jill Allison
Kudelski Security, Inc.

Massoud Amin
University of Minnesota

Anne Bader
The International Cybersecurity Dialogue

Bob Bassett
Centurylink

John Bonhage
InfraGard

Robert Booker
UnitedHealth Group

Andrew Borene
Symantec

Christopher Buse
Office of the Legislative Auditor

Sean Costigan
George C. Marshall Center

Loren Dealy Mahler
Dealy Mahler Strategies

Antonio Enriquez
U.S. Department of Homeland Security

Steen Fjalstad
Midwest Reliability Organization

Mary Frantz
Enterprise Knowledge Partners, LLC

Barb Fugate
United Bankers' Bank

Sam Grosby
Wells Fargo

Judy Hatchett
Fairview Health Services Information Technology

Stefanie Horvath
MNARG; Minnesota IT Services

Bob Hoschka
Computex Technology Solutions

Ken Hoyme
Boston Scientific

Brian Isle
Adventium Labs

Mike Johnson
TLI, University of Minnesota

Faisal Kaleem
Metropolitan State University

Mike Kearn
US Bank

David La Belle
NorSec Foundation

Michael Larson
EcoLab

Jack Lichtenstein
JDL Advisory, LLC

Eileen Manning
Cyber Security Summit

Emily Marier
Slumberland Furniture, Inc.

Tina Meeker
Shutterfly, Inc.

Harshal Mehta
CWT

Jerrod Montoya
OATI

David J. Notch
Medtronic

Patrick O'Brien
Deloitte

Gregory Ogdahl
MoneyGram

Kathy Orner
CWT

Mark Ritchie
Global MN

Frank Ross
General Mills

Tony Sager
Center for Internet Security

Phil Schenkenberg
Briggs and Morgan, P.A.

Melissa Seebeck
Delta Air Lines

Jeremy Swenson
Abstract Forward & Ameriprise

Wade VanGuilder
Symantec

Chris Veltsos
MN State University, Mankato

Aaron Verdell Call
MN.IT Services

Lee Ann Villella
FRSecure

Kathy Washenberger
Deluxe

Kristi Yauch
TCF Bank

2019 Committees

COMMITTEE MEETING HOSTS

Jill Allison Kudelski Security; Barb Fugate, United Bankers' Bank; Bob Hoschka, Computex; Michael Larson, ECOLAB; Emily Marier, Slumberland; Jerrod Montoya, OATI; Greg Ogdahl, MoneyGram; Frank Ross, General Mills; Catharine Trebnick, Dougherty.

GLOSSARY OF TERMS

David LaBelle, NorSec**.

HEALTHCARE/MED DEVICE

Ken Hoyme, Boston Scientific**; Allison Miller, United Health Group**; Robert Booker, UnitedHealth Group; Debra Bruemmer, Mayo Clinic; Todd Carpenter, Adventium Labs; Scott Erven, PWC; Judy Hatchett, Fairview Health Services Information Technology; Brian Isle, Adventium Labs and University of Minnesota Technological Institute; Eran Kahana, Maslon; Matthew Kirkwood, Smiths Medical; Daniel Lyons, Synopsys; Kevin McGrail, InfraShield; Vidya Murthy, Medcrypt; Matt Russo, Medtronic; Chris Tyberg, Abbott Leadership Institute, Adventium Labs; Technological Leadership Institute (TLI), University of Minnesota

INTERNATIONAL DINNER

Harshal Mehta, Carlson Wagonlit Travel**; Karen Andersen, Eide Bailey; Anne Bader, The International Cybersecurity Dialogue; Sean Costigan, ITL Security; Mark Ritchie, MN EXPO CEO; Frank Ross, General Mills; Natasha Shawver, University of Minnesota; Pekka Vepsalainen, Tikkasec Ltd.

PROGRAM & SPEAKER REVIEW

Stefanie Horvath, MNARG, Enterprise Services MN IT; Jill Allison, Kudeleski Security; Bob Bassett, CenturyLink; Tim Crothers, Target Corp.; Mary Frantz, Enterprise Knowledge Partners; Barb Fugate, United Bankers' Bank; Brian Isle, Adventium Labs; Mike Kearn, US Bank; David LaBelle, NorSec; Michael Larson, ECOLAB; Tina Meeker, Shutterfly; David Notch, Medtronic; Greg Ogdahl, MoneyGram; Melissa Seebeck, Delta Airlines; Catharine Trebnick, Dougherty; Kristi Yauch, TCF Bank;

REGISTRATION AMBASSADORS

John Bonhage, InfraGard; Barb Fugate, United Bankers' Bank; Bob Hoschka, Computex; Emily Marier, Slumberland Furniture; Greg Ogdahl, MoneyGram; Melissa Seebeck, Delta Airlines; Wade Van Guilder, Symantec; Lee Ann Villella, FR Secure; Kristi Yauch, TCF Bank.

*(**indicates committee chair)*

ROUNDTABLE DISCUSSIONS

Steen Fjalstad**, Midwest Reliability Organization; Massoud Amin, University of Minnesota; Sam Grosby, Wells Fargo; Brett Hebert, BRIGGS; Tim Herman, MBA Engineering; Brian Isle, Adventium Labs; Menno Kievoet, AMPF; Andrew King, Dougherty & Company; Cyrus Malek, BRIGGS; Emily Marier, Slumberland; Phil Schenkenberg, Briggs; Jeremy Swenson; Ameriprise; Paul Veeneman, MBA Engineering; Ted Wallerstedt, US Bank; Shari Ziebell, Spire Credit Union

SECURITY SOLUTIONS PODCASTS

Tina Meeker, Shutterfly, Inc.**; Bob Hoschka, COMPUTEX; Jen Churchill, The Event Group;

Participants for interviews: Centrify, Fidelis, Rasmussen, Synack, Tanium, Verodin, White Oak Security.

SMALL BUSINESS

Cyrus Malek, Briggs & Morgan, P.A.**; Eric Ebner, Protocol 46; Brett Herbert, Briggs & Morgan, P.A.; Twila Kennedy, U.S. Small Business Administration; Chuck Pellino, Wells Fargo; Deborah Salerna, SCORE; Lyle J. Wright, Minnesota Dept. of Employment & Economic Development.

SPONSORSHIP COMMITTEE

Jen Churchill, The Event Group**; Stephen Burk, The Event Group; Dave Notch, Medtronic. Harold Palmer, PreEmpt; Catharine Trebnick, Dougherty; Lee Ann Villella, FRSecure. Matthew Stellmacher, White Oak Security.

VISIONARY LEADERSHIP AWARDS

Chris Buse, Office of the Legislative Auditor, State of Minnesota**; Todd Carpenter, Adventium Labs; Jennifer Czaplewski, Target Corp.; Steen Fjalstad, Midwest Reliability Organization; Chrysa Freeman, Security Mindedness; Brian Isle, University of Minnesota Technical Leadership Institute & Adventium Labs; Eileen Manning, Cyber Security Summit.

WOMEN IN CYBERSECURITY

Tina Meeker, Shutterfly**; Jill Allison, Kudelski Security; Brenda Bjerke; Target; Sam Crosby, Wells Fargo; Jen Czaplewski, Target; Loren Dealy Mahler, Dealy Mahler Strategies; Chrysa Freeman, Code 42; Barb Fugate, United Bankers' Bank; Sam Grosby, Wells Fargo; Jadee Hanson, Code 42; Judy Hatchett, Fairview Health Services; Stefanie Horvath, MNARG, Enterprise Services MN IT; Eileen Manning, Event Group; Emily Marier, Slumberland Furniture; Allison Miller, Optum; Melissa Seebeck, Delta Airlines; Catharine Trebnick, Dougherty; Lee Ann Villella, FR Secure; Kathy Washenberger, Deluxe Corp.; Kristi Yauch, TCF Bank.

Specialty Events

VIP Reception
Monday, Oct. 28 @ 5:00 PM

Ticketed Event

International Dinner
Monday, Oct. 28 @ 6:30 PM

sponsored by CWT

All Students Welcome

Student Breakfast
Tuesday, Oct. 29 @ 7:00 AM

sponsored by MINNESOTA IT SERVICES

All Welcome

Roundtable Luncheon
Tuesday, Oct. 29 @ 11:45 AM

Invite Only

CISO Luncheon
Tuesday, Oct. 29 @ 11:45 AM

sponsored by MICRO FOCUS

Ticketed Event

Visionary Leadership Award Dinner
Tuesday, Oct. 29 @ 6:00 PM

All Welcome

FBI Breakfast
Wednesday, Oct. 30 @7:15 AM

Invite Only

Legislative Briefing
Wednesday, Oct. 30 @ 12:00 PM

ROOM 101 D

Women in Cyber Security

Monday, October 28 | 9:00 AM–1:00 PM

The Line-Up: Get the inside story on how to launch and navigate a rewarding career in the male-dominated cyber security field. Women experts in the field will lead discussions on career navigation, strategies and challenges followed by a special networking luncheon.

Agenda

9:00–9:15 AM Opening Remarks

Tina Meeker, Shutterfly, Inc.; Steve Aleckson, TEKsystems

9:15–10:00 AM The many (and sometimes hidden) paths to and within cyber

Moderator: Elizabeth Stevens, InfraGard MN Alliance

Panelists: Betty Elliott, Mercer; Judy Hatchett, Fairview Health Services Information Technology; Melissa Seebeck, Delta Air Lines

10:00–10:45 AM Career Goals for everyone! CISOs, Entrepreneurs and Everything in Between

Moderator: Brigadier General Stefanie Horvath, Minnesota IT Services

Panelists: Sahar Ismail, Legacy Armour; Milinda Rambel Stone, Provation Medical

10:45–11:30 AM Being a woman in Cyber isn't always a breeze. Hear from Cyber leaders as they share their stories and strategies

Moderator: Tina Meeker, Shutterfly, Inc.

Panelists: Jill Allison, Kudelski Security, Inc.; Sarah Engstrom, CHS, Inc.; Christine Stevenson, Verodin

Women in Cyber Security Networking Lunch

11:45 AM–1:00 PM

State Senator Melissa Wicklund (DFL-Bloomington) will speak at this special networking event for women attending the Summit.

Sponsor TEKsystems

Want a voice in this conversation?
You're invited to join the 2020 planning team. To help shape future Women in Cyber Security events, email Denise.Wald@eventshows.com.

- Manage Risk
- Increased Understanding
- Increased Productivity
- Decrease Costs

Cybersecurity shouldn't be just another technology that sits in a rack costing you money. It should add value across your entire business.

That means your cybersecurity provider can't be just another vendor collecting a check. They need to be a true business partner to you and help you make better fact-based decisions leading to reduced overall cyber risk, increased compliance and enhanced information security allowing you to build lasting, trusted relationships with the clients you share confidential and regulated data with.

>> Discover what a real cybersecurity partner can do for your business_

>> For information call 844.663.8927
or visit www.protocol46.com/css _

protocol46™ cybersecurity

ROOM 101 D

MedDevs + Health Delivery Orgs + Regulators Gather to Collaborate on Device Security and Safety

Monday, October 28 | 1:00–5:30 PM

Minnesota, and the Twin Cities in particular, are the focal point of Medical Device innovation in North America. As such, our state is home to a high concentration of device manufacturers, healthcare deliverers and regulators. In 2016 we added the first half-day Medical Device session in conjunction with Cyber Security Summit to gauge interest among these stakeholders about getting together annually in a non-regulatory setting to share concerns and collaborate on the issues of security and safety of medical devices. This gathering has achieved unqualified success and we're pleased to continue hosting this dynamic session.

CyberBytes™

Moderated by Ken Hoyme of Boston Scientific and Allison Miller of Optum. Topics covered during this session:

Anatomy of a Medical Device Attack
Jay Radcliffe, Thermo Fisher Scientific

Medical Device Attack Scenarios
Sarah Jopp, Mayo Clinic

How to Make Your Organization Resilient to Attacks on Medical Devices
Damin Barnier and Richard Scott, Optum

24h of a Medical Device Security Disaster
Adam Brand, PwC

How to Use MDS2 Form to Drive Design Decisions
Anita Finnegan, Nova Leah

Agentless Device Security for the Healthcare Industry
Jack Marsal, Armis

How to Make Your Medical Device Secure
Mike Kijewski, MedCrypt

Medical Device Security Logging: The Apache Software Foundation & Time Series Databases
Kevin McGrail, InfraShield

Must-Have Security Contract Language
Eran Kahana, Maslon

Host

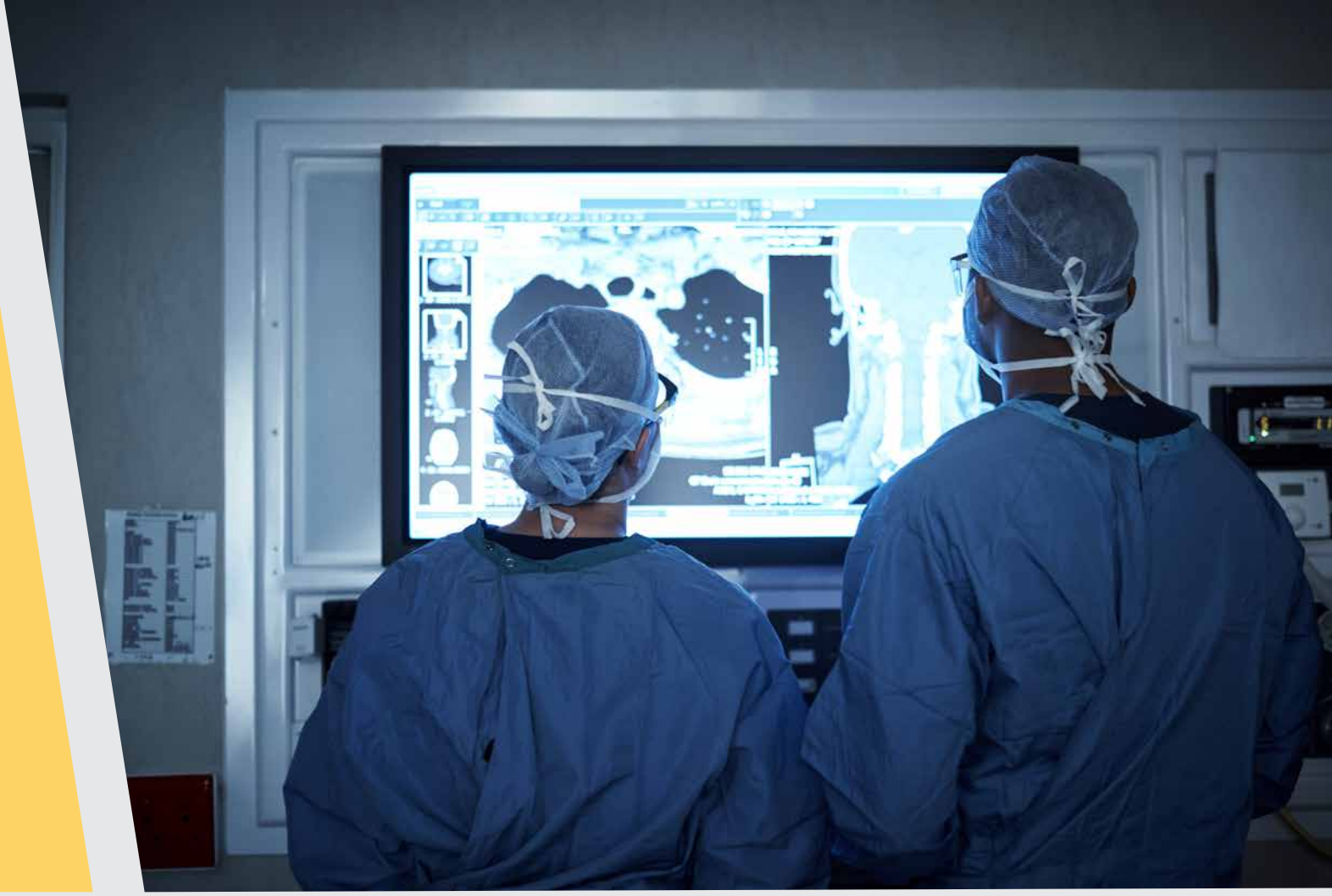
MASLON

Sponsors

medcrypt ARMIS

Supporters

AAMI H-ISAC HEALTH - ISAC MEDICAL ALLEY ASSOCIATION MDMA



AN OUNCE OF PREVENTION...

