



TENTH ANNUAL LEADERSHIP EVENT

# CYBER SECURITY SUMMIT

Security solutions through collaboration.™



# THE RIPPLE EFFECT

The Cascading Impacts  
of Cyber Security

October 26–28, 2020

[cybersecuritysummit.org](https://cybersecuritysummit.org)

#cybersummitMN

## FEATURED SPONSORS

Founding Partner



Presenting Sponsors



TC3 Cybersecurity Collaboration



THOMSON REUTERS

Platinum Sponsors

Corporate Patron



Printing Sponsor



Diamond Sponsors





## The Master's Degree for Security Technology Leaders

[tli.umn.edu](https://tli.umn.edu)

### Become a Security Leader & Shape Tomorrow's Future.

Acquire the skills needed to prevent, protect and respond to today's growing security demands with an **M.S. in Security Technologies (MSST)** from the University of Minnesota's Technological Leadership Institute (TLI). Today's unprecedented challenges have put immense pressure on virtual operations, making cybersecurity professionals in peak demand across all industries to help identify and mitigate risk, and to protect assets, data and our communities. Our proven curriculum and renowned faculty will provide you with the expertise to lead.

4M+

Unfilled Cyber Security  
Jobs Across the Globe

Source: ISC<sup>2</sup>

\$5T+

Estimated Cost  
of Cyber Crime in 2024

Source: Juniper Research

32%

Expected Job Growth  
Into 2028

Source: Bureau of Labor Statistics

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

<https://tli.umn.edu/admissions/information-sessions>

Contact an admissions representative at [MSST@umn.edu](mailto:MSST@umn.edu) for details.

## Thank You Sponsors + Exhibitors

Founding Partner



Presenting Sponsors



TC3 Cybersecurity Collaboration



Corporate Patron



Platinum Sponsors



Printing Sponsor



Ruby Sponsors



Healthcare & Med Device Host



In-house Legal Host



IT/OT/IoT Host



Small Business Host



Notebook Sponsor



Face Mask Sponsor



Silver Sponsors



Education Sponsor



Healthcare & Med Device  
Supporter



In-house Legal  
Supporter



IT/OT/IoT Supporters



Small Business Supporter



Supporters



### Maximize Your Exposure in 2021

The 2020 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 2021 today and receive a 10% discount through December 31, 2020. For more information, contact our sponsorship sales consultant:

Eileen Manning 612-308-1907 [eileen.manning@cybersecuritysummit.org](mailto:eileen.manning@cybersecuritysummit.org)





## Welcome to our Tenth Annual Cyber Security Summit

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

### Tim Crothers

2020 Co-Chair  
Cyber Security Summit

### Catharine Trebnick

2020 Co-Chair  
Cyber Security Summit

### Stefanie Horvath

2020 Program Co-Chair  
Cyber Security Summit

### Wade Van Guilder

2020 Program Co-Chair  
Cyber Security Summit

### Eileen Manning

Executive Producer  
Cyber Security Summit

Thank you for joining us for our tenth annual Summit. We're delighted to virtually host old friends and welcome new ones. It's been quite a year, with heavy challenges all around as we battle the global pandemic.

As an industry, we've done our best to counter the threat, with nearly all organizations sending their employees to work from home (WFH). The sudden shift has spurred a digital transformation that, as one study suggests, would normally have taken six years for many organizations. It is a monumental achievement, to be sure, but also a catalyst for startling new risks and attack vectors that we must now address together.

Fortunately, Summit content evolves as fast as the attack vectors that confront us. Our theme this year, "The Ripple Effect" is relevant across the entire attack surface, ranging from security misconfiguration risks to a security breach, where the attack can stem from one system and cause a series of disruptions across the ecosystem (i.e., suppliers, employees, consumers).

Each year, we bring you world-leading thought leaders to share their insights on the timeliest issues. We're thankful that so many luminaries invest their commitment to promote this Minnesota innovation hub. These leaders who serve in top posts in business, government and

academics graciously also help us recruit yet others to present emerging issues to you.

This tenth Summit considers all aspects of cybersecurity. New this year are 15 complimentary tech sessions and a half-day workshop, thanks to the support of TC3. We've also added two half-day seminars focusing on IoT and In-house Counsel to our Monday programming. And you won't want to miss our Women in Cyber Security program featuring the renowned Pillsbury Theater Company's dramatic leadership experience for diversity. Plus, we have several sessions tailored to Small Business, students, CISOs, legislators, international attendees and more.

In the main two-day Summit, we present dynamic Keynote Speakers and a power-packed line-up of other specialized speakers and panels. For example, on Tues, Oct. 27 join world-class experts and participate in real-time in an 'observed workshop' where a core of global supply chain and cyber security experts will play an interactive role in identifying supply chain vulnerabilities.

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

## Contents

- 01 Thank you Sponsors + Exhibitors
- 02 Welcome
- 03 Summit Highlights
- 04 Think Tank
- 05 Committees + Instructions to Navigate Through our Virtual Summit
- 06 Personal Note of Thanks
- 07 New in 2020 — Monthly Newsletter
- 12 Monday Tech Sessions + Workshop
- 16 Monday Session: WiCyS Minnesota / Women in Cyber Security
- 18 Monday Seminar: Healthcare & Med Device
- 20 Monday Seminar: IT/OT/IoT Convergence
- 22 Monday Seminar: In-house Legal Counsel
- 24 Tuesday Seminar: Small Business
- 26 Cyber Security Summit: 10 Years in Review
- 28 Full Summit Agenda
- 33 TLI — The Rapid Pace of IT Change Just Got Faster, Thank You COVID-19
- 36 Speaker Directory
- 42 Visionary Leadership Awards
- 43 CrowdStrike — Only the Transformational Will Survive
- 46 Sponsors + Exhibitors
- 55 Tanium — The Distributed Endpoint Crisis: A Blessing in Disguise
- 56 Index of Cyber Terminology + Acronyms
- 63 2020 Summit Recommended Reading
- 64 Cybereason's nocturnus researchers discover a new cyber threat against UK and European Union financial technology companies
- 65 New in 2020 — International Webinar Series

## Summit Highlights

### Continuing Professional Education Credits (CPEs)

Summit participation fulfills up to 26 hours of continuing education credits, depending on organization and sessions you participate in.

### Complimentary Technical Sessions and Workshop

Thanks to new support from The Twin Cities Cybersecurity Collaboration — 3M, Best Buy, Cargill, General Mills, Optum, Medtronic, Target, Thomson Reuters — the Monday Workshop and Technical Sessions are complimentary and more robust than ever.

### Expanded Cyber Women Agenda

After the tremendous success of last year's inaugural Women in Cyber Security event, we carry the momentum forward with a four-part program offering essential perspective on diversity, inclusion and team engagement. Join us on Monday for the Women in Cyber Networking Dialogue (11:30 – 12:30 pm) and Tech Sessions 1B, 2B, 3B!

### Inaugural Monday Seminars

Recognizing the need to build strategies and collaboration around new vulnerability fronts, this year we debut two additional Monday seminars: IT / OT / IoT Convergence (Noon – 3:00 PM) and Cybersecurity for In-House Legal Counsel (12:45 – 4:00 PM).

### Rockstars of Cybersecurity

Each year, the Summit brings you a cadre of world-renowned leaders whose insight and innovation drive our industry forward. This 10th Anniversary is no exception with a speaker lineup that boasts a bright array of cyber luminaries (see page 36-41).

### Dynamic International Programming

Starting on Tuesday at 10:45 AM, join us for a two-part International Breakout that takes on one of cybersecurity's most vexing challenges: How to secure the global supply chain. In Part Two (11:30 AM – 1:25 PM), watch in real-time as red teams, with over a dozen internationally renowned observers, zero in on supply chain vulnerabilities in a fascinating simulation.

### Post your comments about the Summit

[in /cyber-security-summit](#) [f /cssummit](#) [t /cs\\_summit](#)

Everyone who *follows* our Twitter, LinkedIn or Facebook page during the Summit will be entered to win a free VIP All-Access Pass to Cyber Security Summit 2021 (\$999 value). Post on all three with the hashtag **#cybersummitMN** to be entered three times! Drawing to be held on Wednesday at 5:00 p.m.



## SUMMIT CO-CHAIRS



**Tim Crothers**  
Target



**Catharine Trebnick**  
Colliers International



**Jill Allison**  
WiCyS MN; Shuriken



**Dr. Massoud Amin**  
University of Minnesota



**Anne Bader**  
The International  
Cybersecurity Dialogue



**John Bonhage**  
InfraGard



**Robert Booker**  
UnitedHealth Group



**Andrew Borene**  
Cybereason



**Christopher Buse**  
Old Republic



**Sean Costigan**  
George C. Marshall  
European Center



**Jennifer Czaplewski**  
Target



**Loren Dealy Mahler**  
Dealy Mahler Strategies



**Steen Fjalstad**  
Midwest Reliability  
Organization



**Mary Frantz**  
Enterprise Knowledge  
Partners, LLC



**Barb Fugate**  
United Bankers' Bank



**Christopher Gabbard**  
CISA



**Michelle Greeley**  
CWT



**Sam Grosby**  
Wells Fargo



**Judy Hatchett**  
Surescripts



**Stefanie Horvath**  
U.S. Cyber Command;  
MNIT



**Brian Isle**  
Technological  
Leadership Institute



**Mike Johnson**  
Technological  
Leadership Institute



**Mike Kearn**  
US Bank



**David La Belle**  
NorSec



**Michael Larson**  
EcoLab



**Eileen Manning**  
Cyber Security Summit



**Emily Marier**  
Slumberland Furniture



**Karl Mattson**  
PennyMac; LA Cyber  
Lab; U of M



**Tina Meeker**  
Sleep Number



**Allison Miller**  
Optum



**Jerrod Montoya**  
OATI



**David Notch**  
Medtronic



**Tom Patterson**  
Unisys Corporation



**Mark Ritchie**  
Global Minnesota; U.S.  
Army; State of Minnesota



**Frank Ross**  
General Mills



**Tony Sager**  
Center for Internet  
Security



**Phil Schenkenberg**  
Taft Law



**Melissa Seebeck**  
Delta Air Lines



**Tom Sheffield**  
Target



**Scott Singer**  
CyberNINES



**Chad Svihel**  
PCs for People



**Jeremy Swenson**  
USSA & Abstract  
Forward



**Rohit Tandon**  
State of Minnesota,  
MN.IT Services



**Wade Van Guilder**  
World Wide Technology



**Paul Veeneman**  
MBA Engineering



**Chris Veltsos**  
Dr. InfoSec



**Lee Ann Villella**  
FRSecure



**Kathy Washenberger**  
Deluxe



**Kristi Yauch**  
TCF Bank

## 2020 Committees

## GLOSSARY OF TERMS

David LaBelle, NorSec\*\*

## HEALTHCARE/MED DEVICE

Ken Hoyme, Boston Scientific\*\*; Judy Hatchett, Surescripts\*\*; Debra Bruemmer, Mayo Clinic; Sean Harrington, Abbott Medical; Eran Kahana, Maslon; Alex Kent, MedCrypt; Darrell Kesti, Ord; Matt Kirkwood, Smiths Medical; Vidya Murthy, MedCrypt; Mike Pinch, Security Risk Advisers; Pekka Vepsäläinen, Tikkasec

## IN-HOUSE LEGAL COUNSEL

Samuel Aintablian II, Minnesota Vikings Football, LLC; Madeleine Findley, Medtronic; Scot Ganow, Taft Stettinius and Hollister LLP; Susan Gelinske, The Opus Group; Brett Hebert, Taft Stettinius and Hollister LLP; Jerrod Montoya, OATI; Phil Schenkenberg\*\*, Taft Stettinius and Hollister LLP; Ken Stieers, The Opus Group

## INTERNATIONAL PROGRAM

Anne Bader, The International Cybersecurity Dialogue\*\*; Simon Bracey-Lane, The Cyber Security Summit; Sean Costigan, ITL Security; Michelle Greeley, Carlson Wagonlit Travel\*\*; Paul Hansen, Government of Canada; Brian Isle, Technological Leadership Institute; Mark Ritchie, Global Minnesota; Natascha Shawver, University of Minnesota; Mohammed Suleh-Yusuf, Nigerian Communications Commission; Chad Svihel, PCs for People; Pekka Vepsäläinen, Tikkasec Ltd.

## IOT

Tim Herman, Universal Network Solutions\*\*; Steve Burk, HGA Architects and Engineers; John Kunelius, Norwich University Applied Research Institute; Michael Larson, Ecolab; Srinu Mirmira, Blue Ridge Networks; Virgil Renz, Kudelski Security; Mangaya Sivagnanam, Trane Technologies; Paul Veeneman, MBA Engineering

## NEWSLETTER

Dr. Chris Veltsos, Dr. InfoSec; Loren Dealy Mahler, Dealy Mahler Strategies

## PROGRAM &amp; SPEAKER REVIEW

Scott Ammon, Insight; Jennifer Czaplewski, Target Corp.; Stefanie Horvath\*\*, Cyber Command, MN IT; Tim Crothers, Target Corp.; Brian Isle, Technological Leadership Institute; David Notch, Medtronic; Tom Sheffield, Target Corp.; Catharine Trebnick, Colliers; Wade Van Guilder\*\*, WWT

## RAPPOREURS

Sherwin Bothello Minnesota State University, Mankato, Info Sec MA; Simon Bracey-Lane\*\*, Institute for Statecraft; Alyssa Chetrick, New School, NYC, Global Studies; Alex Gilbertson; Tanner Manley, Georgetown Qatar, IR; Shelia Padre, Institute for Statecraft; Holly Sullivan

## SMALL BUSINESS

Jill Allison, Shuriken Cyber, Inc.; Lauren S. Beecham Henry, Bremer Bank; Joe Chow, Bremer Bank; Twila Kennedy, U.S. Small Business Administration; Elwin Loomis, Bremer Bank; Scott Singer, CyberNines; Lyle J. Wright, Minnesota Dept. of Employment & Economic Development

## VISIONARY LEADERSHIP AWARDS

Chris Buse\*\*, Old Republic; Eileen Manning, Cyber Security Summit

## WEBINARS

Sean Costigan\*\*, George C. Marshall European Center

## WOMEN IN CYBERSECURITY

Jill Allison, Shuriken Cyber, Inc.; Scott Ammon, Insight; Shelly Blackburn, Cisco; Gretchen Block, Optum Technology | UnitedHealth Group; Kris Boike, Federal Reserve; Betty Burke, General Mills; Jen Czaplewski, Target; Betty Elliott, Mercer; Sam Grosby, Wells Fargo; Judy Hatchett, SureScripts; Stefanie Horvath, Cyber Command; MNIT; Tina Meeker\*\*, Sleep Number; Allison Miller, Optum Technology; Milinda Ramble Stone, Provation Medical; Laurie Rupe, General Mills; Mercy Schroeder, Saviynt; Sherry Smith, Piper Sandler, Realogy Holdings Corp., Tuesday Morning, John Deere; Lee Ann Villella, FRSecure

## VIRTUAL INFRASTRUCTURE

Svetlana Bernstein; Adam Clarkson, Mattermost; Franco Fichtner, OPNsense; Matthew Harmon, Accenture; Elvind Horvik, Protocol 46; John Kisch; David La Belle, NorSec\*\*; Alex Malm, Metropolitan State University; Rob Stevens; Daniel Theisen, Comtech; Kayla Tycholiz; 1Password.com; Shawn Webb, HardenedBSD

\*\* denotes Chair/Co-Chair

If you'd like to join the collaboration and participate on a committee, please contact [Eileen.Manning@cybersecuritysummit.org](mailto:Eileen.Manning@cybersecuritysummit.org).

For instructions to navigate through our virtual Summit, please visit:

<https://welcome.cybersecuritysummit.org>



*Everything in Cybersecurity is interconnected. There are no isolated incidents. Like dropping a pebble into a pond, every action creates a series of follow-on effects. This is the "Ripple Effect" we must constantly manage to stay ahead of threats."*

Tim Crothers, Co-Chair,  
2020 Cyber Security Summit





## A Personal Note of Thanks

What a year! Amid a global pandemic, the amazing cyber warriors that make up the Think Tank came together to lend their expertise and insights while dedicating more hours than this challenging field has ever demanded. The selfless work of these 50+ individuals representing all 16 critical infrastructures — is also a reflection of the broader cyber community working tirelessly to keep our world safe.

These consummate professionals have responded rapidly to secure the expanded attack surface, leading teams working in isolation and thwarting threat actors seeking to exploit a strange economic environment. We have seen them grapple with new work-from-home vulnerabilities, rising ransomware attacks on our healthcare and emergency systems, and physical security threats amid civil unrest in our nation.

All of these factors combine to emphasize the value of collaboration as a community and sharing information with peers and colleagues across organizations globally, which is the heart of the Cyber Security Summit's mission when it was envisioned and created ten years ago. Bringing this mission to greater fruition, this year we launched the monthly Cyber Security Summit newsletter — an insightful medium where we feature thought leadership pieces from a vanguard of experts, including members of the Think Tank. Each edition is thematic with a different area of focus, such as healthcare, election security, leadership and the future of cybersecurity.

I also wish to acknowledge the exceptional work behind our new monthly International webinar series. Led by Sean Costigan and free to attend, each hour-long webinar examines one vexing challenge facing the international community and offers insight, knowledge and perspective from multinational business leaders and government officials. Since its launch in July, the response has been tremendous! We've seen participants logging in from 15 countries, including Nigeria, Ireland, Brazil, India and Finland, just to name a few.

Of course, each year thousands of hours go into producing this event, with amazing leaders stepping up to guide its vision. The 2020 vision was led by Tim Crothers and Catharine Trebnick who

made a spectacular repeat performance as Co-Chairs. Of course, the Summit could not happen without the support and vision of the Think Tank, the dozens of people who work on committees, and the 100+ speakers and panelists who give of their time to share their experience and alert you to what is coming at us. These individuals are highlighted throughout the guide — please connect and thank them for their contributions!

A special thanks also goes out to the TC3 Cyber Security Collaboration and Nicole McKoin for helping to underwrite Monday Tech Sessions which makes it possible to provide over 15 complimentary training sessions.

We have so many sponsors that have stepped up in this very challenging year to make this Summit possible. Please drop into our Virtual Trade Show to connect with them and learn about their solutions to your security challenges. These sponsors were hand-picked for the quality products they offer.

While we were forced to postpone the huge celebration planned for our 10th Anniversary, it is my hope that October 25-27, 2021 has us back together in person to celebrate an even more important milestone: surviving a pandemic! In the meantime, don't let yourself become isolated; set-up virtual networking calls or call me and I will help you connect. I am actually listing my phone number and email below, so please reach out.

Our world is a safer place thanks to all of you cyber warriors, my heartfelt thanks for all you do to keep us safe and our data secure. Never before have we felt such **"A Ripple Effect"** — a theme selected before COVID hit!

*Eileen Manning*

Eileen Manning, Executive Producer  
Cyber Security Summit  
[eileen.manning@cybersecuritysummit.org](mailto:eileen.manning@cybersecuritysummit.org)  
612-308-1907

## New in 2020

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

Welcome to the 2020 Cyber Security Summit!

The collaboration and community you experience this week can continue throughout the year with the introduction of our new 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 the future of cybersecurity, election year security, cyber leadership, women in cyber, and healthcare and medical device security. You'll also be able to view the archive of previous newsletters soon.

