

SEVENTH ANNUAL THOUGHT LEADERSHIP EVENT



# CYBER SECURITY SUMMIT 2017

October 23-25 | Minneapolis Convention Center

Join us to help

**MEEET**  
the Threat.  
**BEAT**  
the Threat.

Featured Sponsors:



TECHNOLOGICAL  
LEADERSHIP INSTITUTE

Booz | Allen | Hamilton



UNISYS | Securing Your  
Tomorrow™



MASTER OF SCIENCE  
SECURITY TECHNOLOGIES

Prevent  
and Protect

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

## Join the Next Cohort of Security Leaders

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

>200K

Unfilled Cyber Security  
Jobs in the U.S.

Source: CyberSeek

\$80B

Global spending to fight  
cyber crime in 2016

Source: Gartner, Inc.

\$170B

Expected Industry Growth  
by 2020

Source: Gartner, Inc.

Priority applications due Feb. 12. Attend an info session to learn more about MSST.

Oct. 30 | Nov. 15 & 27 | Dec. 13 | 5:30 PM to 7:00 PM

Contact TLI admissions ([tli-info@umn.edu](mailto:tli-info@umn.edu) or 612-624-5747) for info.

# Thank You Sponsors + Exhibitors

Founding Partner



Presenting Sponsors



Printing Sponsor



Wifi Sponsor



Platinum Sponsors



Diamond Sponsors



Gold Sponsors



Silver Sponsors



MNIT Student Breakfast



Bronze Sponsors



Exhibitor



AV Partner



Supporting Sponsors



Contributor



## Maximize Your Exposure in 2018

The 2017 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 2018 today and receive a 10% discount through December 31, 2017. For more information, contact our sponsorship sales consultants:

**Companies (A-M)** – Jennifer Churchill 763-548-1306 [jennifer.churchill@eventshows.com](mailto:jennifer.churchill@eventshows.com)  
**Companies (N-Z)** – Paul TenEyck 763-548-1308 [paul.teneyck@eventshows.com](mailto:paul.teneyck@eventshows.com)



# Welcome to 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.**

## **Michael Kearn**

2017 Co-Chair  
Cyber Security Summit

## **Eileen Manning**

Executive Producer  
Cyber Security Summit

## **Elizabeth Stevens**

2017 Co-Chair  
Cyber Security Summit

Thank you for joining us! The past year has brought a steady stream of cybersecurity news and reaffirmed the need for gatherings like this, where we can share information and work toward solutions.

This event marks our seventh annual Summit. The overarching cybersecurity message back in 2011 was “it’s not if, but when.” Today, personally identifiable information is stolen at a mindboggling rate. Denial of service interruptions and ransomware continue to disrupt critical operations for many organizations. The melding of technology and device brought IoT to the common acronym lexicon, and recent headlines indicate potential election manipulation by a nation state. We live in interesting times indeed and our work for the foreseeable future requires collaboration across sectors to solve these problems.

Tactically speaking, patch management and maintaining critical systems remains a significant challenge. Attributing and addressing threat vectors is a complex web of risk. Controlling access with passwords, biometrics, and one-time authorization codes while balancing usability with our need for security adds encumbrance to an already complex equation.

The “bad actors” don’t discriminate any longer. Within the past few years, businesses and

organizations of various sizes and sectors have felt the impact of ransomware. Small businesses are being targeted by adversaries more frequently, and with greater success. How well are they positioned to defend their assets in an environment where skilled security resources are scarce? We have partnered with the Small Business Administration and Better Business Bureau to bring you the Cyber Security for Small and Mid-Size Business forum again this year, for those of you operating in that space to share ideas, learn from each other and hear from some of the best in the profession.

The cadence and tempo of change in our respective industries keep us all busy, and we appreciate that you have taken the time to be here, build relationships, share insights and discover resources. Each of you contributes to this conversation and advances the mission to make the world a more secure place.

The Cyber Security Summit is the culmination of input from our advisory board and the support from our sponsors. Please take time to visit with them and learn about the resources available. We’ve built a collaborative forum to share ideas, but to perpetuate the momentum we need your input as well. Please take a moment and provide your voice for next year’s event when you receive the survey.