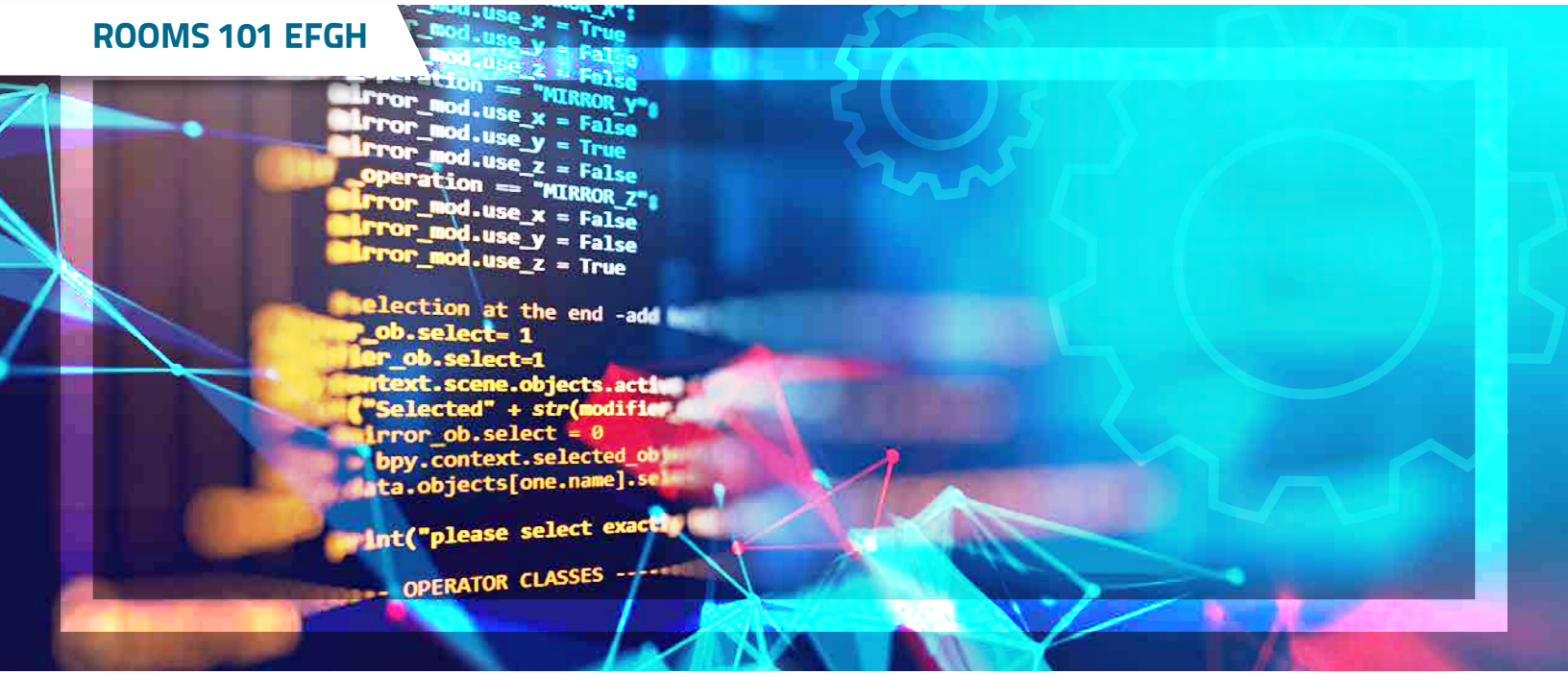
Protecting your sensitive data in a world of increasing threat is no easy operation. Skilled legal counsel is critical to both diagnosing and reducing risk.

Maslon has extensive experience advising medical device and healthcare clients on effective data security practices and privacy law. We're dedicated to helping our clients avoid unnecessary complications.

MASLON LLP
612.672.8200
MASLON.COM

MASLON

ROOMS 101 EFGH



Technical Tracks | Monday, October 28

TECH TRACK ONE / 1:10–2:00 PM

TECHNICAL TRACK 1-A / ROOM 101 E

Blocks and Chains: Realities of Digital Ledgers in Enterprise Security

This presentation will discuss the impact of Blockchain, or digital ledgers, on the enterprise. After the crypto currency crash, has blockchain failed to meet expectations? What should security be focused on.

Michael Anton, Kudelski Security

TECHNICAL TRACK 1-B / ROOM 101 F

Protecting Customers from Themselves

The cyber threat landscape is expanding with trojan and fishing initiated ransomware and malware attackers. Attackers continuously leveraging new attack vectors and rendering our defenses ineffective. The 'Zero Trust" security model looks like a promising solution to mitigate some threats, but rolling it out will be challenging as various dependencies have to be satisfied. To protect ourselves from the ever evolving attack surface, we need to be aware of the current challenges as well as the defensive technologies and approaches that will help us counter threats effectively and efficiently.

Yasir Liaqatullah, a10

TECHNICAL TRACK 1-C / ROOM 101 G

Tackling the Talent Shortage Problem: An Honest Look At Challenges Related To Finding and Retaining Information Security Talent

It's a fact, there aren't enough of us to go around. The unemployment rate is already at 0%, and the future looks bleak for people in need of information security talent. Luckily, the industry is filled with people and organizations willing and able to do something about it. In this session, Evan Francen, CEO and founder of FRSecure gives a look at what it takes to build a good security analyst from the ground up: the foundational skills necessary for someone to break into the security industry, how technical-focused employees and non-technical employees develop successfully within the security industry, and what roles and skills should a CISO have in all of this.

Evan Francen, FRSecure

TECHNICAL TRACK 1-D / ROOM 101 H

Cyber Range for Technical Staff

Join others on a cybersecurity range as a blue team member to protect the range network and systems. This session will put you in the hot seat to learn new tactics and techniques as well as new technology that can make the whole process easier and more efficient. A read-ahead packet will be sent out in advance to help ensure you are orientated to the range prior to attending.

Eric Ebner, Protocol 46

TECH TRACK TWO / 2:10–3:00 PM

TECHNICAL TRACK 2-A / ROOM 101 E

Developing Compliant Patterns for Modern Technologies

This session will articulate the method by which any IT Security organization, regardless of size, can develop compliant patterns for modern technologies. We will discuss overall strategy and walk through 3 real-world examples where teams worked this strategy, overcame various challenges, and delivered repeatable solutions.

Stephen Podobinski, Target

TECHNICAL TRACK 2-B / ROOM 101 F

Secure Midnight Developer (DevSecOps) Evolution of Application Security & OWASP SAMM

This presentation will include practical suggestions aimed at increasing ability to measure, manage, and improve Information Security Programs, while forming stronger relationships with product owners and developers. Presentation It will cover what everyone can expect out of OWASP SAMM 2.0 and what we can all do to help make SAMM 2.0 more helpful and relevant in the future.

Yan Kravchenko, Concord USA

TECHNICAL TRACK 2-C / ROOM 101 G
Using Deception To Close Your Detection Gaps
This session will address how deception technology creates a fabric across the entire enterprise to close detection gaps, provide internal visibility, help meet compliance requirements, and defend against in-network attackers.
Joseph Salazar, Attivo Networks

TECHNICAL TRACK 2-D / ROOM 101 H
Cyber Range for Management
Join others to take part in a cybersecurity response table-top exercise to protect and defend a network. This session does not require technical experience as it works the process in a team environment. As a member of the defense team, you will experience the processes and techniques that are used to protect a network and then see how new technology can make the whole process easier and more efficient.
Eric Ebner, Protocol 46

TECH TRACK THREE / 3:10–4:00 PM

TECHNICAL TRACK 3-A / ROOM 101 E
Your Security Controls are Failing and You Don't Know It
Most of us base our security on assumptions. We assume our security tools, people and processes are working, vendor default configurations are right for us, if something was working before it's still working now, and ongoing configuration changes are accurate. The sad truth is, we've been doing security wrong for so long that it feels right, but statistically, more is broken than working.
Christine Stevenson, Verodin

TECHNICAL TRACK 3-B / ROOM 101 F
The Future SOC: How Machine Learning and Crowd-Powered Big Data is Transforming Security
Data science applied to vendor-independent data, multi-device telemetry, and world-class threat intelligence is rapidly transforming the future of security operations. By pairing machine and human intelligence, organizations with limited resources can now detect and respond to unknown threats faster and with unprecedented accuracy. In an industry forever locked in an adversarial battle with increasingly sophisticated actors, this presentation will explore how to apply the right machine learning and deep learning techniques to the right data and threat intelligence to outpace and outmaneuver adversaries.
Aaron Hackworth, Secureworks

TECHNICAL TRACK 3-C / ROOM 101 G
Understanding Third-Party Risk in the Cloud
Abstract: No matter how strong your organization's security strategy is, your cloud data is likely most at risk via your third-party cloud applications. These apps are often much more susceptible to hackers than other parts of your security perimeter. Your organization is likely using hundreds of these third-party cloud apps, like Slack and Office 365, which means there are hundreds of opportunities for threats to find their way in. You may not even know that sensitive assets in the cloud are vulnerable through these apps either. This is where an understanding of third-party risk is imperative for every organization's security team.This session examines the best ways to mitigate third party risk.
Damian Chung, Netskope

TECHNICAL TRACK 3-D / ROOM 101 H
Cyber Range for Technical Staff
Join others on a cybersecurity range as a blue team member to protect the range network and systems. This session will put you in the hot seat to learn new tactics and techniques as well as new technology that can make the whole process easier and more efficient. A read-ahead packet will be sent out in advance to help ensure you are orientated to the range prior to attending.
Eric Ebner, Protocol 46

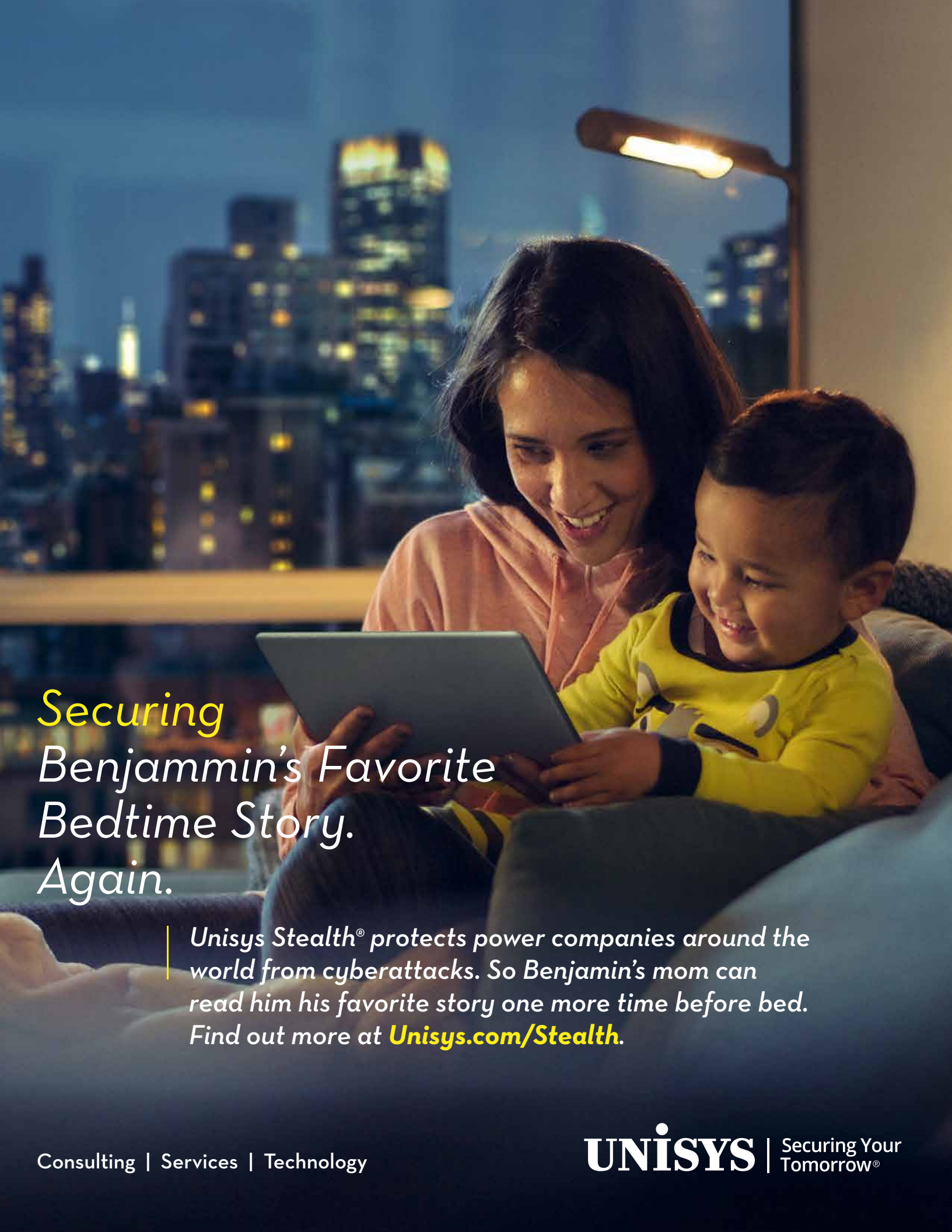
TECH TRACK FOUR / 4:10–5:00 PM

TECHNICAL TRACK 4-A / ROOM 101 E
Zero Trust, CARTA, IoT, CJIS, CSF – OMG, How Can I Address All of These?
You may have heard all of these as buzz words but why are they important and how can you address them with limited time and resources? This engaging session provides an overview to guide agencies protecting against modern cybersecurity threats. It shows how a modern information platform can enable Cyber Security Excellence without busting the budget or throwing out your current investment. Excellence means finding a way both efficiently and effectively to manage cyber risks. Asking the right questions focuses investments in the security controls that matter most and defending critical systems and sensitive information despite persistent threats, ongoing talent shortages, and ever-present budget constraints. This session shows how networks and security tools can be automated for security professionals so they can focus on enhancements to improve overall cyber posture --key topics for security today.
Peter Romness, CISCO

TECHNICAL TRACK 4-B / ROOM 101 F
Incorporating Security Intelligence and Automation Into Digital Transformation
This session will focus on the experiences Microsoft is seeing with organizations embarking on digital transformation journeys. We will discuss overall tactics and solutions organizations are able to incorporate to enable intelligence and automation of cyber security by taking advantage of cloud native solutions.
Chris Raschke, Microsoft

TECHNICAL TRACK 4-C / ROOM 101 G
Dividing by Zero: Establishing Privileged Access Security for Null-Trusted Humans and Robots
In this talk, we'll look at the evolution of the zero-trust security model and how the move to more automation and distribution has lead to challenges related to powerful access for traditional and Cloud environments. Along with a migration to modern environments, there's an ever increasing number of very low trust entities like vendors and applications that are being given greater levels to access. In addition to a number of easily repeatable keyboard attack scenarios that take advantage of a perimeter-less state, we'll share tips to help reduce the attack surface, increase operational efficiencies around remote access, and supplement other zero trust controls by securing the privileged organic and inorganic secrets that allow access into modern environments.
Brandon Traffanstedt, CyberArk

TECHNICAL TRACK 4-D / ROOM 101 H
Cyber Range for Management
Join others to take part in a cybersecurity response table-top exercise to protect and defend a network. This session does not require technical experience as it works the process in a team environment. As a member of the defense team, you will experience the processes and techniques that are used to protect a network and then see how new technology can make the whole process easier and more efficient.
Eric Ebner, Protocol 46


Securing
Benjammin's Favorite
Bedtime Story.
Again.
Unisys Stealth® protects power companies around the world from cyberattacks. So Benjamin's mom can read him his favorite story one more time before bed. Find out more at Unisys.com/Stealth.
Consulting | Services | Technology
UNISYS | Securing Your Tomorrow®

ROOM 102 A

Cyber Security Plan Basics to Protect Small to Mid-Size Businesses

Tuesday, October 29 | 1:00–6:00 PM

Hackers target small to mid-size businesses as low-hanging fruit. Business owners need a plan to leverage practices to protect assets. Build the foundation for cyber security strategy to protect your company's Reputation, Financial Well-Being and Intellectual Property — in short, your livelihood. Learn how to protect yourself, your customers and your assets in a powerful afternoon with top Cyber Security thought leaders to give you knowledge for developing technical, legal and financial aspects of a cyber security plan for your business.