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 [events.bizzabo.com/220749/page/1481018/subscribe-to-our-newsletter](https://events.bizzabo.com/220749/page/1481018/subscribe-to-our-newsletter).

Thank you, and see you in 2021!

**Sign Up Today!**

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, Incorporated

Graphic Design:

**HEIDI BRANES**

Graphic Designer, The Event Group, Incorporated

**Cyber Security Summit**

OCT. 26-28, 2020 | MINNEAPOLIS, MN | [CYBERSECURITYSUMMIT.ORG](http://CYBERSECURITYSUMMIT.ORG) | [#CYBERSUMMITMN](https://twitter.com/CYBERSUMMITMN)

**Cybersecurity Newsletter**

JULY 2020

Security Solutions Through Collaboration

WICyS (Women in Cybersecurity) 2019 conference attendees unite in Pittsburgh, PA.

**Highlight**

To counter cybersecurity's complex and evolving threat landscape, we need talented individuals from all backgrounds. Over the last decade we've made great strides to elevate a new array of perspectives, and as *Time Maker* (Sleep Number) reveals to us, 2019 was a banner year for cyber women in Minnesota!

**CyberBytes™**

**MEASURING SUCCESS BEYOND 'ON PAPER' ACHIEVEMENTS**  
When we evaluate an individual's record of accomplishment, we often look to certificates, lengthy resumes, and tours with well-known companies. But checking all the right boxes often belies true success, writes Loren Dealy Mahler (Dealy Mahler Strategies). Loren proposes a more comprehensive evaluation framework where more intangible characteristics like communication, collaboration and flexibility are also part of the equation.

**KEEPING TEAMS ENGAGED IN REMOTE WORK ENVIRONMENTS**  
Betty Elliot (Mercer) understands the toll COVID-19 has taken on her employees and the need to come together as a team. Drawing from the activities she has instituted including regular Zoom check-ins, virtual happy hours and Pokeno games, Betty has developed five takeaways for boosting morale and well-being.

**FROM NEW TO NEXT NORMAL**  
Shelly Blackburn (Global Security Systems Engineering) believes that while our pre-COVID lifestyles and behaviors may never fully return, cybersecurity challenges haven't missed a beat. To keep our teams engaged in the fight, Shelly recommends putting into routine a series of practices ranging from meaningful remote connections to training to self-care.

**In Case You Missed It**

- 9 Strategies for Retaining Women in Cybersecurity and STEM in 2020 | SecurityIntelligence
- How to do thoughtful work when you just can't focus | Fast Company
- Finding Work-Life Balance When Working From Home | Forbes
- Separating Work from Life: 3 Habits for Remote Workers | The Muse
- What Working From Home Can Teach Us About Leadership | Inc.

**Think Tank Perspective**

**Allison Miller**  
Chief Information Security Officer Optum  
» Bio

Globally, we are in a revolution. A revolution that is changing the way we work, the way we think and the way we live our lives. Technology is the center of this revolution and it will take all of us to learn and make this transformation. Empowering women and girls across our nation, and across the world, is the key to creating the change needed to succeed. Optum, in partnership with industry leaders like Women in Cybersecurity and Cyber Security Summit, is leaning in to this transformation with everything we've got. Diversity, Inclusion and Equity are the keys to success, and we will not stop until they exist for everyone.

**Jill Allison**  
Chair, Board of Directors, WICyS, MN Affiliate  
» Bio

Minnesota's thriving cybersecurity community is built on the strength of our people. The experience, expertise and diversity of thought found here have positioned Minnesota as a national leader, and this year we launched the Minnesota chapter of WICyS (Women in Cyber Security) to further strengthen our community by increasing engagement, encouragement and support for women in our industry. Inspired by the dialogue that began at last year's inaugural Women in Cyber program hosted by the Cyber Security Summit, we are excited to help WICyS-MN grow and develop the next generation of cybersecurity leaders to protect Minnesota and our nation from the next generation of cyber threats.

**Sponsor Spotlight**

**Insight** | Cloud + Data Center Transformation

[www.insight.com](http://www.insight.com)

Insight's Cloud + Data Center Transformation is a complete IT services and solution provider that helps organizations transform technology, operations, and service delivery to meet challenges and future-proof the business. As a client-focused integrator, we're free to recommend the most appropriate solutions — across cloud, IT transformation, next-generation technology, and security. Discover how Insight can help solve your biggest IT challenges.

**Partner Spotlight**

**WICyS**

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

**ISSA**

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. We accomplish this by providing educational forums, publications, and peer interaction opportunities to enhance knowledge





# END CYBER ATTACKS

FROM ENDPOINTS TO EVERYWHERE



cybereason

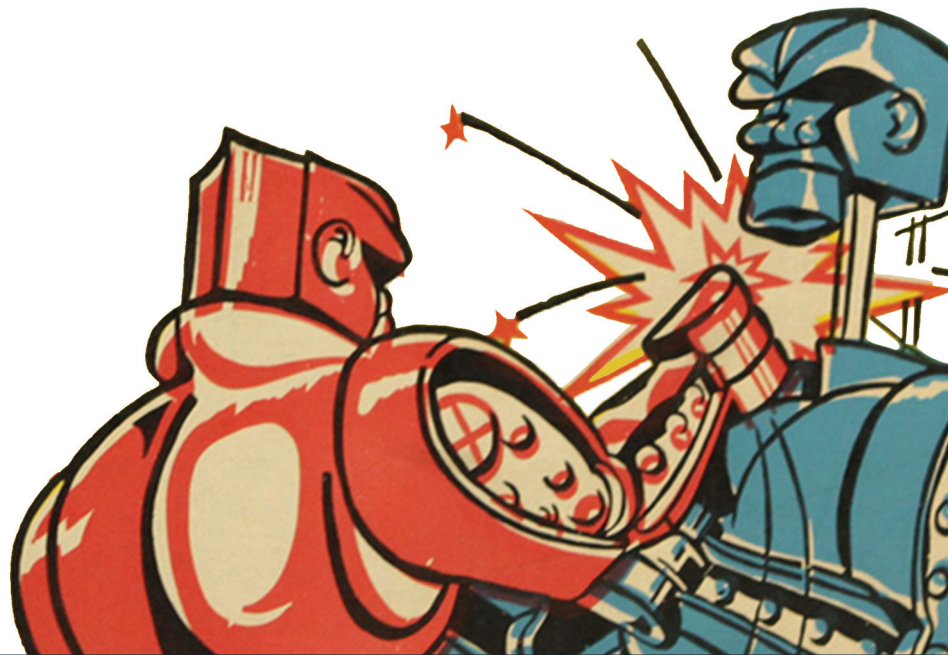


Purple Teams testing is the best way to bring focus to improving cyber defenses. SRA's approach prioritizes MITRE ATT&CK tactics & techniques and Adversary Simulations for your industry, and establishes a process with defined Defense Success Metrics.

SRA is an industry leader in purple team thought leadership and testing, with our contribution embodied by our free VECTR™ platform and taught in several SANS classes.

**SRA.io**

**SecurityRisk**  
ADVISORS



**NETSPI™**

## NetSPI Services

- |   |   |
|---|---|
|  <b>APPLICATION PENTESTING</b> <ul style="list-style-type: none"><li>• Web Application</li><li>• Mobile Application</li><li>• Thick Application</li></ul>   |  <b>STRATEGIC ADVISORY</b> <ul style="list-style-type: none"><li>• AppSec Benchmarking</li><li>• AppSec Roadmap</li><li>• AppSec Metrics</li></ul>                             |
|  <b>CLOUD PENTESTING</b> <ul style="list-style-type: none"><li>• Microsoft Azure</li><li>• Amazon Web Services (AWS)</li><li>• Google Cloud (GCP)</li></ul>   |  <b>ADVERSARIAL SIMULATION</b> <ul style="list-style-type: none"><li>• Detective Control Testing</li><li>• Red Team Security Operations</li><li>• Social Engineering</li></ul> |
|  <b>NETWORK PENTESTING</b> <ul style="list-style-type: none"><li>• Internal &amp; External Network</li><li>• Mainframe Infrastructure</li><li>• Wireless Network</li><li>• Host-Based &amp; Virtual Desktop</li></ul> |  <b>SECURE CODE REVIEW</b> <ul style="list-style-type: none"><li>• SAST &amp; SCR</li><li>• SAST Triaging</li><li>• Remediation Training</li></ul>                             |

## Penetration Testing as a Service

Clients love NetSPI's Penetration Testing as a Service (PTaaS) for the simplicity of scoping new engagements, viewing their testing results in real-time, orchestrating remediation, and the ability to perform always-on continuous testing. NetSPI finds vulnerabilities that others miss and delivers clear, actionable guidance, allowing customers to find, track, and fix their vulnerabilities faster.

**paloalto** NETWORKS | **IGNITE20**

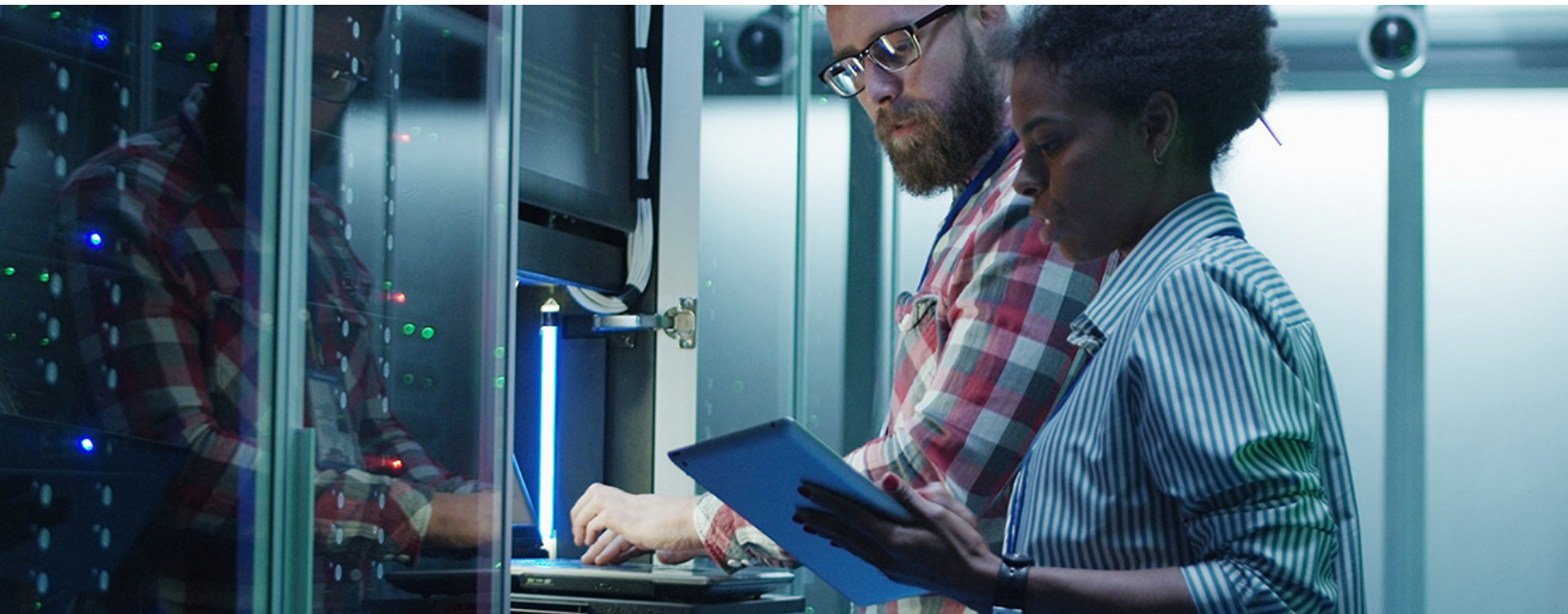
## Secure Today, for a Better Tomorrow

The world's first digital cybersecurity conference dedicated to future-proofing your cybersecurity—from the cloud, to the enterprise, to the edge.

Start securing your tomorrow, today  
Register now at [ignite.paloaltonetworks.com](https://ignite.paloaltonetworks.com)







# Technical Sessions

**Monday, October 26 | 9:30 AM-3:30 PM**

The Monday Technical Sessions are broken down into 15 different sessions from 9:30 a.m. – 3:30 p.m. Each session has a different topic led by a top leader in the field to teach on a specific training item in cybersecurity. Select 5 of 15 sessions to attend.

## TECH SESSION ONE / 9:30–10:20 AM

### TECH SESSION 1A

#### Active Vulnerability Management

Traditional Vulnerability Management programs are incapable of efficiently preventing incidents. Hundreds of thousands of public vulnerabilities, innumerable assets, proliferating vulnerability scan findings, and complex environments can overwhelm Vulnerability Management and IT teams. What is the solution? A threat-based, automated, Active Vulnerability Management program optimized to prevent incidents. This session will discuss implementing and operating an effective Vulnerability Management program with well-defined processes, information sharing, and automation..

*Travis Christian, Lead Info Security Analyst, Target Corporation*

### TECH SESSION 1B

#### Part One - Pillsbury Theater Group presents "Breaking Ice"

"A 50-minute performance exploring how systemic inequities, implicit bias and common misperceptions show up in relationships, creating uncomfortable interactions that inhibit innovation, motivation and productivity in the workplace. With virtual content customized for the 2020 Cyber Security Summit, including real-life examples, this innovative event addresses unconscious bias and learning how to be comfortable with uncomfortable discussions on diversity and inclusion.

- Increased awareness of unconscious bias – what it is, how it shows up in behavior, how it affects people
- Increased appetite for learning around Diversity, Equity and Inclusion – motivation to make it a regular practice
- Understanding of personal accountability for creating inclusive environments – it takes everyone
- Greater comfort with being uncomfortable "

*Mercy Schroeder, Director of Sales, Saviynt*

### TECH SESSION 1C

#### Getting Started on Application Security

In order for an organization to have a successful Application Security Program, there needs to be a centralized governing Application Security team that's responsible for Application Security efforts. In practice, we hear many reasons why organizations struggle with application security, and here are four of the most common myths that need to be dispelled:

1. An Application Security Team is Optional
2. My Organization is Too Small to Have an Application Security Team
3. I Cannot Have an Application Security Team Because We Are a DevOps/ Agile/Special Snowflake Shop
4. An Application Security Team will Hinder Our Ability to Deliver/ Conduct Business

This session will cover taking a strategic approach to application security.

*Nabil Hannan, Managing Director, NetSPI*

## TECH SESSION TWO / 10:30–11:20 AM

### TECH SESSION 2A

#### Not All Threats are External

Studies have indicated that employees caused breaches are rising and can cause devastating damage from the insider as they have legitimate access to your systems and data. Target has developed a new technical approach for detecting, responding and provide quantifiable risk-based visibility into insider threat by leveraging a technical response process to combat this threat. During this session Target's Insider Threat leaders will discuss how they built a technical Insider threat program while leveraging the skills of Incident Response and Insider Threat analysts, as well as the lessons they learned along the way.

*Adam Blake, Principal Engineer, Cyber Security Insider Threat Team, Target Corporation; Jena Hover, Senior Manager, Cyber Security Incident Response Team, Target Corporation*

### TECH SESSION 2B

#### Part Two - Pillsbury Theater Group "Breaking Ice" Event - Dialogue and interactive activity (we all play a part in the solution!)

"Following the ""Breaking Ice"" video performance (Session 1B), trained Breaking Ice facilitators guide participants through discussion and interaction to deepen awareness and cultivate accountability and action.

As a result of participating in the Breaking Ice sessions, participants will be able to:

- Describe insights the Breaking Ice video performance sparked
- Define unconscious bias, micro-aggressions and privilege and cite examples of what they look like in behavior
- Identify a part of the performance that they empathize with
- Identify and commit to one action that they can take to help foster increased inclusivity in their work environment"

### TECH SESSION 2C

#### Application Security Automation in Development

Empowering development teams to deliver at project speed without security getting in the way through automation of security requirements, integrating security by design, partnering with development teams and incorporate security into modern development processes.

*Kori Prins, Technical User Support Analyst, Medtronic; Maria Brown, Sr. Principal Cloud and Application Security Engineer, Medtronic; Chris Perkins, Sr Prin Cybersecurity Specialist, Medtronic; Mike Kennedy, CISSP, Sr. Manager - Global Security Office, Medtronic*

## TECH SESSION THREE / 12:30–1:20 PM

### TECH SESSION 3A

#### Modernizing Security Software Engineering To Secure By Default

With an ever-accelerating software products and hence number of vulnerabilities, our Cyber Security professionals can no longer rely on traditional procedure driven security controls or siloed vendor solutions. They need solutions that integrate functionalities and data from disparate systems, and make the intelligence available to them faster. The modern Software Engineering technologies and practices can be used to meet this demand in-house. This presentation will walk through our experiences in building a highly skilled software engineering team, adopting engineering practice, and delivering security solutions to secure by default the services within Target.

*Joana Cruz, Director of Engineering, Target Corporation; Rudra Panda, Sr. Engineering Manager, Target Corporation*

### TECH SESSION 3B

#### Leading High Performing Teams During a Global Pandemic

Innovative cyber leaders share proven methods and practices of maintaining a high level of engagement, retention, collaboration, and genuine connections during this time of sustained remote work.

*Moderator: Tina Meeker, VP, WiCys Minnesota; Sr. Director, Information Security, Sleep Number*

*Panelists: Betty Elliott, Chief Information Security Officer, Mercer; Milinda Rambel Stone, Chief Information Security Officer, Provation Medical; Sam Grosby, Principal Enterprise Information Security Engineer, Wells Fargo*

### TECH SESSION 3C

#### Are you finding your cloud a little too foggy?

During this innovated session we will deep dive into Cloud Security Posture Management to provide the visibility your organization needs to secure your cloud infrastructure with confidence.

*Christopher Williams, Regional Cloud Architect, Check Point Software Technologies, Ltd.*

## TECH SESSION FOUR / 1:30–2:20 PM

### TECH SESSION 4A

#### Improving Threat Detection with a Detection-Development Life Cycle

Organizations deploy multiple security monitoring tools to detect threats, but they often overlook the most important part of the threat detection process: content. This session describes the role of detection content in security monitoring, and how to optimize it to your advantage with a Detection-Development Life Cycle.

*Augusto Barros, VP of Solutions, Securonix*

### TECH SESSION 4B

#### A Bug Hunters Guide to GCP

Google Cloud Platform (GCP) is an eclectic offering of products ranging from IaaS to PaaS and Identity Services. Knowing where to look for flaws on the platform is an art that requires an understanding of the rules of the road. In this talk you'll hear an overview of what constitutes privilege in GCP and how movement between accounts can occur to obtain privilege. Armed with the knowledge of what an attacker's goal would be, and the mechanisms to get there, we can describe a methodology for documenting escalation paths. There might be a base set of rules on the GCP highway but there are many known and yet to be discovered detours!

*Kat Traxler, Security Professional, Best Buy*

### TECH SESSION 4C

#### Session 4C - Purple Teams Best Practices, Metrics and Freeware

This talk will discuss the objectives, guidance and benefits of starting a purple teams program NOW. Purple teams using the free VECTR.io platform helps to prioritize detection content development, validates MITRE ATT&CK coverage, produces meaningful metrics and can help you realign your cybersecurity program to take a threat-driven approach.

