



11TH ANNUAL LEADERSHIP EVENT

CYBER SECURITY SUMMIT

Security solutions through collaboration.™

October 25-27, 2021
cybersecuritysummit.org

POWER & PERIL OF CONNECTION

#cybersummitMN

FEATURED SPONSORS

Founding Partner



TECHNOLOGICAL
LEADERSHIP INSTITUTE

Presenting Plus
Sponsor

zoom

Presenting Sponsors

 **BlackBerry**
Intelligent Security. Everywhere.

 **CONTRAST**
SECURITY



cybereason

 Recorded Future®

Custom Sponsor


take control.

Printing Sponsor

UNISYS

Platinum Sponsors



 MINNESOTA
IT SERVICES

Diamond Sponsors


AXONIUS


Building a better
working world



THE MASTER'S DEGREE FOR SECURITY TECHNOLOGY LEADERS

tli.umn.edu

Become a Security Leader & Shape Tomorrow's Future

The pandemic has changed the way we live and work, and escalated the importance of security across all 16 sectors of critical infrastructure.

Become a next-generation leader trained with the critical skills and foresight to prevent, protect and respond to today's growing security demands with an **M.S. in Security Technologies**.

3.1 M

Gap in global
cybersecurity
professionals

Source: ISC²

>464K

Open cybersecurity
jobs in the U.S.

Source: Cyberseek.org

33%

Expected Job Growth
for Security Analysts
into 2030

Source: Bureau of Labor and Statistics

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

Nov. 10 at 5 p.m. in-person

Nov. 22 at noon online

Dec. 8 at 5 p.m. in-person

Contact TLI admissions at msst@umn.edu for additional details.

Thank You Sponsors + Exhibitors

Founding Partner



Presenting Plus Sponsor



Presenting Sponsors



Custom Sponsor



Platinum Sponsors



Printing Sponsor



Diamond Sponsors



Ruby Sponsors



Healthcare & Med Device Host



Small Business Host



Seminar Supporters



Silver Sponsors



Partners



Global Minnesota



InfraGard



Twin Cities MN Section



Conference Producer



Maximize Your Exposure in 2022

The 2021 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 2022 today and receive a 10% discount through December 31, 2021. For more information, contact:

Eileen Manning 612-308-1907 eileen.manning@cybersecuritysummit.org



The Power & Peril of Connection

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.

**Cyber Security Summit
2021 Co-chairs:**

JENNIFER CZAPLEWSKI
Senior Director, Cyber Security, Target

WADE VAN GUILDER
*Principal Advisor,
Cybersecurity SLED,
World Wide Technology*

**Cyber Security Summit
2021 Program Chair:**

TOM SHEFFIELD
*Senior Director
Technology, Target*

**Cyber Security Summit
Executive Producer:**

EILEEN MANNING
Co-founder

Connections are powerful. The value of our interpersonal connections in 2020 became clear as the pandemic changed the way we interact with colleagues, friends, and family. This period of isolation from one another has fallen alongside the rapid development of our world's digital connectivity. From smart fridges to smart doorbells, the proliferation of mobile devices and sensors in everyday items has created the most powerful network of interconnected devices imaginable. This connectivity comes with a huge amount of risk. Protecting the estimated 21.5 billion devices in use today requires security professionals to adapt and learn faster than ever before.

This is where the Power of Connection becomes critical. The 11th Annual Cyber Security Summit is our attempt to bring security professionals from around the world together to share ideas and learn from each other to maximize security effectiveness for everyone. The threat landscape is constantly evolving and our ability to Connect plays a significant role in our ability to adapt and adjust for the benefit of everyone.

The Cyber Security Summit strives to ensure that our speakers are horizon scanners. We look forward to hearing from over 100 cyber professionals. For example, Tuesday's opening will be delivered by Jen Easterly, Director of the Cybersecurity and Infrastructure Security Agency (CISA). Ms. Easterly has a long tradition of public service including two tours at the White

House and a two-time recipient of the Bronze Star. Tuesday's closing keynote follows in the same high-quality footsteps. FBI Executive Assistant Director Darrin Jones will provide a briefing on 'The Lawful Access Challenge'. He will describe the challenge faced by many federal, state, local, and tribal law enforcement agencies from "warrant-proof" encryption.

Director Easterly and EAD Jones' keynote speeches demonstrate our desire to provide a platform to leaders working to move the needle in cybersecurity. We want the Cyber Security Summit to equip you with the tools to combat the increasingly diverse array of threats practitioners face every day. Beyond these two fantastic keynote addresses, the Cyber Security Summit features a wide variety of briefings and panel discussions that apply to a broad spectrum of security professionals. From small business to the public sector, we pride ourselves on bringing you speakers that can provide meaningful support to tackle real-world issues.

Producing the Cyber Security Summit is a huge undertaking. Those responsible for its production number too highly to thank individually in this welcome letter. We want to extend our gratitude to the Cyber Security Summit's sponsors, Think Tank and committee members. Finally, we want to thank you, as security professionals, for your tireless work in an ever-changing space is crucial to the safety of our businesses, institutions, and families.

Summit Highlights

By the numbers

- three days
- 110 speakers
- 57 hours of programming
- 26 hours of continuing education credits
- 20 hours of open access programming
- 10 Award Honorees

Made Possible by...

- 45 sponsors and supporting organizations
- Over 70 volunteers collaborating
 - Leadership Team
 - Think Tank Advisors
 - Committee Members
- 12 months of planning, hundreds of hours of meetings, thousands of emails and countless phone calls

Continuing Professional Education Credits (CPEs)

Summit participation fulfills up to 26 hours, depending on the organization and sessions you participate in.

Open Access Sessions

Monday offers 16 hours of complimentary Technical Sessions and thanks to the support of the SBDC, Tuesday afternoon Small Business track is also free to attend and more robust than ever.

Women in Cyber

Begin the Summit networking on Monday morning, followed by online meditation and mindfulness session, moving into panels on mentoring and building and leading diverse teams all underwritten by our sponsors — 8:45–11:30 AM. Over lunch, via your Uber Eats certificate, Mount Everest Mountaineer and Cyber Professional Louise McEvoy inspires others reach their “summit!” Ticketed lunch 11:30 AM–12:30 PM for VIP All Access and Lunch purchased ticket holders.

New Public Sector Track

Eight hours of programming developed by government thought leaders from across the country

Visionary Leadership Awards start Wednesday morning recognizing leaders our peers have nominated and selected to receive Visionary Leadership Awards. (October 27, 2021) Then SAVE THE DATE for celebrating in-person on April 21, 2022 for VIP All-Access pass holders.

Post your comments about the Summit

Everyone who follows our Twitter or LinkedIn during the Summit will be entered to win a free VIP All-Access Pass to Cyber Security Summit 2022.

Post on both with the hashtag **#cybersummitMN** to be entered twice!



Contents

- 01 Thank you Sponsors + Exhibitors
- 02 Welcome from the 2021 Co-chairs
- 03 Summit Highlights
- 04 Think Tank + Committees
- 06 Personal Note of Thanks
- 07 Let's Celebrate this Spring
- 10 Your Virtual Summit Experience
- 12 Public Sector Workshop
- 16 Women in Cyber Security / WiCyS Minnesota
- 20 Tech Sessions
- 23 Cybereason - THREAT ALERT: Microsoft MSHTML Remote Code Execution Vulnerability
- 26 Healthcare & Med Device Seminar
- 28 IoT/IIoT/ICS/SCADA Collaboration
- 32 Small Business Seminar
- 34 The Morries™ Visionary Leadership Awards
- 36 Full Summit Agenda
- 41 Subscribe to our newsletter
- 42 Speaker Directory
- 49 Zoom — How to Upskill the HybridWorkforce with TailoredSecurity Training
- 50 Sponsors + Supporters
- 56 Index of Cyber Terminology
- 61 Save the Date for the 12th Annual Cyber Security Summit
- 62 Cyber Acronyms
- 64 TLI — Does Exponential Growth of Connected Devices Mean Exponentially Increased Risk?
- 65 Cyber Webinar Series

2021 Think Tank

SUMMIT CO-CHAIRS



Jennifer Czaplewski
Target



Wade Van Guilder
World Wide Technology



Jill Allison
Shuriken Cyber



Dr. Massoud Amin
University of MN



Anne Bader
The Int'l Cybersecurity Dialogue



John Bonhage
InfraGard



Andrew Borene
NCSC, ODNI



Christopher Buse
Old Republic



Sean Costigan
George C. Marshall European Ctr.



Tim Crothers
FireEye



Daniel Cunningham
3M



Sam Curry
Cybereason



Idrissa Davis
St Paul Public Schools



Loren Dealy Mahler
Dealy Mahler Strategies



Steen Fjalstad
Midwest Reliability Org.



Mary Frantz
Prescriptive Health, Inc.



Barb Fugate
United Bankers' Bank



Christopher Gabbard
CISA



Michelle Greeley
3M



Sam Grosby
Twilio



Judy Hatchett
Surescripts



Tim Herman
NUARI



Stefanie Horvath
U.S. Cyber Command, MNIT



Mike Johnson
TLI

2021 Committees

Cyber Women

Kris Boike, Federal Reserve Bank of Atlanta; Judy Hatchett, SureScripts; Eileen Manning, Cyber Security Summit; Tina Meeker*, Sleep Number; Milinda Rambel Stone, Bremer Bank; Lee Ann Villella, Proofpoint

Healthcare & Medical Device

Debra Bruemmer, Mayo Clinic; Jon Crosson, H-ISAC; Mary Diner*, Director, Optum; Wendy Feigal, Prime Therapeutics; Shelly L Gustafson, CMDC University of MN; Judy Hatchett*, CISO, SureScripts; Ken Hoyme, Boston Scientific; Judd Larson, Medtronic; Michael Larson, Ecolab; John Seaman, Anxionius; Christofer Sears, Cofense; Benjamin Stock, Ord; Dan Teguis, Armis

IT/OT/IoT/ICS Collaboration

Jamison Utter, Ord; Tom Smertneck, ICA; Paul Veeneman*, Beryllium InfoSec Collaborative; Joe Weiss, Applied Control Solutions, LLC

Leadership Team

Tim Crothers, FireEye; Jennifer Czaplewski*, Target; Judy Hatchett, Surescripts; Brigadier General Horvath, US Cyber Command; Eileen Manning, Cyber Security Summit; Dave Notch, Medtronic; Tom Sheffield, Target; Wade Van Guilder*, World Wide Technology

Newsletter

Benjamin Cook, The Event Group; Loren Dealy Mahler, Dealy Mahler Strategies; Chris Veltsos, Dr Infosec, Cyber Risk Strategist; Digital Trust Advisor

Public Sector

Chris Buse, former MN State CISO, CISO, Old Republic; Stephen Ellis, Government Solutions Lead, Zoom; Renee Heinbuch, Director of Information Technology at Washington County, Minnesota; Ralph Johnson, CISO, LA County; Joel Kennedy, Genesys; Carlos Kizzee*, VP, Stakeholder Engagement, CIS/MS-ISAC; Rick King, MN Blue Ribbon Commission Representative; Darrell Kesti, Director, Ord; Leah Patton, Executive Director, MN County IT Leadership Association at Association of Minnesota Counties; Lisa Meredith, Executive Director at Minnesota Counties Computer Cooperative; Michelle Nolan, Stakeholder Engagement Team, Center for Internet Security; Melissa Reeder, CISO, Chief Information Officer at League of Minnesota Cities; Shawn Riley, CIO, North Dakota; Tony Sager, CIS; Rohit Tandon*, MN State CISO; Wade Van Guilder, WWT (Summit Co-Chair); Gretchen White, CISO, Minnesota Judicial Branch



Mike Kearn
US Bank



Sharon Kennedy-Vickers
City of St. Paul



David La Belle
Charter Solutions



Brett Lawler
Xcel Energy



Mike Lexa
CNH Industrial



Eileen Manning
Cyber Security Summit



Tina Meeker
Sleep Number



Jerrod Montoya
Montoya Law Office, OATI



David Notch



Gregory Ogdahl
MoneyGram



Jeffrey Allen Peal, III
SullivanCotter



Mark Ritchie
Global Minnesota



Erik Roeske
Minnesota State Patrol



Frank Ross
General Mills



Tony Sager
Center for Internet Security



Phil Schenkenberg
Taft Law



Tom Sheffield
Target



Scott Singer
CyberNINES



Chad Svihel
Outsource Consultants



Rohit Tandon
State of MN, MNIT Services



Catharine Trebnick
Colliers International



Chris Veltsos
Dr. InfoSec



Lee Ann Villella
Proofpoint



Kristi Yauch
Winnebago

Program Committee

Scott Ammon, Insights; Tim Crothers, FireEye; Jennifer Czaplowski, Target; Michelle Greeley, 3M; Tim Herman, NUARI; Mike Kearn, US Bank; Mike Lexa, Donaldson; Tina Meeker, Sleep Number; Jeff Peal, SullivanCotter; Tom Sheffield*, Target; Kristi Yauch, Winnebago; Dileep Sivaraman, Target; Wade Van Guilder, World Wide Technology

Small Business

Doris Frost, Bremer Bank; Christopher Gabbard, CISA; Earl Gregorich, SBDC; Twila Kennedy, SBA; Eileen Manning*, Cyber Security Summit; Scott Singer, CyberNINES; Milinda Rambel Stone, Bremer Bank; Andy Tellijohn, Upsize Minnesota; Lyle Wright, SBDC

Rapporteurs

Simon Bracey-Lane, PhD Student, University of Canberra, Australia; Denna Downhour, Information Security Senior Risk Analyst, Bremer Bank; Student, University of Minnesota Technological Leadership Institute; Lindsey Konerza, IT Business Systems Analyst, ASR-IT and Student, University of Minnesota Technological Leadership Institute

Summit Guide

Simon Bracey-Lane, PhD Student, University of Canberra, Australia; Heidi Branes, The Event Group; Libby McGrath, Graphic Design Intern; Andy Tellijohn, Upsize Minnesota

Terminology

Simon Bracey-Lane, PhD Student, University of Canberra, Australia

Virtual Platform

Benjamin Cook*, The Event Group; Heidi Branes, The Event Group; Jennifer Czaplowski, Target; Steen Fjalstad, Midwest Reliability Organization; David LaBelle, Charter Solutions; David Notch, Medtronic; Mike Patten, M J Patten Associates; Mark Ritchie, Global Minnesota; Keely Ross, Zoom; Frank Ross, General Mills; Tom Sheffield, Target; Wade Van Guilder, World Wide Technology

Visionary Leadership Awards

Chris Buse*, Old Republic Title; Mike Kearn, US Bank

Webinars

Benjamin Cook, The Event Group; Sean Costigan, Professor, George C. Marshall European Center

** denotes Chair/Co-chair*

If you'd like to join the collaboration and participate on a committee, please contact

Eileen.Manning@cybersecuritysummit.org.



A Personal Note of Thanks

Dear Friends,

Thank you for joining us!

The decision to go virtual once again, was not an easy one. However, we are grateful to be returning for our 11th Annual Cyber Security Summit to deliver a fantastic array of visionary cybersecurity discussions.

Unfortunately, our current Summit theme 'The Power and Peril of Connection' and last year's "The Ripple Effect" seem ambiguously connected to current events due to both the 'Power' of connecting coupled with the potential 'Peril' associated with gathering en masse.

Prior to printing the Summit Guide I continued to question the decision to go virtual when one of our fully vaccinated team members tested positive for Covid after attending a rock concert. Subsequently our entire team had to be tested with every cough, sneeze and sniffle brought into question! As I sent a notification to my beloved team, I thought how horrible it would be to send a similar note off to the over one thousand cyber warriors attending this Summit. You are just too important to our global security for us to risk connecting in-person at this time.

Without question, this year's Summit offers an unsurpassed lineup of global cybersecurity thought leaders willing to share insider insights on the timeliest of issues. We're thankful that so many luminaries invest their commitment to this Minnesotan based hub of innovation.

This is the second year of both our Newsletter and Webinar series. These resources provide the intellectual bedrock of the Summit throughout the year. Identifying, monitoring, and analyzing trends to be more comprehensively explored at the Summit. Led by Sean Costigan, each free hour-long webinar examines vexing challenges facing the international community and offers knowledge and perspective.

A key element of the Cyber Security Summit is celebrating those on the cutting edge of the field at all levels. Each year the Summit presents awards in a variety of categories, with one special award being selected for Founder's Choice.

This year's category is to recognize an outstanding company whose work improved our national security defense. Our team of Judges agreed that the work done by Mandiant and your leader Kevin Mandia to alert everyone to the SolarWinds breach was particularly noteworthy to recognize with this award.

Whilst all the content at this year's Summit will be highly engaging and educational, one new event series we are excited about is the Public Sector Track. Here, we will focus on the cyber challenges faced by State, Local, Tribal, and Territorial governments and the ecosystem that operates around them. We'll stand back and examine the cyber state-of-play for SLTTs, and drill down to specific examples. We'll look at what this community has in common both internally as well as with the economy at large.

I want to thank our Think Tank for their contributions and offer a special thank-you to this year's Co-Chairs: Jennifer Czaplewski, Wade Van Guilder and Program Chair, Tom Sheffield.