Cyber Risk Awareness Training Agenda

1:00-1:30 PM Why a Cyber Security Strategy is critical to small and mid-size businesses and the impact it can have
Eileen Manning, Cyber Security Summit; Nancy Libersky, U.S. Small Business Administration

1:30-2:00 PM No Longer 'Nice to Have" — Privacy and Security is the Law
Cyrus C. Malek and Brett Hebert, BRIGGS

2:00-2:40 PM Small Business Big Threat — Why Hackers Love Businesses Like Yours
Eric Ebner, Protocol 46

2:45-3:15 PM Resource Break in EXPO

3:15-4:00 PM Third Party Risk Management for Small Business
Chuck Pellino, Wells Fargo

4:00-4:30 PM How the Government is Helping Small to Mid-Sized Businesses Build a Defense
Christopher Gabbard, Region V: Minnesota

4:30-4:50 PM Q&A Panel
Moderator: Cyrus C. Malek, BRIGGS; Panelists: Brett Hebert, BRIGGS; Eric Ebner, Protocol 46; Chuck Pellino, Wells Fargo; Christopher Gabbard, Region V: Minnesota

4:50-5:00 PM Session Takeaways
Cyrus C. Malek, Briggs and Morgan, Professional Association

5:00-6:00 PM Reception in Resource Center

Sponsors BRIGGS protocol46 cybersecurity WELLS FARGO

Co-marketers SBA U.S. Small Business Administration AMERICA'S SBDC MINNESOTA SCORE

Monday, October 28

9:00 AM–1:00 PM	**Women in Cyber Security** — See page 8 for details
11:45 AM–1:00 PM	**Women in Cyber Security Networking Lunch** — See page 8 for details
1:00–5:30 PM	**HealthCare & Med Device** — See page 10 for details
1:10–5:00 PM	**Technical Tracks** — See page 12 for details
5:00–6:15 PM Seasons, 2nd Floor	**VIP Reception** (Ticketed Event)
6:15–8:30 PM Lounge A, 2nd Floor	**International Dinner** (Ticketed Event) *Harshal Mehta, CWT; Dr. Massoud Amin, UofMN; Kathy Orner, CWT; Sean Costigan, ITL Security; Mark Ritchie, Global MN*

Tuesday, October 29

7:00 AM–8:00 AM Ballroom B	**EXPO Breakfast** Summit breakfast in EXPO area. And, while you're at it, scan business enhancements available to your company from the offerings of our leading show vendors.
7:00 AM–8:00 AM Seasons, 2nd Floor	**Student Breakfast (Invitation Only)** Head of cyber security for the State of Minnesota presents timely advice and career-shaping insights for future cyber security professionals. Feed yourself, and your aspirations. A great investment in your future! // *Aaron Verdell Call, MN.IT Services*
8:00 AM–8:45 AM Ballroom	**Welcome & Opening Remarks** This year's theme is 'Pushing the Cyber Security Envelope." The theme was selected to emphasize the importance of leading security versus just trying to stay current for both industry and government and the role each must play in securing our future. *Eileen Manning, Cyber Security Summit; Mike Johnson, TLI, University of Minnesota; Tim Crothers, Target; Catharine Trebnick, Dougherty & Company LLC*
8:45 AM–9:15 AM Ballroom	**Keynote: Pushing the Cyber Security Envelope** Information security has many components that rely not only on its success but the business. Each program designed to handle multiple risks and threats towards the organization and one that takes years for maturing. Most of our programs aren't designed to even handle the basic threats of attackers, let alone advanced adversaries. This talk will dive into the top five areas of importance within an information security program and what is critical in order to push the security envelope forward. In this presentation it'll be a mix of technical concepts as well as program building for a blended program that is designed to threat model risks towards your organization and build a solidified program. We can do this together, and focusing on critical elements around our program can make us successful against tomorrows threats. *David Kennedy, TrustedSec*
9:15 AM–9:45 AM Ballroom	**Discussion: Government Taking Action to Secure the Cyber Domain** This discussion will examine government taking action to promote alliance in cybersecurity. Government is taking action with public and private partnerships to improve information sharing and leverage resources against cybersecurity attacks in multiple critical infrastructure sectors. The discussion addresses explicit examples where Government is taking actions to bolster cybersecurity. *Steen Fjalstad, Midwest Reliability Organization; John Tuma, Minnesota Public Utilities Commission*
9:45 AM–10:15 AM	**Own IT. Secure IT. Protect IT.** As we close out National Cybersecurity Awareness Month, the Director of the Cybersecurity and Infrastructure Security Agency will discuss how his agency is bringing together all levels of government, the private sector, international partners, and the public to strengthen resilience and security of our Nation's critical infrastructure. *Christopher Krebs, Cybersecurity and Infrastructure Security Agency (CISA)*
10:15 AM–10:45 AM Ballroom B	**EXPO Break** Enjoy a light snack and network to establish new professional relationships.

10:45 AM–11:45 AM 102 A	**Management Breakout: Forward Looking View of Cyber Risk** As organizations mature their security programs, identifying vulnerabilities is no longer sufficient.Understanding risk is critical to mature programs and vulnerabilities do not exist in a vacuum - context is key. Presenters discuss how to incorporate practical testing into your deep-dive pentesting process, resulting in more relevant and actionable results. *Kristi Yauch, TCF Bank; Christopher Emerson, White Oak Security*
10:45 AM–11:45 AM Ballroom	**Tech Breakout: Weaponization of Social Media** Review of increase in cyberattacks, and level of sophistication, as social media manipulates human behavior to ignite harmful attacks on individuals and Enterprise network. Includes description of how social media apps are used to steal credentials, followed by demonstration of how apps take and use data. Also covers how to mitigate cyberattacks through user training and the development of specific policies on internet blocking and mobile device management. *Mary Frantz, Enterprise Knowledge Partners, LLC*
11:45 AM–1:15 PM Ballroom AB	**Luncheon Roundtable Discussions & EXPO** Roundtable discussions gather together by topics of interest. Sessions facilitated by Summit Co-Marketing Partners. Time to visit with Solution Providers in EXPO Hall. *Steen Fjalstad, Midwest Reliability Organization*
11:45 AM–1:15 PM Seasons, 2nd Floor	**CISO Lunch: Best Practices for Cyber-risk Reporting and Board Communications** (Invitation Only) According to NACD research, 97% of public companies and 94% of private companies are increasing cybersecurity oversight this year. Our panel discussion will highlight perspectives from leading CISOs on strategies for effective Board communication and aligning security with the changing needs of the organization. CISOs from leading enterprises will share best practices in dialogue with Directors from public and private companies. Highlights include: · Cyber business management implications of people, processes and technology investment. · Cybersecurity strategy visualization, communication and execution. · Cyber-risk reporting and establishing trust and credibility between Security leadership and the Board, and · Information sharing across and within industry sectors. *Michael Gutsche, MicroFocus; Sherry Smith, Piper Jaffray, John Deere; John Hellickson, Kudelski Security; David J. Notch, Medtronic; Jerrod Montoya, OATI*
1:00 PM–6:00 PM **102 A**	**Small Business Track** Everyone is a target for cybercrime, but not every business has a dedicated Chief Information Security Officer and team of security professionals to tackle the problem. That doesn't mean you are defenseless or that you can neglect to do your due diligence. You will come away with actionable information that you can use in your businesses to prevent attacks, mitigate losses, and recover after an incident. Target audience is small to mid-size business CEOs, HR Directors, IT staff and legal advisors. Session includes access to the latest solution strategy resources in the EXPO Hall *Eileen Manning, Cyber Security Summit; Nancy Libersky, U.S. Small Business Administration (SBA); Cyrus Malek, BRIGGS; Brett Hebert, BRIGGS; Eric Ebner, Protocol 46; Charles Pellino, Wells Fargo; Christopher Gabbard, CISA*
1:15 PM–1:45 PM Ballroom	**CyberByte™: Network Security Strategy** Zero Trust Architecture defined and a time traveling overview of restricting trust using the network from 1990 to 2019. As an engineer and implementer, Sam will speak from experience about what worked, what didn't, and whether Zero Trust is a reasonable goal. *Sam Grosby, Wells Fargo*
1:45 PM–2:45 PM Ballroom	**Panel: Zero Trust as the New Network Security Strategy** Hype or new security enforcement model. Zero trust is a security-centered model with no network boundaries enforcing additional authentication on all network requests. Does zero trust truly build better anomaly detection and accelerated response to thwart attacks or is it a great concept but impractical to implement? This panel will deliberate on the usefulness or uselessness of Zero Trust, myths and implementation lessons. *Moderator: Mike Kearn, US Bank; Panelists: Sam Grosby, Wells Fargo; Chris Hawley, Unisys; Peter Romness, CISCO*
2:45 PM–3:15 PM Ballroom B	**EXPO Break** Join your peers for conversation and enjoy a light snack.
3:15 PM–3:45 PM Ballroom	**CyberByte: Reasonable Information Security Standards** What constitutes reasonable information security standards? It depends on who's asking, and you won't find a definitive answer in a rule or regulation. How will government regulators consider this question? What about Boards of Directors? The public? Who can you look to for advice and evaluation? *Carter Leuty, Target*
3:45 PM–4:45 PM Ballroom	**Panel: Reasonable Information Security Standards** Legal Requirements, Practical Considerations for Information Security Professionals and Objective Evaluation will be addressed by the Reasonable Information Security Standards panelists. *Moderator: Carter Leuty, Target; Panelists: Brad Maiorino, Thomson Reuters; Andrew Serwin, DLA Piper; Brian Levine, US Department of Justice; Sai Gadia, KPMG LLP*

4:45 PM–5:00 PM Ballroom	**Closing Takeaways** *Tim Crothers, Target; Catharine Trebnick, Dougherty & Company LLC*
5:00 PM–6:00 PM Ballroom B	**Networking Reception in EXPO** Join us for cocktails and appetizers in the EXPO area where you network with fellow attendees our solution strategy partners.
6:00 PM–8:00 PM Seasons, 2nd Floor	**Visionary Leadership Awards Dinner** (Ticketed Event) Gather with Cyber Security leaders to recognize the 2019 Visionary Leadership Award winners. The Summit has given awards to top leaders in industry, government and academia since 2015. Along with recognition for their accomplishments, award recipients will get a brief opportunity to share their innovative strategies with other visionaries at our annual gala event. *Kathy Orner, CWT; Christopher Buse, Office of the Legislative Auditor*

Wednesday, October 30

7:15 AM–8:00 AM Seasons, 2nd Floor	**Breakfast: Consider a Career with the FBI** Have you ever considered a career with the FBI? Join us for this special breakfast during the 2019 Cyber Security Summit. Representatives from the Bureau will be on hand to speak about the application process, IT, cyber and tech careers in the FBI. They will also take any questions people have. *Stephanie Cassioppi, FBI*
7:15 AM–8:00 AM Ballroom B	**EXPO Breakfast** Summit breakfast in EXPO area. And, while you're at it, scan business enhancements available to your company from the offerings of our solution strategy partners.
8:00 AM–8:30 AM Ballroom	**CyberByte®: AI Machine Learning** How do we sort through the hype and realize the benefits gained from machine learning? AI has potential for evolving antivirus defense and malware scanning but what are the realistic barriers and concerns to investing in AI-centric cybersecurity solutions? *Simon Crosby, SWIM A*
8:30 AM–9:15 AM Ballroom	**Panel: Human vs. Machine** Panel's insightful discussion helps inform the attendee audience on the practical use (and affordability) of current AI/ML solutions. We know historically that investments into tools does not ensure security for network data. The Summit has spent nearly a decade creating a platform for people to hear from top security leaders in order to solve the increasingly complex problem of cyber security. *Moderator: Simon Crosby, SWIM A; Panelists: Josh Cutler, Optum; Eric Lengvenis, Wells Fargo; Dave Diehl, Crowdstrike*
9:15 AM–10:00 AM Ballroom	**Authenticating Service-to-Service Communications in a Multi-Cloud World** Securing network traffic that traverses multiple software stacks and platforms is challenging. Difficulties involving platform-aware applications, supporting multiple authentication schemes, and maintaining complex authorization logic are all commonplace, despite the fact that we'd really rather avoid these things. SPIFFE provides a platform-agnostic identity layer that can be used to authenticate and secure workload communication regardless of where the workload lives. AWS, Azure, and on-prem? Ok! Kubernetes, Mesos, and bare metal? No problem! SPIFFE allows you to mix and match without the need to worry about how workloads within them will securely communicate with each other. In this talk, we will explain how to leverage SPIFFE (and SPIRE) to automatically issue SPIFFE identities across disparate orchestrators and platforms, allowing for seamless authentication of systems within and between *Sunil James, Scytale.io*
10:00 AM–10:30 AM Ballroom B	**EXPO Break** Get the full benefit of the Summit. Enjoy a snack and network with your peers. New connections bring enhanced opportunities.
10:30 AM–11:15 AM Ballroom	**Building Innovation into Cyber Security** Cyber professionals can capitalize on breakthrough technology innovations to reduce cyber risk. This presentation offers strategies to cut through the marketing hype to seek out the right game-changing technologies for an organization - engaging with cyber start-ups, building valuable relationships with venture capital firms, innovation testing and Proofs of Concept, and realizing the control strength and risk reduction opportunities of innovations technologies. *Karl Mattson, City National Bank*

11:15 AM–12:00 PM Ballroom	**Capturing and Convicting The Bayrob Group: What You Need To Know About Working With Law Enforcement** The Bayrob Group was a group of Romanian hackers that developed their own malware which they used to create a botnet of more than 400,000 computers, and to steal millions of dollars and reams of PII. As a result of the Bayrob Group's sophisticated techniques to conceal their identity, it took law enforcement more than ten years to identify them and to obtain enough evidence to indict the group and extradite them from Romania. This past year, the leaders of the Bayrob Group were tried in the U.S. District Court for the Northern District of Ohio and convicted of all 21 counts of the indictment. Learn how the private sector provided invaluable assistance that led to the capture and conviction of the Bayrob Group and what you should know about how to effectively help the government fight cybercrime. *Brian Levine, US Department of Justice*
12:00 PM–1:15 PM Ballroom	**Lunch & EXPO** EXPO Drawing at 1:00 PM
12:00 PM–1:30 PM Seasons, 2nd Floor	**Legislative Briefing** (Invitation Only) Conversation with the Nation's Counterintelligence and Security Director. In this private closed door session, Director Evanina will provide a deep dive on the threat China poses to American businesses and other timely concerns. Session is invitation only, no substitutions. *William Evanina, National Counterintelligence and Security Center*
1:15 PM–2:00 PM Ballroom	**Cyber Risk Management Strategy** This presentation demonstrates the power of metrics in influencing leadership and organizational change around cyber risk. Session presenters will review in detail the data used to build the metrics and communication techniques to present a data infused presentation that accurately portrays the variables important to cyber risk management. *Jennifer Czaplewski, Target*
2:00 PM–2:40 PM Ballroom	**The China Threat and American Business** National Counterintelligence and Security *William Evanina, National Counterintelligence and Security Center*
2:40 PM–3:00 PM Ballroom	**Break**
3:00 PM–3:40 PM Ballroom	**Panel: Too Many Tools, Technology Rationalization** From cyber alert fatigue to increasing regulation to expanding cyber attack landscape, the proliferation of tools knows no-bounds creating an ice cream head ache for too few cyber security professionals to learn and administer. How can info security professionals stay frosty for what is most important using the tools that best help pull out the important signal in a cacophony of cyber noise. *Moderator: Catharine Trebnick, Dougherty & Company LLC; Panelists: Robert Booker, UnitedHealth Group; Chris Eng, Veracode; Eric Sorenson, VMware Carbon Black*
3:40 PM–4:10 PM Ballroom	**CyberByte® Data Breach Investigation Report 2019** VDBIR has been a long-standing surveyor of past incidents that eloquently and often times sarcastically (thankfully) point to the way ahead. What is looming in the 2019 as a prequel to TC's closing on strategy to secure tomorrow. *Brigadier General Stefanie Horvath, MNARG; Minnesota IT Services*
4:10 PM–4:40 PM Ballroom	**Closing Keynote: Strategy to Secure Tomorrow: The Future is Now** At this point the need for Cyber Security has become a cliché. In the last three days you've seen a mix of cutting-edge approaches and hard challenges in front of us. It's easy to become inured to the demands of defending our organizations and miss pivotal changes. Often, the pace of the work keeps us focused on very tactical approaches to cyber security. In this talk we'll discuss the role strategy plays in getting us out of the firefighting and approaches for moving into an intentional approach to cyber security rather than a reactive one. *Tim Crothers, Target*
4:40 PM–5:00 PM Ballroom	**Wrap Up & Practical Takeaways** Our distinguished Event Co-Chairs briefly revisit insights and action steps presented over the past three days by colleagues and collaborators, the accomplished thought leaders who have presented here at CSS19. These snippets will help remind you of ideas to enact and ideas to share with your peers. Stick around for this useful final session! Items you take back with you are icing on the cyber cake. **Drawing for VIP All-Access Cyber Security Summit admission for social media followers and bloggers** (details on page 5) *Tim Crothers, Target; Catharine Trebnick, Dougherty & Company LLC*

SUMMIT CO-CHAIRS

TIM CROTHERS

VP Security Solutions, Target

Tue Oct 29 - 8:45 AM
Opening Remarks
Tue Oct 29 - 4:45 PM
Closing Takeaways
Wed Oct 30 - 4:10 PM
Closing Keynote
Wed Oct 30 - 4:40 PM
Wrap Up & Practical Takeaways

Tim is a seasoned security leader with over 20 years experience building and running information security programs, large and complex incident response and breach investigations, and threat and vulnerability assessments. He has deep experience in cyber-threat intelligence, reverse engineering, computer forensics, intrusion detection, breach prevention, and applying six sigma/lean process to information security. He is author/co-author of 15 books to date as well as regular training and speaking engagements at information security conferences.