*Tim Wainwright, Chief Executive Officer, Security Risk Advisors*

## TECH SESSION FIVE / 2:30–3:20 PM

### TECH SESSION 5A

#### Tailor Your Cyber Threat Intel Program and Optimize Resources

As the sophistication and capabilities of cyber threat actors increase, so does the need for Cyber Threat Intelligence (CTI). However, most organizations do not have the resources for a large CTI team. Organizations can offset this disparity by optimizing resources and focusing on what really matters. Even one CTI analyst can make a significant difference for an organization by identifying relevant assets, aligning those assets to potential threats, and then working with cyber security components to prioritize detection and mitigation efforts. Walk through the process of how to build priority intelligence requirements, learn how to find force multipliers, tailor deliverables, and manage expectations with a CTI team of one. This session is beneficial for CTI practitioners at any level, but optimal for those interested in starting a CTI program or for those building CTI capabilities with limited resources.

*Christa Girtz, Global Security | Manager, Threat Intelligence, General Mills*

### TECH SESSION 5B

#### How Data Classification Tools can Spark Conversation and Drive Change at your Company

At 3M we use Microsoft Azure Information Protection to protect Export Control & Trade Secret documents. In this session we will look at how data classification tools can be used to assist with protecting documents while also spark discussion and changes around legal, R&D and manufacturing processes.

*Charles Collins, Data Loss Prevention Analyst, 3M*





## Technical Sessions (continued)

### TECH SESSION 5C

#### Building an Effective Cyber Security Engineering Organization

As Information Technology delivery models continue to rapidly evolve, Cyber Security organizations need to adapt their operating models to meet the needs of this changing landscape. Building a robust and effective Cyber Security Engineering team, organized around a set of fundamental principles is paramount to meeting these needs and the challenges facing organizations today. Engaging in this activity will enhance your security program, enable your organization to move with agility through uncertain conditions and enable capabilities necessary to advance your cyber security strategies. In this talk, I will cover some of the techniques and strategies we've employed during our journey building a Cyber Security engineering team at General Mills, including some of the challenges we faced along the way. I will also share some outcomes that you can expect to achieve as a result of engaging in this fruitful endeavor.

*Frank Ross, Sr. Manager, Cyber Security Engineering & Operations, General Mills*

## Tech Workshop

Monday, October 26 | 9:00 AM- 12:00 PM


### Identifying and Analyzing Adversary Infrastructure and Malware

Adversaries try as much as possible to blend in with behavior that appears normal. However, their operations result in malicious activity, and therefore must at some point deviate from what is "normal" and develop specific patterns which can be identified over time. This training will teach the audience how to analyze adversary infrastructure used for command and control and delivery, focused on attribution and correlation. The goal of the training is that the audience will be able to identify adversary infrastructure, and find related activity based on their own research.

*Michael Schwartz, Dir. of Threat Intelligence and Detection Engineering, Target Corporation;*  
*Derek Thomas, Sr. Information Security Analyst, Target Corporation*



Thanks to our TC3 cybersecurity collaborators, this year's Tech Monday agenda is complimentary and more robust than ever.

 **3:30-5:00 PM** Join us to explore resources from our solution strategy providers and establish new professional relationships during the **Virtual EXPO Hall Opening**.

## 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](http://www.unisys.com/stealth)

**UNISYS** | Securing Your Tomorrow®





## WiCyS Minnesota | Women in Cyber Security

### Monday, October 26 | Diversity, Inclusion & Leading High Performing Teams in the Cyber Workforce

To counter cybersecurity's complex and evolving threat landscape, we need talented individuals from all backgrounds. This year at the Summit, after the tremendous success of last year's inaugural Women in Cyber Security event, 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, each of these four sessions is complimentary to attend!

### Agenda

#### 9:30-10:20 AM

**Part One -Pillsbury House Theatre presents "Breaking Ice"**  
(Tech Session 1B)

*Mercy Schroeder, Sales Director, Saviynt, Inc.*

#### 10:30-11:20

**Part Two - Interactive Activity (we all play a part!)**

**About "Breaking Ice" - Interactive Diversity Theatre performed by Pillsbury House Theatre**

"Breaking Ice" is an award-winning program of Pillsbury House Theatre that for over 20 years has been opening up a dialogue about diversity, equity, and inclusion in the workplace. A diverse company of professional actors portrays real-life situations that explore how systemic inequities, implicit bias, and common misperceptions show up in relationships, creating friction that inhibits innovation and productivity in the workplace.

#### 11:30 AM-12:30 PM

##### Women in Cyber Security Dialogue

*Moderator: Allison Miller, Optum, Panelists: Jill Allison, WiCyS MN, Shelly Blackburn, CISCO, Gretchen Block, Optum, Janell Straach, WiCyS*

#### 12:30 -1:20 PM

##### Leading High-Performing, Diverse Teams During a Global Pandemic

*Moderator: Tina Meeker, Sr. Director, Sleep Number | VP, WiCyS Minnesota; Panelists: Betty Elliott, CISO of Mercer, Milinda Rambel Stone CISO of Provation Medical, Sam Grobsy, Principal Security Engineer of Wells Fargo*

Join these cyber leaders as they share proven methods and best practices for maintaining a high level of engagement, retention, collaboration, and fostering authentic connections during this time of sustained remote work.



**3:30-5:00 PM** Join us to explore resources from our solution strategy providers and establish new professional relationships during the **Virtual EXPO Hall Opening**.

#### Sponsors



Did you know that Minnesota has a newly formed Chapter of WiCyS?

#### What is the WiCyS National Organization?

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.

#### What has WiCyS Minnesota been up to in its first year?

Our first year has been an active one! WiCyS MN formed up a strategic alliance with the Cyber Security Summit, formed up its inaugural board, and hosted a highly attended WiCyS Golf & Networking Event at White Bear Yacht & Golf Club in Sept 2020.

#### 2020-21 Board Members:

*President* | Jill Allison, CISO Advisor & Founder - Shuriken Cyber

*Vice President* | Tina Meeker, Sr. Director of Information Security - Sleep Number

*Secretary* | Judy Hatchett, CISO - Surescripts

*Board Member* | Kris Boike, Sr. Manager - GRC & IAM Toppan Merrill

*Board Member* | Sherry Smith, Corporate Board Member - Piper Sandler, John Deere, Tuesday Morning, and Realogy Holdings Corp.

*Ally* | Harold Palmer, Strategic Accounts, Onfido

*Ally* | Scott Ammon, Cybersecurity Principal, Insight

#### What does WiCYS have planned for 2020-2021?

WiCYS will offer unique and meaningful events throughout the year. Planned events include a FREE Threat Hunting training course sponsored by RSA (early 2021), a WiCyS Golf Clinic (spring 2021), and the Second Annual Golf & Networking Event (summer 2021)

#### Want to join, become an ally, lead a committee, or become a sponsor?

Visit [www.wicysmn.org](http://www.wicysmn.org) today! Find us on LinkedIn to stay in the know about 2021 events.



# ACCELERATE DIGITAL TRANSFORMATION WITH INTELLIGENT IDENTITY

Deliver Frictionless Access Without Compromising Security on a Flexible and Integrated Identity Platform

[saviynt.com](http://saviynt.com)





## Cyber Security for Healthcare & Med Device

**Monday, October 26 | 12:00–4:00 PM**

The Cyber Security Healthcare and Med Device half-day seminar brings healthcare providers and medical device manufacturers together with security experts and others to advance medical device safety and security. Participants include healthcare delivery organizations, device-makers, regulatory agencies, risk managers, insurers, security experts and more. **Moderated by Ken Hoyme of Boston Scientific and Judy Hatchett of Surescripts**

### Agenda

**12:00–12:30 PM**

**Prioritizing Security Efforts—How to Get Out of Fire Drill Mode**  
Seth Carmody, Vice President of Regulatory Strategy, MedCrypt

**12:30–1:00 PM**

**Securing Telemedicine in a Post-Covid World**  
Steve Caimi, Cybersecurity Specialist, Cisco Systems

**1:00–1:30 PM**

**Vulnerabilities Around Patient Monitoring Systems (GE Carescape)**  
Dave Harvey, Manager of IT Security GRC and Interim IT Security IR Manager, Fairview Health Services

**1:30–2:00 PM**

**Towards a Workable Threat Modeling Approach**  
Arnab Ray, Principal Cybersecurity Systems Engineer, Abbott

**2:00–2:30 PM**

**FDA/MDIC/MITRE Threat Modeling Bootcamps and Playbook**

Steve Christey Coley, Principal Cybersecurity Engineer, The MITRE Corporation; Jithesh Veetil, Program Director (Data Science & Technology), Medical Device Innovation Consortium (MDIC)

**2:30–3:00 PM**

**How to Understand and Use Medical Device Utilization Information for Decision Making**

Darrell Kesti, Regional Sales Manager, Ordr Inc.

**3:00–3:30 PM**

**Things to Think About When Preparing a Product Submission for Regulatory Review**

Nimi Ochoji, Director, Product Security, Medtronic

**3:30–4:00 PM**

**Must-Have Contract Security Language (and a COVID-19 Perspective)**

Eran Kahana, Attorney, Maslon LLP



**4:00–5:00 PM** Following the seminar, explore resources from our solution strategy providers and establish new professional relationships during the **Virtual EXPO Hall Opening**.

Host  
**MASLON**

Supporters

**medcrypt**

**ordr**  
take control

**H-ISAC**  
HEALTH - ISAC

**MDMA**  
MEDICAL DEVICE MANUFACTURERS ASSOCIATION

**MEDICAL ALLEY**  
ASSOCIATION



DO YOU KNOW WHAT  
**EVERY DEVICE**  
ON YOUR NETWORK IS DOING AND  
IF THEY'RE BEHAVING PROPERLY?

Address shadow IoT in minutes.

Discover all IoT devices, profile behavior and risks and automate action with Ordr.

Sign up for IoT Discovery Program at [www.ordr.net/sensor](http://www.ordr.net/sensor)

## Secure your everything

Cyber security that protects today's digitally transformed world.

A unified architecture that prevents fifth generation cyber attacks.

Anywhere, any time, on any device or cloud.

[secure.checkpoint.com](http://secure.checkpoint.com)

**Check Point**  
SOFTWARE TECHNOLOGIES





# Cyber Security for IT/OT/IoT Convergence

**Monday, October 26 | 12:00–3:00 PM**

The Internet of Perilous Things: Converging IT, OT and IoT and What You Need to Know

The IT/OT/IoT Convergence Seminar will showcase thought leaders, strategies, opportunities, and use and business cases of implementing Industrial Internet of Things (IIoT) security solutions across this 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 IIoT/IIoT/ICS/SCADA, to create insights into new technologies and best practices of securing smart, connected operations and facilities, and to progress necessary cybersecurity function.

## Agenda

**12:00–12:30 PM**

**IT/OT Convergence, A Digitalization & Cybersecurity Ripple Effects**

*Virgil Renz, Practice Leader–IoT & OT Security Services, Kudelski Security; Mangaya Sivagnanam, Principal Cybersecurity Architect, Trane Technologies*

**12:30–1:00 PM**

**Landscape IoT Risk Threats across the National Critical Functions (NCFs)**

*Tom Muehleisen, Dir. of Cyber Operations, Norwich University Applied Research Institutes (NUARI); Phil Susmann, Pres., Norwich University Applied Research Institutes (NUARI)*

**1:00–1:30 PM**

**Securing IoT and OT Devices in Manufacturing—Your State of Security**

*Eric Nelson, Systems Engineer, Ordr*

**1:30–2:00 PM**

**Cyber Security Supply Chain of Events**

*Paul Veeneman, VP–Operations, MBA Engineering*

**2:00–2:30 PM**

**Implications of Data Security for Connected Devices**

*Eric Johansen, Regional Sales Engineer, Nozomi Networks; John Bloomer, Director of Engineering, Check Point Software Technologies*

**2:30–3:00 PM**

**IT / OT / IOT – Cyber Defense and Best Practices**

*Mark Webber, Vice President–Sales, Blue Ridge Networks*



**3:30–5:00 PM** Following the seminar, explore resources from our solution strategy providers and establish new professional relationships during the **Virtual EXPO Hall Opening**.

Host



Supporters



**Insight** | Cloud + Data Center Transformation

# No better protection

You've got point solutions. You have a security team and protocols. But is your business fully secure?

As a security services partner with a holistic approach, thousands of certifications, and a broad portfolio, we help you modernize your security environment and systematically reduce risk.

- + Cloud-to-edge strategies
- + Governance, risk, and compliance
- + Identity and access management
- + Incident preparedness and response
- + Managed Security services
- + Virtual CISO program

Whether you need specific gaps addressed or have ongoing security needs — we're here to help you realize the best possible protection for your business.

Learn more at [insightCDCT.com/security](https://insightCDCT.com/security)





## Cyber Security for In-house Legal Counsel

**Monday, October 26 | 12:45–4:00 PM**

In-house legal counsel play an important role in managing and mitigating an organization's cyber risk. Cybersecurity is complicated and important, and most in-house counsel are asked to learn it on the fly. This seminar was created to help in-house counsel understand the legal constructs and terminology widely used within the cybersecurity space, and to provide practical ways they can be more responsive and efficient when cyber issues arise. This discussion will also be valuable to outside counsel in the technology space, and privacy officers looking to better understand how legal risk and cyber risk can be managed together. You will walk away better prepared to understand and manage cyber risk.

### Agenda

**12:45–1:30 PM**

#### Speaking the Language of IT and Security

*Shawn Fleury, Director, Risk Management, The Crypsis Group; Scot Ganow, Chair Privacy & Data Security Practice, Taft Stettinius & Hollister LLP*

**1:30–2:15 PM**

#### Legal Overview and Key Cyber Risks for Businesses

*Scot Ganow, Chair Privacy & Data Security Practice, Taft Stettinius & Hollister LLP*

**2:15–3:00 PM**

#### Panel Discussion: Governance and Working Relationship Considerations in Privacy and Data Security

*Moderator: Madeleine Findley, US Privacy Counsel, Medtronic; Panelists: Aditya C. Bharadwaj, General Counsel, Ascentis Human Capital Management Software; Jerrod Montoya, Deputy Chief Information Security Officer/ Project Manager, OATI; Milinda Rambel Stone, Chief Information Security Officer, Provation Medical*

**3:00–3:30 PM**

#### Best Practices for Managing Cyber Risks in the Contracting Process

*Brett Hebert, Associate, Business Law & Data Security, Taft Stettinius and Hollister LLP; Maggie Lassack, Privacy and Cyber Security Counsel at Polaris Industries*

**3:30–4:00 PM**

#### Crisis Management Considerations

*Loren Dealy Mahler, President, Dealy Mahler Strategies; Phil Schenkenberg, CIPP/US, Partner, Litigation & Cyber Security, Taft Stettinius and Hollister LLP*



**4:00–5:00 PM** Following the seminar, explore resources from our solution strategy providers and establish new professional relationships during the **Virtual EXPO Hall Opening**.

**CLE Credits:** The sponsor, Taft, will apply for 3.25 hours of CLE credits in Minnesota, Wisconsin, Iowa, and Ohio. Attendees seeking CLE credit must attend the full session and log in using the webinar platform to receive credit.

# ENTERPRISE ACCESS

**Your all-access pass to the latest news for the whole team.**

Work never stops. Give your team the resources they need to succeed with an Enterprise Access pass to Minnesota Lawyer.

Everyone gets their own digital access to stay on top of the latest trends and better understand the current marketplace. Enterprise Access includes everything below and more.

- **EXCLUSIVE NEWS & RESOURCES** - Unlock exclusive, in-depth articles for your entire team with 24/7 access to news relative to your industry.
- **DAILY EMAIL ALERTS** - Get daily email updates with the latest local news, industry changes, and resources for your organization.
- **SEARCHABLE ARCHIVES** - Explore years of archives to research current and future opportunities, find past focus sections, resource guides and more.

To see how Enterprise Access can help your business, visit <http://bit.ly/ENT-ACCESS>. You can also contact Shaun Witt at [switt@bridgetowermedia.com](mailto:switt@bridgetowermedia.com) or 405-278-2808.



Host

**Taft**

Supporters

**CRYPSIS** MINNESOTA LAWYER





## Cyber Security for Small Business

**Tuesday, October 27 | 1:30–4:30 PM**

While hackers target small businesses as low-hanging fruit, shrewd business owners know there are resources and strategies they can leverage to protect their assets. Complacency is never an option – why put your reputation, intellectual property and financial well-being at risk?

Join us for a powerful afternoon as we delve into tools and knowledge to hone your small business cybersecurity strategy. Our expert speakers from government and industry will empower you to understand the threats, mitigate risk, navigate federal regulations and know what to do when incidents arise.

### Agenda

**1:30–1:45 PM**

**Introduction to Today's Threats and Resources to Mitigate Them**

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

**1:45–2:00 PM**

**Government Resources for Small Business**

*Speaker: Lyle J. Wright, MM, EDPF | Associate State Director, Mn Small Business Development Center program (Mn\_SBDC)*

**2:00–2:30 PM**

**Efficiently Managing Risk as a Small Business**

*Speakers: Joe Chow, SVP & Director, Specialized Business Services; Elwin Loomis, Digital Strategy Director, Bremer Bank*

**2:30–3:00 PM**

**A Cost-Effective Model to Safeguard Your Small Business from Cybersecurity Threats**

*Speaker: CAPT Scott Singer, USN (ret), President of CyberNINES, past Executive Officer of a Pacific Fleet Cybersecurity Unit (NR CPF MOC DET 601)*

**3:00–3:30 PM**

**How the Government is Helping Small Businesses Build a Defense**

*Speaker: Christopher Gabbard, Cybersecurity Advisor, Region V, Minnesota, CISA, DHS*

**3:30–4:00 PM**

**Protecting Your Business Now & What to do when you have an Incident**

*Moderator: Jill Allison, CISSP, CEO, Shuriken Cyber, Inc.*

**4:15–4:30 PM**

**Key Session Takeaways**

*Speaker: Elwin Loomis, Digital Strategy Director, Bremer Bank*



**4:30–5:00 PM** Following the seminar, explore resources from our solution strategy providers and establish new professional relationships during the Virtual EXPO Hall Closing.

Host

**BREMER BANK**

Supporters



**CyberNINES**



U.S. Small Business Administration



Securonix rated at the Top  
in the **2020 Gartner Critical Capabilities Report**

Source: Gartner (February 2020)

**Gartner.**

[www.securonix.com](http://www.securonix.com)

Copyright ©2020 Securonix Inc. All rights reserved. 1020



**KUDELSKI SECURITY**

**FORRESTER®**  
**WAVE LEADER 2020**

Midsize Managed  
Security Services  
Providers

**MDR is a key offering of any  
MSSP worth its salt**

**And we've integrated it since DAY ONE**

Go to [kudelskisecurity.com](http://kudelskisecurity.com) to see how we stand out.



# 10 Years of Cyber Security Summit



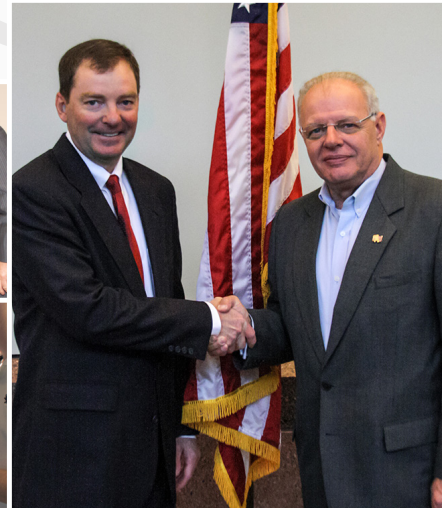
**2011**

Securing  
Our Digital  
Infrastructure



**2013**

Protect Your Data.  
Protect Yourself.