Finally, this event is also the product of teamwork which includes contributions from our Think Tank, committee members and vital support from our sponsors. Please visit our valued solution strategy partners online through our virtual tradeshow to discover the resources available. And, if you want to be part of producing the 12th Annual Summit, please visit the Cyber Security Summit booth.

I look forward to celebrating IN-PERSON, Covid permitting, at our VIP Reception for All-Access pass holders on Thursday, April 21, 2021 and then hopefully back in-person at the 12th Annual Summit on October 24-26, 2022 here in Minneapolis!

Eileen Manning

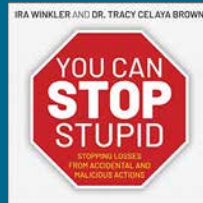
Eileen Manning, Co-Founder & Executive Producer
Cyber Security Summit
cybersecuritysummit.org
eileen.manning@cybersecuritysummit.org
612-308-1907

Cyber Security Summit Spring Gala

Join us Thursday, April 21, 2022

5:00 – 7:00pm – VIP Reception with Casino Party

Doubletree Hotel, Bloomington



JUST ANNOUNCED

Celebrated cybersecurity author **Ira Winkler** will be with us at the Gala for a **VIP Book Signing** of his current best seller, *You CAN Stop Stupid*. Bring your book from the Summit and your dancing shoes.

A key distinction of the Cyber Security Summit is the stellar networking and community relationships we've built over the years at this premier industry forum. Next Spring we are creating a special opportunity to reconnect with peers, honored guests and security leaders as we gather for a Summit gala in the 'Metro'.

Celebrate with friends in style as we honor our 2020 & 2021 Visionary Leadership Award Winners. Join with our Think Tank Advisors, expert speakers and 2022 Summit Co-chairs.

If you've purchased a VIP All Access Pass, you are good to go. Others are welcome to register now at: www.cybersecuritysummit.org

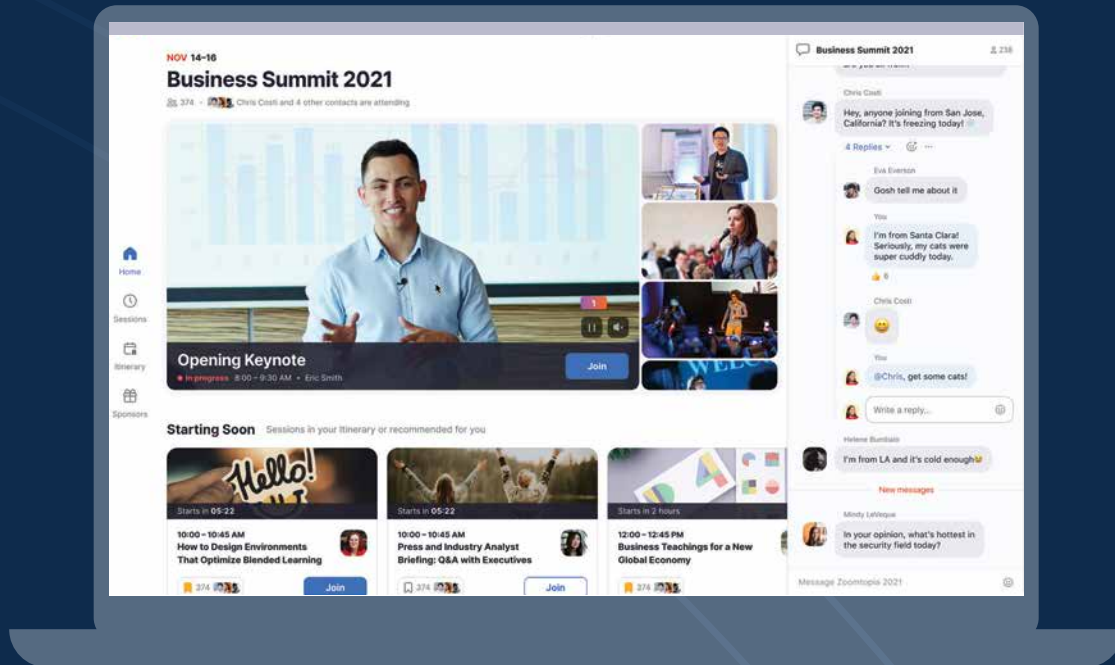
Don't miss this spectacular event – plan to join us, invite your friends and colleagues, and be sure to save the date!



Sponsored by:
your logo here



zoomevents



An **all-in-one solution** with the power to create virtual experiences that attendees will love.

EVENTS.ZOOM.US

Your Virtual Summit Experience

Lobby

Upon entering the virtual lobby during the Summit, you will find a 24/7 Info Desk to assist with any technical questions and easy to navigate links to the Auditorium to view the sessions you have registered for, and the EXPO Hall to visit with Security Solution Providers and quick links to the Scavenger Hunt, LeaderBoard, Job Search and Briefcase of any content you download during the Summit.



Auditorium

Click on the auditorium to easily navigate to the sessions you have registered for. Please go online and build your agenda prior to the start of the Summit.

My Sessions

Start your experience by building your personal agenda and adding your sessions to your calendar.

My Schedule Monday Tuesday Wednesday

OCTOBER 25TH

Public Sector Workshop - Welcome Kickoff

Mon, October 25, 8:00 AM
14 days, 13 hours, 57 minutes

Rate This Presentation

+ Add to My Schedule

+ Add to Calendar

Rohit Tandon, CISO, Minnesota and Carlos Kizze, MS-ISAC Stakeholder Engagement will introduce the Public Sector Summit; outlining key challenges, requirements, capabilities, and solutions being implemented to address and mitigate the cyber security concerns for this unique sector.



Rohit Tandon
Assistant Commissioner, State Chief Information Security Officer, State of Minnesota, MNIT Services



Carlos Kizze
Vice President, Stakeholder Engagement, MS-ISAC, Center for Internet Security

EXPO Hall

Exploring the EXPO Hall you can meet with Security Solution Providers, watch presentations, search for jobs, chat with others, and participate in both the scavenger hunt and leaderboard activities. PLUS download resources to use post Summit from the items you add to your virtual briefcase.



Start Secure. Stay Secure.®



CIS SecureSuite®

- CIS Benchmarks™ for secure configuration guidelines
- CIS-CAT® Pro for assessing and monitoring configuration
- CIS CSAT for tracking implementation of the CIS Critical Security Controls®
- CIS Build Kits for rapidly implementing CIS Benchmarks

Save up to 20% on a new membership

September 15–October 31 • Promo code: SECURE21



MS-ISAC®

Multi-State Information
Sharing & Analysis Center®

CIS SecureSuite is available at no cost to
U.S. SLTTs. Join the MS-ISAC to get started.
Visit www.cisecurity.org for more information.



**Center for
Internet Security®**



NEW

Public Sector Workshop

MONDAY, OCTOBER 25, 2021 | 8:00 AM- 5:00 PM

Event Vision: The public sector - it's more than the government. Our way of life is organized, delivered, and made possible by countless publicly controlled or publicly funded agencies, enterprises, and other entities delivering a wide range of products, services, and programs. And as citizens and taxpayers we expect quality, convenience, and cost-effectiveness from all of these. But the promise of technology and connectivity to deliver these benefits is being undermined by the cybersecurity perils that plague our entire economy and undermine our confidence. In this track, we will focus on the cyber challenges faced by State, Local, Tribal, and Territorial governments and the ecosystem that operates around them.

AGENDA

8:00 AM

Welcome Kickoff

Co-chairs, Rohit Tandon and Carlos Kizzee, will introduce the Public Sector Summit; outlining key challenges, requirements, capabilities, and solutions being implemented to address and mitigate the cyber security concerns for this unique sector.

Rohit Tandon, Assistant Commissioner, State Chief Information Security Officer, State of Minnesota; Carlos Kizzee, Vice President, Stakeholder Engagement, MS-ISAC

8:15 AM

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

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

Speakers: Eugene Kipniss, MS-ISAC Member Programs Manager, Center for Internet Security

8:45 AM

Why Your Organization's Endpoint Data Is Your Greatest Source of Risk

Government agencies and educational institutions are challenged to secure and manage a new kind of hybrid network. Not on-prem and cloud, but work in the office, work from home, work from anywhere. Your organization is more dispersed than ever — leaving you with an incomplete picture of your cyber and data risk.

Start by focusing on one of the greatest challenges you face: endpoint devices. Endpoints have expanded beyond your organization's perimeter and are operating in the badlands of the outside world. This makes them and the data that is on them ideal targets for cyber attackers. Traditional risk scoring systems do not factor endpoint data and may create a false sense of security. Your organization needs visibility to help break down the data silos and close the accountability, control and resiliency gaps to improve your cyber risk.

Speaker: Gary Buonacorsi, Chief Technology Officer, Chief IT Architect, US State and Local Government and Education, Tanium

9:15 AM

Critical Success Factors in Cybersecurity

Irrespective of whether the organization is public or private sector, any information security management program relies on several requirements and expectations at the organizational level to be successful. The degree of success is dependent upon the extent that these success factors are supported by the organization. This presentation will discuss the nature of these success factors.

Speaker: Michael Gregg, Interim CISO, State of North Dakota

9:45 AM — Solutions Strategy Break in EXPO**10:00 AM****How to collaborate Cyber Intelligence and Sharing Cyber Resources**

How someone working at a city and county level can better collaborate across the State and Nation.

Speaker: Col. Teri Williams, DHS

10:30 AM**Grant Funding to Protect Technology from Cyber Threats**

Integrating cyber practices for both givers and receivers of funding. Funding is generally associated with services for residents of your community. Technology plays a critical role in delivering critical services and protecting that technology from cyber threats also requires investment. What are some of the approaches to seek out investment opportunities that defend the technology and protect recipients' data around social services.

Speakers: Rohit Tandon, CISO, State of Minnesota, MNIT Services; Stephen Ellis, Government Solutions Lead, Zoom

11:00 AM**Cybersecurity: Finding Common Ground in the Political Landscape**

Cyber Zeros and Ones should not be red or blue. Explaining to your legislatures how technology has a corner stone impact to all citizens. Consumers have a choice to interact with private sector and provide personal data, however in the public sector the data collected is not optional for residents. This should place a higher burden on public sector to protect the sensitive data. There are also public disclosure expectations. (In the event of a data breach - how does the state rebuild confidence). Purpose - describe the why and suggest how.

Speakers: Jacqui Irwin, Assembly member, 44th District, Chair, Select Committee on Cybersecurity, California State Assembly, DFL; Jim Nash, Assistant Minority Leader, Minnesota House of Representatives, GOP

12:30 PM**Smart Cities / Safe Cities**

Protecting citizens, service programs, infrastructure. How can we prepare for the smart cities that both public and private entities are responsible for defending? What are some strategies to ensure there is a good foundation to build on to protect privacy and defend the way of life.

Speaker: Jerry Dreisson, Deputy CIO, City of San Jose, CA

1:00 PM**Find. Build. Keep. Opening a Cyber Shop in the Public Sector**

How can the public sector find, attract, develop, and retain cyber talent in this competitive market? This session will cover how the Minnesota Judicial Branch and Montana have built their cyber security programs from the ground up, incorporating novel approaches to find talent and cost-effective ways to develop skills, while retaining employees by providing meaningful work in a diverse culture.

Speakers: Andy Hanks, CISO, State of Montana; Gretchen White, CISO, Minnesota Judicial Branch

1:30 PM**Public Sector Cyber Insurance**

Cyber Insurance for public sector is different from private. Models on how to self-insure, municipal risk pools. Vermont and Nevada are doing self-insurance. Presentation on cyber risk insurance in general and how public sector entities are approaching this issue. Attendees will learn the different approaches public entities can consider for insurance and how some select states and groups work together to share the cost and reduce the risk of cyber incidents.

Speaker: Ryan Spelman, VP Cyber Risk, Kroll

2:00 PM**Avoid a Cyber Splash**

In this session we will learn about real life examples of attacks to our utilities and SCADA systems. We hope to offer real steps on what the future holds for this important sector and what our public officials are doing to meet this real and rapidly evolving threat to our citizens.

Speaker: Darrell Kesti, Director, Ordr

2:30 PM**A Better Playbook for the Public Security Cyber Team: Introduction to Programmatic Distributed Empowerment for Information Security ("PDEISTM")**

"Information security isn't about information or security as much as it is about people. ALL PEOPLE. Traditional approaches to information security leave the CISO playing a game he/she can't win while those around them wander aimlessly around the field. Programmatic Distributed Empowerment for Information Security (or PDEISTM) is the method to change the game and put us all in a better position to win."

Speaker: Evan Francen, CEO, Security Studio

3:00 PM**Recommendations and Best Practices for Whole of State Governance to Mitigate Cyber Risk**

State government leaders must manage risk within a context where authority is distributed across sectors and levels and branches of government. Regardless of the structures and local culture that a governor and state legislature must operate within, they must establish cybersecurity governance that provides the mix of control and influence necessary and appropriate for their state, and that includes mechanisms for mitigating and responding to risk.

Speaker: John Gilligan, President and CEO, Center for Internet Security

3:30 PM**IT Operations: Your Cybersecurity Foundation**

Public sector and healthcare sector organizations have been repeatedly targeted by nation-state and ransomware threat actors. Good tools are important, but the best protection against these attacks isn't extra security products, but a focus on excellence in IT hygiene and IT operations.

Speaker: Andrew Coyne, CISO, Mayo Clinic

4:00 PM**Transforming Education and Cyber Operations**

As a national leader in energy and agriculture with a significant military footprint, North Dakota's cybersecurity strategy involves a whole-of-government approach - including training the next generation of cybersecurity professionals. The state's "PK-20W" Initiative aims to make "every student, computer science and cybersecurity educated. Kindergarten through PHD." Shawn will talk through a model that can be applied to any state to bring their students to 21st Century Skills while also protecting the economy of the state, data of citizens, and security of all residents.

Speaker: Shawn Riley, CIO, North Dakota



4:30-5:30 PM Join us in the EXPO Hall to network with fellow attendees and connect with our Solutions Strategy Partners.



UNDEFEATED

IN THE FIGHT

AGAINST RANSOM



WARE

Join the Defenders
CYBEREASON.COM/RANSOM



Women in Cyber Security

MONDAY, OCTOBER 25 | 8:45 AM

To counter cybersecurity's complex and evolving threat landscape, we need talented individuals from all backgrounds. The Summit Leadership Team is very proud of our track record of always having diversity in our Co-Chairs on the Think Tank and amongst our presenters. This year at the Summit, we carry the momentum forward with a four-part program offering essential perspective on diversity, inclusion and keeping teams engaged. What's more, thanks to the generous support of our sponsors, the morning sessions are complimentary to attend!

8:45-9:15 AM

Join WiCyS to Discuss Opportunities to Get Involved and Support Women in Cyber Security

9:00-9:20 AM

Namaste! Meditation and Mindfulness Session

Facilitator: Clark Whiting, Sr. Security Architect, Best Buy

9:30-9:40 AM

Opening and Welcome Remarks

Eileen Manning, Co-founder and Executive Producer, Cyber Security Summit

9:40-10:20 AM

Mentorships, The Circle of Life

Moderator: Tina Meeker, Sr. Director, Sleep Number
Panelists: Amy Fox, VP of Business Development, Ambient Consulting; Milinda Rambel Stone, CISO, Bremer Bank; Carey Lewis, SVP of Strategic Sales, Island

10:30-11:30 AM

Building & Leading Diverse Teams is an Artform

Moderator: Tina Meeker, Sr. Director Sleep Number
Panelists: Adam Mishler, VP, Chief Information Security Officer, Best Buy; Keely Ross, Enterprise Sales Executive, Zoom Video Communications; William Scandrett, Chief Information Security Officer at Allina Health

11:30 AM-12:30 PM

Women in Cyber Luncheon & Keynote

Louise McEvoy, Mountaineer & Cyber Professional

Louise McEvoy has been empowering women in cyber for the past 15 years. She likes taking risks outside of work – mountain biking on weekends and climbing the world's highest mountains on vacations. Louise's personal life goal was to climb Everest and she realized that goal when she summited on May 16, 2018.

Louise is dedicated to helping others reach their "summit" and has spoken to many groups and organizations on that topic, knowing that sometimes the hardest things in life are also the most fulfilling.

Join us for a very enriching account of Louise's Everest Summit journey and how her experience and learnings tie directly into cybersecurity leadership, risk management and goal setting. The Power and Peril of Connection theme for this year's summit could not be more fitting backdrop to this powerful lunchtime keynote.



Join us in the EXPO Hall to network with fellow attendees and connect with our Solutions Strategy Partners.



Presentation descriptions for Women in Cyber Tech Sessions on page 20

Supporters



Cyber Security Summit Partner Spotlight: WiCyS Minnesota



ABOUT THE WICYS NATIONAL ORGANIZATION

Women in Cybersecurity (WiCyS) National Organization, formed in 2012, is only non-profit membership organization with a national reach that is dedicated to bringing together women in cybersecurity from academia, research, and industry to share knowledge, experience, networking, and mentoring. WiCyS helps build a strong cybersecurity workforce with gender equality by facilitating recruitment, retention, and advancement for women in the field.