CATHARINE TREBNICK

Vice President, Senior Research Analyst, Dougherty & Company LLC

Tue Oct 29 - 8:45 AM
Opening Remarks
Tue Oct 29 - 4:45 PM
Closing Takeaways
Wed Oct 30 - 3:00 PM
Panel: Too Many Tools, Technology Rationalization
Wed Oct 30 - 4:40 PM
Wrap Up & Practical Takeaways

Catharine Trebnick serves as VP, Sr. Research Analyst at Dougherty & Company. Trebnick's sector focus is Security, Cloud and Network Infrastructure and Unified Communications. Trebnick began her career on Wall Street at Thinkequity. Her expertise stems from working for industry icons Time Warner Telecom, Level 3 Communications, Lucent Technologies, and AT&T. Fluent in emerging technologies, cloud and infrastructure networks and leverages C-level relationships plus technical knowledge gained over 15 years in senior level product management positions to gain rare insight in order to influence stock prices and provide real-time, accurate intelligence to investors. Trebnick earned a B.S. in Chemistry and minor in Chemical Engineering from Univ. of Maryland. She also earned an M.B.A. from the Univ. of Chicago. Trebnick is a frequent guest on CNBC and received acclaim for her research through published papers and quotes published in Barron's, Wall Street Journal, Reuters, Bloomberg, TheStreet.com, Forbes, Investor's Business Daily and CNNMoney.

Learn More About Our Speakers

For full biographies and other relative information, visit:

cybersecuritysummit.org/speakers

STEVE ALECKSON
Executive Director, TEKsystems Risk & Security

Mon Oct 28 - 9:00 AM
Opening Remarks and Women in Cyber Security Panel

JILL ALLISON
Advisory CISO, Kudelski Security, Inc.

Mon Oct 28 - 10:45 AM
Women in Cyber Security Panel

MASSOUD AMIN
Professor of Electrical and Computer Engineering, University of Minnesota

Mon Oct 28 - 6:30 PM
International Dinner

MICHAEL ANTON
Senior Product Manager, Kudelski Security, Inc.

Mon Oct 28 - 1:10 PM
Technical Track 1-A

DAMIN BARNIER
Senior Security Engineer, UnitedHealth Group

Mon Oct 28 - 2:00 PM
HealthCare & Med Device

ROBERT BOOKER
Senior Vice President & Chief Information Security Officer, UnitedHealth Group

Wed Oct 30 - 3:00 PM
Panel: Too Many Tools, Technology Rationalization

ANDREW BORENE
Honorary Chairman Emeritus; Senior Director, Federal – National Security Group, Symantec

Tue Oct 29 - 9:45 AM - Intro
Wed Oct 30 - 2:00 PM - Intro

ADAM BRAND
Managing Director - Cybersecurity & Privacy, PwC

Mon Oct 28 - 2:30 PM
HealthCare & Med Device

JENNIFER CZAPLEWSKI
Director, Product Security, Target

Wed Oct 30 - 1:15 PM
Cyber Risk Management Strategy

WILLIAM EVANINA
Director, National Counterintelligence and Security Center

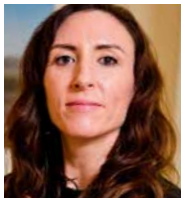
Wed Oct 30 - 12:00 PM
Legislative Briefing
Wed Oct 30 - 2:00 PM
The China Threat and American Business

CHRISTOPHER BUSE
Deputy Legislative Auditor, Office of the Legislative Auditor

Tue Oct 29 - 6:00 PM
Visionary Leadership Awards Dinner

DAVE DIEHL
Tool Using Mammal, Crowdstrike

Wed Oct 30 - 8:30 A
Panel: Human vs. Machine



ANITA FINNEGAN
Founder & CEO, Nova Leah

Mon Oct 28 - 3:00 PM
HealthCare & Med Device

STEPHANIE CASSIOPPI
Supervisory Special Agent, FBI

Wed Oct 30 - 7:15 AM
FBI Breakfast

ERIC EBNER
Chief Technology Officer, Protocol 46

Mon Oct 28 - 1:10 PM
Tech Tracks 1-D, 2-D, 3D, 4D
2:10–5:00 PM
Tue Oct 29 - 2:00 PM
Small Business Track

STEEN FJALSTAD
Security and Mitigation Principal, Midwest Reliability Organization

Tue Oct 29 - 9:15 AM
Panel: Government Taking Action to Secure the Cyber Domain
Tue Oct 29 - 11:45 AM
Luncheon Roundtable Discussions

DAMIAN CHUNG
Business Information Security Officer, Netskope

Mon Oct 28 - 3:10 PM
Technical Track 3-C

BETTY ELLIOTT
Partner & Chief Information Security Officer, Mercer

Mon Oct 28 - 9:00 AM
Opening Remarks and Women in Cyber Security Panel

EVAN FRANCEN
CEO & Founder, FRSecure

Mon Oct 28 - 1:10 PM
Technical Track 1-C

SEAN COSTIGAN
Professor, George C. Marshall European Center for Security Studies

Mon Oct 28 - 6:30 PM
International Dinner

CHRISTOPHER EMERSON
CCSK, CISSP, CISA, GSEC, GWAPT, OSCP, SSCP, White Oak Security, Inc.

Tue Oct 29 - 10:45 AM
Management Breakout: Forward Looking View of Cyber Risk

MARY FRANTZ
Founder & Managing Partner, Enterprise Knowledge Partners, LLC

Tue Oct 29 - 10:45 AM
Tech Breakout: Weaponization of Social Media

SIMON CROSBY
CTO, SWIM AI

Wed Oct 30 - 8:00 AM
CyberByte®: AI Machine Learning
Wed Oct 30 - 8:30 A
Panel: Human vs. Machine

CHRIS ENG
Executive Vice President of Research, Veracode

Wed Oct 30 - 3:00 PM
Panel: Too Many Tools, Technology Rationalization

CHRISTOPHER GABBARD
Cybersecurity Advisor, Region V: Minnesota, CISA

Tue Oct 29 - 1:00 PM
Small Business Track

JOSH CUTLER
Distinguished Engineer & Sr. Director Engineering, Optum

Wed Oct 30 - 8:30 A
Panel: Human vs. Machine

SARAH ENGSTROM
CISO & VP of IT Security, Productivity and Privacy, CHS, Inc.

Mon Oct 28 - 10:45 AM
Women in Cyber Security Panel

SAI GADIA
Partner, KPMG LLP

Tue Oct 29 - 3:45 PM
Panel: Reasonable Information Security Standards

SAM GROSBY
Principal Enterprise Information Security Engineer, Wells Fargo

Tue Oct 29 - 1:15 P
CyberByte™: Network Security Strategy
Tue Oct 29 - 1:45 PM
Panel: Zero Trust as the New Network Security Strategy

MICHAEL GUTSCHE
Chief Security Strategist, Enterprise Security Product Group, MicroFocus

Tue Oct 29 - 11:45 AM
CISO Lunch

AARON HACKWORTH
Senior Executive and Engineering Fellow, Counter Threat Unit Research Group, Office of the CTO - Secureworks, Secureworks

Mon Oct 28 - 3:10 PM
Technical Track 3-B

JUDY HATCHETT
VP, Information Security & CISO, Fairview Health Services Information Technology

Mon Oct 28 - 9:00 AM
Opening Remarks and Women in Cyber Security Panel

CHRIS HAWLEY
Director of Security Controls and Automation, Unisys

Tue Oct 29 - 1:45 PM
Panel: Zero Trust as the New Network Security Strategy

BRETT HEBERT
Attorney, Briggs and Morgan, P.A.

Tue Oct 29 - 1:30 PM
Small Business Track

JOHN HELLICKSON
Vice President of US Advisory Services, Kudelski Security

Tue Oct 29 - 11:45 AM
CISO Lunch

BRIGADIER GENERAL STEFANIE HORVATH
Director of Joint Staff, JFHQ-MN; Executive Director Enterprise Services, MNARG; Minnesota IT Services

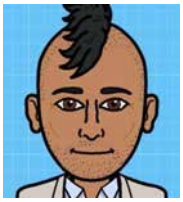
Mon Oct 28 - 10:00 AM
Women in Cyber Security
Wed Oct 30 - 3:40 PM
CyberByte® Data Breach Investigation Report 2019

KEN HOYME
Director, Product and Engineering Systems Security, Boston Scientific

Mon Oct 28 - 1:00 PM
HealthCare & Med Device

SAHAR ISMAIL
CEO, Legacy Armour

Mon Oct 28 - 10:00 AM
Women in Cyber Security Panel



SUNIL JAMES
CEO, Scytale.io

Wed Oct 30 - 9:15 AM
Authenticating Service-to-Service Communications in a Multi-Cloud World

MIKE JOHNSON
Senior Fellow & Honeywell James J. Renier Chair, Security Technologies Program,TLI, University of Minnesota

Tue Oct 29 - 8:45 AM
Welcome & Opening Remarks

SARAH JOPP
CISSP | Sr. Information Security Analyst, Office of Information Security, Mayo Clinic

Mon Oct 28 - 1:30 PM
HealthCare & Med Device

ERAN KAHANA
Attorney, Maslon

Mon Oct 28 - 5:00 PM
HealthCare & Med Device

MIKE KEARN
Vice President, Managing Business Information Security Officer, Security Risk & Technology Consulting, US Bank

Tue Oct 29 - 1:45 PM
Panel: Zero Trust as the New Network Security Strategy

DAVID KENNEDY
Founder, Senior Principal Security Consultant, TrustedSec

Tue Oct 29 - 8:00 AM
Keynote: Pushing the Cyber Security Envelope

MIKE KIJEWSKI
CEO, Medcrypt

Mon Oct 28 - 4:00 PM
HealthCare & Med Device

YAN KRAVCHENKO
Information Security Architect, Concord USA

Mon Oct 28 - 2:10 PM
Technical Track 2-B

CHRISTOPHER KREBS
Director, Cybersecurity and Infrastructure Security Agency (CISA)

Tue Oct 29 - 9:45 AM
Own IT. Secure IT. Protect IT

ERIC LENGVENIS
Operational Risk Consultant, PVSI – AI Controls Team, Wells Fargo

Wed Oct 30 - 8:30 AM
Panel: Human vs. Machine

CARTER LEUTY
Vice President, Law, Target

Tue Oct 29 - 3:15 PM
CyberByte: Reasonable Information Security Standards
Tue Oct 29 - 3:45 PM
Panel: Reasonable Information Security Standards

BRIAN LEVINE
Senior Counsel, US Department of Justice

Tue Oct 29 - 3:45 PM
Panel: Reasonable Information Security Standards
Wed Oct 30 - 11:15 AM
Capturing and Convicting The Bayrob Group: What You Need To Know About Working With Law Enforcement

YASIR LIAQATULLAH
Vice President of Product Management, a10

Mon Oct 28 -1:10 PM
Technical Track 1-B

NANCY LIBERSKY
Minnesota District Director, U.S. Small Business Administration (SBA)

Tue Oct 29 - 1:00 PM
Small Business Track

BRAD MAIORINO
CISO, Thomson Reuters

Tue Oct 29 - 3:45 PM
Panel: Reasonable Information Security Standards

CYRUS MALEK
Attorney, Briggs and Morgan, P.A.

Tue Oct 29 - 1:30 PM
Small Business Track

EILEEN MANNING
Executive Producer and Co-Creator, Cyber Security Summit, Cyber Security Summit; The Event Group Incorporated

Tue Oct 29 - 8:45 AM
Welcome & Opening Remarks
Tue Oct 29 - 1:00 PM
Small Business Track

JACK MARSAL
Senior Director of Product Marketing, Armis

Mon Oct 28 - 3:30 PM
HealthCare & Med Device

KARL MATTSON
CISO, City National Bank

Wed Oct 30 - 10:30 AM
Building Innovation into Cyber Security

KEVIN A. MCGRAIL
Director, Business Growth, InfraShield

Mon Oct 28 - 1:00 PM
HealthCare & Med Device

TINA MEEKER
Director of Information Security GRC, Shutterfly, Inc.

Mon Oct 28 - 10:45 AM
Women in Cyber Security Panel

HARSHAL MEHTA
VP, CISO, CWT

Mon Oct 28 - 6:30 PM
International Dinner

ALLISON MILLER
Vice President, Global Enterprise Information Risk Management, Optum

Mon Oct 28 - 1:00 PM
HealthCare & Med Device

JERROD MONTOYA
Deputy CISO, OATI

Tue Oct 29 - 11:45 AM
CISO Lunch

DAVID J. NOTCH
Strategic Advisor, Enterprise Security & Cloud Architecture, Medtronic

Tue Oct 29 - 11:45 AM
CISO Lunch

HAVE A DRINK, COMPLIMENTS OF THESE SPONSORS

During our Tuesday evening networking reception, you can visit our exhibitor reception sponsors to receive complimentary drink tickets.

The Exhibitor Reception Sponsors are located at:

RAPID7
BOOTH #111

Microsoft
BOOTH #201

VECTRA
BOOTH #206

Drexel University
BOOTH #207

Attivo Networks
BOOTH #211

DIRSEC
BOOTH #300

KATHY ORNER
VP & Chief Risk Officer (CISO M &G), CWT

Mon Oct 28 - 6:30 PM
International Dinner
Tue Oct 29 - 6:00 PM
Visionary Leadership Awards Dinner

PETER ROMNESS
Cybersecurity Solutions Lead, US Public Sector, CTO Office, CISCO

Mon Oct 28 - 4:10 PM
Technical Track 4-A
Tue Oct 29 - 1:45 PM
Panel: Zero Trust as the New Network Security Strategy

ELIZABETH STEVENS
Past President/Executive Board Member, InfraGard MN Alliance

Mon Oct 28 - 9:00 AM
Opening Remarks and Women in Cyber Security Panel:

CHARLES PELLINO
Managing Security Architect, Wells Fargo

Tue Oct 29 - 3:15 PM
Small Business Track

JOSEPH SALAZAR
Attivo Networks

Mon Oct 28 - 2:10 PM
Technical Track 2-C

CHRISTINE STEVENSON
Sales Engineer, Verodin

Mon Oct 28 - 10:45 AM
Women in Cyber Security Panel
Mon Oct 28 - 3:10 PM
Technical Track 3-A

STEPHEN PODOBINSKI
Lead Information Security Analyst, Target

Mon Oct 28 - 2:10 PM
Technical Track 2-A

RICHARD SCOTT
UnitedHealth Group

Mon Oct 28 - 2:00 PM
HealthCare & Med Device

BRANDON TRAFFANSTEDT
Global Director, Solutions Engineering at CyberArk, CyberArk

Mon Oct 28 - 4:10 PM
Technical Track 4-C

JAY RADCLIFFE
Director of Product Security Testing & Research, Thermo Fisher Scientific

Mon Oct 28 - 1:00 PM
HealthCare & Med Device

MELISSA SEEBECK
General Manager, Information Security Risk, Delta Air Lines

Mon Oct 28 - 9:00 AM
Opening Remarks and Women in Cyber Security Panel

JOHN TUMA
Commissioner , Minnesota Public Utilities Commission

Tue Oct 29 - 9:15 AM
Discussion: Government Taking Action to Secure the Cyber Domain

MILINDA RAMBEL STONE
Vice President & CISO, Provation Medical

Mon Oct 28 - 10:00 AM
Women in Cyber Security Panel

ANDREW SERWIN
Partner, Co-Chair, Global Cybersecurity Practice, DLA Piper

Tue Oct 29 - 3:45 PM
Panel: Reasonable Information Security Standards

AARON VERDELL CALL
CISO, Information Security for the State of Minnesota, MN.IT Services

Tue Oct 29 - 7:00 AM
Student Breakfast

CHRIS RASCHKE
Advanced Security Architecture - Global Black Belt, Microsoft

Mon Oct 28 - 4:10 PM
Technical Track 4-B

SHERRY SMITH
Director, Piper Jaffray, John Deere

Tue Oct 29 - 11:45 AM
CISO Lunch

SENATOR MELISSA WIKLUND
State Senator, State of Minnesota

Mon Oct 28 - 11:45 AM
Women in Cyber Security Networking Lunch

MARK RITCHIE
CEO, Global MN

Mon Oct 28 - 6:30 PM
International Dinner

ERIC SORENSON
Regional Account Manager at VMware Carbon Black, Inc., VMware Carbon Black, Inc.