**2015**

Cyber  
Security  
is an  
Everybody  
Issue.



**2017**

Meet the Threat.  
Beat the Threat.



**2019**

Pushing the Cyber  
Security Envelope



**2012**

Plan Globally.  
Act Locally.



**2014**

It's not Just an  
IT Issue. It's an  
Everybody Issue.



**2016**

The Cyber Threat  
and Way Ahead.



**2018**

Securing Our  
Future — From the  
War Room to the  
Board Room



**2020**

The Ripple Effect  
*The Cascading  
Impacts  
of Cyber Security*



View speakers, photos, videos, presenter slides and program guides from past Summits at  
[cybersecuritysummit.org/past-cyber-security-summits](https://cybersecuritysummit.org/past-cyber-security-summits)



# Monday, October 26

9:00 AM-12:00 PM	Workshop: Identifying and Analyzing Adversary Infrastructure and Malware – See page 10 for details
9:30 AM-3:30 PM	Technical Sessions – Series of (15) one-hour technical sessions – See page 12 for details
11:30 AM-12:30 PM	WiCyS (Women in CyberSecurity) – See page 16 for details
12:00 PM-4:00 PM	Seminar: Healthcare & Med Device – See page 18 for details
12:00 PM-3:00 PM	Seminar: IT / OT / IoT Convergence – See page 20 for details
12:45 PM-4:30 PM	Seminar: In-house Legal Counsel (Continuing Legal Education) – See page 22 for details
3:30 PM-5:00 PM	Virtual EXPO Hall Opening – Explore resources from our solution strategy providers

# Tuesday, October 27

7:30 AM-8:00 AM	<b>Cyber Career Exploration</b> Deputy CISO for the State of Minnesota presents timely advice and career-shaping insights for future cyber security professionals. A great investment in your future! <i>Rohit Tandon, Deputy CISO, Information Security, State of Minnesota, MN.IT Services</i>
8:00 AM-8:20 AM	<b>Opening Welcome &amp; Ten Year Retrospective</b> Over the past ten years, Summit topics have progressed from communicating to your CEO what cyber security means and why it is critical to being a top three business concern. Cyber careers have equally changed as we highlight the career paths of 2011 attendees. Featuring Betty Burke, Information Technology Spec 5, State of MN Department of Revenue to Information Assurance Leaders and Vendor Management at Delta Air Lines now; Jerrod Montoya was a UMN MSST studen. to Deputy Chief Information Security Officer, OATI and Past-President InfraGard; Patricia Titus, CISO, Unisys then Chief Privacy and Information Security Officer at Markel Corporation now; Gregory Ogdahl, MN National Guard then to postions within US Cyber Command and MoneyGram now. <i>Mike Johnson, Director of Graduate Studies and Renier Chair, Technological Leadership Institute; Eileen Manning, Co-Founder, Executive Producer, The Cyber Security Summit</i>
8:20 AM-8:30 AM	<b>10 Minute. Year in Review</b> The Six Most Impactful Cyber and Business Tech Trends of 2020 and What it Means for 2021 <i>Mamady Konneh, Sr. Identity and Access Management Analyst, Health Partners; Jeremy Swenson, Senior Manager, USAA &amp; Abstract Forward</i>
8:30 AM-8:45 AM	<b>The Ripple Effect</b> This year's theme is "The Ripple Effect." The theme was selected to emphasize the interconnectedness of cyber security today - how one change can cause cascading impacts elsewhere. <i>Tim Crothers, Cyber Security Summit Co-chair; VP Security Solutions, Target</i>
8:45 AM-9:15 AM	<b>Keynote: The White House’s National Cyber Moonshot -- What it Means for State and Local Governments</b> The White House's National Cyber Moonshot calls for the 'whole of nation' to come together to make our critical infrastructure on the Internet safe by 2028. Hear from Tom Patterson, the Moonshot's Executive Director, about the six pillars of change coming, three national grand challenges, and today's optimal interactions at the state and local levels. <i>Tom Patterson, Chief Trust Officer for Unisys and Moonshot’s Executive Director</i>
9:15 AM-9:45 AM	<b>Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers</b> "Sandworm" chronicles the hacker group of the same name, diving into the hectic moments behind the Russian outfit's attacks, which have hit targets from the Ukrainian power grid to international shipping conglomerates. The book shows that attacks like BlackEnergy, NotPetya and Olympic Destroyer do not happen in a vacuum. Greenberg weaves them and others into a narrative that illuminates the personalities responsible for studying or thwarting Sandworm's attacks. The net result is a story that's miles away from technical jargon, exploring cyberwar's ultimate consequence – the danger to people's lives. <i>Andy Greenberg, Senior Writer &amp; Author, Wired Magazine</i>
9:45 AM-10:15 AM	<b>Cyber Byte™ – Corporations and Proto-Governance ~ Promise or Harbinger</b> Historically corporations were commonly acknowledged to be the owner/operators of critical infrastructures, and the providers of digital services, today their contributions are both broader and deeper. No one can doubt the expertise and operational experience possessed by private corporations in capitalist economies. Less highlighted, but nonetheless as important are the important strides in risk awareness and risk management efficacy also achieved by private corporations. Not only are these entities increasingly operating sensor infrastructures that deliver near - real time insights on the risk exposure of key cyber physical systems, but the risk experience of consumers are increasingly known to corporate actors before coming to the attention of governments. This superior risk - contact has potential importance for the future of governance. This is what my brief remarks will discuss - drawing some near and medium term implications for democratic governance and for the role of business. <i>Dr. David Mussington, Professor of the Practice and Director, Center for Public Policy and Private Enterprise, University of Maryland - College Park</i>

10:15 AM-10:45 AM	EXPO Break – Converse and connect with our Solution Strategy Providers
10:45 AM-11:45 AM	<b>Management Breakout: AI &amp; Machine Learning – Hype vs. Reality. Value or a new set of vulnerabilities?</b> Machine learning and AI play a powerful role in security. Not only are they being used by attackers and create new forms of risk that we need to deal with they can also be powerful capabilities to help battle the volume and complexity of the risk cycle we are experiencing. In this talk I will explore not only the promise but the perils of ML & AI. I will share insights on how to leverage these capabilities to help you fight through the noise and improve your controls to better manage and mitigate risk as well as lower total cost of controls. I will also explore some of the marketetur. that some in the industry has used to create the illusion that they have AI/ML capabilities in their solutions when they dont. I will offer advise on how to "spot the fake". I will also discuss the risks associated with AI/ML more broadly that we need to understand so we can understand not only the information risks that could be created but also the ethical implications on how AI/ML is developed and deployed. <i>Malcolm Harkins, Chief Security and Trust Officer, Cymatic</i>
10:45 AM-11:45 AM	<b>Tech Breakout: Security of Operational Technology (OT) Environment</b> Digital Transformation has increased the connectivity of the between the IT and the OT environments and has increased business dependence on the data captured within the OT environment. With this improved connectivity between the environments how do you appropriately secure the OT environment which is burdened with exponential growth of IoT devices without duplicating every security system in your IT environment to your OT environment. <i>Jason Rader, National Director Network &amp; Cloud Security, Insight</i>
10:45 AM-11:30 AM	<b>International Breakout Part One: Deep Dive into the Global Supply Chain: Risk, AI and Data Analytics</b> Join this fast track visual briefing with Interos CEO and Founder, Jennifer Bisceglie, to see the results of her dramatic move in 2015 from traditional risk management to emerging technologies. The conversation will be joined by International Co-Chairs Michelle Greeley, Anne Bader and renowned Forensic Scientist and STEM Champion Mary Frant. an. Global Minnesota's President Mark Ritchie to hear how international governments, corporations and the research community secure today's global supply chain. <i>Anne Bader, Founder, The International Cybersecurity Dialogue LLC; Jennifer Bisceglie, Chief Executive Officer, Interos Inc; Mary Frantz, Chief Information Security Officer; Founder, Prescriptive Health, Inc.; Enterprise Knowledge Partners, LLC; Michelle Greeley, Sr. Director, Global Risk Management, CWT; Mark Ritchie, U.S. Army; State of Minnesota, President; Civilian Aide to Secretary of the Army; Former MN Sec. of State (2007-2015), Global Minnesota</i>
11:30 AM-1:25 PM	<b>International Breakout Part Two: Securing the Global Supply Chain through Red Team Analysis. See and hear Two Red Teams Search for Vulnerabilities in . Real Time Scenario</b> Join World Class exper. Dr. Lynette Nusbache. in an "Observed Workshop" where supply chain and cyber security experts play an interactive role in identifying supply chain vulnerabilities. Dr. Amy Kircher will provide a realistic scenario using FPDl's CRYSTAL supply chain simulator. Watch and listen as Team 1 assumes the role of cyber criminals focused on financial gain via ransomware. Team 2 will assume the role of corporate competitors searching for ways to adulterate the food supply chain. Rapporteurs will provide a play-by-play account and post your questions and comments in text commentary throughout the exercise. Move on to join the "Hot Wash" after action discussion. Participants will be able to see the entire session and witness both Red Team's analysis in live stream. Attendees will receive a report of the proceedings at the close of the Summit. <i>Anne Bader, Founder, The International Cybersecurity Dialogue LLC; Michelle Greeley, Sr. Director, Global Risk Management, CWT; Brian Isle, Senior Fellow, Technological Leadership Institute; Dr. Amy Kircher, Co-Director, Strategic Partnerships and Research Collaborative Senior Advisor, Food Protection and Defense Institute, University of Minnesota; Dr. Lynette Nusbacher, Futurist, Strategist, Analyst, Facilitator, Advisor, Nusbacher &amp; Associates; Pekka Vepsalainen, Cyber Security and GDPR Consultant, Entrepreneur, Tikkasec, Ltd.</i>
11:45 AM-1:15 PM	<b>CISO Forum (Invitation Only)</b> Digital Transformation in the New World Order CXO Perspectives – Sponsored by Kudelski Security This panel will help empower business leaders in C-Suites and Board Rooms to move forward in the face of an unprecedented strategic dilemma between the immediate demand for digital transformation to a telecommuting workforce, and the need to conserve cash expenses as they wait out a global crisis created by COVID-19. Meanwhile, nation-state threats from foreign governments against the US and allied private sectors are increasing as the number of end-points expands and the demand for cloud usage and data-in-motion volumes explode across a new 5G global infrastructure.  This expert panel of current and former CEOs, CISOs and transformational leaders will discuss lessons learned from successes and failures in the wake of 2020's dual-crisis for enterprise IT and Security leaders. Topics will include best practices in digital transformation and cyber security resiliency including topics related to robotic process automation, AI/ML, supply chain optimization, cloud migration, insider threat and other areas to increase organizational effectiveness and continue business delivery in the face of the pandemic. <i>Moderator: Andrew Howard, CEO, Kudelski Security, Inc.; Panelists: Andrew Borene, Managing Director, US Public Sector, Cybereason; James Eckart, Chief Security Advisor, Microsoft; Jason Hicks, Global CISO, Kudelski Security, Inc.; Steve Jensen, President &amp; CEO, SunStream Business Services</i>
11:45 AM-1:15 PM	<b>EXPO Lunch Hour</b> While taking a session break, please visit with our solution strategy providers.




# Wednesday, October 28

1:30 PM-5:00 PM	<b>Seminar: Small Business</b> Hackers target small businesses as low-hanging fruit. Learn how to protect yourself, your customers and your assets in a powerful afternoon with top Cyber Security thought leaders to give you knowledge for developing technical and financial aspects of a cyber security plan for your business. Hear from cyber warriors on how to protect your business and Government agency's on resources available. <i>Moderator: Jill Allison, Chair, Board of Directors; Security Consultant, WiCyS MN Affiliate; Shuriken; Panelists: Joseph Chow, SVP &amp; Director, Specialized Business Services, Bremer Bank; Christopher Gabbard, Cyber Security Advisor – Region V, Office of Cybersecurity &amp; Communications, Cybersecurity and Infrastructure Security Agency (CISA); Elwin Loomis, Digital Strategy Director, Bremer Bank; Brian McDonald, District Director, U.S. Small Business Administration; Scott Singer, President, CyberNINES; Lyle Wright, Associate State Director at Minnesota Small Business Development Center, DEED</i>
1:30 PM-2:00 PM	<b>Cyber Byte™ – Living Off the Land - "Fileless" Malware Attacks</b> Over the last several years, the use of legitimate applications to deliver malicious code has become commonplace for attackers as a way to avoid detection and move quickly across victim networks. We'll take a look at how "fileless" attacks work, who is using them and why, and how you can better deter, detect, and disrupt fileless malware attacks on your organization's network. <i>Paul Melson, Sr Director, Cyber Threat Intelligence &amp; Detection, Target</i>
2:00 PM-2:45 PM	<b>Cyber Byte™ – Security and Privacy for Humans</b> Traditionally, security and privacy research focused mostly on technical mechanisms and was based on the naive assumptions that Alice and Bob were capable, attentive, and willing to jump through any number of hoops to communicate securely. However, 20 years ago that started to change when a seminal paper asked "Why Johnny Can't Encrypt" and called for usability evaluations and usable design strategies for security. Today a substantial body of interdisciplinary literature exists on usability evaluations and design strategies for both security and privacy. Nonetheless, it is still difficult for most people to encrypt their email, manage their passwords, and configure their social network privacy settings. In this talk I will highlight some of the lessons learned from the past 20 years of usable privacy and security research, and explore where the field might be headed. <i>Lorrie Cranor, Professor &amp; Director, CyLab Security and Privacy Institute, Carnegie Mellon University</i>
2:45 PM-3:15 PM	<b>EXPO Break</b> – Converse and connect with our Solution Strategy Providers
3:15 PM-3:45 PM	<b>Cyber Byte™ – Winning the Cyber War with Zero Trust</b> With our new distributed Work-From-Home reality and the continued proliferation of connected devices, the need to effectively segment cybersecurity risks has never been more critical. Hear from John Kindervag, the founder of Zero Trust, about how the principles of 'never trust, always verify' can help you dramatically improve your cybersecurity posture and enable your organization's mission. <i>John Kindervag, Field CTO, Palo Alto Networks</i>
3:45 PM-4:15 PM	<b>Cyber Byte™ – How building and maintaining a remote work force has forced us to think of business success from different dimensions.</b> Zero Trust is now a part of what we do not just something we talk about. Securing our IT without borders has offered up additional challenges that we have all had to deal with over the last year. For example passwords expiration had to be paused because computer had to be on main network. How do we deal endpoints that never touch our internal network. How has COVID forced us to think about security very differently. How are we thinking about identity differently. <i>Tris Lingen, Chief Information Security Officer, 3M</i>
4:15 PM-4:45 PM	<b>Cyber Byte™ – Tomorrow's Cyber Threats: Staying One Step Ahead</b> Despite predictions for the past few years that ransomware would become obsolete, it has actually spread more prolifically than anyone could have guessed. In this talk, we will break down the evolution of ransomware and walk through a timeline of an attack our elite research team has actually seen. Learn the latest about this threat so you can stay one step ahead. <i>Israel Barak, CISO, Cybereason</i>
4:45 PM-5:00 PM	<b>Closing Takeaways</b> <i>Tim Crothers, Cyber Security Summit Co-chair; VP Security Solutions, Target; Catharine Trebnick, Cyber Security Summit Co-chair; VP Equity Research (Security and UCaaS), Colliers International</i>
5:00 PM-6:00 PM	<b>Networking Reception in EXPO Hall</b> Join us in the EXPO area and network with fellow attendees and our solution strategy partners

8:00 AM-8:30 AM	<b>Cyber Byte™ – From Chaos to Clarity: Gaining Visibility and Control in Your Distributed Workforce</b> 2020 has quickly forced the way organizations now work – rapidly and radically transforming the state of IT. Distributed workforces revealed a hard truth: many organizations have critical visibility gaps and are operating from a lower maturity level in their endpoint security and response capabilities that are challenging even the most secure enterprises. A recent survey revealed that... - 90% of CXOs reported an increase in cyberattacks since the world stayed home. - 47% of IT leaders plan to improve patch processes - The #1 concern among IT leaders is identifying remote endpoints  How do you prepare for what lies ahead when you're in the midst of playing catch-up? To address this transformation, organizations up-ended their traditional IT infrastructure and adopted decentralized networks, cloud-based services and widespread usage of employees' personal devices. During Tanium's session, Dylan DeAnda, Vice President of Enterprise Services at Tanium, will share use cases around gaining visibility and control in a distributed workforce operating environment. <i>Dylan DeAnda, Vice President of Enterprise Services, Tanium</i>
8:30 AM-9:30 AM	<b>Panel – It's Raining Breaches and the Number One Culprit is Ransomware</b> This expert panel will provide insightful CISO to legal viewpoints on... · How we prevent ransomware attacks? · Are there things we should do to prepare for the inevitable? · If we are hit by a ransomware attack, how should we respond? · Should we pay ransomware? If so, how do we do that? · Do we have to worry about our suppliers?  <i>Moderator: Brad Maiorino, EVP and Chief Strategy Officer, FireEye; Panelists: Richard Agostino, Senior Vice President and Chief Information Security Officer , Target Corporation; John Carlin, Morrison &amp; Foerster, LLP, Chair, Global Risk &amp; Crisis Management; Siobhan Gorman, Partner, Brunswick Group</i>
9:30 AM-10:00 AM	<b>Cyber Byte™ – Heading to the Cloud. Learn how to mitigate your risks.</b> As we all move to the cloud we have new risks to manage. The attack surface is different. The responsibility model is different. The tools, architecture and deployment model are all new and present new challenges. In this session we'll share lessons learned and provide guidance on how to secure your move to the cloud. <i>Dan Larson, Senior Vice President Product Strategy, Arctic Wolf; David Notch, Enterprise Security &amp; Cloud Architecture, Medtronic</i>
10:15 AM-11:00 AM	<b>Cyber Byte™ – Zero Trust: The Journey to Zero Trust</b> Zero trust is not as simple as implementing a new product or technology. It is a shift in the strategy of how users' access and leverage organizations data and intellectual property. This is a business decision. Discuss why is it important to the business/mission. Why the demand. Primally a shift to mobility and cloud services. Assets are no longer within the walls of the organization. Why the shift. COVID19 is a perfect example. Organizations need to remain competitive, so speed and agility are important and traditional security models do not solve the problem with mobile users and cloud applications. Access anywhere anytime from anything is becoming the norm. <i>Alex Weinert, Director of Identity Security, Microsoft</i>
11:00 AM-11:30 AM	<b>Cyber Byte™ – Threat Assessment Intelligence</b> What are the trade offs in using open source threat intel versus paid intel. What are the requirements for decisions ans how do you decide what's best for your organization? Should threat intel be free?  Malware free attacks exploit different attack mechanisms. Chinese are extremely capable at this using services and functions. The response requires a different more difficult response. Techniques are different as you aren't looking for a virus or hack. Larger threat intel, do organizations still need to pay for threat intel anymore. <i>Jason Rivera, Director: Strategic Threat Advisory Group; Crowdstrike</i>
11:30 AM-12:00 PM	<b>Cyber Byte™ – Failed Response: Breach Response for Leadership</b> A botched response to a breach is worse than the breach itself. Figuring it out on the fly isn't advisable, so to whom should you turn as a guide? How do you lead through something that you've never yourself done? For this in leadership, breach response is both part art and science. It's the translation of atomic indicators to board members and while explaining the sins of the past to external auditors and lawyers – and you can't afford to get it wrong without disastrous and expensive outcomes. Equal parts leadership and grit, learn from past mistakes, and firsthand experiences from someone who has done it and helped others do it. Hear from Stephen Moore, a guy forced to figure it out on the fly during one of the most significant breaches ever. <i>Stephen Moore, Vice President and Chief Security Strategist, Exabeam</i>
1:15 PM-2:15 PM	<b>Cyber Byte™ – Election Security</b> With U.S. elections less than two-weeks away, this session will look at what has been learned over the past year about both election threats and protection measures that will be tested in this election cycle. Former Minnesota Secretary of State, Mark Ritchie, is co-author of the national report on Safe Voting in the Midst of the COVID-19 Pandemic will be joined by election protection experts working on the front-lines to ensure free and fair elections in November. Topics that will be covered include overt and covert attacks on election systems, including voter registration databases, impact of voting by mail, and success stories from states, cities, and counties across the country. <i>Mark Ritchie, U.S. Army; State of Minnesota, President; Civilian Aide to Secretary of the Army; Former MN Sec. of State (2007-2015); Global Minnesota; Dr. Michael Schmitt, Professor of International Law, University of Reading Law School</i>