WICYS MINNESOTA - ESTABLISHED IN 2019

WiCyS MN formed up a strategic alliance with the Cyber Security Summit, formed up its inaugural board, and hosted highly attended WiCyS Golf & Networking Events at the beautiful White Bear Yacht & Golf Club and Hazeltine Golf Courses.

In 2021-22 our focus will be to grow membership, elect new leadership/committee members and host the best cyber networking & learning events in the region!

GET INVOLVED! LEADERSHIP AND SPONSORSHIP OPPORTUNITIES AVAILABLE NOW!

Express your interest in being considered for 2022 board positions, committee leadership or founding/sustaining sponsorships. Contact: wicysminnesota@wicys.org

2021-22 BOARD MEMBERS:

President (Interim):

Judy Hatchett, CISO - Surescripts

Vice President:

Tina Meeker, Sr. Director of Information Security - Sleep Number

Secretary:

Kris Boike Information Security Director of Retail Payments - Federal Reserve Bank of Atlanta

Treasurer:

Michael Larson, Principal Security Architect, Ecolab

Become a member today! Visit: wicysmn.org

A large advertisement for Ordr. On the left, a close-up of a white robotic head with a large, glowing blue eye. The head is wearing a white collared shirt. On the right, the Ordr logo is in the top right corner. Below it, the text 'WORRIED ABOUT RANSOMWARE?' is written in large, bold letters, with 'RANSOMWARE?' in red. Below this, a paragraph of text asks if the user has identified and segmented high-risk devices, found abnormal behavior, and can lock down compromised devices. Below the text are three bullet points, each with a red icon: an eye for 'SEE', a lightbulb for 'KNOW', and a shield for 'SECURE'. At the bottom right, there is a call to action to bring Ordr to connected devices and sign for a demo at www.ordr.net.

ordr

WORRIED ABOUT RANSOMWARE?

Have you identified and automatically segmented your high-risk devices? Can you find devices behaving abnormally? Can you rapidly lock down a compromised device?



SEE every device and network flow.



KNOW every risk, vulnerability and abnormal behavior.



SECURE every thing with proactive, reactive and retrospective policies.

Bring Ordr to your connected devices.

Sign for a demo at www.ordr.net

SECURITY RESPONDS TO CYBERTHREATS. INTELLIGENT SECURITY PREVENTS THEM.

Our Cylance® artificial intelligence can protect you from the latest threats.



 **BlackBerry®**

Intelligent Security. Everywhere.



THE APPLICATION SECURITY PLATFORM FOR LEADING ENTERPRISES

CONTRAST ASSESS | CONTRAST SCAN | CONTRAST OSS | CONTRAST PROTECT

WWW.CONTRASTSECURITY.COM

**Abandoning the basics
left doors wide open**
when the sudden shift to a
work-from-home culture
exposed critical IT gaps,
challenging even the most
secure enterprises.



*Get advice from our experts as they address
the most urgent IT management and security
issues and how they plan to solve them.*

[LEARN MORE AT TANIUM.COM](http://TANIUM.COM)



Technical Sessions

MONDAY, OCTOBER 25 | 9:30 AM-3:30 PM

The Monday Technical Sessions are offered at no charge and are open to all cyber professionals and those considering a career in cyber. This grouping also includes the Cyber Women Series. Sign-on early to network at 8:45 AM, give meditation a try at 9:00 AM and then spend the day exploring the variety of topics ranging from considering a career in cyber to building diverse cyber teams to exposing ransomware and hacktivism. The Monday tech sessions offer a wide breath of learning opportunities thanks to the support of our sponsors and speakers. At the end of the day, beginning at 3:30 PM, please enter the EXPO to connect with our Solution Strategy partners, investigate career opportunities through the job postings and look for prize opportunities! Enjoy your day.

AGENDA

8:45-9:15 AM

Join WiCyS to Discuss Opportunities to Get Involved and Support Women in Cyber Security

9:00-9:20 AM

Namaste! Meditation and Mindfulness Session

Facilitator: **Clark Whiting**, Sr. Security Architect, Best Buy

TECH SESSIONS 9:30-10:20 AM

Women in Cyber - Mentorships, The Circle of Life

Moderator: **Tina Meeker**, Sr. Director, Sleep Number

Panelists: **Amy Fox**, VP of Business Development, Ambient

Consulting; **Carey Lewis**, SVP of Strategic Sales, Island:

Milinda Rambel Stone, CISO, Bremer Bank;

Mentorships are the circle of life throughout a cybersecurity or business career, and it is even more critical in providing support and unlocking career opportunities to advancing our profession to be the best it can be. Join this panel of impressive information security and business executive as they share stories and strategies to how mentorship helped boost their growth both as mentors and mentees.

Consider a Career in Cyber

Moderator: **Judy Hatchett**, CISO, Surescripts:

Jennifer Czaplewski, Senior Director, Cyber Security, Target;

Brigadier General Stefanie Horvath, Mobilization Assistant to the Director of Operations; Executive Director Enterprise Services, U.S.

*Director of Operations, Executive Director Enterprise Services, U.S. Cyber Command, MNIT; **Faisal Kaleem**, Professor, Department of Computer Science and Cybersecurity, Metropolitan State (MN)*

University; **Jim Nash**, Assistant Minority Leader, Minnesota House of Representatives

The session will showcase leaders in cyber security to discuss the career opportunities, salary ranges, and broad range of industries in which you can be employed, how a non-traditional tech background can be valuable and the growth opportunity for women in this traditionally male dominated field.

Taking a People-Centric Approach to Securing the Remote Workforce

Brian Reed, Director, Cybersecurity Strategy, Proofpoint

Today's threat landscape is constantly evolving, and securing your remote workforce is critical to success. Understanding people risk and protecting your most important asset—your people—with a people-centric approach to security, should be the fundamental focus of your cybersecurity program

TECH SESSIONS 10:30-11:20 AM**Cloud Email and Collaboration Vulnerabilities**

Michael Hansen, Sr Solutions Engineer, Avanan, a Checkpoint Company

Cloud Email and Collaboration tool has quickly become the go-to applications for remote work, accelerating dramatically in usage over the last year. Millions of users turned to Cloud Email and Collaboration Tools to help keep businesses going since the start of the pandemic—and hackers have noticed. As these tools are still relatively new, much is unknown about how it operates and how hackers will approach it. While the increased usage has been well-documented, what's not been documented is whether the app is vulnerable to hacking. We will talk about discoveries that have already been made, potential risks that we see in the future, and how to best secure this relatively new communication vector.

Did You Just Click That?!

Michael Wyatt | Director, Threat Management | Surescripts LLC

We are all trained in our jobs and personal lives to be weary of suspicious emails and never click links or open attachments in them. But what happens when you do? We will look at phishing emails we have received and actually click links and/or open attachments to see what they try to do to our systems and accounts. Afterwards we'll try and answer any security questions around phishing campaigns and or phishing in general.

Women in Cyber - Building & Leading Diverse Teams is an Artform

Tina Meeker, Sr. Director, Information Security, Sleep Number;
Adam Mishler, VP, Global Chief Information Security Officer,
Best Buy; Keely Ross, Enterprise Sales Executive, Zoom Video
Communications; William Scandrett, Chief Information Security
Officer, Allina Health

Building & Leading Diverse teams is an artform. Success means making a clear and visible commitment through recruiting, leading, and guiding team members through change and evolution while positioning your organization to pivot quickly to changing demographics, team member needs and market trends. Learn strategies and practices from this panel of proven architects of diverse teams.

11:30 AM-12:30 PM**Networking Break with Solutions Strategy Partners in EXPO****TECH SESSIONS 12:30-1:20 PM****The Significance of AI & ML in Cybersecurity**

Tom Cameron, Solutions Architect, BlackBerry powered by Cylance AI

Artificial intelligence (AI) has become a security industry buzzword so broadly applied as to become almost meaningless. When every product boasts AI capabilities, security decision makers may quickly become cynical, even in the face of the most exciting innovation shaping cybersecurity today.

- What is the benefit of a cybersecurity solution powered by Artificial Intelligence and Machine Learning?
- Why does the number of generations of AI matter?
- How smart is the AI machine?
- How does AI provide a predictive advantage to prevent breaches for my organization?
- How can a 'Prevention First' cybersecurity approach help my business?

A walk on the darkside - exposing the ransomware actors

Dave Gold, VP, Business Strategy, SentinelOne

Over the past few years, Ransomware attacks have evolved from an economic nuisance to a full-blown threat to public health, safety, and even national security. Ransomware has taken over as the malware of choice for financially motivated attacks. Ransomware groups have become professional enterprises with very profitable businesses and brands built around encrypting and holding your data hostage. While ransomware attacks are not new, many organizations are not properly prepared to handle a ransomware attack. This talk will dig into the history of ransomware, the groups and methods being used to target you, and a discussion on how to better prepare your organization to stop ransomware attacks.

Insights from Target's Enterprise Journey to adopt FIDO

Tom Sheffield, Senior Director Technology, Target

Join us to hear Target's journey to adopt FIDO as a primary authentication capability across the Enterprise. We will share stories of some of the challenges and obstacles we had to overcome along the way. Our goal was not to drive users to our help desk so clarity of messages was key requirement in our program so we will talk about the importance of clear communication. We will share some of the key metrics that we identified along the way and how they helped to influence our program execution.

TECH SESSIONS 1:30-2:20 PM**Grow Your Security Operations Metrics**

Alex Volk, Senior Engineer, ReliaQuest

Quantifying the effectiveness of a security operations program is a challenging prospect for many organizations. As such, we turn measuring busyness of our SOC personnel instead of effectiveness. This presentation speaks to some of the ways you can use metrics to drive a security operations program that aligns to risk mitigation efforts for the business.

CIAM in an Uncertain World

D. Keith Casey, API Problem Solver, Okta, Inc

In today's uncertain world, organizations must find ways to ensure their customers can engage with their services at any time, from any device, in a secure and safe manner. That is where customer identity and access management comes in or "CIAM". A CIAM solution must not only meet today's security and compliance standards, but also create frictionless customer experiences to meet customers where they are and in the ways they need. Join our sessions as we discuss CIAM in more detail, how priorities have shifted this year and what CIAM maturity looks like.

Key Challenges, Tips and Findings on Effective Risk Management Programs

Bob Bennett, Co-Founder, NaviLogic

Risk programs, and especially third-party risk programs, are made up of a lot of components. Based on our experience, we will talk about both the challenges and solutions we see working in the marketplace today, and give attendees some helpful ideas to help improve their risk programs in practice.



TECH SESSIONS 2:30-3:20 PM

Hacktivism: Its past, present and future and what can we learn from it

Dr. Vasileios Karagiannopoulos, Reader in Cybercrime and Cybersecurity, Portsmouth University

This talk will initially define the different dimensions of hacktivism and provide an overview of its history up to the present day. It will then discuss the organizational and tactical aspects of hacktivist groups and will highlight some lessons we can learn from past examples regarding dealing with hacktivism in the future.

Cheaper by the Dozen: Application Security on a Limited Budget

Chris Romeo, CEO, Security Journey

Everyone wants to improve application security in their organization, but what if you don't have a million dollars to spend? How do small/medium organizations make any progress with application security? What if you could experience a catalog of application security open-source projects and receive advice on knitting them together into a program?

Explore the various application security open-source projects that exist in the OWASP universe. Learn how to choose suitable projects to match your organizational needs. Training/awareness, process/measurement, and tools are the categories available. Each project includes purpose, a plan for use, a risk rating, human resources for success, and impact. Explore how to engage your organization with a plan, experience enormous advances, and change application security forever.

Why Asset Management Fails for Cybersecurity (and How to Fix it)

John Seaman, Regional Director, Axonius

Despite the fact that every major cybersecurity framework lists asset management as the most foundational element, security teams still struggle with the downstream impact of incomplete, inaccurate, and outdated asset data. Without an accurate understanding of everything in an environment, all other initiatives suffer.

But there's good news. It doesn't have to be this way.

Join this session to learn:

- How security frameworks like the CIS 20 and industry-specific mandates like NIST and HIPAA approach asset management requirements
- How previous approaches to solving asset management fall short
- How cybersecurity initiatives like incident response, vulnerability management, and CMDB reconciliation are impacted
- A new approach that leverages existing data to solve the asset management challenge for cybersecurity

3:30 PM-5:00 PM



Join us in the EXPO Hall to network with fellow attendees and connect with our Solutions Strategy Partners.



Supporters



Search for Cyber Jobs

Visit the Cyber Security Summit virtual EXPO and log in with your attendee credentials at

virtual.cybersecuritysummit.org

Job postings are listed in EXPO booths on the Careers link in the white navigation bar below the booth.



THREAT ALERT: Microsoft MSHTML Remote Code Execution Vulnerability

by Cybereason Global SOC Team | September 10, 2021



The Cybereason Global Security Operations Center (SOC) issues Cybereason Threat Alerts to inform customers of emerging impacting threats. The Alerts summarize these threats and provide practical recommendations for protecting against them.

WHAT'S HAPPENING?

The Cybereason GSOC Managed Detection and Response (MDR) team is investigating CVE-2021-40444, a critical vulnerability in the Microsoft Hypertext Markup Language (MSHTML) web content rendering engine that Microsoft Office applications use. This vulnerability enables attackers to use malicious ActiveX controls to execute arbitrary code on target systems.

This Threat Alert focuses on the CVE-2021-40444 vulnerability as exploited via malicious Office documents. However, other applications that also use the MSHTML engine, such as Internet Explorer, can also be vectors for exploiting the vulnerability.

KEY OBSERVATIONS

- **Zero-day vulnerability:** Adversaries have been exploiting CVE-2021-40444 as a zero-day vulnerability to execute malicious code on target systems.
- **Social engineering:** To exploit the CVE-2021-40444 vulnerability, the attacker tricks a user into opening a specifically crafted Office document and clicking **Enable Content** to disable the Microsoft Office **Protected View** feature. The **Protected View** feature is enabled by default and blocks the execution of potentially malicious code in the context of Office documents.
- **No patch available:** No patch for CVE-2021-40444 is available at the time of writing of this Threat Alert. Cybereason recommends that you disable ActiveX controls if these controls are not necessary on the machine. The Cybereason team provides further recommendations in the Cybereason Recommendations section below.

ANALYSIS

CVE-2021-40444 is a critical vulnerability in the MSHTML rendering engine. Microsoft Office applications use the MSHTML engine to process and display web content. An adversary who successfully exploits CVE-2021-40444 could

achieve full control over a target system by using malicious ActiveX controls to execute arbitrary code.

Malicious actors are exploiting CVE-2021-40444 by using specifically crafted Microsoft Office documents. A typical such document uses the MSHTML engine to open a malicious website hosted on an attacker-controlled endpoint. This website exists as a MIME HTML (MHTML) Object Linking and Embedding (OLE) object in the context of the document. The website executes JavaScript code and ActiveX controls that then execute malicious code on the system where the malicious Office document was opened. This code is hosted at the attacker-controlled endpoint in the form of a dynamic-link library (DLL).

To exploit the CVE-2021-40444 vulnerability, the attacker tricks a user into opening a specifically crafted Office document and clicking **Enable Content** to disable the Microsoft Office **Protected View** feature. The **Protected View** feature is enabled by default and blocks the execution of potentially malicious code in the context of Office documents.

CYBEREASON RECOMMENDATIONS

Cybereason recommends the following:

- Disable ActiveX controls if these controls are not necessary on the machine. To do this, configure the associated registry values by executing the following [Windows Registry \(.reg\) file](#) and rebooting the system.
- If you do not want to disable ActiveX controls, make sure that you do not click **Enable Content** when you view Office documents that originate from untrusted sources. Clicking **Enable Content** disables the Microsoft Office **Protected View** feature.
- Educate users so that they do not open Office documents that originate from untrusted sources, or do not click **Enable Content** when they open such documents.
- **Threat Hunting with Cybereason:** The Cybereason MDR team provides its customers with custom hunting queries for detecting specific threats - to find out more about threat hunting and [Managed Detection and Response](#) with the Cybereason Defense Platform, [contact a Cybereason Defender here](#). For Cybereason customers: More details [available on the NEST](#) including custom threat hunting queries for detecting this threat and a list of indicators of compromise (IOCs) related to the threat.

OUR DEVICES SET THE WORK ***OUR SECURITY IS SETTING THE***

First, we protected devices, now we're bringing safety and prod



 **BlackBerry®**

Intelligent Security. Everywhere.

ING WORLD FREE.

HE WORLD FREE.

activity everywhere around the world.

re.





Cyber Security for Healthcare & Med Device

MONDAY, OCTOBER 25 | 9:30 AM-5:30 PM

The Healthcare and Med Device Seminar brings together healthcare providers and medical device manufacturers to share knowledge that advances device safety and security. With a diverse set of speakers and range of industry perspectives, the full-day event emphasizes actionable lessons from large manufacturers and hospital systems that can also be applied to small and mid-size organizations to strengthen security programs. Participants include healthcare delivery organizations, device-makers, regulatory agencies, risk managers, insurers, security experts and more.