Wed Oct 30 - 3:00 pm
Panel: Too Many Tools, Technology Rationalization

KRISTI YAUCH
Cyber Security Director, T CF Bank

Tue Oct 29 - 10:45 AM
Management Breakout: Forward Looking View of Cyber Risk

TECHNOLOGICAL LEADERSHIP INSTITUTE

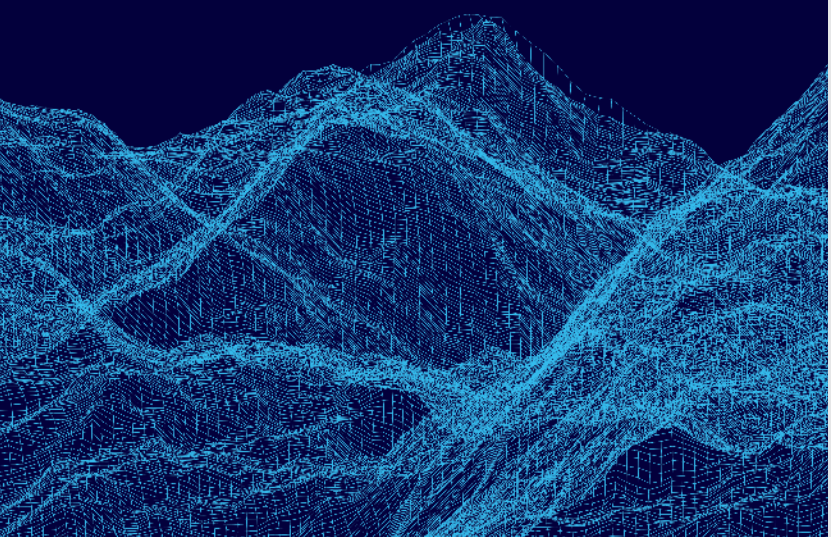
ARE YOU DRIVEN TO FIGHT CYBER CRIME?

Graduate Minor in Cyber Security

Every industry needs cybersecurity professionals, and the demand for them is greater than ever. Gain the skills from industry-leading faculty to protect the information and systems we rely on with a **graduate minor in cyber security from the Technological Leadership Institute (TLI)** at the University of Minnesota. Courses are open to both U of MN students and non-degree seeking professionals.

Contact TLI admissions at tli-info@umn.edu or 612-624-5747 for more info. tli.umn.edu

Secure what matters most



Our solutions:

- ArcSight
- Fortify
- Interset
- Secure Content Management
- NetIQ
- Vertica
- Voltage
- ZENworks

Cyber threats are escalating. Aging apps and processes (along with new ones) are full of unforeseen risks. Privacy and compliance requirements are mounting. And point solutions don't offer the scope, vision, or cross-silo analytics needed for these company-wide challenges. With our solutions, you can take a holistic, analytics-driven approach to securing what matters most—identities, applications, and data.

microfocus.com/srg

MICRO FOCUS

2019 Visionary Leadership Awards

The Morries

The winners will be recognized at the Visionary Leaders Awards Dinner, hosted on the evening of October 29th. Along with recognition for their accomplishments, award recipients will get a brief opportunity to share their innovative strategies with their peers and attendees of the Summit.

2019 Honorees

Academic Leader

CHRISTOPHE VELTSOS

Professor, Minnesota State University Mankato

Applications Security Leader

MIKE KIJEWSKI

CEO, MedCrypt

Global Security Leader

ANDREW BORENE

Senior Director, Symantec National Security Group; Director Homeland Security Program at George Mason University Law School

Governance Champion

SUZANNE SPAULDING

Senior Adviser, Homeland Security, International Security Program, CSIS

Many traditions stem from a story. The Visionary Leadership Awards we will confer tonight are called The Morries. They're named for Robert Tappan Morris, progenitor of the first known national cyber hacking event on Nov. 2, 1988, one year before the formation of the World Wide Web. Morris was a gifted college student programmer. He unwittingly unleashed a self-propagating worm into the national system. His worm slowed university and military computers to a crawl. Morris claimed that his worm had been conceived as an experiment that accidentally created havoc. Though he could have been imprisoned under then-current law, he was fined and sentenced to perform public service. As the first cyber hacker, Morris gives us a fitting source for the name of our awards.

Information Technology Audit Leader

MARY FRANTZ

CEO, Enterprise Knowledge Partners, LLC (EKP)

Security Awareness Program Leader

JERROD MONTOYA

Deputy Chief Information Security Officer, Open Access Technology International (OATI); President, InfraGard Minnesota Chapter

Security Operations Leader

JOHN ISRAEL

Security Operations Manager – Security Operations Center (SOC), Incident Response, and Forensics, State of Minnesota

Security Program and Oversight Leader

JODIE KAUTT

President, Cyber Security, Target Corp.

Center for Internet Security®

Founders Award: National Cyber Defense Leadership

CENTER FOR INTERNET SECURITY, INC. (CIS®)

THANKS TO OUR CORPORATE TABLE SPONSORS

Centrify ZERO TRUST PRIVILEGE · KPMG · preempt · RASMUSSEN COLLEGE · TECHNOLOGICAL LEADERSHIP INSTITUTE · VERACODE · ekp ENTERPRISE KNOWLEDGE PARTNERS, LLC

Special thanks to our Visionary Leadership Awards committee judges:

Chris Buse, Office of the Legislative Auditor, State of Minnesota; Todd Carpenter, Adventium Labs; Jennifer Czaplewski, Target Corp.; Steen Fjalstad, Midwest Reliability Organization; Chrysa Freeman, Security Mindedness; Brian Isle, University of Minnesota Technical Leadership Institute & Adventium Labs; Eileen Manning, Cyber Security Summit.

TECHNOLOGICAL
LEADERSHIP INSTITUTE

Building and retaining your security team

Mike Johnson serves as the director of graduate studies for the Master of Science in Security Technologies degree program at the Technological Leadership Institute at the University of Minnesota. In his role, he oversees, develops and teaches graduate level courses in security technologies innovation, management and leadership. He also delivers custom short courses and professional development programs for businesses. He has 25 years of risk management experience in security and financial services, serving as CISO and Operations Risk Director at Bremer Bank.

If you are a cybersecurity leader/hiring manager, you are probably getting tired of being reminded that there aren't enough skilled cybersecurity staff to fill your open positions. We know already, can we stop complaining about it? Yes, there are currently 500K open cyber positions in the US and nearly 3 million open positions globally, (1) and the need is definitely not expected to shrink in the coming years. So maybe it's time to think outside of the box when it comes to staffing our teams.

The Cybersecurity Unicorn may exist but we can't find them, and even if we did we can't afford them. How are we supposed to keep our SOC or our security engineering teams fully functional if we don't have anyone that can do the job? We consider our options. While it is always prudent to recruit new talent from recent college graduates at reputable IT and security education programs, and there always seems to be the regular musical chairs of security staff that shift from organization to organization, I don't think that's the only answer. As security leaders, what are we doing to help ourselves?

Most organizations already know that it's cheaper to keep staff than replace them. Once an employee becomes familiar with an organization's activities and operations they are more effective even with just the skills they already have. So rather than investing in a few of the most expensive security resources on the market, maybe we should invest even more in those employees we already have. And I'm not just talking about the current members of the security team, we need to expand these options to all of our employees (think other IT staff and business lines), and even consider hiring new employees that have strong IT aptitude but maybe not the lofty required level of experience we typically list in our entry-level security analyst job postings. Training the needed technology skills after a promising but inexperienced employee joins the organization (from another department or outside the organization) may seem counter-intuitive but can result in more effective results, including fully staffed teams. It also shows staff that there are opportunities beyond the role they are entering at the moment, which is another boost to staff retention.

Mature security programs have been including training opportunities in their weekly activities for some time now, and that is why they continue to have effective programs, reduced turnover and strong staff knowledge and expertise. Training at these organizations isn't just the standard "Learning Management System" videos or outside classes (although they both have a place), but include active learning through internal exercises like capture the flag or red team/blue team competitions, time during the week for reading and self-directed learning, and job shadowing/skills transfer activities.

Providing training opportunities to your teams on an ongoing basis can improve both their skills and retention numbers. It also establishes a more robust security culture, as all employees can see by your actions that security is important to the organization. And even if some of the staff are already highly skilled, the world is changing fast. The continuous influx of new business technologies, new security regulations and requirements, new security tools and technologies, and new threats and vulnerabilities requires that your teams update and refresh skills and knowledge constantly. And don't forget about non-tech skills like effective communication and business acumen, both of which can improve the success of business impacting implementations and processes.

"The only thing worse than training employees and losing them is to not train them and keep them." – Zig Ziglar

While improving the skill level of your existing employees may take time, effort, and money, and some will use their new skills to find jobs elsewhere, it will also give you the resources to continue to have an effective security program and may be the only way you can keep all those seats filled.

1 2018 $(ISC)^2$ Cybersecurity Workforce Study

Upcoming Industry Events

NOVEMBER 18

InfraGard | Chapter Meeting

Cargill @1:00 PM
Covering IT Infrastructure, BC/DR, IT Security, Data Storage, and Enterprise Communications, you'll find presentations, panel discussions, and exhibits offering a variety of topics, as well as the latest innovations and best practices.

NOVEMBER 20

MHTA | 2019 Tekne Awards

Minneapolis Convention Center @5:00 PM
Recognizing Minnesota's best and brightest innovations leaders in science and technology.

NOVEMBER 21

ISACA MN | Effective Use Cases For Siem, Ueba, And Automation

Target Northern Campus @3:30 PM
Good, Bad, and Ugly of SIEM, UEBA, and SOAR. Use cases and justification. David Swift is a security practitioner, presenter and published researcher with over 25 years of experience having worked with Apple, Microsoft, Chevron, Visa, Costco, and may others to improve SIEM, SOC and UEBA practices.

DECEMBER 17

MNISSA | Chapter Meeting

St. Mary's University Center @1:00 PM
Join us for our informative presentations and great networking. Open to members and non-members. Agenda includes social networking, program and Happy Hour. Speaker: Tony James, Director of Payment Security, Target Corp. CISSP, CISA and CRSC. Presentation will cover the benefits of having PCI ISA(s) on the team.

APRIL 29

US Naval Academy Alumni | 4th Annual Heartland Leadership Forum

McNamara Alumni Center
Keynote speaker is Admiral Mike Rogers, former NSA Director and Commander of Cyber Command.

A PERSONAL NOTE OF THANKS

The Cyber Security Summit could not happen without the support and vision of the over 40 members that make up the Think Tank, along with dozens of people who work on committees, plus the nearly 100 speakers and panelists that give of their time to share their experience to alert you to what is coming at us. These individuals are highlighted within the guide.

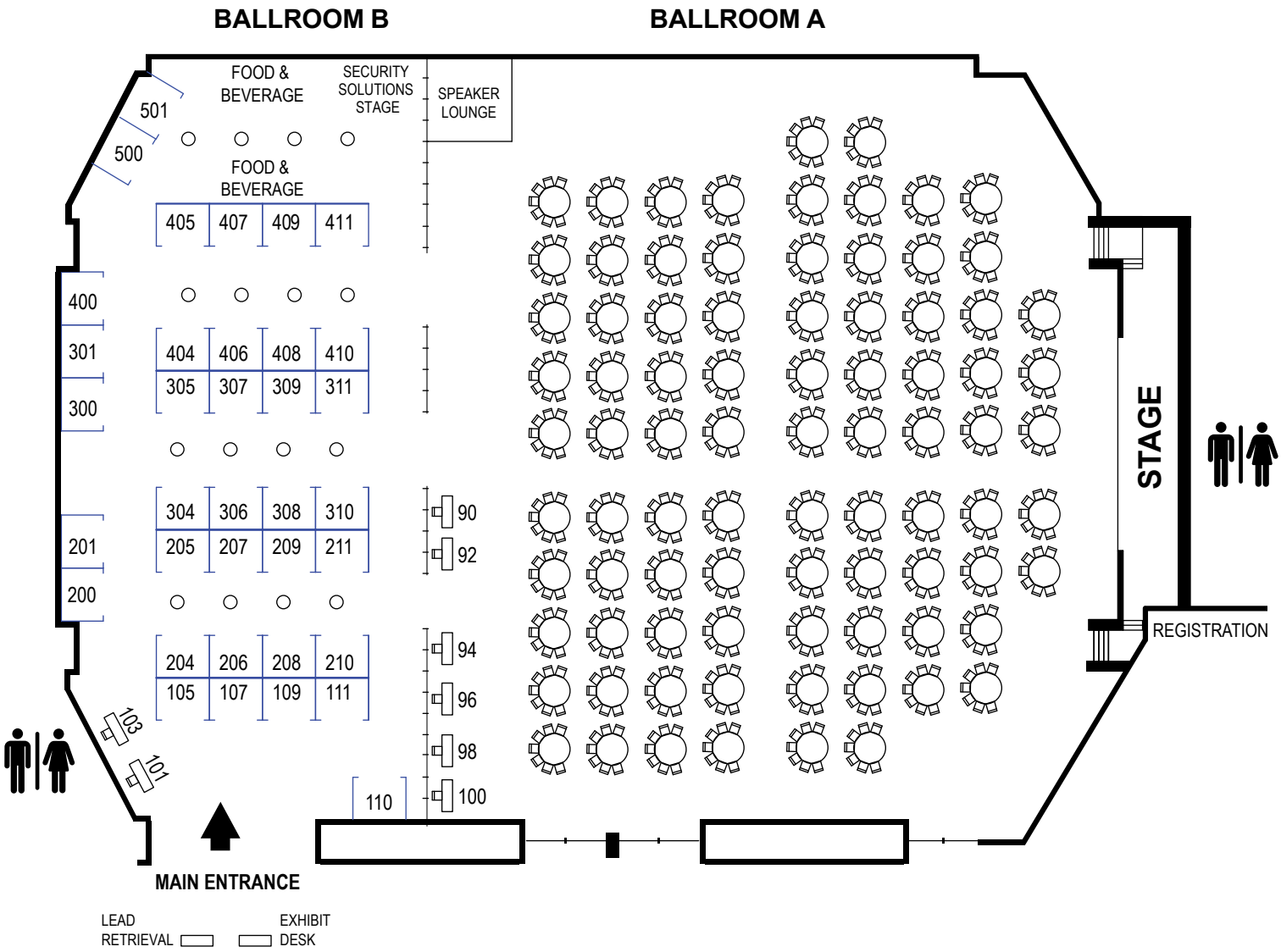
Literally, thousands of hours go into producing this Summit. Each year amazing leaders step up and take on the role of guiding our vision. This year, Tim Crothers and Catharine Trebnick Co-Chaired with the help of 2018 Co-Chairs General Stef Horvath and David Notch. So many other amazing people chaired committees, such as Ken Hoyme, Allison Miller, Tina Meeker, Harshal Mehta, Steen Fjalstad, Cyrus Malek, Jill Allison, and Chris Buse. And others worked in the background on special projects such as Matthew Harmon and David LaBelle.