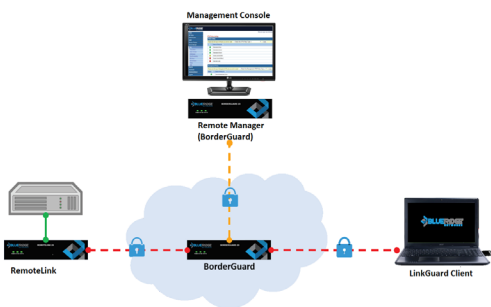
2:15 PM-2:45 PM	<b>Cyber Byte™ – Preparing for Multi-Domain Cyber Challenges</b> Multiple simultaneous cyber security events are the new normal that challenges all aspects of an organization's security system including staffing, technology, and remedies. This session will provide real life examples of the broad range of cyber events and resulting challenges to providing IT services while protecting the organization's data and infrastructure. The session will provide practical guidance for response to multiple cyber events including planning, prioritization, and anticipating the unknown. <i>Rohit Tandon, Deputy CISO, Information Security, State of Minnesota, MN.IT Services</i>
2:45 PM-3:00 PM	<b>Break</b>
3:00 PM-3:30 PM	<b>Cyber Byte™ – How Threat Modeling Brings Security To Development</b> "Security said we can't ship this!" If you've ever been in that situation, you know it was a painful discussion. That pain could have been avoided if security had been integrated into software development. Threat modeling is a family of techniques to do just that. Learn the four simple questions that will get you started and improve development today. <i>Adam Shostack, Consultant and advisor delivering strategic security and privacy innovation, Shostack &amp; Associates</i>
3:30 PM-4:00 PM	<b>Cyber Byte™ – Emerging Issues, Future Challenges and Trajectories and Countermeasures</b> How fast the world will change over next ten years. Rate at new viruses are coming out is increasing, become more prevalent, here's why you will need to build into your plan. How you need to manage your cyber. Within next 18 months new virus we have never seen before. Few customers had solid infectious disease adaptive plan. This needs to be standard. <i>Dr. Massoud Amin, Professor / Cofounder/Past Chairman CSS, University of Minnesota</i>
4:00 PM-4:40 PM	<b>Closing Keynote. Cyber Has Become Like The Air We Breath – It Touches Everything</b> For the last 20 years Mr. Rodriguez has building communities of interest and trust through public - private partnership models for the US Secret Service, US Postal Service and The Departments of Defense, Energy and Homeland Security. He will share his journey and the key elements of bringing together a trusted network of global investors, buyers and innovators into a global marketplace. <i>Robert Rodriguez, Chairman &amp; Founder of SINET and a Venture Partner at SineWave Ventures</i>
4:40 PM-5:00 PM	<b>Wrap Up &amp; Practical Takeaways</b> Our distinguished Event Co-Chairs briefly revisit insights and action steps presented over the past three days by colleagues and collaborators, the accomplished thought leaders who have presented here at CSS 2020. These snippets will help remind you of ideas to enact and ideas to share with your peers. Stick around for this useful final session! Items you take back with you are icing on the cyber cake and hear from 2021 Co-Chairs. <i>Tim Crothers, Cyber Security Summit Co-chair; VP Security Solutions, Target; Jennifer Czaplewski, Director, Product Security, Target; Catharine Trebnick, Cyber Security Summit Co-chair; VP Equity Research (Security and UCaaS), Colliers International; Wade Van Guilder, Principal Advisor, Cybersecurity SLED, World Wide Technology</i>



**Resilient – Reliable – Efficient**  
**Zero Trust Cybersecurity Solutions**

**DON'T JUST RESPOND - DEFEND!**

**LinkGuard® - ZERO TRUST DEFENSE**




**Protecting Critical Infrastructure and National Defense**

**SECURE**    **Critical Infrastructure**

**HIDE**        **Valuable Assets from Threats**

**SEGMENT**   **Network devices from lateral attack**

**PROTECT**    **Legacy devices from TODAY'S threats**



**Reduces Attack Surface**  
**Eliminates Persistent Vulnerabilities**  
**Effective, Compatible Defense-in-Depth**

# The Rapid Pace of IT Change Just Got Faster, Thank You COVID-19



Mike Johnson  
Technological Leadership Institute

The sudden onset of the novel coronavirus health crisis earlier this year has had many impacts on organizations, one of the most significant being how quickly organizations were required to change their IT and business processes in order to continue conducting activities in a socially distant environment. These changes significantly increased the pace of major technology implementations like cloud migration, remote employee access and online collaboration tools. While some of these changes may have been planned for the future, COVID-19 has forced these projects into very short delivery timeframes and increased the stakes of being successful. Additionally, surveys indicate that many of these IT changes will continue and be made a permanent part of organizational infrastructure and process going forward. All of this rapid change and adoption of new technologies is probably a good thing for businesses and demonstrates how IT can adapt and create resilient systems; but it also exacerbates a problem that has plagued most organizations who consider change: ensuring that tools and systems implemented to solve business problems retain or improve on the data security needs of the organization.

New technology capabilities have always moved faster than the understanding of the security risks of those systems or the implementation of appropriate controls. As security professionals, we are familiar with the desire to build security into a tool or process before it is implemented, but we know this takes time and may slow business plans. The repercussions of not doing a good job of understanding the potential risks of new technology can be significant, as

demonstrated by the many security issues uncovered when video conferencing platforms expanded exponentially to meet demand at the beginning of the crisis. In that case, the vendors did an admirable job fixing issues after they were identified and often exploited, but those companies and their clients were still subjected to reputation impacts and business disruptions from the incidents. Preventing rather than responding to those issues would have been a far better plan for them and for their customers.

As we move forward in our new environment, all organizations need to step back and make sure their business and IT plans align with their security needs. The faster things change in an organization, the more likely they are to experience negative impacts from issues with an immature tool, a rapidly deployed process change or staff that isn't properly trained to mitigate the risks. While there are many potential changes that could cause impact, COVID-19 has possibly had the most impact on changes to remote/secure remote access, SaaS and cloud migration, increased reliance on a supply chain that may have become less reliable during the last 6 months, and security programs that may have relied on endpoints and assets being located within an organization's data center in order to be effective.

As organizations continue to move forward with needed advancements in their IT and process areas, it is critically important that the security teams are part of the initial efforts and work closely with business and IT leadership to minimize unplanned negative impacts that could tip an organization into a business ending situation.

At the [Technological Leadership Institute](#), we strive to understand the holistic impact of any situation or change so organization leaders can make good decisions that support both business objectives and security needs. Security and IT leaders need to be focused on both the technical solutions and the business needs and impacts in order to effectively steer their organization through such difficult times as we are facing today.



WE STOP



SO YOU CAN GO

LEARN MORE AT  
[crowdstrike.com/summit](https://crowdstrike.com/summit)



## SUMMIT CO-CHAIRS

**TIM CROTHERS**

*VP Security Solutions, Target*

TUE OCT 27, 8:30 AM

The Ripple Effect

Tue Oct 27, 4:45 PM

Closing Takeaways

WED OCT 28, 4:40 PM

Wrap Up & Practical Takeaways

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

**CATHARINE TREBNICK**

*Cyber Security Summit Co-chair;  
VP Equity Research (Security and UCaaS), Colliers International*

TUE OCT 27, 4:45 PM

Closing Takeaways

WED OCT 28, 4:40 PM

Wrap Up & Practical Takeaways

Catharine Trebnick serves as Vice President, Equity Research at Colliers. Ms. Trebnick sector focus is Security, Cloud and Network Infrastructure and Unified Communications. Ms. Trebnick began her career on the Wall Street at ThinkEquity in 2005. Ms. Trebnick is fluent in emerging technologies, cloud and infrastructure networks and leverages C-level relationships plus technical knowledge gained from over 15 years in senior level product management positions to gain rare insight in order to influence stock prices and provide real-time, accurate intelligence to investors. Ms. Trebnick earned a Bachelor's of Science Degree in Chemistry and minor in Chemical Engineering from University of Maryland. She also earned a Master's of Business Degree from the University of Chicago. Ms. Trebnick is a frequent guest on CNBC and received acclaim for her research through published papers and quotes published in Barron's, Wall Street Journal, Reuters, Bloomberg, TheStreet.com, Forbes, Investor's Business Daily and CNNMoney.

## Learn More About Our Speakers

For full biographies and other relative information, visit:  
[cybersecuritysummit.org/speakers](https://cybersecuritysummit.org/speakers)

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

**RICHARD AGOSTINO**

*Senior Vice President and  
Chief Information Security  
Officer, Target Corporation*

WED OCT 28 - 8:30 AM

Panel - "It's Raining Breaches" and the Number One Culprit is Ransomware

**JILL ALLISON**

*Chair, Board of Directors,  
WiCyS MN Affiliate; Security  
Consultant, Shuriken*

WED OCT 26 - 12:30 PM

Women in Cyber Security Dialogue

TUE OCT 27, 1:30 PM

Seminar: Small Business

**DR. MASSOUD AMIN**

*Professor | Cofounder/Past  
Chairman CSS, University of  
Minnesota*

WED OCT 28 - 3:30 PM

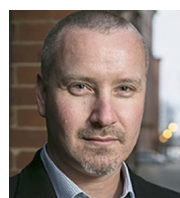
Cyber Byte™ - Emerging Issues, Future Challenges and Trajectories and Countermeasures

**ANNE BADER**

*Founder, The International  
Cybersecurity Dialogue LLC*

TUE OCT 27 - 10:45 AM-1:25 PM

International Breakout Part One and Part Two

**ISRAEL BARAK**

*CISO, Cybereason*

TUE OCT 27 - 4:15 PM

Cyber Byte™ - "Tomorrow's Cyber Threats - Staying One Step Ahead"

**AUGUSTO BARROS**

*VP of Solutions, Securonix*

MON OCT 26 - 1:30 PM

Tech Session 4A - Improving Threat Detection with a Detection-Development Life Cycle

**ADITYA BHARADWAJ**

*General Counsel, Ascentis  
Human Capital Management  
Software*

MON OCT 26 - 12:45 PM

Seminar: In-house Legal Counsel (Continuing Legal Education)

**JENNIFER BISCEGLIE**

*Chief Executive Officer, Interos*

TUE OCT 27 - 10:45 AM

International Breakout Part One: Deep Dive into the Global Supply Chain: Risk, AI and Data Analytics

**SHELLY BLACKBURN**

*Vice President, Global Cyber  
Security Systems Engineering,  
Cisco*

MON OCT 26 - 11:30 AM

Women in Cyber Security Dialogue

**ADAM BLAKE**

*Principal Engineer, Cyber  
Security Insider Threat Team,  
Target Corporation*

MON OCT 26 - 10:30 AM

Tech Session 2A - Not All Threats are External

**GRETCHEN BLOCK**

*Vice President, Optum*

MON OCT 26 - 11:30 AM

Women in Cyber Security Dialogue

**JOHN BLOOMER**

*Director of Engineering, Check  
Point Software Technologies,  
Ltd.*

MON OCT 26 - 12:00 PM

Seminar: IT / OT / IoT Convergence

**ANDREW BORENE**

*Managing Director, US Public  
Sector, Cybereason*

TUE OCT 27 - 11:45 AM

CISO Lunch (Invitation Only)

**MARIA BROWN**

*Sr. Principal Cloud and  
Application Security Engineer,  
Medtronic*

MON OCT 26 - 10:30 AM

Tech Session 2C - Application Security Automation in Development

**STEVE CAIMI**

*Cybersecurity Specialist, Cisco  
Systems*

MON OCT 26 - 12:00 PM

Seminar: Healthcare & Med Device

**JOHN CARLIN**

*Morrison & Foerster, LLP,  
Chair, Global Risk & Crisis  
Management*

WED OCT 28 - 8:30 AM

Panel - "It's Raining Breaches" and the Number One Culprit is Ransomware

**SETH CARMODY**

*Vice President of Regulatory  
Strategy, MedCrypt*

MON OCT 26 - 12:00 PM

Seminar: Healthcare & Med Device

**JOSEPH CHOW**

*SVP & Director, Specialized  
Business Services, Bremer  
Bank*

TUE OCT 27 - 1:30 PM

Small Business

**STEVE CHRISTEY COLEY**

*Principal Cybersecurity  
Engineer, The MITRE  
Corporation*

MON OCT 26 - 12:00 PM

Seminar: Healthcare & Med Device

**TRAVIS CHRISTIAN**

*Lead Info Security Analyst,  
Target Corporation*

MON OCT 26 - 9:30 AM

Tech Session 1A - Active Vulnerability Management

**CHARLES COLLINS**

*Data Loss Prevention  
Analyst, 3M*

MON OCT 26 - 2:30 PM

Tech Session 5B - How Data Classification Tools can Spark Conversation and Drive Change at your Company

**LORRIE CRANOR**

*Professor & Director, CyLab  
Security and Privacy Institute,  
Carnegie Mellon University*

TUE OCT 27 - 2:00 PM

Cyber Byte™ - Security and Privacy for Humans

**JOANA CRUZ**

*Director of Engineering,  
Digital Security, Target  
Corporation*

MON OCT 26 - 12:30 PM

Tech Session 3A - Modernizing Security Software Engineering To Secure By Default

**JENNIFER CZAPLEWSKI**

*Director, Product Security,  
Target*

WED OCT 28 - 4:40 PM

Wrap Up & Practical Takeaways

**LOREN DEALY MAHLER**

*President, Dealy Mahler  
Strategies*

MON OCT 26 - 12:45 PM

Seminar: In-house Legal Counsel (Continuing Legal Education)

**DYLAN DEANDA**

*Vice President of Enterprise  
Services, Tanium*

WED OCT 28 - 8:00 AM

Cyber Byte™ - From Chaos to Clarity: Gaining Visibility and Control in Your Distributed Workforce

**JAMES ECKART**

*Chief Security Advisor,  
Microsoft*

TUE OCT 27 - 11:45 AM

CISO Lunch (Invitation Only)

**BETTY ELLIOTT, CISSP**

*Partner, Chief Information  
Security Officer, Mercer*

MON OCT 26 - 12:30 PM

Tech Session 3B - Leading High Performing Teams During a Global Pandemic



**MADELINE FINDLEY**

*US Privacy Counsel,  
Medtronic*  
MON OCT 26 - 12:45 PM  
Seminar: In-house Legal  
Counsel (Continuing Legal  
Education)

**MICHELLE GREELEY**

*Sr. Director, Global Risk  
Management, CWT*  
TUE OCT 27 -  
10:45 AM-1:25 PM  
International Breakout Part  
One and Part Two

**BRETT HEBERT**

*Associate Attorney, Taft  
Law*  
MON OCT 26 - 12:45 PM  
Seminar: In-house Legal  
Counsel (Continuing  
Legal Education)

**STEVE JENSEN**

*President & CEO, SunStream  
Business Services*  
TUE OCT 27 - 11:45 AM  
CISO Lunch (Invitation Only)

**DR. AMY KIRCHER**

*Co-Director, Strategic  
Partnerships & Research  
Collaborative Senior Advisor,  
Food Protection and Defense  
Institute, University of MN*  
TUE OCT 27 - 11:30 AM  
International Breakout  
Part Two...

**EILEEN MANNING**

*Co-Founder, Executive  
Producer, The Cyber Security  
Summit*  
TUE OCT 27 - 8:00 AM  
Opening Welcome

**SHAWN FLEURY**

*Director, Risk Management,  
The Crispis Group*  
MON OCT 26 - 12:45 PM  
Seminar: In-house Legal  
Counsel (Continuing Legal  
Education)

**ANDY GREENBERG**

*Senior Writer & Author, Wired  
Magazine*  
TUE OCT 27 - 9:15 AM  
Sandworm: A New Era of  
Cyberwar and the Hunt  
for the Kremlin's Most  
Dangerous Hackers

**SHAWN HENRY**

*President, Services  
Division, and Chief  
Security Officer,  
CrowdStrike*  
WED OCT 28 - 11:00 AM  
CISO Lunch (Invitation  
Only)

**ERIC JOHANSEN**

*Regional Sales Engineer -  
Midwest, Nozomi Networks*  
MON OCT 26 - 12:00 PM  
Seminar: IT / OT / IoT  
Convergence

**MAMADY KONNEH**

*Sr. Identity and Access  
Management Analyst, Health  
Partners*  
TUE OCT 27 - 8:20 AM  
10 Minute: Year in Review

**BRIAN MCDONALD**

*District Director, U.S. Small  
Business Administration*  
TUE OCT 27 - 1:30 PM  
Small Business

**MARY FRANTZ**

*Chief Information Security  
Officer; Founder, Prescriptive  
Health, Inc.; Enterprise  
Knowledge Partners, LLC*  
TUE OCT 27 - 10:45 AM  
International Breakout Part  
One: Deep Dive into the  
Global Supply Chain...

**SAM GROSBY**

*Principal Enterprise  
Information Security Engineer,  
Wells Fargo*  
MON OCT 26 - 12:30 PM  
Tech Session 3B - Leading  
High Performing Teams  
During a Global Pandemic

**JASON HICKS**

*Global CISO, Kudelski  
Security*  
TUE OCT 27 - 11:45 AM  
CISO Lunch (Invitation  
Only)

**MIKE JOHNSON**

*Director of Graduate  
Studies and Renier Chair,  
Technological Leadership  
Institute*  
TUE OCT 27 - 8:00 AM  
Opening Welcome

**DAN LARSON**

*Senior Vice President  
Product Strategy, Arctic Wolf*  
WED OCT 28 - 9:30 AM  
Cyber Byte™ - Heading to  
the Cloud? Learn how to  
mitigate your risks.