AGENDA

9:30-9:40 AM

Opening and Welcome Remarks

*Judy Hatchett, Chief Information Security Officer, Surescripts;
Mary Diner, Security Director, Optum*

9:40-10:10 AM

Healthcare Security Threat Landscape

Bill Aerts, Archimedes Center for Medical Device Security

This session will be a high-level summary of current security threats to medical devices and healthcare, and the efforts in place to address the risks. The end result will be a general understanding of the situation, terminology and players.

10:10-10:40 AM

What it Takes to Start a Medical Device Security Program

Ben Stock, Director of Healthcare Product Management, Ord

The healthcare industry is continuously on the bleeding edge of innovation, deploying connected medical devices that significantly improve the quality and delivery of care. With nearly 15 connected devices per bed, the need for visibility and security of these devices is more critical than ever. But, while healthcare technology management (HTM), cybersecurity, and information technology teams share a common objective, there are still barriers to building a successful medical device security program. Join Ben Stock, Director of Healthcare Product Development at Ord, to discuss ways to build a successful medical device security program and getting HTM, IT, and cybersecurity to work together.

10:40-11:10 AM

Why Does Cybersecurity Asset Management Matter for Healthcare?

John Seaman, Axonius

Join this session to learn more about the emerging area of cybersecurity asset management, why all major security frameworks consider asset management to be foundational, and how healthcare organizations can use data from the tools already in place to solve asset management for cybersecurity.

11:10-11:40 AM

Mayo Clinic Cybersecurity Resilience Program

Debra Bruemmer, Security Resilience - Senior Manager, Mayo Clinic; Sarah Jopp, Mayo Clinic

Mayo Clinic will share its journey to develop and implement a proactive, ongoing asset "certification/validation" process spanning the life-cycle of an asset. The talk will focus on one foundational asset, Windows servers, and key deliverables: secure baseline requirements, certification program, asset drift, and risk measurement. The program measures cybersecurity risk empirically at the asset level, which is consolidated to a fleet view.

11:40 AM-12:45 PM

Solutions Strategy Break in EXPO

12:45-1:15 PM**Wrangling Ransomware Worry With Words**

Judd Larson, Principal Technologist, Global Quality-Product Security Office, Medtronic

Ransomware has been frighteningly pervasive in the news over the past months. Through the lens of medical device security, we'll scope out what ransomware is, box in legitimate fears, and drive out uncertainty and doubt.

1:15-1:45 PM**Legal Aspects of Incident Response**

Eran Kahana, Attorney, Maslon

Ransomware is but one type of "incident." Now, incidents are defined in various ways and contractual provisions can (and typically do) add a layer of complexity and urgency to getting it done right. To that end, it is necessary to begin by referencing the incident response plan and assembling the response team, which includes the company's legal counsel. This presentation will highlight the critical legal aspects relative to an incident response and is aimed to assist in how to properly leverage legal counsel's assistance.

1:45-2:15 PM**Securing the Patient Journey-Lessons from the trenches**

Sumit Sehgal, Strategic Product Marketing Director, Armis

Learn practical examples of how to leverage information security data to enable improvements to clinical risk and patient safety. Extending beyond the medical device security, we will showcase insights that require a holistic approach to what security in the next 2 to 3 years will look like related to healthcare device ecosystems.

2:15-2:30 PM**Solutions Strategy Break in EXPO****2:30-3:00 PM****The Human Element**

Keith Ibarguen, Chief Product Officer, Cofense

Healthcare and medical device companies are some of the most targeted organizations in the world. Humans, when appropriately involved in your phishing defense, can be very effective sensors against these attacks.

Through empowering people, we can create a resilience not achieved by technology alone. The power of this collective is achieved through a comprehensive, positive, human-focused program looking at the issues from end to end. Join us to discuss how you can build a better employee: one who can better identify, report, mitigate and remediate zero-day attacks.

3:00-3:30 PM**Healthcare and the Cloud, What to be Prepared for When Moving or Consuming Applications to the Cloud**

Richard Scott, Chief Security Architect, Optum

David Mott, Senior Principal Engineer TLCP, Optum

To be able to successfully utilize public cloud platforms with healthcare applications one has to address a number of foundations items in which we transform the way we look at risk. Security, Risk and Compliance now spans a variety of stakeholders between the Cloud Service provider, Technology teams and the Healthcare Provider. Understanding the basic platform consumption models, your responsibilities and expectations are critical for safe and secure use of public cloud.

In this session, we cover the basic tenets of using public cloud hosted healthcare solutions differentiating between IaaS, PaaS, SaaS consumption patterns and what you should be aware of.

3:30-4:30 PM**Breaking into Medical Device Cybersecurity: Career Transition**

Andrew Bonnett, VP & CISO, Boston Scientific; Shruti Iyer, Principal Innovation Architect, Oracle; Michael Johnson, Technological Leadership Institute (TLI); Judd Larson, Principal Technologist, Global Quality - Product Security Office, Medtronic; Daniel Mooradian, Technological Leadership Institute (TLI)

The global demand for Cybersecurity professionals is high, and the need for experts in cyber for medical devices is at the top of that list. This panel will discuss options and opportunities for employees from a wide variety of backgrounds to transition or prepare for a career in med device cybersecurity. The conversation will include perspectives from those who have made the transition as well as hiring managers.

4:30-5:30 PM

Join us in the EXPO Hall to network with fellow attendees and connect with our Solutions Strategy Partners.

Host



Supporters





Cyber Security for IoT/IIoT/ICS/SCADA Collaboration

MONDAY, OCTOBER 25 | 1:00-5:30 PM

The IoT/IIoT/ICS/SCADA Collaboration Seminar will showcase thought leaders, strategies, opportunities, and business cases of implementing security solutions across a broad spectrum of industries. IT, OT and IoT Cyber Security decision makers and practitioners will discuss and evaluate the security risks in the context of IoT/IIoT/ICS/SCADA. Executive Orders have instructed Industry and Government to ensure critical infrastructure is accurately inventoried, monitored, and suitable tactics are developed to make the nation more secure.

AGENDA

1:00-1:30 PM

Keeping together is progress. Working together is success.” – Henry Ford

Paul Veeneman, CISSP, CISM, CRISC, CMMC RP, President & COO, Beryllium InfoSec Collaborative

1:30-2:00 PM

Standards and Risks; Cybercrime and the Internet of Things

Sean Costigan, Professor, George C. Marshall European Center for Security Studies

2:00-2:30 PM

A Private Sector Perspective on the OT Focused Executive Orders and Policies

*Moderator: Karen Andersen, Principal Consultant, Optiv, Inc
Presenter: Robert Lee, CEO, Dragos*

2:30-2:45 PM – Solutions Strategy Break in EXPO

2:45-3:15 PM

OT...Not just another form of IT Security

Joe Weiss, Managing Partner, Applied Control Solutions, LLC

3:15-3:45 PM

Vulnerability Risk Assessments Guidance on IOT Controls

Ted Gutierrez, CEO, Co-founder, SecurityGate.io

3:45-4:15 PM

Architecting a Successful Digital Transformation Solution


David Schultz, President, G5 Consulting & Engineering Services

4:15-4:45 PM

Here's Where We Are, Don't over Rotate

Jamison Utter, Sr Director, Product and Solutions Evangelism, Ord

4:45-5:30 PM

 Join us in the EXPO Hall to network with fellow attendees and connect with our Solutions Strategy Partners.



Presentation descriptions are online at: cybersecuritysummit.org/2021-iiot-ics-scada-collaboration

Host



Supporters



Be cyber ready. Become future proof.

**Digitally transform with
cyber confidence.**

Disruptive technologies wait for no one. That's why you need to be cyber ready on your digital transformation journey. KPMG can help you implement a strategic approach to cyber-preparedness that safeguards data and enables agility for growth now and in the future. Learn more at [KPMG.com/us/cyber](https://www.kpmg.com/us/cyber)

Anticipate tomorrow. Deliver today.



CYBER
THREAT
ANALYSIS

Recorded Future®

By Insikt Group®
CTA-2020-0714

ONLINE SURVEILLANCE,
CENSORSHIP, AND
DISCRIMINATION FOR LGBTQIA+
COMMUNITY WORLDWIDE

MALWARE/
TOOLS
PROFILE

Recorded Future®

By Insikt Group®
August 4, 2021

Protect Against
BlackMatter Ransomware
Before It's Offered

Recorded
Future®

Our goal is simple and direct; it is to always provide intelligence analysts and leaders can trust but also know is encompassing of all available sources, free of bias, and can be used to make their own assessments on what is best for their organization.

This is not the case for all intelligence providers as many have been acquired or have merged with larger entities and can no longer guarantee that their solution or analysis isn't being influenced by what is "best for the parent company" in terms of their technical bias or only taking into account a single source of intelligence.

By basing collection on your mission and needs, having the most diverse and widest range of sources, delivering intelligence where your analyst's need it most, and independence-led product development, Recorded Future remains an independent intelligence company and our ability to deliver trusted intelligence remains intact.

Trusted and Independent Intelligence only at recordedfuture.com

CYBER
THREAT
ANALYSIS
CHINA

Recorded Future®

By Insikt Group®
July 27, 2021

China's Digital Colonialism:
Espionage and Repression
Along the Digital Silk Road

CYBER
THREAT
ANALYSIS

Recorded Future®

By Insikt Group®

CTA-2021-0209

Top Exploited Vulnerabilities in 2020 Affect Citrix, Microsoft Products

CYBER
THREAT
ANALYSIS

Recorded Future®

By Insikt Group®

CTA-2021-0225

THE BUSINESS OF FRAUD: An Overview of How Cybercrime Gets Monetized

CYBER
THREAT
ANALYSIS

RUSSIA

Recorded Future®

By Insikt Group®

August 17, 2021

Operation Secondary Infektion Continues Targeting Democratic Institutions and Regional Geopolitics

The Record. BY RECORDED FUTURE

The Record by Recorded Future gives you exclusive, behind-the-scenes access to leaders, policymakers, researchers, and the people in the shadows of the cyber underground. We break news and interview those that matter in the fast-changing field of cybersecurity.

Get the Latest News on Security at www.therecord.media



Cyber Security for Small Business

TUESDAY, OCTOBER 26 | 1:00-5:00 PM

Cyber security is the biggest threat to small businesses. Unfortunately, too many small businesses think they are too small to be a target. Attack bots are deployed online 24/7 looking for cracks in your company security, regardless of company size.

Join us as we cover recent attack examples that have taken down companies, insurance coverage, technical protection, cost-effective safeguards, free assessment services offered by the government, recommendations on what to look at for managed service providers and cyber practices to position your company for growth.

The cyber threat has never been more real for small businesses. Sign-up today for an afternoon of complimentary resources designed to protect against ransomware, phishing attacks and how to respond when an incident happens.

AGENDA

1:00-1:10 PM

Opening Welcome "The New Normal"

Speaker: Lyle J. Wright, MM, EDPF | Associate State Director, SBDC

1:10-1:25 PM

Resources for Even the Smallest Businesses

Speaker: Brian McDonald, District Director, U.S. Small Business Administration

1:25-2:15 PM

Practical Ways to Manage Risk as a Small Business

Moderator: Milinda Rambel Stone, CISO, Bremer Bank

Panelists: Joseph Chow, Specialized Business Solutions Center Director, Bremer Bank; Laura Burr, Deposit Administration Manager, Bremer Bank; Meredith Winegar, Mortgage and Trust Operations Director, Bremer Bank; Robert Worden, Insurance & Sales Education, Bremer Insurance

2:15-2:45 PM

Expanding Government Cybersecurity Requirements for Suppliers

Speaker: Scott Singer, President, CyberNINES, Ret. USN Captain

2:45-3:00 PM — Solutions Strategy Break in EXPO

3:00-3:30 PM

How the Federal Government Can Help Defend Small Business

Speaker: Chris Gabbard, Cybersecurity Advisor, Region 5, Cybersecurity and Infrastructure Security Agency

3:30-4:30 PM

Cybersecurity Resources for Small Businesses — SBDC Cybersecurity Task Force

Speaker: Earl Gregorich, CBA, Area Manager & Business Consultant, Greenville Area Small Business Development Centers, In partnership with Clemson University

4:30-5:00 PM

Q&A Session for Taking Actionable Steps

Moderator: Andrew Telljohn, Upsize Minnesota

Panelists: Christopher Gabbard, CISA; Earl Gregorich, SBDC; Milinda Rambel Stone, Bremer Bank; Scott Singer, CyberNINES

5:00-5:30 PM



Join us in the EXPO Hall to network with fellow attendees and connect with our Solutions Strategy Partners.



Presentation descriptions are online at: cybersecuritysummit.org/2021-cyber-security-for-small-business

Host



Supporters



ALWAYS SECURE.

ALWAYS COVERED.

**We track, monitor, and secure
your enterprise, 24/7/365.**

From real-time threat intelligence and advanced cyber analytics to zero-trust cloud architecture and a host of managed SOC services, we have the proven solutions and expertise to keep your enterprise safe.

www.ECStech.com



TECHNOLOGICAL LEADERSHIP INSTITUTE



Graduate Minor in Cyber Security **ARE YOU DRIVEN TO FIGHT CYBER CRIME?**

The statistics speak to the booming need:

- The cost of ransomware increased 225% last year - IC3.gov
- Losses from cybercrime in the U.S. reached \$1 trillion in 2020 - McAfee

**Empower yourself with the knowledge to
adapt and lead in this vital area of security.**

The Graduate Cyber Minor courses are open to both UMN students and non-degree seeking professionals.

Contact admissions at msst@umn.edu for more information or visit tli.umn.edu.

The Morris™

Once again, the 11th Annual Cyber Security Summit's Visionary Leadership Awards occur against the back-drop of COVID-19.

Sadly, the pandemic has perpetuated the need for a virtual celebration of their contribution to cybersecurity. But this does nothing to dampen the impact their work has on moving the needle to better secure our businesses, organizations and nation states.

We are excited to celebrate all our Visionary Leadership Awardees on Wednesday morning at the opening session and again in-person in the spring! Along with recognition for their accomplishments, award recipients and VLA All-Access ticket holders are invited to a VIP reception on April 21, 2022.



2021 Honorees



Visionary Student

ALEX HEPP

Student, Metropolitan State University



Visionary Governance Champion

JIM NASH

State Representative, Minnesota House of Representatives



Visionary Academic Leader

DR. AMBAREEN SIRAJ

Professor/Director, CEROC, Tennessee Tech & Founder, WiCyS



Visionary Applications Security Leader

JAY JACOBS

Chief Data Scientist, Cyentia



Visionary Security Program and Oversight Leader

JOHN VALENTE

Security Consultant



Visionary Global Leader

MALCOLM HARKINS

Chief Security & Trust Officer, Epiphany



Visionary Governance, Risk and Compliance Leader

KUMAR DASANI

Director, Cyber Security and IT DevOps, Medtronic



Founders Award

KEVIN MANDIA

Mandiant



Visionary Security Awareness Program Leader

TALYA GEPNER

Director, Target Corporation




Visionary Security Operations Leader

DEBRA STAFFORD

Security Manager, Minnesota IT services

Many traditions stem from a story. The Visionary Leadership Awards that we confer are called The Morris™. They are named after 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. As a gifted college student programmer, Morris unwittingly unleashed a self-propagating worm into the national system which 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.