Thank you, friends, for building this Summit. For all the meetings, phone calls and emails. Your support is helping to showcase the amazing talent here in Minnesota, and more importantly, globally Pushing the Cyber Security Envelope

Eileen Manning

Eileen Manning, Executive Producer,
Cyber Security Summit

If you'd like to join the collaboration and participate in a committee, please contact Eileen.Manning@eventshows.com.



Exhibitor Directory

209 A10 Networks
408 Armis
500 Atomic Data
211 Attivo
107 Backbone Consultants
100 BCPA
404 Centrify
311 Cisco
406 ControlCase
94 CSA MN Chapter
305 CyberArk
300 DirSec
207 Drexel University
407 Fidelis
308 FRSecure
90 InfraGard
92 ISACA Minnesota
98 (ISC)2 Twin Cities
96 ISSA MN Chapter
411 Kudelski Security
410 Metropolitan State University
304 Micro Focus
201 Microsoft
307 NaviLogic
409 Netskope
204 ProcessBolt
306 Proofpoint
110 Protocol46
111 Rapid7
210 Rasmussen College
405 Secureworks
200 Synack
205 Tanium
101 Target
105 Technological Leadership Institute (TLI)
109 TEKsystems
400 Tiffin University
501 TrustedSec
103 USNA
206 Vectra
310 Veracode
309 Verodin
301 White Oak Security
208 Wipfli

Gold Sponsor

About A10 Networks A10 Networks (NYSE: ATEN) provides Reliable Security Always™, with a range of high-performance application networking solutions that help organizations ensure that their data center applications and networks remain highly available, accelerated and secure. Founded in 2004, A10 Networks is based in San Jose, Calif., and serves customers globally with offices worldwide.

www.a10networks.com | @A10Networks

Supporter

AAMI is a diverse global community of over 7,000 members dedicated to one important mission – the development, management, and use of safe and effective healthcare technology.

www.aami.org

Silver Sponsor / Heatlthcare & Med Device Supporter

Armis is the first agentless, enterprise-class security platform to address the new threat landscape of unmanaged and IoT devices. Fortune 1000 companies trust Armis' unique out-of-band sensing technology to discover and analyze all managed and unmanaged devices, analyze endpoint behavior to identify risks and attacks, and protect information and systems.

www.armis.com

Atomic Data

Silver Sponsor

Atomic Data is an on-demand, always-on, pay-as-you-go expert extension of the enterprise's IT team and infrastructure, always acting in the client's and the community's best interest. Atomic Data – SAFE. SIMPLE. SMART.

www.atomicdata.com

Attivo

Silver Sponsor

Attivo Networks® provides accurate detection, analysis, and automated response to in-network threats. The ThreatDefend™ platform efficiently detects advanced, stolen credential, insider, and ransomware attacks within user networks, data centers, cloud, branch, and specialty environments by deceiving attackers into revealing themselves. ThreatOps™ playbooks and 3rd party integrations provide accelerated incident response.

www.attivonetworks.com

Backbone Consultants

Silver Sponsor

Backbone Consultants provides IT Risk Advisory, and Security services. Our industry certified consultants are proven IT Security, Audit, and Privacy professionals who provide end to end services necessary to help protect your business. In simple terms, we are certified experts who help you protect your company's 'Backbone' -if you will.

www.backboneconsultants.com

Supporter

The Business Continuity Planners Association (BCPA), a non-profit, mutual-benefit group, supports professionals in business recovery, crisis management, emergency management, disaster preparedness planning, or a related professional vocation. The BCPA provides exchange of experience, professional growth in an educational environment supporting the mutual interest to the membership.

www.bcpa.org

Gold / Cyber Security for Small and Mid-Size Businesses Sponsor

Briggs and Morgan's Privacy and Data Security attorneys are committed to helping our clients prevent, prepare for, respond to, and minimize the impact of data security breaches and cyber attacks. From data protection to navigating complex legislation, we offer a full range of services related to privacy and information security.

www.briggs.com

Diamond Sponsor

Carlson Wagonlit Travel (CWT) is a privately held travel management company wholly owned by Carlson managing business travel, meetings and events for companies and governments. CWT is a global leader in the travel industry attaining over $23B in transaction volumes in 2017 with over 18,000 employees in nearly 150 countries.

www.carlsonwagonlit.com

Centrify

Silver Sponsor

Centrify is redefining the legacy approach to Privileged Access Management by delivering cloud-ready Zero Trust Privilege to secure modern enterprise use cases. Zero Trust Privilege mandates a 'never trust, always verify, enforce least privilege" approach. Centrify Zero Trust Privilege helps customers grant least privilege access based on verifying who is requesting access, the context of the request, and the risk of the access environment.

www.centrify.com

Cisco

Diamond Sponsor

Cisco is building truly effective security solutions that are simple, open and automated. Drawing on unparalleled cloud, endpoint and network presence as well as the industry's broadest and deepest technology and talent, Cisco delivers ultimate visibility and responsiveness to detect more threats and remediate them faster. With Cisco Security, companies are poised to securely take advantage of a new world of digital business opportunities.

www.cisco.com

ControlCase

Silver Sponsor

ControlCase is a global provider of certification and continuous compliance services. ControlCase is committed to partnering with clients to develop strategic information security and compliance programs that are simplified, cost effective and comprehensive in both on-premise and cloud environments. ControlCase provides the best experts, customer experience and technology for regulations including PCI DSS, HITRUST, ISO 27001, SOC1, SOC2, PCI PIN, PCI P2PE, PCI TSP, PA DSS, CSA STAR, HIPAA, GDPR and FedRAMP

www.controlcase.com

CSAMN cloud security Minnesota Chapter alliance®

Supporter

The MN Chapter of the Cloud Security Alliance advances the next generation of cloud security professionals. Our CSA Members represent the Minnesota Fortune 500 companies. Our Executive Advisory Board is comprised of Fortune 100 CISOs, CIOs, and CEOs that advise on curriculum, meeting topics, deliverables, and special projects.

www.csamn.com

CYBERARK

Diamond Sponsor

CyberArk is the global leader in privileged access security, a critical layer of IT security to protect data, infrastructure and assets across the enterprise, in the cloud and throughout the DevOps pipeline. CyberArk delivers the industry's most complete solution to reduce risk created by privileged credentials and secrets. The company is trusted by the world's leading organizations, including 50 percent of the Fortune 500, to protect against external attackers and malicious insiders.

www.cyberark.com

DirSec

Silver Sponsor

DirSec is a Colorado based reseller and integrator specializing in IT security solutions. We work with over 30 leading cybersecurity technology partners while continually adding disruptive, cutting-edge technologies to our portfolio. Since 2001, DirSec has been a trusted security advisor for a wide range of clients ranging from large enterprise to government and education. We leverage our partners to provide the most complete and robust security plan to best protect your IT environment.

www.dirsec.com

Drexel University

Silver Sponsor

Founded in 1891, Drexel University is a top-ranked, research university, located in the heart of Philadelphia. Known as an academic center of excellence and innovation, Drexel was a pioneer in technology-enhanced education for working adults. Today, nearly two decades after launching its first online courses, this transformative university offers more than 150 online degree and certificate programs.

www.duo.online.drexel.edu

Fidelis

Silver Sponsor

Fidelis Cybersecurity is a leading provider of threat detection, hunting and response solutions. Fidelis combats the full spectrum of cyber-crime, data theft and espionage by providing full visibility across hybrid cloud / on-prem environments, automating threat and data theft detection, empowering threat hunting and optimizing incident response with context, speed and accuracy.

www.fidelissecurity.com

Finance & Commerce

Supporter

Finance & Commerce media has a rich history and a reputation for quality content and a highly engaged audience. Through a multi-media distribution channel, Finance & Commerce serves the commercial real estate, construction and economic development sectors while Minnesota Lawyer is the premiere news source for legal matters in Minnesota.

www.finance-commerce.com

VERACODE AT THE FOREFRONT OF THE TRANSFORMATION

By providing a comprehensive and accurate view of software security defects, companies can create secure software and ensure the software they buy or download is free of vulnerabilities. As a result, companies using Veracode are free to boldly innovate, explore, pioneer, discover, entertain, and change the world.

VERACODE

You change the world, we'll secure it.

VISIT US AT
VERACODE.COM

FRSECURE | Gold Sponsor

FRSecure is an information security consultancy based out of Minnetonka, MN. Recognizing the information security industry is broken, FRSecure has developed tools, services, and teams to help companies of all sizes to identify and manage their most critical assets and risks through education and partnership.

www.frsecure.com

H-ISAC HEALTH - ISAC | Supporter

H-ISAC is a trusted community of critical infrastructure owners and operators within the Health Care and Public Health sector (HPH). The community is primarily focused on sharing timely, actionable and relevant information that can include data such as indicators of compromise, tactics, technique and procedures (TTPs) of threat actors, advice and best practices, mitigation strategies and other valuable material.

www.h-isac.org

INFRAGARD | Supporter

InfraGard is a Federal Bureau of Investigation (FBI) program that began in the Cleveland Field Office in 1996. It was a local effort to gain support from the information technology industry and academia for the FBI's investigation efforts in the cyber arena. InfraGard and the FBI have developed a relationship of trust and credibility in exchange of information concerning various terrorism, intelligence, criminal and security matters.

www.infragard.org

ISACA Trust in, and value from, information systems | Supporter

With approximately 1,000 members from over 100 organizations, the Minnesota chapter of ISACA provides a gateway to a global organization offering security , risk, control, and governance certifications. Additionally, ISACA offers a new security knowledge platform and professional program Cybersecurity Nexus (CSX). For more information please visit the chapter website.

www.engage.isaca.org/minnesotachapter

(ISC)² CHAPTER TWIN CITIES AREA | Supporter

Our mission is to create a safe environment where information security practitioners can openly share expertise and ideas, providing practical, relevant, useful and timely information that, when applied, will develop and promote the (ISC)2 CISSP CBK® and help support the Information Security and Cyber Security Communities of the Upper Midwest.

www.isc2tc.org

ISSA Information Systems Security Association MINNESOTA CHAPTER | Supporter

The Minnesota Chapter of the Information Systems Security Association (ISSA) is a not-for-profit organization of information security professionals and practitioners focused on promoting a secure digital world. Our goal is to be the community of choice for cybersecurity professionals dedicated to advancing individual growth, managing technology, risk and protecting critical information and infrastructure. We accomplish this by providing educational forums and peer interaction opportunities that enhance the knowledge, skill, and professional growth of our members.

www.mn.issa.org

KPMG | Gold Sponsor

At KPMG, our network of cyber security professionals understands that businesses cannot be held back by cyber risk. We recognize that cyber security is about risk management – not risk elimination. KPMG can help you reach your destination: a place of confidence that you can operate without crippling disruption from a cyber security event. Working shoulder-to-shoulder with you, our professionals can help you work through strategy and governance, organizational transformation, cyber defense and cyber response.

www.KPMG.com

KUDELSKI SECURITY | Gold Sponsor

Kudelski Security, a division of the Kudelski Group (SIX: KUD.S), is an innovative, independent provider of tailored cybersecurity solutions to enterprises and public sector institutions. Kudelski Security is headquartered in Cheseaux-sur-Lausanne, Switzerland, and Phoenix, Arizona, with operations in countries around the world.

www.kudelskisecurity.com

MapleLane MEDIA | AV Partner

Maple Lane Media is an event technology company that provides reliable service to businesses and associations. As a trustworthy partner, we utilize today's technologies to communicate your vision. Whether it's a multi-day conference, live web broadcast or produced video, Maple Lane Media is connecting people through technology on every project.

www.maplelanemedia.com

MASLON

Heatlthcare & Med Device Session Host

Maslon's Technology, IP & Media Law Group offers skilled cybersecurity lawyers with in-depth knowledge of regulatory requirements, industry standards, and best practices—enhanced by serving in advisory roles for the Governor, the FBI, and national cyber security summits. We will assess your cybersecurity risk profile and current practices and provide you with proactive, up-to-date, and practical advice that will help you build and sustain a legally reasonable cybersecurity strategy.

www.maslon.com

MEDICAL ALLEY ASSOCIATION

Supporter

Founded in 1984, the Medical Alley Association supports and advances the global leadership of Medical Alley's healthcare industry, and its connectivity around the world. MAA delivers the collective influence, intelligence and interactions that support Medical Alley.

www.medicalalley.org

MedCrypt

Heatlthcare & Med Device Supporter

MedCrypt gives medical device vendors access to advanced cybersecurity features in a few lines of code.

The exponential growth of connected devices in healthcare combined with the FDA mandate to "bake in" security into devices means the best solution is one that secures devices, not the hospital network.

www.medcrypt.com

Metropolitan State University

Bronze Sponsor

Metropolitan State University offers a variety of technical and professional graduate programs designed specifically for working adults. Our Master of Management Information Systems (MMIS), MIS Graduate Certificates, Master in Computer Science, MBA and DBA programs are high quality, affordable, practical and flexible to accommodate busy lifestyles.

www.metrostate.edu

mhta

Supporter

MHTA is a non-profit association of more than 300 technology companies and organizations. Together, we fuel Minnesota's prosperity through innovation and technology. Our members include some of the world's leading corporations, mid-sized companies and startups. We are united behind a common vision to make Minnesota one of the country's top five technology states.

www.mhta.org

MICRO FOCUS

Diamond Sponsor

Micro Focus helps you run your business and transform it. Our software provides the critical tools you need to build, operate, secure, and analyze your enterprise. By design, these tools bridge the gap between existing and emerging technologies—which means you can innovate faster, with less risk, in the race to digital transformation.

www.microfocus.com

MDMA

Supporter

The Medical Device Manufacturers Association (MDMA) is a national trade association based in Washington, DC providing educational and advocacy assistance to innovative and entrepreneurial medical technology companies. Since 1992, MDMA has been the voice for smaller companies, playing a proactive role in helping to shape policies that impact the medical device innovator.

www.medicaldevices.org

Microsoft

Silver Sponsor

Microsoft is the leading platform and productivity company for the mobile-first, cloud-first world. We are uniquely positioned to help empower organizations to achieve more by unlocking the security, compliance, and identity capabilities of the intelligent cloud and next generation AI, helping them on their secure digital transformation journey.

www.microsoft.com

AMERICA'S SBDC MINNESOTA

Cyber Security for Small and Mid-Size Businesses Supporter

The Minnesota Small Business Development Center (MnSBDC) network philosophy is based on the principle that helping our small businesses is critical to our economy and the quality of our communities. The MnSBDC offers customized technical assistance and support to businesses at any point in their entire life cycle, from start-up to growth to exit strategies.

www.mn.gov/deed/business

Minnesota IT Services — Student Breakfast Sponsor

Minnesota IT Services is a cutting-edge organization that is emerging as a national leader in government IT. Our mission is to provide high-quality, secure and cost effective information technology that meets the business needs of government, fosters innovation, and improves outcomes for the people of Minnesota.

www.mn.gov/mnit

NaviLogic — Lanyard Sponsor

NaviLogic is a security consulting and IT integrator that uses its expertise and technology insights to provide leading-edge cybersecurity solutions and managed services. Our nimble, creative and highly knowledgeable team works hand-in-hand with our clients to help solve business-critical security, risk, and compliance concerns.

www.navilogic.com

Netskope — Gold Sponsor

The Netskope security cloud provides unrivaled visibility and real-time data and threat protection when accessing cloud services, websites, and private apps from anywhere, on any device. Only Netskope understands the cloud and delivers data-centric security from one of the world's largest and fastest security networks, empowering the largest organizations in the world with the right balance of protection and speed they need to enable business velocity and secure their digital transformation journey. Reimagine your perimeter with Netskope.

www.netskope.com

proofpoint. — Gold Sponsor

Proofpoint protects your people, data, and brand from advanced threats and compliance risks across email, mobile apps, and social media. We help you safely manage critical data as you send, store, and archive it. And we give you the intelligence, insight, and tools to respond quickly when things go wrong.

www.proofpoint.com

protocol46 cybersecurity — Platinum Sponsor

Protocol 46 is a veteran-owned cybersecurity dedicated to protecting American small and mid-size businesses. Our cyber intelligence veterans have created a comprehensive, homogeneous cybersecurity platform that seamlessly protects a company's networks and data, with a suite of tools that cross talk with each other and our SOC in a 24/7/365 real-time environment. We have a virtual cyber team of security and intelligence experts experienced in cyber defense for critical systems, response to cyber events, and recovery in case of a breach. Protocol 46 Cybersecurity Platform provides enterprise-level protection at a price that small businesses can afford.

www.protocol46.com

Rapid7 — Silver Sponsor

Organizations around the globe rely on Rapid7 technology, services, and research to securely advance. The visibility, analytics, and automation delivered through our Insight cloud simplifies the complex and helps security teams reduce vulnerabilities, monitor for malicious behavior, investigate and shut down attacks, and automate routine tasks.

www.rapid7.com

Rasmussen College — Silver Sponsor

Rasmussen College works with industry leaders and experts to offer innovative online programs that emphasize the skills and tools needed to be career-ready. Our School of Technology features a full spectrum of credentials, from Associate's to Master's degrees, with a wide variety of program offerings, including a Cyber Security Bachelor's degree. Through relevant, rigorous coursework, mentoring from faculty who are industry professionals, and hands-on virtual labs, the College's goal is to help students develop the technical skills and training sought by employers.

www.degrees.rasmussen.edu

Secureworks — Silver Sponsor

Secureworks® (NASDAQ: SCWX) is a technology-driven cybersecurity leader that protects organizations in the digitally connected world. Built on proprietary technologies and world-class threat intelligence, our applications and solutions help prevent, detect, and respond to cyber threats. More than 4,000 customers across over 50 countries are protected by Secureworks, benefit from our network effect and are Collectively Smarter. Exponentially Safer.™

www.secureworks.com

SCORE — Supporter

Get Your Business Going and Growing with SCORE.