**TINA MEEKER**

*Sr. Director, Information  
Security, Sleep Number*  
MON OCT 26 - 12:30 PM  
Tech Session 3B - Leading  
High Performing Teams  
During a Global Pandemic

**CHRISTOPHER GABBARD**

*Cyber Security Advisor - Region  
V, Office of Cybersecurity &  
Communications, Cybersecurity  
and Infrastructure Security  
Agency (CISA)*  
TUE OCT 27 - 1:30 PM  
Small Business

**NABIL HANNAN**

*Managing Director, NetSPI*  
MON OCT 26 - 9:30 AM  
Tech Session 1C - Getting  
Started on Application  
Security

**JENA HOVER**

*Senior Manager, Cyber  
Security Incident  
Response Team, Target  
Corporation*  
MON OCT 26 - 10:30 AM  
Tech Session 2A - Not All  
Threats are External

**ERAN KAHANA**

*Attorney, Maslon LLP*  
MON OCT 26 - 12:00 PM  
Seminar: Healthcare & Med  
Device

**MAGGIE LASSACK**

*Privacy & Cyber Security  
Counsel, Polaris Industries*  
MON OCT 26 - 12:45 PM  
Seminar: In-house Legal  
Counsel (Continuing Legal  
Education)

**PAUL MELSON**

*Sr Director, Cyber Threat  
Intelligence & Detection,  
Target*  
TUE OCT 27 - 1:30 PM  
Cyber Byte™ - Living Off the  
Land - "Fileless" Malware  
Attacks

**SCOTT GANOW**

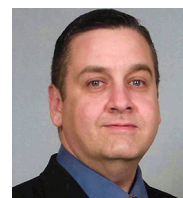
*Chair Privacy & Data Security  
Practice, Taft Law*  
MON OCT 26 - 12:45 PM  
Seminar: In-house Legal  
Counsel (Continuing Legal  
Education)

**MALCOLM HARKINS**

*Chief Security and Trust Officer,  
Cymatic*  
TUE OCT 27 - 10:45 AM  
Management Breakout: AI &  
Machine Learning - Hype vs.  
Reality. Value or a new set of  
vulnerabilities?

**ANDREW HOWARD**

*CEO, Kudelski Security,  
Inc.*  
TUE OCT 27 - 11:45 AM  
CISO Lunch (Invitation  
Only)

**MIKE KENNEDY, CISSP**

*Sr. Manager - Global Security  
Office, Medtronic*  
MON OCT 26 - 10:30 AM  
Tech Session 2C -  
Application Security  
Automation in  
Development

**TRIS LINGEN**

*Chief Information Security  
Officer, 3M*  
TUE OCT 27 - 3:45 PM  
Cyber Byte™ - How building  
and maintaining a remote  
work force has forced us to  
think of business success  
from different dimensions.

**ALLISON MILLER**

*Chief Information Security  
Officer, Optum*  
MON OCT 26 - 11:30 AM  
Women in Cyber Security  
Dialogue

**CHRISTA GIRTZ**

*Global Security | Manager,  
Threat Intelligence, General  
Mills*  
MON OCT 26 - 2:30 PM  
Tech Session 5A - Tailor  
Your Cyber Threat Intel  
Program and Optimize  
Resources

**DAVE HARVEY**

*Manager of IT Security GRC  
and Interim IT Security IR  
Manager, Fairview Health  
Services*  
MON OCT 26 - 12:00 PM  
Seminar: Healthcare & Med  
Device

**KEN HOYME**

*Director, Product and  
Engineering Systems  
Security, Boston Scientific*  
MON OCT 26 - 12:00 PM  
Seminar: Healthcare &  
Med Device

**DARRELL KESTI**

*Regional Sales Manager, Ord*  
MON OCT 26 - 12:00 PM  
Seminar: Healthcare & Med  
Device

**ELWIN LOOMIS**

*Digital Strategy Director,  
Bremer Bank*  
TUE OCT 27 - 1:30 PM  
Small Business

**JERROD MONTOYA**

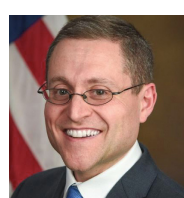
*Deputy CISO, OATI*  
MON OCT 26 - 12:45 PM  
Seminar: In-house Legal  
Counsel (Continuing Legal  
Education)

**SIOBHAN GORMAN**

*Partner, Brunswick Group*  
WED OCT 28 - 8:30 AM  
Panel - "It's Raining  
Breaches" and the Number  
One Culprit is Ransomware

**JUDY HATCHETT**

*CISO, Surescripts*  
MON OCT 26 - 12:00 PM  
Seminar: Healthcare & Med  
Device

**BRIAN ISLE**

*Senior Fellow, Technological  
Leadership Institute*  
TUE OCT 27 - 11:30 AM  
International Breakout  
Part Two: Securing the  
Global Supply Chain  
through Red Team  
Analysis: ...

**JOHN KINDERVAG**

*Field CTO, Palo Alto Networks*  
TUE OCT 27 - 3:15 PM  
Cyber Byte™ - Winning the  
Cyber War with Zero Trust

**BRAD MAIORINO**

*EVP and Chief Strategy  
Officer, FireEye*  
WED OCT 28 - 8:30 AM  
Panel - "It's Raining  
Breaches" and the Number  
One Culprit is Ransomware

**STEPHEN MOORE**

*Vice President and Chief  
Security Strategist, Exabeam*  
WED OCT 28 - 11:30 AM  
Cyber Byte™ - Failed  
Response: Breach Response  
for Leadership





**TOM MUEHLEISEN**  
Director of Cyber Operations,  
Norwich University Applied  
Research Institutes (NUARI)  
MON OCT 26 - 12:00 PM  
Seminar: IT / OT / IoT  
Convergence



**DR. DAVID MUSSINGTON**  
Professor of the Practice and  
Director, Center for Public  
Policy and Private Enterprise,  
University of Maryland -  
College Park  
TUE OCT 27 - 9:45 AM  
Cyber Byte™ — Corporations  
and Proto-Governance...



**ERIC NELSON**  
Systems Engineer, Ordr  
MON OCT 26 - 12:00 PM  
Seminar: IT / OT / IoT  
Convergence



**DAVID NOTCH**  
Enterprise Security & Cloud  
Architecture, Medtronic  
WED OCT 28 - 9:30 AM  
Cyber Byte™ - Heading to the  
Cloud? Learn how to  
mitigate your risks.



**DR. LYNETTE NUSBACHER**  
Futurist, Strategist, Analyst,  
Facilitator, Advisor, Nusbacher  
& Associates  
TUE OCT 27 - 11:30 AM  
International Breakout Part  
Two: Securing the Global  
Supply Chain through Red  
Team Analysis...



**NIMI OCHOLI**  
Senior Director, Product  
Security, Medtronic  
MON OCT 26 - 12:00 PM  
Seminar: Healthcare & Med  
Device



**RUDRA PANDA**  
Senior Engineering Manager,  
Target Corporation  
MON OCT 26 - 12:30 PM  
Tech Session 3A -  
Modernizing Security  
Software Engineering To  
Secure By Default



**TOM PATTERSON**  
Chief Trust Officer for Unisys  
and Moonshot's Executive  
Director  
TUE OCT 27 - 8:45 AM  
Keynote: The White House's  
National Cyber Moonshot --  
What it Means for State and  
Local Governments



**CHRIS PERKINS**  
Sr. Principal Security Architect,  
Medtronic  
MON OCT 26 - 10:30 AM  
Tech Session 2C - Application  
Security Automation in  
Development



**KORI PRINS**  
Technical User Support  
Analyst, Medtronic  
MON OCT 26 - 10:30 AM  
Tech Session 2C -  
Application Security  
Automation in  
Development



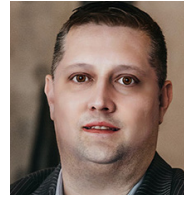
**JASON RADER**  
National Director Network &  
Cloud Security, Insight  
TUE OCT 27 - 10:45 AM  
Tech Breakout: Security of  
Operational Technology  
(OT) Environment



**MILINDA RAMBEL STONE**  
Chief Information Security  
Officer, Provation Medical  
MON OCT 26, 12:30 PM  
Tech Session 3B  
MON OCT 26, 12:45 PM  
Seminar: In-house Legal  
Counsel



**ARNAB RAY**  
Principal Cybersecurity  
Systems Engineer, Abbott  
MON OCT 26 - 12:00 PM  
Seminar: Healthcare & Med  
Device



**VIRGIL RENZ**  
Practice Leader & VP -  
Product & IoT/OT Security  
Services, Kudelski Security  
MON OCT 26 - 12:00 PM  
Seminar: IT / OT / IoT  
Convergence



**MARK RITCHIE**  
President; Civilian Aide to Secretary  
of the Army; Former MN Sec. of State  
(2007-2015), Global Minnesota; U.S.  
Army; State of MN  
TUE OCT 27, 10:45 AM  
Int'l Breakout Part One  
WED OCT 28, 1:15 PM  
Cyber Byte™ - Election Security



**ROBERT RODRIGUEZ**  
Chairman & Founder; Venture  
Partner, SINET; SineWave  
Ventures  
WED OCT 28 - 4:00 PM  
Closing Keynote: Cyber  
Has Become Like The Air  
We Breath - It Touches  
Everything



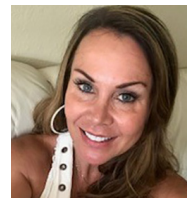
**FRANK ROSS**  
Sr. Manager, Cyber Security  
Engineering & Operations,  
General Mills  
MON OCT 26 - 2:30 PM  
Tech Session 5C - Building  
an Effective Cyber Security  
Engineering Organization



**PHIL SCHENKENBERG**  
Partner, Litigation & Cyber  
Security, Taft Law  
MON OCT 26 - 12:45 PM  
Seminar: In-house Legal  
Counsel (Continuing Legal  
Education)



**DR. MICHAEL SCHMITT**  
Professor of International  
Law, University of Reading  
Law School  
WED OCT 28 - 1:15 PM  
Cyber Byte™ - Election  
Security



**MERCY SCHROEDER**  
Sales Director, Saviynt, Inc.  
MON OCT 26 - 9:30 AM  
Tech Session 1B - Part One  
- Pillsbury Theater Group  
"Breaking Ice" event...



**MICHAEL SCHWARTZ**  
Director of Threat Intelligence  
and Detection Engineering,  
Target Corporation  
MON OCT 26 - 9:00 AM  
Workshop: Identifying  
and Analyzing Adversary  
Infrastructure and Malware



**ADAM SHOSTACK**  
Consultant and advisor  
delivering strategic security  
and privacy innovation,  
Shostack & Associates  
WED OCT 28 - 3:00 PM  
Cyber Byte™ - How Threat  
Modeling Brings Security To  
Development



**SCOTT SINGER**  
President, CyberNINES  
TUE OCT 27 - 1:30 PM  
Small Business



**MANGAYA SIVAGNAMAM**  
Principal Cybersecurity  
Architect, Trane Technologies  
MON OCT 26 - 12:00 PM  
Seminar: IT / OT / IoT  
Convergence



**JANELL STRAACH**  
Chairman of the Board, WiCyS  
Women in Cyber Security  
MON OCT 26 - 11:30 AM  
Women in Cyber Security  
Dialogue



**PHIL SUSMANN**  
President, Norwich University  
Applied Research Institutes  
(NUARI)  
MON OCT 26 - 12:00 PM  
Seminar: IT / OT / IoT  
Convergence



**JEREMY SWENSON**  
Senior Manager, USAA &  
Abstract Forward  
TUE OCT 27 - 8:20 AM  
10 Minute: Year in Review



**ROHIT TANDON**  
Assistant Commissioner,  
State Chief Information  
Security Officer, State of  
Minnesota, MN.IT Services  
TUE OCT 27, 7:30 AM  
Cyber Career Exploration  
TUE OCT 27, 7:30 AM  
Cyber Byte™ - Preparing for  
Multi-Domain Cyber Challenges



**DEREK THOMAS**  
Sr. Information Security  
Analyst, Target Corporation  
MON OCT 26 - 9:00 AM  
Workshop: Identifying  
and Analyzing Adversary  
Infrastructure and Malware



**TAREK TOMES**  
Chief Information Officer, State  
of Minnesota, MN.IT Services  
WED OCT 28 - 8:00 AM  
Cyber Byte™ - From Chaos to  
Clarity: Gaining Visibility and  
Control in Your Distributed  
Workforce



**KAT TRAXLER**  
Security Professional, Best  
Buy  
MON OCT 26 - 1:30 PM  
Tech Session 4B - A Bug  
Hunters Guide to GCP



**WADE VAN GUILDER**  
Principal Advisor,  
Cybersecurity SLED, World  
Wide Technology  
WED OCT 28, 4:40 PM  
Wrap Up & Practical  
Takeaways



**PAUL VEENEMAN**  
Vice President of Operations,  
MBA Engineering  
MON OCT 26 - 12:00 PM  
Seminar: IT / OT / IoT  
Convergence



**JITHESH VEETIL**  
Program Director (Data  
Science & Technology),  
Medical Device Innovation  
Consortium (MDIC)  
MON OCT 26 - 12:00 PM  
Seminar: Healthcare & Med  
Device



**PEKKA VEPSALAINEN**  
Cyber Security and GDPR  
Consultant, Entrepreneur,  
Tikkasec, Ltd.  
TUE OCT 27 - 11:30 AM  
International Breakout Part  
Two: Securing the Global  
Supply Chain through Red  
Team Analysis...



**TIM WAINWRIGHT**  
Chief Executive Officer,  
Security Risk Advisors  
MON OCT 26 - 1:30 PM  
Tech Session 4C - Purple  
Teams Best Practices,  
Metrics and Freeware



**MARK WEBBER**  
Vice President, Sales, Blue  
Ridge Networks  
MON OCT 26 - 12:00 PM  
Seminar: IT / OT / IoT  
Convergence



**ALEX WEINERT**  
Director of Identity Security,  
Microsoft  
WED OCT 28 - 10:15 AM  
Cyber Byte™ - Zero Trust -  
The Journey to Zero Trust



**CHRISTOPHER WILLIAMS**  
Regional Cloud Architect,  
Check Point Software  
Technologies, Ltd.  
MON OCT 26 - 12:30 PM  
Tech Session 3C - Are you  
finding your cloud a little  
too foggy?



**LYLE WRIGHT**  
Associate State Director at  
Minnesota Small Business  
Development Center, DEED  
TUE OCT 27 - 1:30 PM  
Small Business

# Save the Date!



11th Annual  
Cyber Security Summit  
Minneapolis, MN  
October 25-27, 2021

Join our newsletter for the latest information!  
[events.bizzabo.com/220749/page/1481018/  
subscribe-to-our-newsletter.](https://events.bizzabo.com/220749/page/1481018/subscribe-to-our-newsletter)



# Visionary Leadership Awards



This year's award winners are very special friends of the Summit. Amid a relentless pandemic, they have demonstrated greatness in securing our global infrastructure and developing future visionary leaders. And without their support, this 10th Anniversary would not have been possible. When so many were saying, "table it for another year," these cyber warriors kept pushing the Summit forward recognizing that cybercriminals weren't taking a break and that global thought leadership must never be sidelined.

While next year we will recognize award winners across all categories, this year we threw out the guidelines to honor this distinguished selection of leaders whose contributions to Summit have been immeasurable.

## 2020 Honorees



### JILL ALLISON

Chair, Board of Directors,  
WiCyS MN Affiliate;  
Security Consultant,  
Shuriken



### TIM CROTHERS

VP Security Solutions,  
Target



### DAVID LA BELLE

Security Business  
Systems Analyst, NorSec



### ANNE BADER

Founder, The International  
Cybersecurity Dialogue  
LLC



### LOREN DEALY MAHLER

President, Dealy Mahler  
Strategies



### DAVID NOTCH

Enterprise Security  
& Cloud Architecture,  
Medtronic



### SEAN COSTIGAN

Professor, George C.  
Marshall European Center  
for Security Studies;  
Director and Co-founder,  
ITL Security



### MATTHEW J. HARMON

Cyber Defense  
Infrastructure Architect,  
Global Technology,  
Accenture Security



### CATHARINE TREBNICK

VP Equity Research  
(Security and UCaaS),  
Colliers International

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.

## Only the Transformational Will Survive

by George Kurtz, CEO, CrowdStrike



**CROWDSTRIKE**



The title of this article might seem harsh, but in today's world we are in uncharted territory and the cold reality is that the strongest will survive and thrive, but they must transform first. If you talk to many CEOs and CIOs these days — and I do — you're probably hearing a lot about digital transformation.

That's good, because there's a lot to say. My only word of advice to these leaders is, before you pull the trigger on a major digital transformation initiative, you need to transform your security first.

The global pandemic has profoundly affected businesses that rely on people leaving the shelter of their homes, gathering together in large groups or generally doing things that put individuals at risk of coming into contact with other humans. That describes pretty much every business and workplace in the world — or at least it did.

Social distancing and shelter-at-home policies have forced nearly all organizations to redistribute their workforce and seek new ways to survive and thrive in a primarily online work environment. The sudden move to a "work from anywhere" economy has been a massive driver and accelerator for digital transformation in private and public sectors globally. On its [COVID-19 resource center webpage](#), industry analyst firm IDC states, "The pandemic underscored the importance of digital transformation in the eyes of CEOs who now find themselves at a decision point — to follow the same course of cost cutting as previous recessions have dictated — or to flatten their own organization's recessionary curve by leveraging technology."

### Instant Transformation

Typically, massive transformations don't occur overnight. Only in the movies. But in the case of COVID-19, government and business leaders had to act fast. It was literally a life or death decision. Many companies that had digital transformation strategies in place had to radically compress the rollout of these scenarios, from months and years to days and weeks. In large part, the transformative activity has focused on accelerated adoption of the cloud to replace outdated on-premises technologies. The ones who have been able to negotiate this pivot successfully, experiencing the least downtime, disruption and devaluation, have tended to be the ones that already accomplished a different type of transformation: a security transformation.

### Shedding Light on Dark Times

CrowdStrike saw the global threat landscape take a dark turn earlier this year. As the pandemic moved out and across new geographies, we could clearly see increased threat levels — attempted intrusions, [ransomware attacks](#) and other malicious activities — moving in lockstep with the progression of the disease itself. The threat actors we track so assiduously were unrelenting in their efforts to prey on the fears of the populace and profit from the misery of others.

By and large, [our customers](#) recognized the magnitude of those threats, and we found ourselves working feverishly to help modernize and streamline their security infrastructures to pave the way for — and coincide with — their fast-tracked digital transformation plans. Even organizations that until a few years ago still considered the term "[cloud security](#)" to be an oxymoron were plunging ahead into those uncharted waters, trusting CrowdStrike's unique [cloud-native security platform](#) to keep them and their newly distributed workforce safe. I'm proud to say we did not let them down.

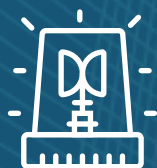
### Transform Securely

History will judge us by the way we respond to today's extraordinary challenges, and to paraphrase Winston Churchill, history isn't always written by the victors — but it's definitely written by the survivors. I believe the organizations that not only survive but actually thrive in this current environment will be the ones that seize the opportunity to jettison their obsolete on-premises architectures and applications, and fully commit to the cloud. Just remember, for your digital transformation to succeed, you must transform your security, too.

The CEO and co-founder of CrowdStrike, George Kurtz is an internationally recognized entrepreneur, security expert, author, and speaker. He has more than 26 years of experience in the cybersecurity field, driving revenue growth and scaling organizations across the globe, most recently leading CrowdStrike's IPO. Co-author of the all-time best-selling "[Hacking Exposed](#)" book series, Kurtz has been quoted or featured in many major publications, media outlets, and television programs including CNN, Fox News, ABC World News, Bloomberg, CNBC, New York Times, USA Today, Wall Street Journal, The Washington Post, Associated Press, Network World, and many others. He also authored the best-selling security book of all time, [Hacking Exposed: Network Security Secrets & Solutions](#).

[crowdstrike.com/summit](https://crowdstrike.com/summit)





**90%**

of CXOs reported an increase in cyberattacks since the world stayed home.



Tanium helps you take control of  
endpoint environment and address the  
root cause of endpoint risk.