MONDAY, OCTOBER 25

8:00 AM-5:00 PM	Public Sector Workshop — See page 12 for details
8:45 AM-12:30 PM	Women in Cyber — See page 16 for details
8:45 AM-5:00 PM	Technical Sessions — Series of one-hour technical sessions — See page 20 for details
9:30 AM-5:00 PM	Healthcare & Med Device Seminar — See page 26 for details
1:00 PM-5:00 PM	IoT/IIoT/ICS/SCADA Collaboration Seminar — See page 28 for details
3:30 PM-5:00 PM	 Networking in EXPO — Explore resources from our Solution Strategy Providers


TUESDAY, OCTOBER 26



7:30 AM-8:00 AM	Cyber Career Exploration Deputy CISO for the State of Minnesota presents timely advice and career-shaping insights for future cyber security professionals. <i>Rohit Tandon, Assistant Commissioner, CISO, State of Minnesota, MNIT; Nancy Skuta, Senior Information Security Analyst, ITS4, Threat and Vulnerability Management, MNIT Services</i>
8:00 AM-8:20 AM	Opening Welcome An eleven-year journey brings us to today. Eleven years ago, the University of MN, Technological Leadership Institute had the foresight to raise concerns that cyber security was to become a household concern, and the Summit was born. <i>Eileen Manning, Co-Founder, Executive Producer, Cyber Security Summit; Mike Johnson, Director of Graduate Studies and Renier Chair, TLI; Allison Hubel, PhD, Director, TLI at University of Minnesota</i>
8:20 AM-8:35 AM	The Power and Peril of Connections Connections are powerful. Most of us realized the value of our interpersonal connections in 2020 as the pandemic changed the way we interact with colleagues, friends and family. The proliferation of mobile devices and sensors in everyday items has created the most powerful network of interconnected devices imaginable. But with great power comes great responsibility. Protecting the estimated 21.5 billion devices in use today requires security professionals to adapt and learn faster than ever before. <i>Jennifer Czaplewski, Senior Director, Cyber Security, Target; Wade Van Guilder, Sr. Manager for Solutions and Architectures for WWT / SLED</i>
8:35 AM-9:00 AM	Opening Keynote: Solving the puzzle: Collaboration, Imagination and Cybersecurity Jen Easterly serves as the Director of the Cybersecurity and Infrastructure Security Agency (CISA), where she's leading the national effort to understand, manage and mitigate risk to our physical and cyber infrastructure. Under Director Easterly's leadership, CISA is working to change the thinking on cybersecurity through imagination and to increase our national cyber preparedness through collaboration with the public and private sectors. She'll provide insight into the benefits of a truly unified effort to secure the nation from cyber threats and how we can act now, together, to realize the greatest impact. Key themes will include how promoting better collaboration and strengthening cooperation between public and private sectors are the most critical pieces to solving the cybersecurity puzzle. <i>Jen Easterly, Director, Cybersecurity and Infrastructure Security Agency (CISA)</i>
9:00 AM-9:30 AM	Staying out of Trouble: DOJ's Former Top Cyber Prosecutor On Staying Safe Now a cybersecurity leader at EY, Brian Levine served for the last 20 years as a cybercrime prosecutor with the U.S. Department of Justice, National Coordinator for all 300 federal cybercrime prosecutors, an Assistant Attorney General with the New York Attorney General's Office, and a civil litigator. Brian will address how those of us in security can stay out of legal and regulatory trouble, including discussing such topics as breach communications, incident reports, informed consent, ransom payments, hack back, bug bounty programs, and more. <i>Brian Levine, Managing Director, Cybersecurity & Data Privacy, EY</i>

9:30 AM-10:15 AM	Ransomware Panel Ransomware, to pay or not to pay? Hear from experts from the FBI, Incident Response, Insurance Industry and Healthcare during this dialogue on issues surrounding response to a ransomware attack. Moderator: <i>Tom Sheffield, Senior Director Technology, Target</i> Panelists: <i>Aaron McKee Campbell, FBI Computer Scientist, FBI; Dan Hanson, Senior VP Management Liability and Client Experience, Marsh & McLennan Agency; Yan Kravchenko, Information Security Director, Hennepin Healthcare; Peter Martinson, Director of Incident Response, Blue Team Alpha</i>
10:15 AM-10:45 AM	 Networking Break in EXPO Converse and connect with our Solution Strategy Providers.
10:45 AM-11:15 AM	Five hard questions for a cyber insurance broker. In this fireside chat, a top cyber insurance broker will answer 5 hard-hitting questions about coverage and underwriting trends, and best practices for companies to better navigate the buying and claims process. Panelists: <i>Mario Paez, Director, Cyber & Technology E&O, Marsh & McLennan Agency LLC; Phil Schenkenberg, Partner, Litigation & Cyber Security, Taft Law</i>
11:15 AM-11:45 AM	Defragging Our Cyber Strategy We must improve our system performance to defend American interests in the cyber domain. Come hear Cyber Command's BG Horvath combine military strategic examples and cybersecurity analysis to visualize a stronger defensive cyber strategy with a focus on how to lead with collaboration while solving hard security problems our nation faces. <i>Brigadier General Stefanie Horvath, Mobilization Assistant to the Director of Operations; Executive Director Enterprise Services, U.S. Cyber Command, MNIT</i>
11:45 AM-1:00 PM	 Networking Break in EXPO Converse and connect with our Solution Strategy Providers.
1:00 PM-5:00 PM	Small Business Seminar — See page 32 for details
1:00 PM-2:00 PM	Human Factors in Cybersecurity: Threats from Within Whether as a malicious act or inadvertent actions by careless employees, the greatest threat to an organization's information system is often on the inside. Subject matter experts from the National Counterintelligence and Security Center (NCSC) and the Department of Justice will examine the role of insider threat mitigation in cybersecurity. Join our panelists for a discussion on the threats and vulnerabilities of insiders operating in the cyber realm and the role of insider risk programs in deterring, detecting, and mitigating risk while protecting the privacy and civil liberties of the workforce. Discussion will cover the current risk environment, including heightened vulnerabilities created by the Global Pandemic; potential threats posed by trusted insiders and the adversaries and competitors who seek to co-opt or exploit them; best practices and resources to mitigate risk; and a live Q&A with audience. Moderator: <i>Sean Costigan, Professor, George C. Marshall European Center for Security Studies</i> Panelists: <i>Andrew Borene, Civil Liberties & Privacy Officer, National Counterintelligence and Security Center (NCSC), Office of the Director of National Intelligence; W. Anders Folk, Acting United States Attorney, U.S. Department of Justice; Rebecca Morgan, Deputy Assistant Director, Insider Threat; Deputy Director, National Insider Threat Task Force, National Intelligence and Security Center</i>
2:00 PM-2:30 PM	Shift Left: Easier said than done Shift Left. A phrase that is easy to say, but a strategy that many organizations struggle to effectively implement. This talk, presented by industry expert Larry Maccherone, will discuss the top 5 reasons that "shift left" is hard and the best ways to overcome the challenges. <i>Larry Maccherone, DevSecOps Transformation, Contrast Security</i>
2:30 PM-3:00 PM	 Networking Break in EXPO Converse and connect with our Solution Strategy Providers.

3:00 PM-3:30 PM	<p>Securing the Development & Supply Chain of Open Source Software (OSS)</p> <p>Open Source Software (OSS) is being distributed and consumed today on a massive scale through software supply chains. While OSS delivers tremendous benefit in terms of accelerated development and innovation, it is an increasing common target of cyber adversaries. Join Derek for a discussion of how OSS is developed, distributed, maintained, and attacked.</p> <p>Derek will reveal insights on how open source projects with 1.5x more frequent releases and 530x faster open source dependencies upgrades harness this speed to dramatically improve security within their code. He will also share insights on how high performance enterprise software development teams simultaneously boost productivity and security - achieving 15x faster deployments and 26x faster remediation of application security vulnerabilities. Derek then will show how you can apply these exemplary practices to stay a step (or more) ahead of your adversaries by sharing a set of best practices and attack countermeasures.</p> <p><i>Derek Weeks, Senior Vice President, The Linux Foundation</i></p>
3:30 PM-4:00 PM	<p>Future Proof Security for a Connected World</p> <p>2020 was a year of learning, with surges in ransomware, nation states infecting supply chains from Solar Winds to Microsoft, and radical new work models that might presage a "new normal." The biggest problem in security, though, continues to be a lack of alignment between security functions and their core businesses or organizational missions. In this session, we'll examine how to automate the automateable, what to do to secure the apparently insecureable, and how to future-proof security programs. Preparing in peacetime for the crisis is important and getting the hygiene right matters, but that's where the game starts. The advanced game tunes the SOC for efficiency and scale and focuses on application of Human, carbon-based intelligence as ruthlessly as possible to make life miserable for attackers. We'll make some predictions for the future, but the choice for attendees is critical: will they choose to build future-proof programs or remain with the strategies of the last cyber generation?</p> <p><i>Sam Curry, CSO, Cybereason</i></p>
4:00 PM-4:40 PM	<p>You CAN stop stupid</p> <p>"The User Problem" is the most costly problem to most security programs. The perceived solution is to create "The Human Firewall" through improved awareness. While awareness is important, it is a tactic and not a comprehensive strategy to address the problem. Using strategies from accounting, counterterrorism, safety sciences, etc., which have all been addressing human issues, Ira provides a comprehensive and workable strategy to apply to cybersecurity to significantly reduce losses from user actions.</p> <p><i>Ira Winkler, CISO, Skyline Technology Solutions</i></p>
4:40 PM-5:10 PM	<p>Closing Keynote: The Lawful Access Challenge:</p> <p>Many federal, state, local, and tribal law enforcement agencies are facing challenges due to the phenomenon sometimes referred to as "warrant-proof" encryption.</p> <p>Commercial service providers, device manufacturers, and application developers are increasingly deploying and aggressively marketing products and services with a form of strong encryption that can only be decrypted or accessed by the end users or device owners.</p> <p>Because of warrant-proof encryption, the government often cannot obtain the electronic evidence necessary to investigate and prosecute threats to public and national safety, even with a warrant or court order. End-to-end encryption and other forms of warrant-proof encryption create, in effect, lawless spaces that criminals, terrorists, and other bad actors can exploit.</p> <p><i>Darrin E. Jones, Executive Assistant Director, FBI</i></p>
5:10 PM-5:30 PM	<p> Networking in EXPO</p> <p>Join us to network with fellow attendees and connect with our Solutions Strategy Partners.</p>

WEDNESDAY, OCTOBER 27

8:00 AM-8:30 AM	Visionary Leadership Awards <p>Start the day inspired by the accomplishments of the 2021 honorees. The Morries™ Visionary Leadership Awards recognize innovative practitioners from across the cybersecurity ecosystem working to develop and foster strategies that protect critical systems and data. Join us as we honor the exemplary leadership of our colleagues in the field, including security awareness leaders, audit leaders, academic leaders, governance champions and more.</p> <p><i>Christopher Buse, SVP, Chief Information Security Officer, Old Republic</i></p>
8:30 AM-9:15 AM	The Psychology behind Security Leadership: Making Strategic Impacts <p>With the evolution of technology, cyber threats continue to impact people and organizations daily even with enhanced technical controls in place. Because of this, there is a heightened importance on the direction that information security executives provide organizations to ensure timely and proactive remediation. However, research indicates that the leadership methodologies deployed by security leaders are not always the same as other leadership roles within organizations. This presentation explores the methodologies behind the roles and decisions of these executives and how they impact the strategic futures of information security.</p> <p><i>Shayla Treadwell, Ph.D., Executive Director, Cybersecurity Center of Excellence, Governance, Risk & Compliance, ECS</i></p>
9:15 AM-10:00 AM	How to leverage the power of ISACs <p>Information Sharing & Analysis Centers (ISACs) have been an integral part of the nation's cyber defenses since the late 1990's. ISACs operate within many of the nation's critical infrastructures, bringing together practitioners and operators to share information, intelligence, collection and analysis on cyber and physical threats, as well as develop best practices for mitigation. ISACs are designed to be active, ongoing communities of trust that cut through the noise and complexity of cyber issues and help their members focus on things that really matter to their sector and organizations.</p> <p>"Sharing and Analysis" can be misleading – however ISACs can be powerful resources leading to better engagement and collaborative environments - delivering higher confidence public sector services.</p> <p>The public sector touches all aspects of critical infrastructures, and in this session we'll look at the wide range of activities, partnerships, and business models seen across the ISAC community. Representatives from the Multi-State ISAC (MS-ISAC), and Retail & Hospitality ISAC (RH-ISAC) will provide detailed insight and explore examples of actionable information sharing, products and services that are available, and success stories of cybersecurity improvements.</p> <p>ISACs require active engagement to maximize value, so we'll also focus on how to make the best use of being a member of an ISAC.</p> <p><i>Christopher Buse, SVP, Chief Information Security Officer, Old Republic; Carlos Kizzee, Vice President, Stakeholder Engagement, MS-ISAC, Center for Internet Security; Ryan Miller, Director of Cyber Threat & Fraud Intelligence, Target</i></p>
10:00 AM-10:20 AM	 Networking Break in EXPO <p>Converse and connect with our Solution Strategy Providers.</p>
10:20 AM-10:50 AM	Forging the Future <p>We've demonstrated that we can be incredibly productive in multiple constructs - together - and apart; so, how do we make sure that we get the most of both? We have an opportunity to reimagine how we use the space we work in and optimize our workforce and that's an exciting place to be. In this presentation, we will discuss how to prepare your company for as offices reopen to be successful in this new work from anywhere model.</p> <p><i>Gary Sorrentino, Global Deputy CIO, Zoom Video Communications, Zoom</i></p>
10:50 AM-11:45 AM	Software Supply Chain Security <p>Once considered an esoteric domain of cybersecurity, Software Supply Chain security is now a Board Room conversation. Action must be taken to protect and safeguard us. The conversation will cover the current policy landscape, which includes actions from all branches of government, as well as how thinking on risk has evolved over the past several years. Our panel will touch on the notion of shared risk and how to think through responsibilities for government, the private sector, software vendors and the consumer.</p> <p>Moderator: <i>Sailesh Gadia, Partner, KPMG</i> Panelists: <i>Gretchen Block, Vice President, Optum Technology; Joyce Corell, Director, Supply Chain and Technology Security, Office of the National Cyber Director, Executive Office of the President, White House; Harshal Mehta, VP, CISO, CWT</i></p>

11:45 AM-1:00 PM	 Networking Break in EXPO Converse and connect with our Solution Strategy Providers.
1:00 PM-1:30 PM	The Attack of the Cyber Supply Chain SolarWinds defined the attack of the cyber supply chain. One of the most extensive, stealthy attacks ever discovered, organizations were attacked through trojanized updates to legitimate monitoring and management software. SolarWinds provides a discussion opportunity of the infinite horizon, the importance of attribution, and improvements to information sharing. <i>Jon Ford, Managing Director, Mandiant</i>
1:30 PM-2:00 PM	Artificial Intelligence in Cybersecurity Present and Future Role Have you ever wondered about Artificial Intelligence (AI) in Cybersecurity? Maybe you are curious to know how it is currently being applied or how it might be applied in the future? Better yet, how AI relates to the current threat landscape and even your environment. If so, join us! Where we will break it down using real-world examples. This is a zero to hero session so you don't need a PhD in math or data science to enjoy the topic and learn something new. <i>Tony Lee, VP, Global Services Technical Operations, Blackberry</i>
2:00 PM-2:30 PM	Threat Adaptation and the Commercialization of Cybercrime Cybercriminals, like criminals in many other domains, show unique capabilities to adapt to controls emplaced to thwart their criminal efforts. Most recently, the world has seen an adaptation from the 'lone wolf' attacker to more structured, specialized groups focused on specific areas of cybercrime. Consider Ransomware today. There are groups that specialize in targeting and compromising an organization and other groups who specialize in receiving, and laundering the money. These tactics are not new and reflect threat adaptation and security cycle theory. Learn about some of the more advanced attacks and concepts that underpin the commercialization of cybercrime. Examples will be used from BEC, and Ransomware, among others. <i>Chris Mark, National Practice Director - Payment Security, Fraud, and IAM</i>
2:30 PM-3:00 PM	 Networking Break in EXPO Converse and connect with our Solution Strategy Providers.
3:00 PM-3:30 PM	Work Your Way & Be Secure Hear from 3M's CISO Tris Lingen as she reviews how the past year has changed how we work. It taught us that we can and need to reimagine how our organizations operate. We learned that a more flexible way of working is essential for continued growth. Our workforce security considerations and cybersecurity capabilities are aligned to support working differently. <i>Tris Lingen, VP, Enterprise Chief Information Security Officer, 3M</i>
3:30 PM-4:00 PM	Cyber Defense Operations in an Interconnected World The speed of adversarial advancement is at an all time high. Cyber Defense Operations must mature almost in real time to keep pace. The added complexity of defending remote workers in the face of unprecedented ransomware attacks puts the potential business impact of a miss at severe levels. In this talk we'll examine ideologies and real-world war stories of organizational defense in 2021. We'll look at lessons learned where cyber defense operations were key to effective defense with approaches from the organizations that are succeeding. <i>Tim Crothers, SVP, Chief Security Officer, Mandiant</i>
4:00 PM-4:30 PM	Adversary Trends: What You Need to Know The adversarial landscape has broadened and deepened in recent years. Enterprises are expected to defend against complex, protracted attacks like SolarWinds while also protecting users from lightning-fast, adaptable ransomware attacks. We'll review the latest trends in adversaries including what we see on the horizon from attackers, and discuss how intelligence can be leveraged throughout the enterprise to plan and maximize an effective response. <i>Jason Steer, Principal Security Strategist, Recorded Future</i>
4:30 PM-4:45 PM	Wrap Up and Practical Takeaways Review Summit Highlights, Takeaways and Call to Action to solidify action items to take back to your organization. <i>Jennifer Czaplewski, Senior Director, Cyber Security, Target; Wade Van Guilder, Sr. Manager for Solutions and Architectures for WWT / SLED</i>

Monthly Newsletter

Experience the Cyber Security Summit year-round with industry insight, expert perspective and breaking news analysis delivered straight to your inbox!

The collaboration and community you experience this week can continue throughout the year with our Cyber Security Summit newsletter. Every month we bring together a range of perspectives on a different topic relevant to the challenges and opportunities we all face in securing our organizations.

Past topics have included security as a business function, supply chain security, incident-response and election security and international collaboration. An archive of previous newsletters is now available on our website.

If you are interested in continuing the learning and engagement you've experienced this week, please sign-up for our monthly Cyber Security Summit newsletter at cybersecuritysummit.org.

Thank you, and see you in 2022!

Newsletter Editors:



LOREN DEALY MAHLER

President, Dealy Mahler Strategies



CHRIS VELTSOS

Cyber Risk Strategist; Digital Trust Advisor,
Dr. InfoSec

Marketing:

BENJAMIN COOK

Senior Marketing Specialist,
The Event Group

Graphic Design:

HEIDI BRANES

Graphic Designer,
The Event Group



SUMMIT CO-CHAIRS



Learn More About Our Speakers

For full biographies and other relative information, visit: **virtual.cybersecuritysummit.org/en/speaker-s**

Summit content represents the views of each individual speaker and not necessarily that of the Cyber Security Summit or the speaker's organization.