We're here to help you get your business started and growing. Work with one of our experienced business mentors. Expand your skills with business workshops and webinars. Write a professional business plan using our templates and resources.

www.score.org

CANN CON MN 2019 SYMPOSIUM

November 6, 2019
8am - 4:20 pm

Renaissance Minneapolis Hotel,
the Depot, Minneapolis, MN

Morning Keynote Speaker

MPG MARIJUANA POLICY GROUP

Adam Orens, Founder

Salmeron Barnes, Partner

The Marijuana Policy Group

Their presentation will show actual data from Colorado and other legal states and a high-level estimation of the potential Minnesota market and economic impacts.

House Majority Leader Ryan Winkler Community Conversations and the House Majority Perspective: Representative Winkler will discuss the House Majority perspective on moving a bill forward and what he is hearing from our community conversations.

Minneapolis Mayor Jacob Frey will offer opening comments on the opportunities to advance racial equity and promote inclusive economic growth.

Download your FREE copy of the report
The Economic Impact of Marijuana Legalization in Colorado
http://bit.ly/CannConReport

Who Should Attend?

- Attorneys and Law Firm Administration
- Human Resources, Insurance and Financial Professionals
- Commercial Real Estate Brokers, agents, landlords and investors
- Legislators and lobbyists

If your business has the potential to service the cannabis industry, you must attend this conference!

Sponsored by:

GOFF PUBLIC

COZEN O'CONNOR

FINANCE & COMMERCE

Fredrikson & BYRON, P.A.

MPLS REGIONAL CHAMBER

MINNESOTA CANNABIS LAW

U.S. Small Business Administration — Supporter

The U.S. Small Business Administration (SBA) was created in 1953 as an independent agency of the federal government to aid, counsel, assist and protect the interests of small business concerns, to preserve free competitive enterprise and to maintain and strengthen the overall economy of our nation. Through an extensive network of field offices and partnerships with public and private organizations, SBA delivers its services to people throughout the United States, Puerto Rico, the U.S. Virgin Islands and Guam.

www.sba.gov

Symantec — Bronze Sponsor

Symantec Corporation, the world's leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure.

www.symantec.com.

Synack — Silver Sponsor

Synack, the most trusted crowdsourced security testing platform, delivers smarter penetration testing for dynamic attack surfaces on a continuous cadence. The company's hacker-powered, AI-enabled pen test provides access to the best worldwide talent, scalable and smart technology, and insights that secure our nation's critical infrastructure and leading brands and businesses.

www.synack.com

Tanium — Silver Sponsor

Tanium offers a proven platform for endpoint visibility and control that transforms how organizations manage and secure their computing devices with unparalleled speed and agility. Many of the world's largest and most sophisticated organizations, including half of the Fortune 100, top retailers and financial institutions, and four branches of the US Armed Forces rely on Tanium to make confident decisions, operate efficiently and effectively, and remain resilient against disruptions. Tanium recently ranked 4th on the Forbes list of 'Top 100 Private Companies In Cloud Computing For 2018" and 55th on FORTUNE's list of the '100 Best Medium Workplaces".

www.tanium.com

TARGET — Presenting Sponsor

Minneapolis-based Target Corporation serves guests at 1,797 stores and at Target.com. Since 1946, Target has given 5 percent of its profit to communities, which today equals more than $4 million a week.

For a behind-the-scenes look at Target, visit Target.com/abullseyeview or follow @TargetNews on Twitter.

www.target.com/pressroom

TEKsystems — Gold Sponsor

TEKsystems Risk and Security helps redefine security processes and rethink risk. We'll safeguard your business to stay ahead of what's next. We're partners in transformation. As an industry leader in Full-Stack Technology and Talent Services, we work with progressive leaders to drive change. TEKsystems is an Allegis Group company.

www.teksystems.com

Tiffin University — Silver Sponsor

Tiffin University offers accredited campus and online undergraduate and graduate degrees in Cyber Security and Digital Forensics. These professionally-focused programs are designed to provide practical operational skills, not just theory. They are based on the NICE Cybersecurity Workforce Framework, so graduates are career-ready for both the private and public sectors.

www.tiffin.edu

TECHNOLOGICAL LEADERSHIP INSTITUTE — Founding Partner

The Technological Leadership Institute is an interdisciplinary center at the University of Minnesota led by world-renowned faculty. Its mission is to develop local and global leaders for technology-intensive enterprises through its three Master of Science degree programs in Security Technologies, Management of Technology and Medical Device Innovation, and three minors.

www.tli.umn.edu

TrustedSec — Bronze Sponsor

TrustedSec is an information security consulting team at the forefront of attack simulations with a focus on strategic risk-management. Our goal is to help organizations defend against threats of all kinds and change the security industry for the better.

With a team handpicked not only for expertise and technical skill, but for ethical character and dedication, TrustedSec is committed to increasing the security posture of organizations around the world. TrustedSec is an ally to any organization working to develop and improve their security program.

www.trustedsec.com

mhta
Minnesota High Tech Association
presents

tekne™ 2019 AWARDS

CELEBRATE INNOVATION!

Wednesday, November 20
Minneapolis Convention Center

tekneawards.org

Sponsors*

Presenting: OPTUM, THOMSON REUTERS

Gold: padilla, TWIN CITIES BUSINESS, BEST BUY

Silver: at&t, COMCAST, ROBINS KAPLAN LLP REWRITING THE ODDS

Bronze: accenture, TARGET, Xcel Energy

*as of October 8, 2019

USNA
ALUMNI ASSOCIATION
UPPER MIDWEST CHAPTER

4th Annual
DONALD W. McCARTHY
HEARTLAND LEADERSHIP FORUM
APRIL 29, 2020

Keynote Speaker:
ADMIRAL MIKE ROGERS
Former NSA Director and Commander of Cyber Command

USNAUPPERMIDWEST.ORG

UNISYS | Securing Your Tomorrow™ — Printing Sponsor

Unisys is a global information technology company that builds high-performance, security-centric solutions for the most digitally demanding businesses and governments on Earth. Unisys offerings include security software and services; digital transformation and workplace services; industry applications and services; and innovative software operating environments for high-intensity enterprise computing. Visit us online for more information on how Unisys builds better outcomes securely for its clients across the Government, Financial Services and Commercial markets.

www.unisys.com

Vectra — Silver Sponsor

Vectra® is transforming cybersecurity by applying advanced AI to detect and respond to hidden cyberattackers before they do damage. Powered by AI, Vectra and its flagship Cognito® platform enable the world's most consequential organizations to detect attackers in real time and empower threat hunters to perform conclusive incident investigations.

www.vectra.ai

Verodin — Silver Sponsor

Verodin, part of FireEye, is a platform that has made it possible for organizations to validate the effectiveness of cyber security controls, thereby protecting their reputation and economic value. The Verodin Security Instrumentation Platform (SIP) proactively identifies gaps in security effectiveness attributable to equipment misconfiguration, changes in the IT environment, evolving attacker tactics, and more.

www.verodin.com

White Oak Security — Silver Sponsor

White Oak Security is a practitioner-led information security firm acting as our clients' trusted adviser. We help your organization understand your risks and vulnerabilities; whether in software, infrastructure, people, or process through deep-dive, client-focused technical testing as well as strategic services to help you build or mature your security practices.

www. whiteoaksecurity.com

VERACODE — Platinum Sponsor

Veracode gives companies a comprehensive view of security defects so they can create secure software, and ensure the software they are buying or downloading is free of vulnerabilities. As a result, companies using Veracode are free to boldly innovate, explore, discover, and change the world.

www.veracode.com

WIPFLI — Bronze Sponsor

Ensure your security strategy and solutions are as fluid and agile as the evolving cyber landscape with expert assistance from Wipfli. Our comprehensive Cybersecurity Services help you proactively address mounting threats and effectively respond in the event of an incident. Protect, Detect, Respond and Recover with Wipfli Cybersecurity Services.

www.wipfli.com/cybersecurity

International Dinner

Monday, October 28 | 6:15-8:30 PM

Mission

As the cyber threat reaches beyond national borders, so must collaboration to prevent cyber attacks. The Cyber Security Summit International Committee's mission is to unify defenses in the cyber domain through 1) An international consortium increasing situational awareness 2) Information sharing on emerging policy formulation and technologies 3) Using the platform of the Summit to showcase Minnesota as an international hub of business.

Sponsor CWT

Agenda

5:00–6:15 PM VIP Reception

6:30 PM Dinner

7:15 PM International Panel Discussion

Moderator: Harshal Mehta, CWT

Panelists: Dr. Massoud Amin, UofMN; Kathy Orner, CWT; Sean Costigan, ITL Security

7:45 PM Audience Q&A

8:15 PM Closing Remarks

Mark Ritchie, Global MN

WELLS FARGO

Gold Sponsor

Wells Fargo & Company (NYSE: WFC) is a diversified, community-based financial services company with $1.9 trillion in assets. Wells Fargo's vision is to satisfy our customers' financial needs and help them succeed financially. Founded in 1852 and headquartered in San Francisco, Wells Fargo provides banking, investment and mortgage products and services, as well as consumer and commercial finance, through 8,050 locations, 13,000 ATMs, the internet (wellsfargo.com) and mobile banking, and has offices in 38 countries and territories.

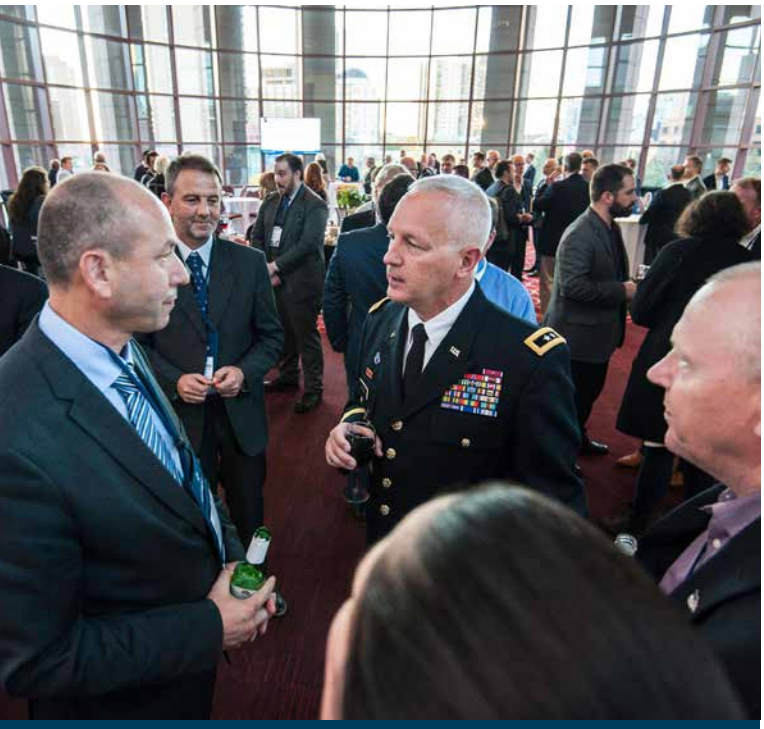
www.wellsfargo.com

ProcessBolt

Silver Sponsor

ProcessBolt automates vendor risk assessments for both enterprises and their vendors. Our hosted platform saves time, improves efficiency and reduces risk through improved workflow and collaboration. Customers include small, mid-sized and enterprise companies in North America and Europe including multiple Fortune 500 clients.

www.processbolt.com



Cyber Security Terminology

ACCESS CONTROL
The process of granting or denying specific requests for or attempts to: 1) obtain and use information and related information processing services; and 2) enter specific physical facilities

ADVANCED PERSISTENT THREAT (APT)
An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception).

AIR GAP
To physically separate or isolate a system from other systems or networks.

ATTACK PATH
The steps that an adversary takes or may take to plan, prepare for, and execute an attack.

ATTACK PATTERN
Similar cyber events or behaviors that may indicate an attack has occurred or is occurring, resulting in a security violation or a potential security violation.

ATTACK SIGNATURE
A characteristic or distinctive pattern that can be searched for or that can be used in matching to previously identified attacks.

AUTHENTICATION
The process of verifying the identity or other attributes of an entity (user, process, or device).

AUTHORIZATION
A process of determining, by evaluating applicable access control information, whether a subject is allowed to have the specified types of access to a particular resource.

BACKDOOR
A backdoor is a tool installed after a compromise to give an attacker easier access to the compromised system around any security mechanisms that are in place.

BEHAVIOR MONITORING
Observing activities of users, information systems, and processes and measuring the activities against organizational policies and rule, baselines of normal activity, thresholds, and trends.

BLACKLIST
A list of entities that are blocked or denied privileges or access.

BLUE TEAM
A group that defends an enterprise's information systems when mock attackers (i.e., the Red Team) attack, typically as part of an operational exercise conducted according to rules established and monitored by a neutral group (i.e., the White Team).

BOT
A computer connected to the Internet that has been surreptitiously / secretly compromised with malicious logic to perform activities under the command and control of a remote administrator.

BUG
An unexpected and relatively small defect, fault, flaw, or imperfection in an information system or device.

CHECKSUM
A value that is computed by a function that is dependent on the contents of a data object and is stored or transmitted together with the object, for the purpose of detecting changes in the data.

CIP
Critical Infrastructure Protection. The North American Electric Reliability Corporation (NERC), which FERC directed to develop Critical Infrastructure Protection (CIP) cyber security reliability standards.

CIPHERTEXT
Data or information in its encrypted form.

CLOUD COMPUTING
A model for enabling on-demand network access to a shared pool of configurable computing capabilities or resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

COMPUTER (DIGITAL) FORENSICS
The processes and tools to create a bit by bit copy of a an electronic device (collection and acquisition) for the purpose of analyzing and reporting evidence; gather and preserve evidence that is legally defensible and does not alter the original device or data.

CONTINUITY OF OPERATIONS PLAN
A document that sets forth procedures for the continued performance of core capabilities and critical operations during any disruption or potential disruption.

CRITICAL INFRASTRUCTURE
The systems and assets, whether physical or virtual, so vital to society that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of these matters.

CRYPTANALYSIS
The operations performed in defeating or circumventing cryptographic protection of information by applying mathematical techniques and without an initial knowledge of the key employed in providing the protection.

CSIRT
Cyber Security Incident Response Team

CYBER MUNITIONS
Technology system that has a purpose of causing harm and destruction by altering the running state of another system without permission.

DATA BREACH
The unauthorized movement or disclosure of sensitive information to a party, usually outside the organization, that is not authorized to have or see the information.

DATA LOSS PREVENTION
A set of procedures and mechanisms to stop sensitive data from leaving a security boundary.

DATA MINING
The process or techniques used to analyze large sets of existing information to discover previously unrevealed patterns or correlations.

DENIAL OF SERVICE (DOS)
An attack that prevents or impairs the authorized use of information system resources or services.

DIGITAL FORENSICS
The processes and specialized techniques for gathering, retaining, and analyzing system-related data (digital evidence) for investigative purposes.