LEARN MORE AT  
<https://world-at-home.tanium.com/>





Supporter

1Password is the world's most-loved password manager. By combining industry-leading security and award-winning design, the company provides private, secure, and user-friendly password management to businesses and consumers globally. More than 60,000 business customers, including IBM, Slack, PagerDuty, Dropbox, GitLab, and Roche, trust 1Password as their enterprise password manager.

[1password.com/press](https://1password.com/press)



TC3 Collaboration

Best Buy Co., Inc. is an American multinational consumer electronics retailer headquartered in Richfield, Minnesota. It was originally founded by Richard M. Schulze and James Wheeler in 1966 as an audio specialty store called Sound of Music.

[www.bestbuy.com](https://www.bestbuy.com)



Supporter

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

[hwww.bcpa.org](https://hwww.bcpa.org)



TC3 Collaboration

The 3M Company is an American multinational conglomerate corporation operating in the fields of industry, worker safety, US health care, and consumer goods.

[www.3m.com](https://www.3m.com)



IT/OT/IoT Host

Blue Ridge Networks delivers network segmentation, remote access, and endpoint cybersecurity solutions that eliminate vulnerabilities and prevent exfiltration of data. The company has provided resilient, scalable, and affordable cybersecurity systems, software, and managed services for over 20 years, protecting government and enterprise customers with no reported breaches of its solutions.

[www.blueridgenetworks.com](https://www.blueridgenetworks.com)



TC3 Collaboration

Located globally, impacting locally.

Cargill provides food, agriculture, financial and industrial products and services to the world. Together with farmers, customers, governments and communities, we help people thrive by applying our insights and 150 years of experience. We have 155,000 employees in 70 countries / regions who are committed to feeding the world in a responsible way, reducing environmental impact and improving the communities where we live and work.

[www.cargill.com](https://www.cargill.com)



Platinum

Arctic Wolf® is the market leader in security operations, and provides security operations as a concierge service. Our security experts work as an extension of your team to monitor and detect threats, and continually strengthen your security posture.

[arcticwolf.com](https://arcticwolf.com)



Small Business Host

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.

[www.bremer.com](https://www.bremer.com)



Ruby

Check Point Software Technologies is a leading provider of cyber security solutions that protects customers from 5th generation cyber-attacks with an industry leading catch rate of malware, ransomware and other types of attacks. We offer multilevel security architecture which defends enterprises' cloud, network and mobile device held information.

[www.checkpoint.com](https://www.checkpoint.com)



# THE MARKET LEADER IN SECURITY OPERATIONS

## Strengthening your security posture through:

- ▶ Agnostic, cloud-native technology platform
- ▶ MDR, managed vulnerability assessment, and cloud monitoring
- ▶ Delivered by our Concierge Security® Team

[arcticwolf.com](https://arcticwolf.com)





Cybersecurity needs to clear a path and protect your business without getting in the way. The Cisco Secure platform simplifies your experience, accelerates your success, and secures your future. Protect what's now and what's next with the most comprehensive integrated cybersecurity platform on the planet.

[www.cisco.com/c/en/us/products/security/index.html](http://www.cisco.com/c/en/us/products/security/index.html)



CrowdStrike® Inc. (Nasdaq: CRWD), a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. CrowdStrike Falcon correlates over 3 trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security. There's only one thing to remember about CrowdStrike: We stop breaches.

[crowdstrike.com/summit](http://crowdstrike.com/summit)



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

[www.csamn.com](http://www.csamn.com)



FireEye is the leader in intelligence-led security-as-a-service. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence, and world-renowned Mandiant® consulting. FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent, and respond to cyber-attacks.

[www.fireeye.com](http://www.fireeye.com)



We are a leading global manufacturer and marketer of branded consumer foods sold through retail stores. We manufacture our products in 13 countries and market them in more than 100 countries. Over the years, we've continued to adapt and evolve our portfolio to serve our consumers and drive growth. We're proud of the portfolio we've built, highlighted by eight iconic brands that each represent more than \$1 billion dollars in retail sales worldwide.

[www.generalmills.com](http://www.generalmills.com)



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.

[www.globalminnesota.org](http://www.globalminnesota.org)



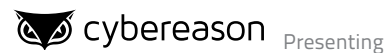
Carlson Wagonlit Travel (CWT) is a privately held travel management company wholly owned by Carlson managing business travel, meetings and events for companies and governments. CWT is a global leader in the travel industry attaining over \$23B in transaction volumes in 2017 with over 18,000 employees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

[www.carlsonwagonlit.com](http://www.carlsonwagonlit.com)



The Crypsis Group is a security advisory firm focused on data breach response and risk management, supporting our clients as a trusted security advisor before, during, and after a breach. The combination of our deep security knowledge and proprietary technology allows us to rapidly identify, contain, and eradicate attacks for organizations.

[www.crypsisgroup.com](http://www.crypsisgroup.com)



Cybereason is the world's most powerful cybersecurity analytics platform, built from the ground up, to secure your enterprise. Our full-stack, behavior-based hunting system analyzes more data, more deeply, than anyone else on the market — giving you unprecedented visibility and the power to stay one step ahead of the ever-evolving threat. EDR | MDR | NGAV | 24x7 MONITORING & RESPONSE | IR SERVICES

<https://www.cybereason.com>



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.

[www.h-isac.org](http://www.h-isac.org)



Illusive Networks empowers organizations to eliminate high-risk pathways to critical systems, detect attackers early in the attack process, and capture real-time forensics to focus and accelerate incident response and improve resilience. This agentless technology, offers a simple solution for organizations to continuously improve their cyber risk posture and function with greater confidence.

[www.illusivenetworks.com](http://www.illusivenetworks.com)



MN 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. We accomplish this by providing educational forums, publications, and peer interaction opportunities to enhance knowledge, skills, and professional growth.

[mn.issa.org](http://mn.issa.org)



At CyberNINES, we not only provide assessment, security and protection services from cybersecurity threats for small and medium sized businesses, we offer you Compliance Without Complexity™. Our customized, cost-effective turnkey program to managing and maintaining your cybersecurity compliance for regulatory purposes.

<https://cybernines.com/>



Career focused and student centered. Dunwoody's Computer Technology programs prepare tomorrow's professionals to be leaders in the rapid-change world of IT. Students learn hands-on in courses created in partnership with industry. Training in computer networking and web development, along with stackable degree options, allow students to grow in their profession.

<http://www.dunwoody.edu/computer>



Exabeam is the Smarter SIEM(TM) company. We help security teams work smarter, allowing them to detect, investigate and respond to cyberattacks in 51 percent less time. With the modular Exabeam Security Management Platform, analysts can collect unlimited log data, use behavioral analytics to detect attacks, and automate incident response.

[www.exabeam.com](http://www.exabeam.com)



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.

[www.infragard.org](http://www.infragard.org)



Insight's Cloud + Data Center Transformation is a complete IT services and solution provider that helps organizations transform technology, operations, and service delivery to meet challenges and future-proof the business. As a client-focused integrator, we're free to recommend the most appropriate solutions — across cloud, IT transformation, next-generation technology, and security.

[www.insight.com/en\\_US/home.html](http://www.insight.com/en_US/home.html)



With approximately 1200 members from over 100 organizations, the Minnesota chapter of ISACA provides a gateway to a global organization offering security, risk, control, and governance certifications. Additionally, ISACA offers a new security knowledge platform and professional Cybersecurity certification program (CSX) for both students and recent grads (Fundamental) as well as those with experienced skillsets (Practitioner.) For more information please visit the chapter website.

[mnisaca.org](http://mnisaca.org)





Diamond

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

[www.kudelskisecurity.com](http://www.kudelskisecurity.com)



IT/OT/IoT Supporter

MBA Engineering applies industry and regulatory standard Security Control frameworks, Defense-in-Depth and Zero-Trust methodologies to deliver cyber security strategies, solutions and a comprehensive approach to securing Industrial Controls, Operations Technology and Industrial IoT environments, mitigating the high-level risk of today's sophisticated and prolific cyber-attacks against the nation's critical infrastructure.

[www.mbaengineering.biz](http://www.mbaengineering.biz)



Supporter

Founded in 1984, the Medical Alley Association supports and advances the global leadership of Medical Alley's healthcare industry, and its connectivity around the world. The Medical Alley Association delivers the collective influence, intelligence, and interactions that support Medical Alley, The Global Epicenter of Health Innovation and Care™.

[medicalalley.org](http://medicalalley.org)



Healthcare &amp; Med Device Host

Maslon LLP offers skilled cybersecurity counsel 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 cybersecurity summits. We will assess your cybersecurity risk profile and provide practical advice to sustain a legally reasonable cybersecurity strategy.

[www.maslon.com](http://www.maslon.com)



Supporter

Mattermost, Inc. is a company based on the Mattermost open source project, which is a messaging collaboration platform for team communication across mobile, web and PC with instant search, continuous archiving and unlimited integrations. Mattermost software is used by thousands of organizations around the world in 16 languages.

[mattermost.org](http://mattermost.org)



Healthcare &amp; Med Device Supporter

MedCrypt gives medical device vendors access to advanced cybersecurity features in a few lines of code. Vendors used to ship a device, hope that there were no cybersecurity issues, and address problems as they were found. Today, leading device vendors proactively secure devices and win market share as a result.

[www.medcrypt.com](http://www.medcrypt.com)



Supporter

MDMA is a national trade association that provides educational and advocacy services to medical device innovators. For over 25 years, MDMA has represented the industry in DC and beyond and provided professional development services to member company personnel ranging from small innovators to the largest device companies in the world.

[www.medicaldevices.org](http://www.medicaldevices.org)



TC3 Collaboration

Medtronic plc is a medical device company that generates the majority of its sales and profits from the U.S. healthcare system but is headquartered in the Republic of Ireland for tax purposes.

[www.medtronic.com/us-en/index.html](http://www.medtronic.com/us-en/index.html)



Education

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

[www.metrostate.edu](http://www.metrostate.edu)

## CISCO SECURE

# Securing Telemedicine in a Post-COVID World

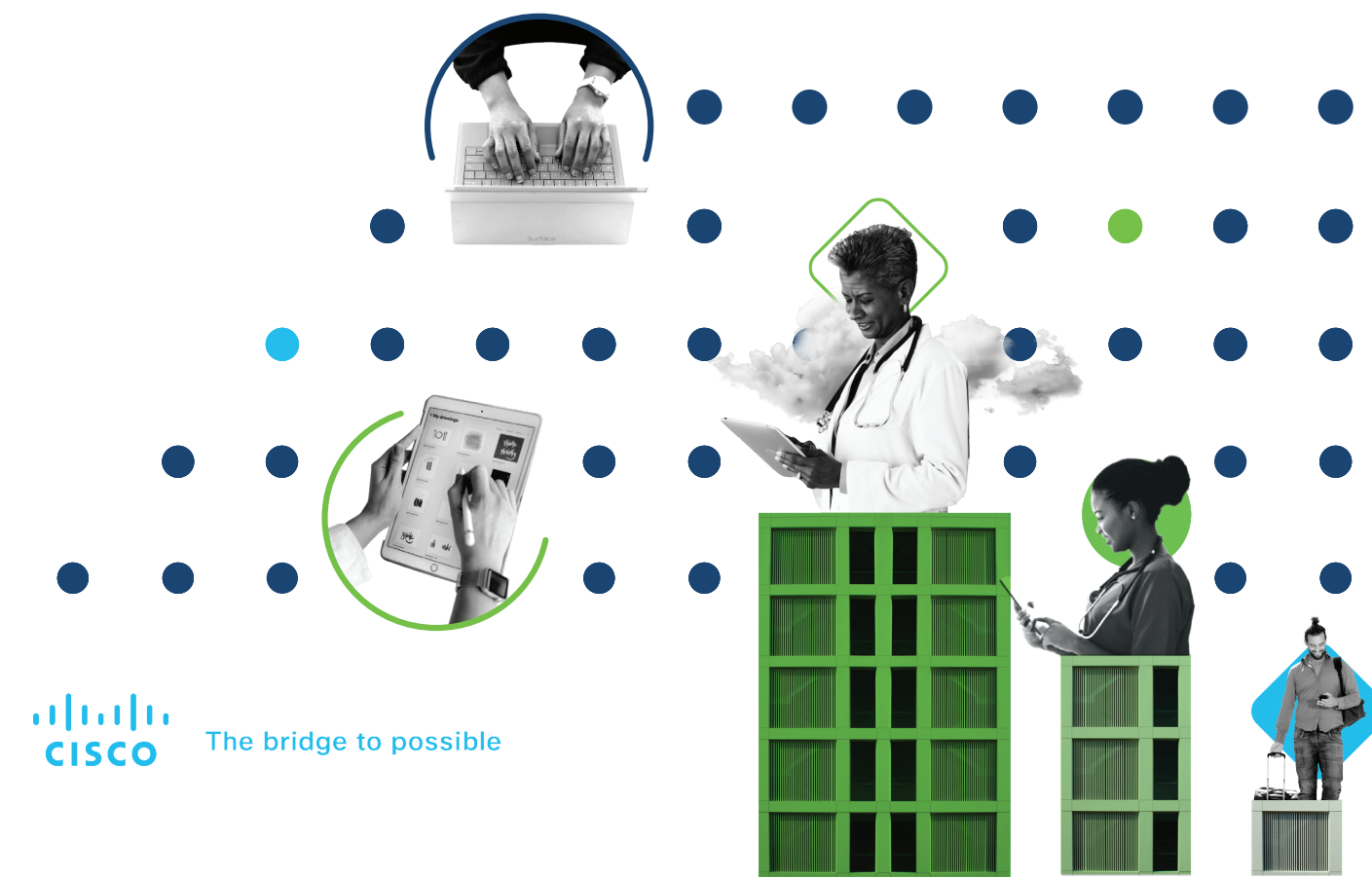
Join our session to learn how to prepare for a bright future of secure, connected health

Seminar: Healthcare & Med Device  
Monday, October 26, 12:30–1 p.m.



Speaker:

Steve Caimi

Cybersecurity Specialist  
Cisco





Ruby

Microsoft's mission is to empower every person and organization on the planet to achieve more. With \$1 trillion lost annually to cyberattacks, security and risk management are essential to digital transformation. Harnessing the power of the cloud and our operations expertise, we solve customer challenges across security, compliance, and identity.

[aka.ms/security](https://aka.ms/security)



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](https://mn.gov/mnit)



Supporter

Minnesota Lawyer provides the latest legal news and information for the legal community in Minnesota. Supreme Court case digests, expert testimony, bar buzz, people and practices, and case studies keep you informed. New attorneys receive a complimentary 4 week trial. To begin receiving your free subscription email [dehrler@bridgetowermedia.com](mailto:dehrler@bridgetowermedia.com).

[minnlawyer.com](https://minnlawyer.com)



Diamond

Ordr is IoT device security made simple. Ordr discovers every connected device, profiles device behavior and risks, and then automates response through dynamic policy generation and segmentation. Organizations use Ordr to understand risks, bring devices into compliance, and support device procurement decisions.

[www.ordr.net](https://www.ordr.net)



Platinum

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life.

[www.paloaltonetworks.com](https://www.paloaltonetworks.com)



Ruby

Saviynt offers complete access governance and intelligence solutions for critical Data, Workloads, DevOps Resources, and Access to critical applications on Cloud and Enterprise. Saviynt combines granular application access, risk and usage analytics, real-time prevention with out-of-box risk signatures and SOD rules to address security & compliance needs for the enterprise.

[saviynt.com](https://saviynt.com)



Supporter

We believe Minnesota's technology-driven companies achieve the greatest success when they have access to exceptional talent, dedicated public policy advocates, and are part of an innovative, inclusive technology community. For more than 30 years, the Minnesota Technology Association has helped nurture each of these attributes within our state, enabling Minnesota technology-driven businesses, professionals, and communities to thrive.

[mntech.org](https://mntech.org)



Face Mask

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.

[www.navilogic.com](https://www.navilogic.com)



Ruby

NetSPI is the leader in enterprise security testing and vulnerability management. Our experts perform deep dive manual penetration testing of application, network, and cloud attack surfaces. We find vulnerabilities that others miss and deliver clear, actionable recommendations allowing our customers to find, track, and fix their vulnerabilities faster.

[www.netspi.com](https://www.netspi.com)



Supporter

The Minnesota Small Business Development Center (MnSBDC) network philosophy is based on the principle that helping our small businesses is critical to our economy and the quality of our communities. The MnSBDC offers customized technical assistance and support at no cost, to businesses at any point in their entire life cycle, from start-up to growth to exit strategies.

[www.mn.gov/deed/business](https://www.mn.gov/deed/business)



Ruby

Security Risk Advisors delivers technology security services and provides cybersecurity expertise to Fortune and Global 1000 companies. We have extensive experience working in partnership with CIOs, CISOs and IT Audit. Our approach emphasizes training and knowledge transfer to our clients, to help them sustain strengthened security management processes.

[sra.io](https://sra.io)



Ruby

Securonix is redefining SIEM for today's hybrid cloud, data-driven enterprise. Built on big data architecture, Securonix delivers SIEM, UEBA, SOAR, Security Data Lake, NTA, and vertical-specific applications as a pure SaaS solution with unlimited scalability and no infrastructure cost. Securonix reduces noise, prioritizes high fidelity alerts, and detects and responds to advanced insider and cyber threats with behavioral analytics technology that pioneered the UEBA category.

[www.securonix.com](https://www.securonix.com)



Supporter

The NorSec Foundation was established with the goal of advancing cyber security education in corner stores and board rooms alike, empowering them to make sound security decisions. Our mission is to facilitate research and development of tools and techniques that support the whole cyber security industry

[www.norsec.org](https://www.norsec.org)



IT/OT/IoT Supporter

NUARI provides cyber security exercises, secure network monitoring, custom consulting, research, and education on critical national security issues. We do this through our DECIDE platform, our SOC, rapid technology development and deployment, production of research deliverables, and in-person and online cyber workforce training around the globe.

[nuari.net](https://nuari.net)



TC3 Collaboration

Optum, a part of UnitedHealth Group, is a pharmacy benefit manager and care services group operating across 150 countries in North America, South America, Europe, Asia Pacific and the Middle East.

[www.optum.com](https://www.optum.com)



Supporter

The U.S. Small Business Administration makes the American dream of business ownership a reality. It provides small businesses resources and support to start, grow, expand and recover. Services are delivered through an extensive network of SBA field offices and partnerships with public and private organizations.

[www.sba.gov](https://www.sba.gov)



In-house Legal Host

Taft is a modern law firm with more than 600 attorneys who have been delivering exceptional legal services since 1885. The firm's award-winning team represents virtually every area of law. As the employer of choice, Taft offers a one-class partnership and decentralized leadership structure in its 11 offices.

[www.taftlaw.com](https://www.taftlaw.com)



Presenting

Tanium provides unified endpoint management and security built for the world's most demanding IT environments. Our breakthrough approach decentralizes data collection, aggregation and distribution down to the endpoint, dramatically reducing direct client-to-server communications to deliver transformational scale, speed, and reliability. This is why the world's most sophisticated organizations — including nearly half of the Fortune 100 — trust Tanium to help them confidently manage performance, detect and respond to threats, and ensure compliance across their operations.