JENNIFER CZAPLEWSKI

Senior Director, Cyber Security, Target

MON OCT 25 – 9:30 AM - Tech Session

TUE OCT 26 – 8:25 AM

The Power and Peril of Connections

WED OCT 27 – 4:30 PM

Wrap Up and Practical Takeaways

Ms. Czaplewski is an innovative cyber security leader known for building and delivering critical security functions. She is an industry leader in DevSecOps and frequently shares insights at thought leadership forums like RSA, the Cyber Security Summit, DevOps.com and All Day DevOps. She is a patent holder and her work has been featured in SC Magazine and Dark Reading.

Jennifer is currently a Senior Director in Target's Cyber Security team, leading Product Security, Vulnerability Management and Endpoint Protection. She is the 2021 co-chair of the Cyber Security Summit.

WADE VAN GUILDER

Sr. Manager for Solutions and Architectures for World Wide Technology (WWT), State & Local Government and Education (SLED)

TUE OCT 26 – 8:25 AM

The Power and Peril of Connections

WED OCT 27 – 4:30 PM

Wrap Up and Practical Takeaways

Mr. Van Guilder is a seasoned leader with over 25 years of experience in the industry. As a Sr. Manager of Solutions and Architectures for WWT, he is responsible for Cyber Security, Workforce Transformation, Multicloud, and Digital strategy for SLED East. He spends much of his time consulting with Sr. Business and Technical Leaders identifying and delivering business impacting solutions.

In support of the Public Sector market, Wade has served on multiple technical advisory councils focused on helping various OEMs improve the impact they have on serving our government. He is passionate about making business impact through the effective use of secure technology.

**BILL AERTS**

Executive Director, Archimedes Center for Healthcare and Device Security

MON OCT 25 – 9:40 AM
Healthcare Med Device

**BOB BENNETT**

Co-Founder, NaviLogic

MON OCT 25 – 1:30 PM
Tech Session



ANDREW BOMETT
VP & CISO, Boston Scientific

MON, OCT 25 – 3:30 PM
Healthcare Med Device

**KAREN ANDERSEN**

Principal Consultant, IAM Advisory | Cybersecurity | eDiscovery/ESI Consultant

MON OCT 25 – 2:00 PM
IoT/IIoT/ICS/SCADA

**GRETCHEN BLOCK**

Vice President, Optum Technology

WED OCT 27 – 10:50 AM
General Session

**ANDREW BORENE**

Civil Liberties & Privacy Officer, NCSC, Office of the Director of National Intelligence

TUE OCT 26 – 1:00 PM
General Session



DEBRA BRUEMMER
Senior Manager, Mayo Clinic
MON OCT 25 - 11:10 AM
Healthcare Med Device



JOSEPH CHOW
SVP, Director of Specialized Business Solutions, Bremer Bank
TUE OCT 26 - 1:25 PM
Small Business



MARY DINER
Security Director, Optum Technology
MON OCT 25 - 9:30 AM
Healthcare Med Device



GARY BUONACORSI
Chief Technology Officer, Chief IT Architect, US State and Local Government and Education, Tanium
MON OCT 25 - 8:45 AM
Public Sector



JOYCE CORELL
Director, Supply Chain and Technology Security, Office of the National Cyber Director, Executive Office of the President, White House
WED OCT 27 - 10:50 AM
General Session



JERRY DRIESSEN
Assistant Chief Information Officer / Chief Technology Officer, City of San José
MON OCT 25 - 12:30 PM
Public Sector



LAURA BURR
VP, Deposit Administration Manager, Bremer Bank
TUE OCT 26 - 1:25 PM
Small Business



SEAN COSTIGAN
Professor, George C. Marshall European Center for Security Studies
MON OCT 25 - 1:30 PM
IoT/IIoT/ICS/SCADA
TUE OCT 26 - 1:00 PM
General Session



JEN EASTERLY
Director, Cybersecurity and Infrastructure Security Agency (CISA)
TUE OCT 26 - 8:35 AM
General Session



CHRISTOPHER BUSE
SVP, CISO, Old Republic
WED OCT 27 - 8:00 AM
General Session
WED OCT 27 - 9:15 AM
General Session



ANDREW COYNE
CISO, Mayo Clinic
MON OCT 25 - 3:30 PM
Public Sector



STEPHEN ELLIS
Government Solutions Lead, Zoom Video Communications
MON OCT 25 - 10:30 AM
Public Sector



TOM CAMERON
Solutions Architect, BlackBerry powered by Cylance AI
MON OCT 25 - 12:30 PM
Tech Session



TIM CROTHERS
SVP, Chief Security Officer, Mandiant
WED OCT 27 - 3:30 PM
General Session



W. ANDERS FOLK
Acting United States Attorney, U.S. Department of Justice
TUE OCT 26 - 1:00 PM
General Session



AARON MCKEE CAMPBELL
Computer Scientist, FBI
TUE OCT 26 - 9:30 AM
Ransomware Panel



SAM CURRY
CSO, Cybereason
TUE, OCT 26 - 3:30 PM
General Session



JON FORD
Managing Director, Mandiant
WED OCT 27 - 1:00 PM
General Session



D. KEITH CASEY
API Problem Solver, Okta, Inc
MON OCT 25 - 10:30 PM
Tech Session



JENNIFER CZAPLEWSKI
Senior Director, Cyber Security, Target
MON OCT 25 - 9:30 AM
Tech Session
TUE OCT 26 - 8:25 AM
General Session
WED OCT 27 - 4:30 PM
General Session



AMY FOX
VP of Business Development, Ambient Consulting
MON OCT 25 - 9:30 AM
Women in Cyber



EVAN FRANCEN
CEO, SecurityStudio
MON OCT 25 – 2:30 PM
Public Sector



TED GUTIERREZ
CEO, SecurityGate.io
MON OCT 25 – 3:15 PM
IoT/IIoT/ICS/SCADA



KEITH IBARGUEN
Chief Product Officer,
Cofense
MON OCT 25 – 2:30 PM
Healthcare Med Device



CHRISTOPHER GABBARD
Cyber Security Advisor –
Region V, Office of
Cybersecurity &
Communications, CISA
TUE OCT 26 – 3:00 PM
Small Business



ANDY HANKS
CISO, State of Montana
MON OCT 25 – 1:00 PM
Public Sector



JACQUI IRWIN
Assembly member,
44th District; Chair,
Select Committee on
Cybersecurity, California
State Assembly
MON OCT 25 – 11:00 AM
Public Sector



SAILESH GADIA
Partner, KPMG
WED OCT 27 – 10:50 AM
General Session



MICHAEL HANSEN
Sr Solutions Engineer,
Avanan a Checkpoint
Company
MON OCT 25 – 10:30 AM
Tech Session



SHRUTI IYER
Principal Innovation
Architect, Oracle
MON OCT 25 – 3:30 PM
Healthcare Med Device



JOHN GILLIGAN
President and Chief
Executive Officer, Center
for Internet Security
MON OCT 25 – 3:00 PM
Public Sector



DAN HANSON
Senior Vice President
Management Liability and
Client Experience, Marsh &
McLennan Agency
TUE OCT 26 – 9:30 AM
General Session



MIKE JOHNSON
Director of Graduate Studies
and Renier Chair, TLI
MON OCT 25 – 3:30 PM
Healthcare Med Device
TUE OCT 26 – 8:00 AM
General Session



DAVE GOLD
VP, Business Strategy,
SentinelOne
MON OCT 25 – 12:30 PM
Tech Session



JUDY HATCHETT
CISO, Surescripts
MON OCT 25 – 8:45 AM
Tech Session
MON OCT 25 – 9:30 AM
Healthcare Med Device



DARRIN E. JONES
Executive Assistant
Director, FBI
TUE OCT 26 – 4:40 PM
General Session



MICHAEL GREGG
Interim CISO, State of
North Dakota
MON OCT 25 – 9:15 AM
Public Sector



**BRIGADIER GENERAL
STEFANIE HORVATH**
Mobilization Assistant to
the Director of Operations;
Executive Director
Enterprise Services, U.S.
Cyber Command, MNIT
TUE OCT 26 – 11:15 AM
General Session



SARAH JOPP
Principal Information
Security Analyst, Mayo
Clinic
MON OCT 25 – 11:10 AM
Healthcare Med Device



EARL GREGORICH
Area Manager and Business
Consultant at Greenville
Area Small Business
Development Center, SBDC
TUE OCT 26 – 3:30 & 4:30 PM
Small Business



ALLISON HUBEL, PHD
Director, Technological
Leadership Institute at
University of Minnesota
TUE OCT 26 – 8:00 AM
General Session



ERAN KAHANA
Attorney, Maslon
MON OCT 25 – 1:15 PM
Healthcare Med Device

**FAISAL KALEEM**

Professor, Department of Computer Science and Cybersecurity, Metropolitan State (MN) University

MON, OCT 25 - 9:30 AM
Tech Session

**ROBERT LEE**

CEO, Dragos
MON OCT 25 - 2:00 PM
IoT/IIoT/ICS/SCADA

**CHRIS MARK**

National Practice Director - Payment Security, Fraud, and IAM

WED OCT 27 - 2:00 PM
General Session

**DR. VASILEIOS KARAGIANNOPOULOS**

Reader in Cybercrime and Cybersecurity, Portsmouth University

MON OCT 25 - 2:30 PM
Tech Session

**TONY LEE**

VP, Global Services Technical Operations, Blackberry

WED OCT 27 - 1:30 PM
General Session

**PETER MARTINSON**

Director of Incident Response, Blue Team Alpha

WED OCT 27 - 9:30 AM
General Session

**DARRELL KESTI**

Director, HealthCare Sales, Ord

MON OCT 25 - 2:00 PM
Public Sector

**BRIAN LEVINE**

Managing Director, Cybersecurity & Data Privacy, EY

TUE OCT 26 - 9:00 AM
General Session

**JASON STEER**

Principal Security Strategist, Recorded Future

WED OCT 27 - 4:00 PM
General Session

**EUGENE KIPNISS**

MS-ISAC Member Programs Manager, Center for Internet Security

MON OCT 25 - 8:15 AM
Public Sector

**CAREY LEWIS**

SVP of Strategic Sales, Island

MON OCT 25 - 9:30 AM
Women in Cyber

**BRIAN MCDONALD**

District Director, SBA

TUE OCT 26 - 1:10 PM
Small Business

**CARLOS KIZZEE**

VP, Stakeholder Engagement, MS-ISAC, Center for Internet Security

MON OCT 25 - 8:00 AM
Public Sector
WED OCT 27 - 9:15 AM
General Session

**TRIS LINGEN**

VP, Enterprise Chief Information Security Officer, 3M

WED OCT 27 - 3:00 PM
General Session

**LOUISE MCEVOY**

Mountaineer & Cyber Professional

MON OCT 25 - 11:30 AM
Women in Cyber

**YAN KRAVCHENKO**

Information Security Director, Hennepin Healthcare

TUE OCT 26 - 9:30 AM
General Session

**LARRY MACCHERONE**

DevSecOps Transformation, Contrast Security

TUE OCT 26 - 2:00 PM
General Session

**TINA MEEKER**

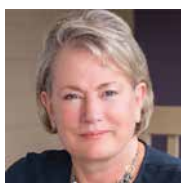
Sr. Director, Information Security, Sleep Number

MON OCT 25 - 8:45 AM
Women in Cyber
MON OCT 25 - 10:30 AM
Women in Cyber

**JUDD LARSON**

Principal Technologist, Global Quality - Product Security Office, Medtronic

MON OCT 25 - 12:45 PM
Healthcare Med Device

**EILEEN MANNING**

Co-Founder, Executive Producer, Cyber Security Summit

TUE OCT 26 - 8:00 AM
General Session

**HARSHAL MEHTA**

VP, CISO, CWT

WED OCT 27 - 10:50 AM
General Session



RYAN MILLER
Director of Cyber Threat & Fraud Intelligence, Target
 WED OCT 27 – 9:15 AM
 General Session



MILINDA RAMBEL STONE
VP, CISO, Bremer Bank
 MON OCT 25 – 9:30 AM
 Women in Cyber
 TUE OCT 26 – 1:25 & 4:30 PM
 Small Business



DAVID SCHULTZ
Senior Consultant, G5 Consulting & Engineering Services
 MON, OCT 25 – 3:45 PM
 IoT/IIoT/ICS/SCADA



ADAM MISHLER
VP, Global Chief Information Security Officer, Best Buy
 MON OCT 25 – 10:30 AM
 Women in Cyber



BRIAN REED
Director, Cybersecurity Strategy, Proofpoint
 MON OCT 25 – 9:30 AM
 Tech Session



RICHARD SCOTT
Chief Security Architect, Optum Technology
 MON OCT 25 – 3:00 PM
 Healthcare Med Device



DANIEL MOORADIAN
Director of Graduate Studies for the MS in Medical Device Innovation Program, TLI - University of Minnesota
 MON OCT 25 – 3:30 PM
 Healthcare Med Device



SHAWN RILEY
CIO, North Dakota Information Technology Department
 MON OCT 25 – 4:00 PM
 Public Sector



JOHN SEAMAN
Regional Director, Axonius
 MON OCT 25 – 10:40 AM
 Healthcare Med Device
 MON OCT 25 – 2:30 PM
 Tech Session



REBECCA MORGAN
Deputy Assistant Director, Insider Threat; Deputy Director, National Insider Threat Task Force, National Intelligence and Security Center
 TUE OCT 26 – 1:00 PM
 General Session



CHRIS ROMEO
CEO, Security Journey
 MON OCT 25 – 2:30 PM
 Tech Session



SUMIT SEHGAL
Strategic Product Mktg Director, Armis
 MON OCT 25 – 1:45 PM
 Healthcare Med Device



DAVID MOTT
Senior Principal Engineer TLCP, Optum Technology
 MON OCT 25 – 3:00 PM
 Healthcare Med Device



KEELY ROSS
Enterprise Sales Executive, Zoom Video Communications
 MON OCT 25 – 10:30 AM
 Women in Cyber



TOM SHEFFIELD
Senior Director Technology, Target
 MON OCT 25 – 2:30 PM
 Tech Session
 TUE OCT 26 – 9:30 AM
 General Session



JIM NASH
Assistant Minority Leader, Minnesota House of Representatives
 MON OCT 25 – 11:00 AM
 Public Sector



WILLIAM SCANDRETT
Chief Information Security Officer, Allina Health
 MON OCT 25 – 10:30 AM
 Women in Cyber



SCOTT SINGER
President, CyberNINES, Ret. USN Captain
 TUE OCT 26 – 2:15 PM
 Small Business



MARIO PAEZ
Director, Cyber & Technology E&O, Marsh & McLennan Agency LLC
 TUE OCT 26 – 10:45 AM
 General Session



PHIL SCHENKENBERG
Partner, Litigation & Cyber Security, Taft Law
 TUE OCT 26 – 10:45 AM
 General Session



NANCY SKUTA
Senior Information Security Analyst, ITS4, Threat and Vulnerability Management, MNIT Services
 TUE OCT 26 – 7:30 AM
 General Session



GARY SORRENTINO
Global Deputy CIO, Zoom
Video Communications,
Zoom

WED OCT 27 - 10:20 AM
General Session



WADE VAN GILDER
Sr. Manager for Solutions
and Architectures for
WWT / SLED

TUE OCT 26 - 8:25 AM
General Session
WED OCT 27 - 4:30 PM
General Session



COL. TERI WILLIAMS
Commander, 91st Cyber
Brigade, Virginia Army
National Guard; DHS

MON OCT 25 - 10:00 AM
Public Sector



RYAN SPELMAN
VP Cyber Risk, Kroll

MON OCT 25 - 1:30 PM
Public Sector



PAUL VEENEMAN
President & COO,
Beryllium Infosec
Collaborative

MON OCT 25 - 1:00 PM
IoT/IIoT/ICS/SCADA



MEREDITH WINEGAR
Operations Director of
Mortgage, Trust and
Insurance, Bremer Bank

TUE OCT 26 - 1:25 PM
Small Business



BENJAMIN STOCK
Director of Healthcare
Product Management, Ord

MON OCT 25 - 10:10 AM
Healthcare Med Device



ALEX VOLK
Senior Engineer,
ReliaQuest

MON OCT 25 - 1:30 PM
Tech Session



IRA WINKLER
CISO, Skyline Technology
Solutions

TUE OCT 26 - 4:00 PM
General Session



ROHIT TANDON
Assistant Commissioner,
State CISO, State of
Minnesota, MNIT Services

MON OCT 25 - 8:00 & 10:30 AM
Public Sector
TUE OCT 26 - 7:30 AM
General Session



DEREK WEEKS
Senior Vice President,
The Linux Foundation

TUE OCT 26 - 3:00 PM
General Session



ROBERT WORDEN
SVP, Community Sales and
Support Manager, Bremer
Bank

TUE OCT 26 - 1:25 PM
Small Business



ANDREW TELLJOHN
Editor and Publisher,
Upsize Minnesota

TUE OCT 26 - 4:30 PM
Small Business



JOE WEISS
Managing Partner,
Applied Control
Solutions, LLC

MON OCT 25 - 2:45 PM
IoT/IIoT/ICS/SCADA



LYLE WRIGHT
Associate State Director,
Minnesota Small
Business Development
Center

TUE OCT 26 - 1:00 PM
Small Business



**SHAYLA TREADWELL,
PH.D.**
Executive Director,
Cybersecurity Center of
Excellence, Governance,
Risk & Compliance, ECS

WED OCT 27 - 8:30 AM
General Session



GRETCHEN WHITE
CISO, Minnesota Judicial
Branch

MON OCT 25 - 1:00 PM
Public Sector



MICHAEL WYATT
Director, Threat
Management,
Surescripts LLC

MON OCT 25 - 10:30 AM
Tech Session



JAMISON UTTER
Sr Director Product and
Solution Evangelism, Ord

MON OCT 25 - 4:15 PM
IoT/IIoT/ICS/SCADA



CLARK WHITING
Lead Security Architect,
Best Buy

MON OCT 25 - 9:00 AM
Women in Cyber



WHY AXONIUS?