DIGITAL RIGHTS MANAGEMENT (DRM)
A form of access control technology to protect and manage use of digital content or devices in accordance with the content or device provider's intentions.

DIGITAL SIGNATURE
A value computed with a cryptographic process using a private key and then appended to a data object, thereby digitally signing the data.

DISTRIBUTED DENIAL OF SERVICE (DDOS)
A denial of service technique that uses numerous systems to perform the attack simultaneously.

DMZ
DeMilitarized Zone. A physical or logical subnetwork where publicly facing internet connections occur; a subnetwork where an organization's external-facing services are exposed to an untrusted network (i.e. internet).

DOXING
The process or technique of gathering personal information on a target or subject, and building a dossier with the intent to cause harm.

DYNAMIC ATTACK SURFACE
The automated, on-the-fly changes of an information system's characteristics to thwart actions of an adversary.

ELECTRONIC SIGNATURE
Any mark in electronic form associated with an electronic document, applied with the intent to sign the document.

ENTERPRISE RISK MANAGEMENT
A comprehensive approach to risk management that engages people, processes, and systems across an organization to improve the quality of decision making for managing risks that may hinder an organization's ability to achieve its objectives.

EVENT LOGS
The computer-based documentation log of all events occurring within a system.

EXFILTRATION
The unauthorized transfer of information from an information system.

EXPLOIT
A technique to breach the security of a network or information system in violation of security policy.

EXPOSURE
The condition of being unprotected, thereby allowing access to information or access to capabilities that an attacker can use to enter a system or network.

FIREWALL
A physical appliance or software designed to control inbound and/or outbound electronic access.

HASH VALUE
A numeric value resulting from applying a mathematical algorithm against a set of data such as a file.

HASHING
A process of applying a mathematical algorithm against a set of data to produce a numeric value (a "hash value") that represents the data. The result of hashing is a value that can be used to validate if a file has been altered. Frequently used hash functions are MD5, SHA1 and SHA2

IDENTITY AND ACCESS MANAGEMENT
The methods and processes used to manage subjects and their authentication and authorizations to access specific objects.

INCIDENT
An occurrence that actually or potentially results in adverse consequences to an information system or the information that the system processes, stores, or transmits and that may require a response action to mitigate the consequences.

INCIDENT HANDLER (CYBER SECURITY)
The person assigned to lead a team of subject matter experts in cyber security and how to respond to adverse security events.

INDUSTRIAL CONTROL SYSTEM
An information system used to control industrial processes such as manufacturing, product handling, production, and distribution or to control infrastructure assets.

INTEGRITY
The property whereby information, an information system, or a component of a system has not been modified or destroyed in an unauthorized manner.

INTRUSION DETECTION
The process and methods for analyzing information from networks and information systems to determine if a security breach or security violation has occurred.

KEYLOGGER
Software or hardware that tracks keystrokes and keyboard events, usually surreptitiously / secretly, to monitor actions by the user of an information system.

MACRO VIRUS
A type of malicious code that attaches itself to documents and uses the macro programming capabilities of the document's application to execute, replicate, and spread or propagate itself.

MALWARE
Software that compromises the operation of a system by performing an unauthorized function or process.

MITIGATION
The application of one or more measures to reduce the likelihood of an unwanted occurrence and/or lessen its consequences.

MOVING TARGET DEFENSE
The presentation of a dynamic attack surface, increasing an adversary's work factor necessary to probe, attack, or maintain presence in a cyber target.

MSSP
Managed Security Service Provider

NIST
National Institute of Standards and Technology. The 800 series (NIST 800) covers cyber and information security.

OPEN SOURCE
Denoting software whose original source code is made free and available with no restrictions on use, selling, distribution or modification of the code.

OPEN SOURCE INTELLIGENCE
Intelligence collected from publicly available sources

OPEN SOURCE TOOLS
Tools that are made with open source code.

OPERATIONAL EXERCISE
An action-based exercise where personnel rehearse reactions to an incident scenario, drawing on their understanding of plans and procedures, roles, and responsibilities.

PACKET CAPTURES
The process of collecting, or capturing, network packets as they are being sent and received; used in diagnosing and solving network problems.

PENETRATION TESTING (PEN TEST)
An evaluation methodology whereby assessors actively probe for vulnerabilities and attempt to circumvent the security features of a network and/or information system.

PHISHING
A digital form of social engineering to deceive individuals into providing sensitive information.

PRIVATE KEY
A cryptographic key that must be kept confidential and is used to enable the operation of an asymmetric (public key) cryptographic algorithm.

PUBLIC KEY
The publicly-disclosed component of a pair of cryptographic keys used for asymmetric cryptography.

RDP
Remote Desktop Protocol. A Microsoft protocol through which a desktop or server may be accessed by a remote client.

RECOVERY
The activities after an incident or event to restore essential services and operations in the short and medium term and fully restore all capabilities in the longer term.

RED TEAM
A group authorized and organized to emulate a potential adversary's attack or exploitation capabilities against an enterprise's cybersecurity posture.

REDUNDANCY
Additional or alternative systems, sub-systems, assets, or processes that maintain a degree of overall functionality in case of loss or failure of another system, sub-system, asset, or process.

RESILIENCE
The ability to adapt to changing conditions and prepare for, withstand, and rapidly recover from disruption.

RESPONSE
The activities that address the short-term, direct effects of an incident and may also support short-term recovery.

RISK MANAGEMENT
The process of identifying, analyzing, assessing, and communicating risk and accepting, avoiding, transferring or controlling it to an acceptable level considering associated costs and benefits of any actions taken.

ROAMING PROFILE
A configuration in which the user profile within the domain is stored on a server and allows authorized users to log on to any computer within a network domain and have a consistent desktop experience.

ROOTKIT
A set of software tools with administrator-level access privileges installed on an information system and designed to hide the presence of the tools, maintain the access privileges, and conceal the activities conducted by the tools.

SCRIPTKIDDIE
An unskilled or non-sophisticated individual using pre-made hacking techniques and software to attack networks and deface websites.

SECURITY AUTOMATION
The use of information technology in place of manual processes for cyber incident response and management.

SECURITY POLICY
A rule or set of rules that govern the acceptable use of an organization's information and services to a level of acceptable risk and the means for protecting the organization's information assets.

SIEM
System Incident and Event Management. Tools and processes that collect data generated from devices and services to perform real time and historical correlated analysis to detect security, compliance and service levels events.

SIGNATURE
A recognizable, distinguishing pattern.

SITUATIONAL AWARENESS
Comprehending information about the current and developing security posture and risks, based on information gathered, observation and analysis, and knowledge or experience.

SOFTWARE ASSURANCE
The level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at any time during its lifecycle, and that the software functions in the intended manner.

SPEARPHISHING
An email or electronic communications scam targeted towards a specific individual, organization, or business.

SPOOFING
Faking the sending address of a transmission to gain illegal or unauthorized entry into a secure system. Extended The deliberate inducement of a user or resource to take incorrect action. Note: Impersonating, masquerading, piggybacking, and mimicking are forms of spoofing.

SPYWARE
Software that is secretly or surreptitiously installed into an information system without the knowledge of the system user or owner.

TABLETOP EXERCISE
A discussion-based exercise where personnel meet in a classroom setting or breakout groups and are presented with a scenario to validate the content of plans, procedures, policies, cooperative agreements or other information for managing an incident.

THREAT AGENT
An individual, group, organization, or government that conducts or has the intent to conduct detrimental activities.

THREAT ASSESSMENT
The product or process of identifying or evaluating entities, actions, or occurrences, whether natural or man-made, that have or indicate the potential to harm life, information, operations, and/or property.

TICKET
In access control, data that authenticates the identity of a client or a service and, together with a temporary encryption key (a session key), forms a credential.

TOPOLOGY DIAGRAM
A schematic diagram displaying how the various elements in a network communicate with each other. A topology diagram may be physical or logical.

TRAFFIC LIGHT PROTOCOL
A set of designations employing four colors (RED, AMBER, GREEN, and WHITE) used to ensure that sensitive information is shared with the correct audience.

TROJAN HORSE
A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program.

VIRUS
A computer program that can replicate itself, infect a computer without permission or knowledge of the user, and then spread or propagate to another computer.

VULNERABILITY
A characteristic or specific weakness that renders an organization or asset (such as information or an information system) open to exploitation by a given threat or susceptible to a given hazard. Extended Characteristic of location or security posture or of design, security procedures, internal controls, or the implementation of any of these that permit a threat or hazard to occur. Vulnerability (expressing degree of vulnerability): qualitative or quantitative expression of the level of susceptibility to harm when a threat or hazard is realized.

WHITE TEAM
A group responsible for refereeing an engagement between a Red Team of mock attackers and a Blue Team of actual defenders of information systems.

WHITELIST
A list of entities that are considered trustworthy and are granted access or privileges.

WORK FACTOR
An estimate of the effort or time needed by a potential adversary, with specified expertise and resources, to overcome a protective measure.

WORM
A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself.

ZERO DAY
"The Zero Day is the day a new vulnerability is made known. In some cases, a zero day exploit is referred to an exploit for which no patch is available yet. (Day one is day at which the patch is made available).
Comprehending information about the current and developing security posture and risks, based on information gathered, observation and analysis, and knowledge or experience."

Cyber Security Acronyms

3DES	Triple Data Encryption Standard
ACL	Access Control List
ADP	Automated Data Processing
AES	Advance Encryption Standard
AH	Authentication Header
AIS	Automated Information System
AO	Area of Operations
APT	Advanced Persistent Threat
BCP	Business Continuity Plan
BIA	Business Impact Analysis
BoD	Beginning of Day
BYOD	Bring Your Own Device
CA	Certificate Authority
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CSO	Chief Security Officer
CAPEC	Common Attack Pattern Enumeration and Classification
CERT	Computer Emergency Response Team
DES	Data Encryption Standard
DHS	Department of Homeland Security
DRP	Disaster Recovery Plan
DAC	Discretionary Access Control
DNS	Domain Name System
ECC	Elliptical Curve Cryptography
EFT	Electronic Funds Transfer
ESP	Encapsulation Security Payload
EW	Electronic Warfare
FISMA	Federal Information Security Act
FTP	File Transfer Protocol
FO	Forward Observer
GRC	Governance Risk Management and Compliance
HIPPA	Health Insurance
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IDS	Intrusion Detection System
IaaS	Infrastructure as a Service
IANA	Inernet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IG	Interior Guard
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
IPX	Internetwork Packet Exchange
IS	Information Systems
ISO	International Standards Organization
ISP	Internet Service Provider
KRI	Key Risk Indicator
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MAC	Mandatory Access Control
MAC Address	Media Access Control
MAN	Metropolitan Access Network
NAT	Network Address Translation
NetBIOS	Network Basic Input/Output System
NIC	Network Interface Control
NIAP	National Information Assurance Partnership
NIST	National Institute for Standards and Technology
NNTP	Network News Transfer Protocol
OpSec	Operational Security
OS	Operating System
OSI	Open Systems Interconnect
OWASP	Open Web Application Security Project
PaaS	Platform as a Service
PIN	Personal Identification Number
PKI	Public Key Infrastructure
POTS	Plain Old Telephone Service
PSTN	Public Switched Telephone Network
RA	Registration Authority
RAS	Remote Access Service
ROI	Return On Investment
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SaaS	Software as a Service
SCADA	Supervisory Control and Data Acquisition
SDLC	Software Development Life Cycle
SDO	Service Delivery Objectives
SecaaS	Security as a Service
SET	Secure Electronic Transaction
SET	Social-Engeneer Toolkit
SFA	Single Factor Authentication
SLA	Service Level Agreement
S/MIME	Secure Multipurpose Internet Mail Extension
SMTP	Simple Mail Transfer Protocol
SoD	Segregation/Seperation of Duties
SoD	Start of Day
SPX	Sequenced Packet Exchange
SSH	Secure Shell
SSL	Secure Socket Layer
TCO	Total Cost of Ownership
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TKIP	Temperal Key Integrety Protocol
TLS	Transport Layer Security
URL	Uniform Resource Locator
UDP	User Datagram Protocol
VLAN	Vitrual Local Area Network
VPN	Virtual Private Network
VoIP	Voice Over Internet Protocol
WAN	Wide Area Network
WAP	Wi-Fi Protected Access
WAP2	Wi-Fi Protected Access II
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
XSS	Cross-site Scripting

Cyber Security Resources

CNSSI 4009, National Information Assurance (IA) Glossary, June 2006.

CISSPÆ All-in-One Exam Guide, Forth Edition, Shon Harris, The McGraw-Hill Companies, 2008.

Official (ISC)2 Æ Guide To The CISSPÆ CBK by Harold F. Tipton, et. al., Auerbach Publications, 2006.

Official (ISC)2 Æ Guide To The CISSPÆ Exam by Susan Hansche, et. al., Auerbach Publications, 2004.

NIST SP 800-16, Information Technology Security Training Requirements: A Role- and Performance-Based Model, April 1998.

NIST SP 800-30, Risk Management Guide for Information Technology Systems, July 2002.

NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, May 2004.

NIST SP 800-53, Rev. 2, Recommended Security Controls for Federal Information Systems, December 2007.

NIST SP 800-64 Rev. 1, Security Considerations in the Information System Development Life Cycle, June 2004.

NIST SP 800-61, Computer Security Incident Handling Guide, January, 2004.

NIST SP 800-65, Integrating IT Security into the Capital Planning and Investment Control Process, January 2005.

NIST SP 800-67, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, May 2004.

NIST SP 800-77, Guide to IPsec VPNs, December 2005.

FIPS 46-3, Data Encryption Standard (DES), October 1999.

FIPS 140-2, Security Requirements for Cryptographic Modules, May 2001.

FIPS 180-2, Secure Hash Standard (SHS), August 2002.

FIPS 185, Escrowed Encryption Standard, February 1994.

FIPS 186-2, Digital Signature Standard (DSS), January 2000.

FIPS 197, Advanced Encryption Standard, November 2001.

FIPS 198, The Keyed-Hashed Message Authentication Code (HMAC), March 2002.

FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, December 2003.

FIPS 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006.

Information Assurance Technical Framework (IATF), Release 3.1, NSA IA Solutions Technical Directors, September 2002.

ISO/IEC 15408-1:2005, Evaluation Criteria for IT Security ñ Part 1: Introduction and General Model, 2005.

ISO/IEC 15408-2:2005, Evaluation Criteria for IT Security ñ Part 2: Security Functional Requirements, 2005.

ISO/IEC 15408-3:2005, Evaluation Criteria for IT Security ñ Part 3: Security Assurance Requirements, 2005.

BS ISO/IEC 17799:2005, Code of Practice for Information Security Management, 2005.

Control Objectives for Information and related Technology (COBIT), Release 4.0, IT Governance Institute, 2005.

ISO/IEC 21827, Systems Security Engineering ñ Capability Maturity Model (SSE-CMMÆ), 2002.

ISO/IEC 27001, Information Security Management Systems ñ Requirements, 2005.

Draft MIL-STD-499C, Systems Engineering, Aerospace Corporation, April 15, 2005.

ISO/IEC 15288:2008(E), IEEE Std 15288-2008, Systems and Software Engineering ñ System Life Cycle Processes, February 1, 2008.

IEEE STD 1220-2005, IEEE Standard for Application and Management of the Systems Engineering Process, September 9, 2005.

IEEE/EIA 12207.0-1996, Industrial Implementation of International Standard ISO/IEC 12207:1995 Software Life Cycle Processes, March 1998.

IEEE/EIA 12207.1-1997, Industrial Implementation of International Standard ISO/IEC 12207:1995 Software Life Cycle ProcessesóLife Cycle Data, April 1998.

IEEE/EIA 12207.2-1997, Industrial Implementation of International Standard ISO/IEC 12207:1995 Software Life Cycle ProcessesóImplementation Considerations, April 1998.

DoD 5200.28-STD, Department of Defense Trusted Computer System Evaluation Criteria, December 1985. (a.k.a. Orange Book).

NCSC-TG-003, Version-1 A, Guide to Understanding Discretionary Access Control in Trusted Systems, September 30, 1987. (a.k.a. Neo-Orange Book).

Information Technology Security Evaluation Criteria (ITSEC), Version 1.2, June 1991.

10th Anniversary Cyber Security Summit Minneapolis, MN

SAVE THE DATE

OCTOBER 26–28, 2020

Stay connected to **cybersecuritysummit.org** to follow updates on next year's event!

/cyber-security-summit /cssummit /cs_summit cybersummitmn