[www.tanium.com](https://www.tanium.com)





TC3 Collaboration

Minneapolis-based Target Corporation (NYSE: TGT) serves millions of guests at stores and at Target.com. Investing in our communities has always been and continues to be a cornerstone of our company. It's why, since 1946, Target has invested 5 percent of our profit to communities where our guests and team members live, work and play. For more information, visit Target.com/Pressroom. For a behind-the-scenes look at Target, visit Target.com/abulleyview or follow @TargetNews on Twitter.

[corporate.target.com/press](https://corporate.target.com/press)



THOMSON REUTERS

TC3  
Collaboration

Thomson Reuters is one of the world's most trusted providers of answers, helping professionals make confident decisions and run better businesses. Our customers operate in complex arenas that move society forward — law, tax, compliance, government, and media — and face increasing complexity as regulation and technology disrupts every industry.

[www.thomsonreuters.com/en.html](https://www.thomsonreuters.com/en.html)



Supporter

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](https://wicysmn.org)

TECHNOLOGICAL  
LEADERSHIP INSTITUTEFounding  
Partner

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

[tli.umn.edu](https://tli.umn.edu)



United in security leadership

Supporter

UMSA (Upper Midwest Security Alliance) is a nonprofit alliance of security and risk-related organizations that serves business, government and education professionals in the upper Midwest, collaborating with professional associations, educators and industry-leading companies to provide professional development opportunities that contribute to a stronger security foundation for organizations. UMSA is the host of the Secure360 Conference in the Twin Cities as well as the annual Student360 event.

[umsa-security.org](https://umsa-security.org)

World Wide Technology

Silver

World Wide Technology can provide complete turnkey implementation solutions including network design, staging and burn-in of new equipment, site preparation, equipment configuration and installation, initial training, de-installation, consulting and follow-on support as required.

[www.wwt.com](https://www.wwt.com)



TC3 Collaboration

The Twin Cities Cybersecurity Collaboration (TC3) is a partnership between leading cybersecurity programs that work together to build the talent pipeline and foster the next generation of cybersecurity professionals in the Twin Cities. Thanks to TC3's generous support of the Summit this year, the Monday Technical Sessions will be complimentary and more robust than ever.

UNISYS | Securing Your  
Tomorrow™

Printing

Unisys is a global information technology company that works with many of the world's largest companies and government organizations to solve their most pressing IT and business challenges. Unisys specializes in providing integrated, leading-edge solutions to clients in government, financial services and commercial markets. With more than 20,000 employees serving clients around the world, Unisys offerings include cloud and infrastructure services, application services, security solutions, and high-end server technology.

[www.unisys.com](https://www.unisys.com)



Event Producer

The Event Group, Incorporated, based in Minneapolis, MN, is a full-service event production and marketing agency focused on corporate events, global marketing, production, and strategic planning. The Event Group provides a fresh, innovative approach, blending its enthusiasm and expertise with your corporate objectives, resulting in strategic ROI — all executed brilliantly!

[www.plantoastound.com](https://www.plantoastound.com)

## The Distributed Endpoint Crisis: A Blessing in Disguise



www.tanium.com

Endpoints matter to every company in Minnesota.

This state is home to many large, renowned companies — including 16 companies on the FORTUNE 500 list. These companies represent every major global industry — from healthcare, to manufacturing, to retail. And each of these companies, in each of these industries, now runs on one thing — endpoints.

Endpoints power their employee productivity. Endpoints drive their customer experience.

And in 2020, a flood of diverse, and distributed endpoints allowed these companies to keep the lights on right when the foundations of their day-to-day operations were shattered by crisis. But even though new endpoints have become the driving force behind the operations for many companies, IT leaders still struggle to manage and secure them.

In this short piece, we will explore the endpoint challenges these IT leaders have faced over the past six months, and why these challenges might actually be a blessing in disguise.

### What Happened: Companies Lost Control

Nobody saw it coming.

The pandemic struck. Companies were forced to send their employees home. Employees began to work from a diverse, distributed set of endpoints. And, overnight, most organizations began to operate a radically new endpoint environment — one that many IT leaders were unprepared to manage and secure.

In a recent survey, 85 percent of IT leaders thought they were ready to make this overnight transition, but 98 percent experienced at least one major security challenge along the way.

These challenges included:

- Identifying new personal computing devices on their network.
- Performing patching and vulnerability scans on remote devices.
- Managing overwhelming VPN capacity and requirements.

Each of these challenges — and many more like them — revolved around a single central issue: Many IT leaders found that they could not maintain visibility and control over an endpoint environment that was more diverse and distributed than they were used to.

And this issue created some serious consequences.

More than 93 percent of the report's respondents were forced to delay or cancel security priorities during their transition to a distributed workforce — right at the same moment 90 percent of these respondents experienced an increased frequency of attacks.

We don't know how many of these attacks were successful. We don't know how many companies are continuing to operate without visibility and control over their new endpoint environments.

But we do know one thing.

As bad as these last six months have been for some IT leaders, they might have been a blessing in disguise. The pandemic has

revealed endpoint management and security challenges that IT leaders would have been forced to face even if COVID-19 never occurred. And it's given IT leaders a chance to solve these challenges before they truly blew up.

### The Blessing in Disguise: Getting Ahead of the Distributed Endpoint Issue

Diverse, distributed endpoint environments have been the face of the future for some time now, due to a few trends that have nothing to do with COVID-19.

**First, remote work** was already expanding for many companies. They just didn't anticipate the scale and speed of adopting a primarily WFH workforce.

**Second, customer demand** has already been shifting to remote, internet-first services for years, if not decades, and continues to accelerate in that direction.

**Third, new technologies** — from Cloud computing to 5G — were already giving companies an explosion of diverse, distributed endpoints to deal with.

Each of these trends began long before the pandemic struck, and they will last long after the pandemic passes. Each speaks to a far more foundational set of transformations that are occurring within most companies and industries.

And each of these trends have already been quietly transforming some of Minnesota's biggest industries, and will continue to transform them for decades to come.

Consider just a few examples:

**Healthcare:** Patients are demanding more and more telemedicine services, while connected devices are revolutionizing patient care and experiences.

**Retail:** Customers are demanding omnichannel retail, driving the need for scalable eCommerce operations, inventory management and mobile POS.

**Manufacturing:** Factories, warehouses and transportation systems are already filled with operational technology and IoT devices that will really scale when 5G truly arrives.

In short: Large-scale, diverse, distributed endpoint environments have been inevitable for some time now.

Yes, recent events have accelerated this move. But sooner or later, IT leaders would have had to make it anyway. And when they did, they would have experienced the same challenges managing and securing those environments as they experienced over the last six months — but at, perhaps, and even greater scale.

In that way, the last six months have been a harsh but necessary wakeup call for IT leaders. The pandemic has alerted IT leaders to gaps in their ability to manage and secure the operational environment of the future. And it has given them a chance to fill these gaps before diverse, distributed endpoints become truly everywhere — and the consequences of losing visibility and control over those endpoints would be an even bigger crisis.



# 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.

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

With a record **8.4 billion security breaches** in the first quarter of 2020 alone, the need for cybersecurity professionals is greater than ever. Gain skills from industry leaders to protect the information and systems our communities rely on with a **graduate minor in cyber security from the Technological Leadership Institute (TLI)** at the University of Minnesota. Cyber minor courses are open to both UMN students and non-degree seeking professionals.

Contact MSST admissions at [msst@umn.edu](mailto:msst@umn.edu) for more info or visit us at [tli.umn.edu](https://tli.umn.edu).

# BIG IDEAS BIG EVENTS

In our increasingly connected and digital world, there's still no better way to communicate your message than face to face. We make even small events feel big and specialize in bringing people together to share innovative ideas. Let us help you that your gathering to the next level.

We don't just plan events.  
We plan to astound.



[www.plantoastound.com](https://www.plantoastound.com)



**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.

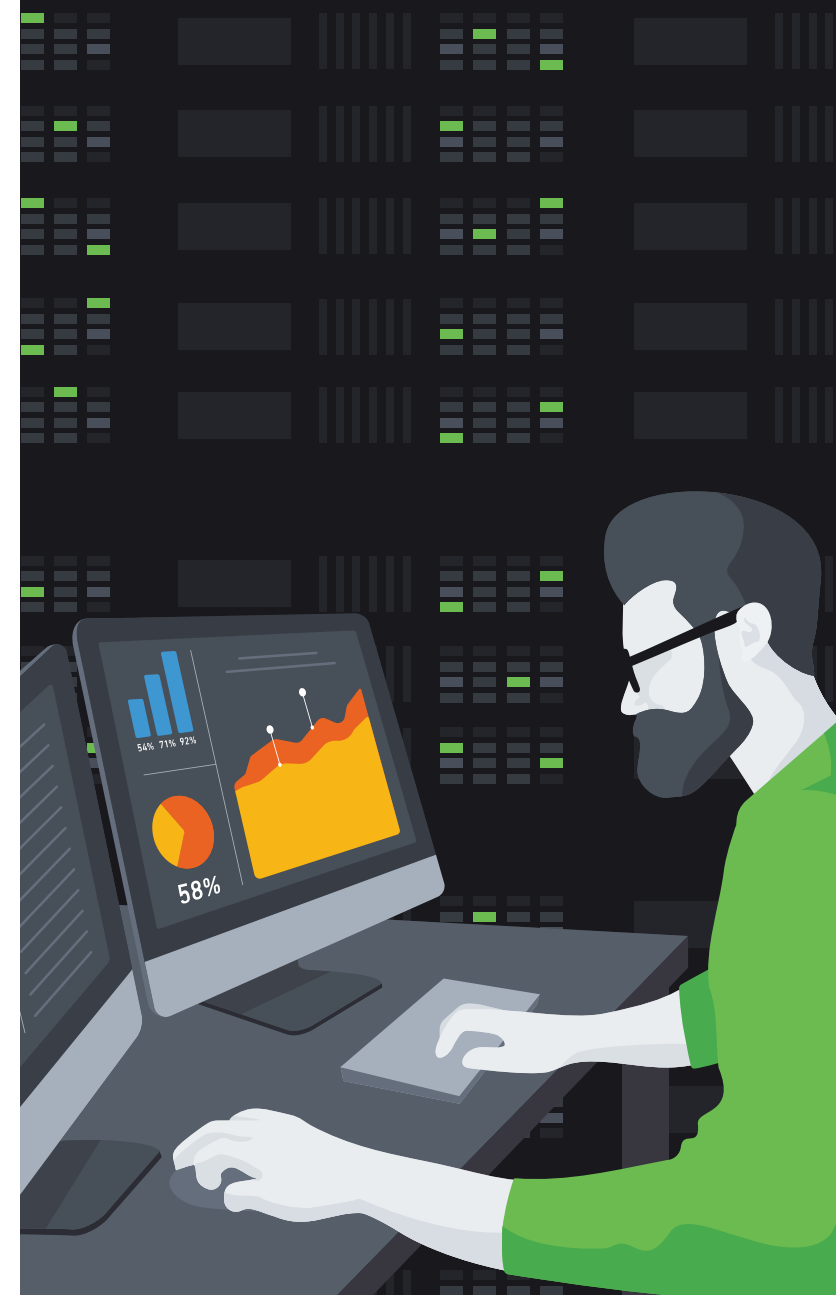
# SMARTER SIEM = Smarter SOC

## Modernize your SOC with Advanced Analytics

Add intelligence to your existing security investments to detect compromised credentials and insider threats, and to add context to alerts from your security applications.

- Augment your SIEM with advanced analytics
- Improve visibility into lateral movement
- Make faster decisions with actionable insights

Work smarter with Exabeam. Learn more at [www.exabeam.com](http://www.exabeam.com).

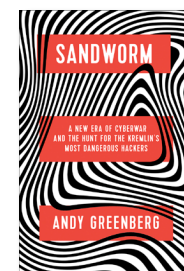




# Cyber Security Acronyms

3DES	Triple Data Encryption Standard	MAN	Metropolitan Area Network
ACL	Access Control List	NAT	Network Address Translation
ADP	Automated Data Processing	NetBIOS	Network Basic Input/Output System
AES	Advance Encryption Standard	NIC	Network Interface Controller or Network Interface Card
AH	Authentication Header	NIAP	National Information Assurance Partnership
AIS	Automated Information System	NIST	National Institute for Standards and Technology
AO	Area of Operations	NNTP	Network News Transfer Protocol
APT	Advanced Persistent Threat	OpSec	Operational Security
BCP	Business Continuity Plan	OS	Operating System
BIA	Business Impact Analysis	OSI	Open Systems Interconnect
BoD	Beginning of Day	OWASP	Open Web Application Security Project
BYOD	Bring Your Own Device	PaaS	Platform as a Service
CA	Certificate Authority	PIN	Personal Identification Number
CIO	Chief Information Officer	PKI	Public Key Infrastructure
CISO	Chief Information Security Officer	POTS	Plain Old Telephone Service
CSO	Chief Security Officer	PSTN	Public Switched Telephone Network
CAPEC	Common Attack Pattern Enumeration and Classification	RA	Registration Authority
CERT	Computer Emergency Response Team	RAS	Remote Access Service
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 Act	SET	Social-Engineer Toolkit
FTP	File Transfer Protocol	SFA	Single Factor Authentication
FO	Forward Observer	SLA	Service Level Agreement
GRC	Governance Risk Management and Compliance	S/MIME	Secure Multipurpose Internet Mail Extension
HIPAA	Health Insurance Portability and Accountability Act	SMTTP	Simple Mail Transfer Protocol
HTTP	Hypertext Transfer Protocol	SoD	Segregation/Seperation of Duties
HTTPS	Hypertext Transfer Protocol Secure	SoD	Start of Day
IDS	Intrusion Detection System	SPX	Sequenced Packet Exchange
IaaS	Infrastructure as a Service	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	Temperal 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	Vitrual 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		XSS	Cross-site Scripting
Address	Media Access Control		

## 2020 Summit Recommended Reading



*Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*

by Andy Greenberg  
October release

Buy on Amazon at:

[www.amazon.com/Sandworm-Cyberwar-Kremlins-Dangerous-Hackers/dp/0385544405](https://www.amazon.com/Sandworm-Cyberwar-Kremlins-Dangerous-Hackers/dp/0385544405)

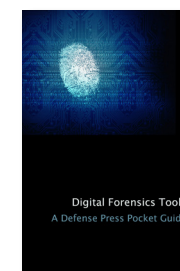


*THE GREAT REBOOT: Succeeding In A World Of Catastrophic Risk And Opportunity*

by Chris Veltsos, Bob Zukis, Paul Ferrillo  
Just released

For more info and to buy on Amazon, visit

[www.thegreatreboot.info](https://www.thegreatreboot.info)



*Digital Forensics Tools:*

Coming soon from our partner, Defense Press  
November release

[www.defensepress.com](https://www.defensepress.com)



*American Cyberspace*

by Major General Mari K. Eder

October release



*Weekly International Cybersecurity Briefing*

by Anne C. Bader and Richard Stiennon

[www.cybersecuritydialogue.org](https://www.cybersecuritydialogue.org)

# SECURE360

REGISTRATION IS NOW OPEN!

May 11-12, 2021  
Mystic Lake Event Center  
Prior Lake, MN

REGISTER TODAY:  
[Secure360.org/Secure360-Twin-Cities](https://Secure360.org/Secure360-Twin-Cities)

80+ sessions

90+ exhibitors

800+ attendees





## Cybereason's nocturnus researchers discover a new cyber threat against UK and European Union financial technology companies

Sep 3, 2020

Cybereason, a leader in endpoint security, today unveiled new research from its Nocturnus Research team, titled [No Rest for the Wicked: EvilNum Unleashes PyVil RAT](#). The research details a new targeted and widespread threat against UK and European Union financial technology companies by the EvilNum APT Group. Cybereason researchers also discovered PwVil, a new Python-scripted Remote Access Trojan (RAT), being deployed to steal passwords, documents, browser cookies and email credentials.

Nocturnus discovered EvilNum using several new tricks to deploy the PwVil RAT malware, including a significant deviation from previously observed tools, from the infection chain through persistence and infrastructure, including:

- Modified versions of legitimate executables employed in an attempt to remain undetected by security tools.
- Infection chain shift from a JavaScript Trojan with backdoor capabilities to a multi-process delivery procedure of the payload.
- The new Python-scripted RAT dubbed PyVil RAT was compiled with py2exe, which has the capability to download new modules to expand functionality.

"The EvilNum group is continuing the time-tested infection method of using phishing emails to infect enterprises. Enterprises need to constantly evolve

their security stack to enable easier discovery and remediation of threats. The employees of enterprises shouldn't open email attachments from unknown sources and should avoid downloading information from dubious websites," said Tom Fakterman, Threat Researcher, Cybereason.

For a copy of the EvilNum research, visit: <https://www.cybereason.com/blog/no-rest-for-the-wicked-evilnum-unleashes-pyvill-rat>

### About Cybereason

Cybereason, creators of the leading Cybereason Defense Platform, gives the advantage back to the defender through a completely new approach to cybersecurity. Cybereason offers endpoint prevention, detection and response and active monitoring. The solution delivers multi-layered endpoint prevention by leveraging signature and signatureless techniques to prevent known and unknown threats in conjunction with behavioral and deception techniques to prevent ransomware and fileless attacks. Cybereason is a privately held, international company, headquartered in Boston, MA with customers in more than 30 countries.

Learn more: <https://www.cybereason.com>  
Follow us: [Blog](#) | [Twitter](#) | [Facebook](#)

## New in 2020

### International Webinar Series



**CYBER SECURITY**  
Summit  
*Security solutions through collaboration.*

In today's ever-evolving threat landscape, strengthening our global connections has never been more important. That's why this summer, we embarked on a monthly webinar series that examined some of the critical issues we will address during the Summit's international 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 international 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; Director and Co-Founder, ITL Security

**INTERNATIONAL  
WEBINAR  
SERIES**



### What you missed...

#### JULY WEBINAR The New Data Privacy Norm



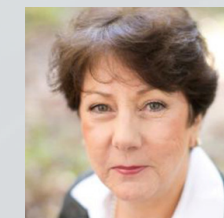
**CHRISTEL CAO-DELEBARRE**  
Global Privacy Officer  
CWT, London Office

#### AUGUST WEBINAR The Nexus of Cybersecurity and Disinformation



**DANIEL BAGGE**  
Cyber Attaché of the Czech Republic to the U.S. and Canada, National Cyber and Information Security Agency

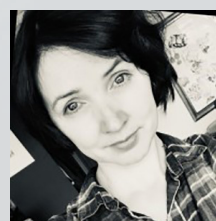
#### SEPTEMBER WEBINAR Cybersecurity Successes and Failures – How Public Institutions Can Do Better



**MAJOR GENERAL  
MARI K. EDER**  
(USA Ret.)

### Upcoming...

#### NOVEMBER WEBINAR Cyber Norms in a Changing World



**DR. ENEKEN TIKK**  
Executive Producer at the Cyber Policy Institute

To get involved, contact:

**EILEEN MANNING**

Executive Producer  
Cyber Security Summit  
612-308-1907

[eileen.manning@cybersecuritysummit.org](mailto:eileen.manning@cybersecuritysummit.org)

Sponsored by



For updated information and to register for upcoming webinars, visit  
[cybersecuritysummit.org/international-webinar-series](https://cybersecuritysummit.org/international-webinar-series)





## **INTELLIGENCE-LED SECURITY**

using a single platform that blends:

- **Innovative technologies**
- **Nation-state grade threat intelligence**
- **World-renowned Mandiant consulting**

Now, you can end the complexity and effort required to prepare for, prevent and respond to cyber attacks.

For more information, visit [www.FireEye.com](http://www.FireEye.com)