**BECAUSE NO ONE GOT INTO
CYBERSECURITY TO SPEND ALL
THEIR TIME GATHERING ASSET DATA.**

SEE AXONIUS IN ACTION.

Sign up for a 20-minute platform overview webinar.

axonius.com/ccssumit

How to Upskill the Hybrid Workforce with Tailored Security Training



Gary Sorrentino
Global Deputy CIO

With discussions circulating around going back into the office and employees still craving flexibility, leaders everywhere need to examine what it means to establish a successful and secure [hybrid workforce](#).

To keep information and devices secure as employees travel in and out of the office, organizations will need to create a security strategy rooted in the variability of the everywhere workforce, one that helps workers understand the role they play in securing this [new model](#).

Security leaders must create a training program tailored to the human variable and focused on real-life scenarios that will emerge in this new hybrid future.

The value of training

The [IBM 2021 X-Force Threat Intelligence Index](#) reports 95% of cybersecurity breaches are due to human error. Training employees isn't just important, it's essential for an organization's survival.

Training creates a vital sense of awareness of today's complex threat landscape and the role end users play in it. It encourages a sense of responsibility and accountability by showing that end user actions have a direct correlation to the overall security posture of an organization. Training also creates a culture of security, where all parties feel invested in the overall protection of an organization, even if they're disconnected from a physical office.

Going beyond the basics

To combat today's complex threats, training has to go beyond the basics. While employees need continuous learning on threat detection and data protection best practices, IT leaders need to also tailor their programming to the unique needs of the hybrid workforce. Therefore, training must focus on the following:

Technology tutorials: The hybrid workforce isn't possible without the [technology that enables employees to do their job from anywhere](#).

Businesses should adopt user-friendly solutions that have controls in place and make sense to the people who use them every day; implementation should be paired with dedicated tutorials and training sessions on the software.

Scenario-focused threat awareness: IT also needs to build training scenarios tailored to the variability of a distributed workforce — lessons that speak to the threat of information flowing in and out of the office, to the dangers of working from public areas, to the kinds of attacks that target at-home workers, and more. A few of these attack scenarios should include:

- Shoulder surfing
- Business email compromise
- Elicitation
- Brute-force password attacks
- Phishing schemes

Training should ultimately be designed as a memorable experience versus a quarterly task that employees feel obligated to complete. For example, at Zoom we distribute a "Work-From-Home Security Best Practices" checklist and conduct annual security training with our employees, but have expanded our efforts to encompass situational training as well. We've launched monthly phishing simulations and follow-up education to have employees practice identifying and reporting phishing emails in a safe environment, transforming the threat of phishing into a tangible reality.

Combining the strengths of training & technology

The human variable of the hybrid workforce can either be your organization's biggest threat or its strongest competitive advantage. Success in today's complex landscape will be determined by how you pivot your strategy around that variable. As you evolve the way you upskill the hybrid workforce, you need an intuitive communications platform that can keep pace. Designed for seamless and secure collaboration, the Zoom platform keeps you and your team connected so you can get more done, no matter where you are. Our solutions are built with security top of mind to help protect the crucial information shared across our platform.

For Zoom Meetings specifically, we've created an [end-to-end encryption \(E2EE\) feature](#), which, when enabled, uses the same 256-bit AES GCM encryption that supports standard Zoom Meetings but the cryptographic keys are known only to the devices of the meeting participants.

With the right mix of training and technology supporting your workforce, hybrid is no longer a novel concept, but a sustainable reality that can support greater flexibility, efficiency, and security for your organization.



*Women in Cyber
Sponsor*

Based in Minnetonka, Ambient Consulting is celebrating 20 years success within IT Staffing. Ambient is recognized for quality delivery, authenticity and the ultimate customer service. With its appealing business model and tenured team, companies trust Ambient to best identify, secure and retain mission-critical, high demand IT and Business talent.

ambientconsulting.com



Ruby Sponsor

Armis® is the leading unified asset visibility & security platform designed to address the new threat landscape created by connected devices. Fortune 1000 companies trust our real-time, continuous, and agentless protection to see all managed, unmanaged, and IoT devices with full context, including medical devices (IoMT), operational technology (OT) and industrial control systems (ICS).

armis.com



Diamond Sponsor

Axonius is the cybersecurity asset management platform that gives organizations a comprehensive asset inventory, uncovers security solution coverage gaps, and automatically validates and enforces security policies. By seamlessly integrating with hundreds of security and management solutions, Axonius is deployed in minutes, improving cyber hygiene immediately.

axonius.com



Intelligent Security. Everywhere.

Presenting Sponsor

BlackBerry® provides intelligent security software and services to enterprises and governments around the world. The company secures more than 500M endpoints. The company leverages AI and Machine Learning, powered by Cylance, to deliver innovative solutions in cybersecurity, endpoint security, management, encryption and embedded systems. BlackBerry's vision is clear — to secure a connected future you can trust.

blackberry.com



Ruby Sponsor

Bremer Financial Corporation is a privately held, \$13 billion regional financial services company jointly owned by the Otto Bremer Trust and Bremer employees. Founded in 1943 by Otto Bremer, the company provides a comprehensive range of banking, mortgage, investment, wealth management, and insurance services throughout Minnesota, North Dakota and Wisconsin.

bremer.com



Partner

The Center for Internet Security, Inc. (CIS®) is responsible for globally recognized best practices for securing IT systems and data including the CIS Benchmarks™ and CIS Controls®. Our CIS Hardened Images provide secure, on-demand, scalable computing environments in the cloud.

cisecurity.org



*Tech Sessions
Supporter*

Check Point is a leading provider of cyber security solutions globally, protecting customers from 5th generation attacks with an industry leading catch rate of malware, ransomware and other types of attacks. We offer multilevel security architecture, "Infinity" Total Protection with Gen V advanced threat prevention, which defends enterprises' cloud, network and mobile device held information.

checkpoint.com



Co-marketer

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.

csamn.com



*Healthcare & Med
Device Host*

Cofense® is the leading provider of phishing detection and response solutions. Designed for enterprise organizations, the Cofense Phishing Detection and Response (PDR) platform leverages a global network of over 25 million people actively reporting suspected phishing, combined with advanced automation to stop phishing attacks faster and stay ahead of breaches.

cofense.com



*Presenting
Sponsor*

Contrast Security is the leader in modernized application security, embedding code analysis and attack prevention directly into software. Contrast's patented deep security instrumentation completely disrupts traditional application security approaches with integrated, comprehensive security observability that delivers highly accurate assessment and continuous protection across an entire application portfolio.

contrastsecurity.com



*Presenting
Sponsor*

Cybereason is the champion for today's cyber defenders providing future-ready attack protection that unifies security from the endpoint, to the enterprise, to everywhere the battle moves. The Cybereason Defense Platform combines the industry's top-rated detection and response (EDR and XDR), next-gen anti-virus (NGAV), and proactive threat hunting to deliver context-rich analysis of every element of a MalOp (malicious operation). The result: defenders can end cyber attacks from endpoints to everywhere. Cybereason is a privately held, international company headquartered in Boston with customers in more than 30 countries.

cybereason.com/platform



*Small Business
Supporter*

CyberNINES provides cybersecurity consultation and managed services to businesses, with a significant focus on those companies supporting the U.S. Department of Defense (DoD). Services include assessing, securing, and protecting companies from increasing cybersecurity threats. With 50% of the CyberNINES employees veterans, there is a strong sense of mission to protect our country's supply chains.

cybernines.com



Ruby Sponsor

Headquartered in Fairfax, Virginia, ECS has more than 3,000 employees throughout the U.S. We are proud to build successful customer relationships with some of the world's leading agencies in both the public and private sectors. Inspired by the ability to create, innovate, and serve, our highly skilled teams work together to solve complex challenges and provide advanced technology, science, and engineering solutions.

ecstech.com



Diamond Sponsor

EY exists to build a better working world, helping create long-term value for clients, people and society and build trust in the capital markets. Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate. Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

ey.com



Global **Minnesota**

Co-marketer

Global Minnesota is a nonprofit, nonpartisan organization that connects individuals, organizations, and communities to the world. Through a unique lineup of programs, Global Minnesota takes relevant and timely information on international issues, foreign policy, and cultural topics, and provides the space and opportunity for engagement and discussion.

globalminnesota.org



*Healthcare & Med
Device Co-marketer*

Health-ISAC is a trusted community of critical infrastructure owners and operators within the global Healthcare and Public Health sector (HPH). The community is primarily focused on sharing timely, actionable and relevant information with each other including intelligence on threats, incidents and vulnerabilities and best practices, mitigation strategies and more. Sharing occurs both machine-to-machine and person-to-person. H-ISAC also fosters the building of relationships and networking through worldwide educational events and whitepapers. Working groups and committees focus on topics of importance to the sector and member-vetted shared services offer enhanced services to leverage the H-ISAC community for the benefit of all.

h-isac.org



Silver Sponsor

Imperva is the cybersecurity leader whose mission is to protect data and all paths to it. More than 6,200 customers trust Imperva to protect their applications, data and websites from cyber attacks. With an integrated approach that combines edge, application and data security, Imperva protects companies through all stages of their digital journey.

imperva.com



InfraGard

Co-marketer

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 investigative 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.

infragard.org



Twin Cities MN
Section

Co-marketer

The Twin Cities Section of International Society of Automation (Twin Cities ISA) is a 75-year-old nonprofit and local focus for automation training, certification, and standards development. ISA is author of the globally respected ISA/IEC 62443, the only consensus-based series of IACS standards and a key component of the U.S. government's cybersecurity plan.

ISA Twin Cities: twincities-isa.org

ISA National: isa.org



Co-marketer

With approximately 1200 members from over 100 organizations, the Minnesota chapter of ISACA provides a gateway to a global organization offering security, risk, control, privacy, and governance certifications. Additionally, ISACA offers a Certified Information Security Manager (CISM) certificate, as well as a Cybersecurity certification program (CSX) for both students and recent grads (Fundamental) as well as those with experienced skill sets (Practitioner.)

mnisaca.org



Island

Silver Sponsor

The security stack has never been more powerful -- and somehow, working securely, privately, and productively has never been more difficult. We think it's time to revisit security. To take a whole new approach - where security is built into the enterprise, not on top of it. Where work is secure by design. We're building something special, and we can't wait to share it with you soon.

island.io



Co-marketer

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, publications, and peer interaction opportunities that enhance the knowledge, skill, and professional growth of our members.

mnissa.org



Platinum

KPMG has experience across the continuum — from the boardroom to the data center. In addition to assessing your cyber security and aligning it to your business priorities, we can help you develop advanced approaches, implement them, monitor ongoing risks and help you respond effectively to cyber incidents. So no matter where you are on the cyber security journey, KPMG can help you reach the destination.

kpmg.com/us/cyber



Silver Sponsor

Through the strength of their management team, geographic presence and world class services, Marsh McLennan Agency provides public and private companies with risk management and employee benefit support that helps them flourish. They are proud to provide their clients with best-in-class services that meet their growing needs.

marshmma.com



*Healthcare & Med
Device Supporter*

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.

maslon.com



Silver 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.

metrostate.edu



Platinum

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.

mn.gov/mnit



*Public Sector
Partner*

The Multi-State Information Sharing and Analysis Center® (MS-ISAC®), is the key resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial (SLTT) governments. The mission of the MS-ISAC is to improve the cybersecurity posture of the nation's SLTT governments through coordination, collaboration, and cooperation.

ciscure.org/ms-isac



Ruby Sponsor

NaviLogic is an IT consulting and security reseller/integrator with extensive expertise in both cybersecurity and governance risk and compliance (GRC.) Our uniquely holistic approach identifies what needs to be optimized, augmented or replaced to ensure your organization is maximizing efficiencies while minimizing costs, and, more importantly, security and governance risk.

navilogic.com



*Custom
Sponsorship*

Ordr secures the millions of enterprise IoT and unmanaged devices such as manufacturing machines, building systems, medical equipment, printers and more that run within global networks. The Ordr Systems Control Engine uses machine learning to automatically discover and classify every IoT and unmanaged device, map all communications, detect and prioritize vulnerabilities, and then proactively secure each device through dynamic policy generation and segmentation. Organizations use Ordr to discover their devices, track usage, achieve proactive protection and compliance.

ordr.net



Ruby Sponsor

Proofpoint, Inc. (NASDAQ: PFPT) is a leading cybersecurity and compliance company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web.

proofpoint.com



*Presenting
Sponsor*

Recorded Future is the world's largest provider of intelligence for enterprise security. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future delivers intelligence that is timely, accurate, and actionable. Recorded Future is trusted by over 1,000 businesses and government organizations around the world.

recordedfuture.com



Silver Sponsor

As your security ally, Red Canary enables your team to focus on the highest priority security issues impacting your business. By removing your need to build and manage a threat detection operation, we help you focus on running your business securely and successfully.

redcanary.com



Ruby Sponsor

ReliaQuest, the leader in Open XDR-as-a-Service, is known for being the force multiplier for security operations teams. ReliaQuest GreyMatter is a cloud-native Open XDR platform that brings together telemetry from any security and business solution, whether on-premises or in one or multiple clouds, to unify detection, investigation, response, and resilience. ReliaQuest combines the power of technology and 24/7/365 security expertise to give organizations the visibility and coverage they require to make cybersecurity programs more effective.

reliaquest.com



Small Business Host

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 at no cost, to businesses at any point in their entire life cycle, from start-up to growth to exit strategies.

mnsbdc.com



*Public Sector
Supporter*

SecurityStudio is a SaaS company dedicated to simplifying information security fundamentals and making them available to everyone. The SecurityStudio platform (S2) enables Programmatic Distributed Empowerment for Information Security (PDEIS™) through tools such as S2Org (organizational risk management), S2School, S2Vendor, S2Team, and S2Me.

securitystudio.com



SentinelOne is a pioneer in delivering autonomous security for the endpoint, datacenter and cloud environments to help organizations secure their assets with speed and simplicity. SentinelOne unifies prevention, detection, response, remediation and forensics in a single platform powered by artificial intelligence.

sentinelone.com



Our purpose is to serve the nation with the single most trusted and capable health information network, built to increase patient safety, lower costs and ensure quality care. Since 2001, Surescripts has led the movement to turn data into actionable intelligence, and convened the Surescripts Network Alliance™ to enhance prescribing, inform care decisions and advance the healthcare industry. Visit us online and follow us at twitter.com/surescripts. surescripts.com



Tanium gives the world's largest enterprises and government organizations the unique power to secure, control, and manage millions of endpoints across the enterprise within seconds. Serving as the "central nervous system" for enterprises, Tanium empowers security and IT operations teams to ask questions about the state of every endpoint across the enterprise in plain English, retrieve data on their current and historical state, and execute change as necessary, all within seconds. With the unprecedented speed, scale, and simplicity of Tanium, organizations now have complete and accurate information on the state of endpoints at all times to more effectively protect against modern day threats and realize new levels of efficiency in IT operations.

tanium.com



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 (MSST), Management of Technology (MOT) and Medical Device Innovation (MDI).

tli.umn.edu



Unisys is a global IT services company that delivers successful outcomes for the most demanding businesses and governments. Unisys offerings include digital workplace services, cloud and infrastructure services and software operating environments for high-intensity enterprise computing. Unisys integrates security into all of its solutions. For more information on how Unisys delivers for its clients across the government, financial services and commercial markets, visit:

unisys.com



Upsize Minnesota is a "how-to" media company that aims through its magazine, website and multimedia products to provide small business owners with actionable information they can use to grow their companies.

upsizemag.com



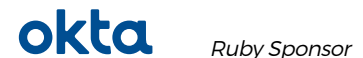
Women in CyberSecurity (WiCyS) is the only non-profit membership organization with a national reach that is dedicated to bringing together women in cybersecurity from academia, research and industry to share knowledge, experience, networking and mentoring. WiCyS helps build a strong cybersecurity workforce with gender equality by facilitating recruitment, retention and advancement for women in the field.

wicysmn.org



Zoom helps people stay connected so they can get more done together. From meetings, chat, phone, and webinars to conference room systems and online events, Zoom powers all your communication needs. Our secure, reliable video platform offers a high-quality experience that is easy to manage, use, and customize.

zoom.us



Okta is the leading independent provider of identity for the enterprise. The Okta Identity Cloud enables organizations to securely connect the right people to the right technologies at the right time. With over 6,500 application integrations, Okta customers can easily and securely use the best technologies for their business.

www.okta.com

Your Definitive Guide to Reducing Risk

Security intelligence is the most powerful weapon defenders have against their adversaries.

The latest edition of Recorded Future's popular book paints a clear picture of security intelligence, as well as actionable guidance for disrupting the threat actors targeting your organization right now — and in the future.

"The Security Intelligence Handbook" is your definitive guide for proactive risk reduction. This edition has been updated to include a new foreword about the unprecedented state of cyber and physical security, a sharpened focus on six critical security functions, an expanded discussion of security intelligence's applications for specific teams, and a new conclusion that explores the results you may achieve with security intelligence.

**DOWNLOAD YOUR
FREE COPY TODAY**

THE SECURITY INTELLIGENCE HANDBOOK

Reduce Risk With Security Intelligence

A business-centric approach to reducing risk that combines security, intelligence, and business insights. This handbook provides fast, informed decisions, and drive a risk reduction throughout your entire organization.

Security intelligence delivers value across every security function.

THE
**SECURITY
INTELLIGENCE
HANDBOOK**

How to Disrupt Adversaries and Reduce Risk
With Security Intelligence



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).

ADWARE

Software that displays unwanted advertisements on your computer. Bothersome but usually not dangerous, popping up unwanted advertising or even installing new toolbars.

AIR GAP

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

AUTORUN WORMS

Malicious programs introduced via external storage devices and designed to rapidly spread via Windows autorun feature. These worms search for security holes, permitting the hacker to steal information, money or both.

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.

ATTACK VECTOR

The path or means by which a hacker gains access to a computer or network server in order to deliver a payload or malicious outcome. Attack vectors enable hackers to exploit system vulnerabilities, including the human element.

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.

BLENDED ATTACK

A cyber attack that comprises multiple attack vectors and malware is known as a blended attack. Such attacks usually cause severe damage to targeted systems.

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.

BROWSER HIJACKER

If you find that your Internet browser's settings have changed on its own, including your selected search engine and default homepage, then you have got a browser hijacker in your system.

BRUTE FORCE ATTACK

In a brute force attack hackers try to crack encrypted data (passwords) by trying all possible combinations of words or letters.

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.

CLICKJACKING

Clickjacking is a technique used by an attacker to inject malicious code in clickable content in websites. Clickjacking is usually done to record the victim's clicks on the Internet or drop a malware infection on the system.

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.

CONTENT SPOOFING

Content spoofing is carried out by an attacker to trick their victims into visiting a fraudulent site that looks like the real one.

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.

CROSS SITE SCRIPTING (XSS)

Also known as XSS attacks, cross site scripting is a technique used by hackers to plant a malicious code into a genuine website. This allows hackers to gather user's information and use it for nefarious purpose.

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.

EMAIL SPOOFING

Email spoofing is how an attacker crafts the header of a malicious email so that user is tricked into viewing it. This technique is typically used in phishing attacks.

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.

IDENTITY THEFT

A menace in the IT security world, identity theft occurs when an attacker gathers personal information and use it to impersonate their victim. This way, the attacker can open illegal bank accounts, obtain credit cards, carry out transactions, etc., using the victim's name.

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.

INSTANT MESSAGING (IM) WORM

Worm are malware that are capable of self-replicating and spreading across the Internet or the compromised network. Worms that spread via instant messaging networks are called IM worms.

INSIDER ATTACK

When someone with an authorized system access carries out malicious activities on a network or a computer, it is known as an insider attack or insider threat. The attacker might be an employee of the targeted business, or an outsider posing as an employee.

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.

LIKEJACKING

Likejacking is a part of the clickjacking technique. It usually targets users of the social network community such as Facebook. Scammers share unusual or compelling posts or videos to trick users into liking or sharing them thus, spreading the scam to other users.

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.

MAN-IN-THE-MIDDLE ATTACK

Abbreviated as MITM, this attack is launched by a hacker to intercept, record, and control the communication between two users.

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.

PHARMING

Pharming is when a user is redirected to a fake website without their consent or knowledge. In most cases, the fake website looks exactly similar to the actual website that the user intended to visit.

PHISHING

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

POLYMORPHIC VIRUS

A polymorphic virus is a malicious program that modifies itself when it replicates. This technique enables it to evade detection by security software.

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.

PURPLE TEAMING

A team established to bring the red and blue teams together, better leveraging an organizations expertise.

RAT (REMOTE ACCESS TROJANS)

A RAT is a malicious program that can allow a hacker to take over a system from another physical location. Using this malware, the attacker can access and steal confidential and personal data from the infected machine.

RANSOMWARE

Ransomware is a malicious program that performs the following malicious activities after infecting a computer:

- Makes the system non-functional unless the victim agrees to pay a ransom.
- Encrypts the computer's data and demands a ransom to release it to the victim.

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.

REVERSE SOCIAL ENGINEERING ATTACK

In this kind of cyberattack, the attacker convinces a user that they have a problem and that the attacker has a solution to the problem. For instance, an attacker creates a problem for the target. Then the attacker advertises themselves as the solution provider, with an intention of luring the victim to divulge sensitive information.

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.

SESSION HIJACKING

Session hijacking is an attack wherein a hacker takes control of a computer session to perform illegal activities such as taking over the victim's online accounts.

SHOULDER SURFING

Shoulder surfing refers to spying on a user to obtain personal or private information such as PINs, passwords, security codes, etc. Here, the criminal usually looks over a person's shoulder while the latter might be using an ATM, phone or other electronic device.

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.

SMISHING

SMiShing is a type of a phishing attack where targets are sent fake or malicious SMSs. These SMSs are designed to steal personal information from the target, or trick them into visiting a phishing website.

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.

SPAM

Spam is defined as unwanted or unexpected emails sent in bulk. Mostly, spam is used to distribute malware.

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.

SQL INJECTION

An SQL injection is performed by an attacker to exploit a poorly-designed application to produce unwanted database query results. For instance, an attacker can insert a malicious code into a Web form that is used for user authentication. Via this code, the attacker can send his request to the database and perform illicit activities.

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.

TARGETED ATTACK

A targeted attack is a highly focused attack on specific individuals or an organization. Hackers use this technique to persistently pursue its target while remaining anonymous, for a long-term period.

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.

URL SPOOFING

A technique used by hackers to create a fake URL that impersonates the URL of a secure or legitimate website. A spoofed URL looks exactly like the one of the original website, but redirects users to a phishing or a malicious site.

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.

VISHING

Voice phishing where a hacker uses voice calls to trick users into divulging personal or financial information.

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.

WEBSITE SPOOFING

Website spoofing refers to creating a fake site that looks exactly like a trusted and popular website, in order to collect personal or financial information from users. Spoofed websites are created using legitimate logos, colors, designs, etc., to make them look realistic.

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.

Save the Date!

12th Annual Cyber Security Summit

Minneapolis, MN October 24–26, 2022



12TH ANNUAL LEADERSHIP EVENT
CYBER SECURITY
— SUMMIT —

Join our newsletter for the latest information!

cybersecuritysummit.org

Cyber Security Acronyms

3DES	Triple Data Encryption Standard	MAC	Media Access Control Address
ABAC	Access-Based Access Control	ADDRESS	Media Access Control Address
ACL	Access Control List	MAN	Metropolitan Area Network
ADP	Automated Data Processing	MFA	Multi Factor Authentication
AES	Advance Encryption Standard	NAT	Network Address Translation
AH	Authentication Header	NETBIOS	Network Basic Input/Output System
AIS	Automated Information System	NIC	Network Interface Controller or Network Interface Card
AO	Area of Operations	NIAP	National Information Assurance Partnership
ASR	Attack Surface Reduction	NIST	National Institute for Standards and Technology
APT	Advanced Persistent Threat	NNTP	Network News Transfer Protocol
BCP	Business Continuity Plan	OPSEC	Operational Security
BIA	Business Impact Analysis	OS	Operating System
BOD	Beginning of Day	OSI	Open Systems Interconnections
BYOD	Bring Your Own Device	OWASP	Open Web Application Security Project
CA	Certificate Authority	PAAS	Platform as a Service
CIO	Chief Information Officer	PIN	Personal Identification Number
CISO	Chief Information Security Officer	PKI	Public Key Infrastructure
CSO	Chief Security Officer	POTS	Plain Old Telephone Service
CAPEC	Common Attack Pattern Enumeration and Classification	PSTN	Public Switched Telephone Network
CERT	Computer Emergency Response Team	RA	Registration Authority
CMMC	Cybersecurity Maturity Model Certification	RAS	Remote Access Service
CWPP	Cloud Workload Protection Platform	RBAC	Role-Based Access Control
DES	Data Encryption Standard	ROI	Return On Investment
DHS	Department of Homeland Security	RPO	Recovery Point Objective
DRP	Disaster Recovery Plan	RTO	Recovery Time Objective
DAC	Discretionary Access Control	SAAS	Software as a Service
DNS	Domain Name System	SCADA	Supervisory Control and Data Acquisition
ECC	Elliptical Curve Cryptography	SDLC	Software Development Life Cycle
EFT	Electronic Funds Transfer	SDO	Service Delivery Objectives
ESP	Encapsulation Security Payload	SECAAS	Security as a Service
EW	Electronic Warfare	SET	Secure Electronic Transaction
FISMA	Federal Information Security Modernization Act	SET	Social-Engineer Toolkit
FTP	File Transfer Protocol	SFA	Single Factor Authentication
FO	Forward Observer	SLA	Service Level Agreement
GRC	Governance Risk and Compliance	S/MIME	Secure Multipurpose Internet Mail Extension
HIPAA	Health Insurance Portability and Accountability Act	SMTD	Simple Mail Transfer Protocol
HTTP	Hypertext Transfer Protocol	SOD	Segregation/Separation of Duties
HTTPS	Hypertext Transfer Protocol Secure	SOD	Start of Day
IAAS	Infrastructure as a Service	SPX	Sequenced Packet Exchange
IAM	Identity & Access Management	SSH	Secure Shell
IANA	Internet Assigned Numbers Authority	SSL	Secure Socket Layer
ICMP	Internet Control Message Protocol	TCO	Total Cost of Ownership
IDS	Intrusion Detection System	TCP	Transmission Control Protocol
IETF	Internet Engineering Task Force	TCP/IP	Transmission Control Protocol/Internet Protocol
IG	Interior Guard	TKIP	Temporal Key Integrity Protocol
IP	Internet Protocol	TLS	Transport Layer Security
IPS	Intrusion Prevention System	URL	Uniform Resource Locator
IPSEC	Internet Protocol Security	UDP	User Datagram Protocol
IPX	Internetwork Packet Exchange	VLAN	Virtual Local Area Network
IS	Information Systems	VPN	Virtual Private Network
ISO	International Standards Organization	VOIP	Voice Over Internet Protocol
ISP	Internet Service Provider	WAN	Wide Area Network
KRI	Key Risk Indicator	WAP	Wi-Fi Protected Access
LAN	Local Area Network	WAP2	Wi-Fi Protected Access II
LDAP	Lightweight Directory Access Protocol	WEP	Wired Equivalent Privacy
MAC	Mandatory Access Control	WLAN	Wireless Local Area Network
MAC	Media Access Control	XSS	Cross-Site Scripting
		XDR	Extended Detection and Response
		2FA	Two Factor Authentication

Cybersecurity

We put cybersecurity at the heart of our clients' business strategy, to support innovation and help them gain a competitive edge in the digital world.

ey.com



UNIFIED ASSET VISIBILITY AND SECURITY

VISIBILITY

See and secure every thing™.

INSIGHTS

Unify your security goals with your business objectives.

ACTION

Remediate and eliminate threats in real-time.

armis.com





Does Exponential Growth of Connected Devices Mean Exponentially Increased Risk?



Mike Johnson
**Technological Leadership
Institute**

With all the technological advances we have seen over the last decade it sometimes feels like there is nothing that can't be accomplished through technology. We've seen dramatic gains in efficiency and effectiveness through connected systems and sensors in areas like manufacturing and facilities management. These improvements have also supported our recent need to stay safe while still accomplishing important tasks during the pandemic. One area of technology that has really benefited from new and innovative connections is medical care.

The growth in tools available to treat medical conditions or improve general health has been tremendous, from wearable devices that can monitor conditions, track activity, and promote good health decisions to implantable devices that actually keep patients alive and can be remotely managed 24/7 by a healthcare provider. This real time monitoring and management ability has given providers a significant tool in improving patient care. This rapid growth of connected health devices has also given rise to an additional category of the Internet of Things, the Internet of Medical Things. The seemingly exponential growth of connected devices wouldn't be happening if they didn't provide significant value to businesses and consumers. Due to the growth of all IoT devices, the number of connected IoT devices actually exceeded the number of non-IoT devices at the end of last year for the first time ever (IoT Analytics).

While all of these new devices may have many benefits, are we fully accounting for the increased risks they pose? In the consumer market there are thousands of IoT devices that may not have been designed with security in mind. And do we really need to connect things like toilets and egg trays to the internet? While the impact from poorly designed smart toilets might not seem like a significant issue, how about those things that manage our power systems or keep us healthy and may even be installed inside our bodies? We should look at these advances considering that the more capable or functional the devices are, the more they might impact us if misused by a hacker.

We all have a responsibility to ensure a safe and secure future by promoting a more secure IT ecosystem and environment, from manufacturers and businesses to consumers. While the problem of poorly designed technology that doesn't adequately address security risks is certainly not a new one, given the dramatic potential increased exposure from newly connected devices it has become even more critical to the safety of all connected users and environments. The concept of security by design, where the threats and risks to systems are fully considered during product development and controls are designed into systems to mitigate those risks, should be required baseline activities for all new (or newly connected) devices. If we don't take action and make progress in this area, we risk creating an environment that introduces significantly more risk than the value we get from the connected systems. It is up to purchasers to demand secure products, and manufacturers to invest in the skilled professionals that understand this delicate balance of risk and value so we don't continue to make this problem worse and experience increased impacts from the things that are supposed to help us be more effective, efficient, and even healthy.

Webinar Series



CYBER SECURITY
Security solutions through collaboration.™ **SUMMIT**

In today's ever-evolving threat landscape, strengthening our global connections has never been more important. That's why we embarked on a monthly webinar series that examines some of the critical issues we will address during the Summit's programming. The webinars are the last Tuesday of each month.

Complimentary and open to all, each hour-long webinar explores one vexing challenge facing the cyber community and offers insight, knowledge and perspective from multinational business leaders and government officials.



Moderator:

SEAN COSTIGAN

Professor, George C. Marshall
European Center for Security Studies

Upcoming webinar:

UPCOMING: NOVEMBER 30

Making Employees the CISOs
of Their Workspaces



GARY SORRENTINO
Global Deputy CIO, Zoom Video
Communications, Zoom

Past webinars:

SEPTEMBER WEBINAR

The Significance of AI &
ML In Cybersecurity



TOM CAMERON
Solutions Architect, BlackBerry
powered by Cylance AI

AUGUST WEBINAR

Ransomware Unplugged:
What Does the Most Recent Cyber
Plague Mean?



SAM CURRY
Chief Security Officer, Cybereason

JULY WEBINAR

RaaS and the Rise Of Ransomware Extortion Ecosystem



ALLAN LISKA
Sr. Solutions Architect,
Recorded Future



DMITRY SMILYANETS
Expert Threat Intelligence
Analyst, Recorded Future

JUNE WEBINAR

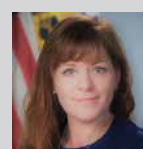
What Is a SIEM and Why Do You
Need One?



MARY FRANTZ
Chief Information Security Officer,
Prescriptive Health

MAY WEBINAR

The Confluence of Insider Threat
and Cybersecurity



REBECCA MORGAN
Deputy Assistant Director,
National Intelligence and Security Center

APRIL WEBINAR

Supply Chain Strategies –
A Call To Action



JOYCE CORELL
Assistant Director, National
Counterintelligence and Security Center

MARCH WEBINAR

Anatomy of Solarwinds and Implications For Supply Chain Security



CHRIS HALLENBECK
CISO, Americas at Tanium



SEAN S. COSTIGAN
Professor, George C. Marshall
European Center for Security Studies;
Director and Co-Founder, ITL Security



MARK RITCHIE
President, Global Minnesota;
Civilian Aide to the Secretary
of the Army

To get involved, contact:

For updated information and to register for upcoming webinars, visit
cybersecuritysummit.org/webinar-series

Eileen Manning, Executive Producer
Cyber Security Summit
612-308-1907

eileen.manning@cybersecuritysummit.org

You Can't Prevent an Attack. You Can Control the Chaos.

With Unisys Stealth®, your security will be identity-centric and Zero Trust.

Simple, seamless integration that scales to your evolving network infrastructure.

Lock down unauthorized access while hiding valued networks.

Stealth™ is designed to manage unexpected and unanticipated attacks of tomorrow.

Learn more at www.unisys.com/stealth

UNISYS | Securing Your Tomorrow®