## Contents

- 03 Thank you Sponsors + Exhibitors
- 04 Welcome to Minneapolis
- 05 Summit Highlights
- 06 2017 Advisory Board
- 07 2017 Committees + Specialty Events
- 08 HALF DAY: Future-proofing Medical Device Security
- 11 HALF DAY: Investment Town Hall
- 12 HALF DAY: Demystifying DevSecOps with Veracode
- 15 HALF DAY: Cyber Security for Small and Mid-size Businesses
- 16 Full Summit Agenda
- 19 Upcoming Industry Events
- 20 Maslon: Effective Leadership: The Key to Building and Maintaining a Reasonable Cybersecurity Regime
- 21 Security Solutions Stage
- 22 2017 Speakers
- 26 Conference Map + Exhibitor Directory
- 29 2017 Sponsors + Exhibitors
- 41 Save the Date!
- 42 Index of Cyber Terminology
- 46 TL: Breaches, Breaches + More Breaches
- 47 Notes
- 50 Booz Allen Hamilton: 3 Keys to Effective Incident Response

## Questions?

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



Network: cyber security summit  
Password: css2017!

## Highlights

### Continuing Education Credits

Summit participation fulfills up to 12 hours of continuing education credits, depending on the organization.

### Networking

Build relationships with delegates from 29 states and 8 countries.

### Expo Reception

Network with industry thought leaders and our fantastic exhibitors at our Expo Reception after the Summit on Tuesday.



### Mobile Survey

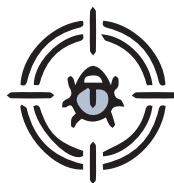
This year we will utilize a mobile survey platform to solicit real time feedback from the audience. When the poll is active, respond at [PolleEV.com/css17](http://PolleEV.com/css17) OR text css17 to 37607.

Sponsored by:  TECHNOLOGICAL LEADERSHIP INSTITUTE



### Tuesday HH meetup @ The Local

Whether you are in from out of town or just want to keep the conversation going, join us at The Local (4 blocks away) on Tuesday from 6:30-9 p.m.



### Cyber Bytes™

These quick-hit presentations deliver information on today's hottest topics in a condensed format that gets right to the point.



### Security Solutions Stage

Hear additional presentations and interviews with industry experts on our Security Solutions Stage, located within the Expo Area.

Sponsored by:  Centrify™  
THE BREACH STOPS HERE™

## 2018 VIP All Access Pass Giveaway

Everyone who follows our Twitter or Facebook page during the Summit and posts with the hashtag #CSSMN17 will be entered to **win a free VIP All Access Pass to Cyber Security Summit 2018 (\$999 value)**. Post on both Facebook and Twitter to be entered twice!



Michael Kearn  
U.S. Bank



Elizabeth Stevens  
UnitedHealth Group



Jill Allison  
ASIS International



Massoud Amin  
University of MN TLI



Bonnie Anderson  
HCMC



Michele Azar  
Retail Executive



Anne Bader  
International Cybersecurity  
Dialogue



Ken Barnhart  
Highground Cyber



John Bonhage  
InfraGard



Andrew Borene  
Booz Allen Hamilton



Chris Buse  
MNIT Services



Loren Dealy Mahler  
Dealy Mahler Strategies



Emily Duke  
Amplifon Americas



Antonio Enriquez  
DHS



Steen Fjalstad  
Midwest Reliability  
Organization



Mary Frantz  
EKP, LLC



Sam Grosby  
Wells Fargo



Heather Hanscom  
SUPERVALU INC.



Col. Stefanie Horvath  
MN ARNG



Bob Hoschka  
Computex



Brian Isle  
Adventium Labs



Mike Johnson  
University of MN TLI



Faisal Kaleem  
Metropolitan State  
University



David La Belle  
NorSec Foundation



Michael Larson  
Security Executive



Jack Lichtenstein  
JDL Advisory, LLC



Eileen Manning  
The Event Group  
Incorporated



Tina Meeker  
Beacon Information  
Security, LLC



Jerrod Montoya  
OATI



Dave Notch  
Medtronic



Stefan Pittinger  
CenturyLink



Frank Ross  
General Mills



James Ryan  
Litmus Logic, LLC



Glenn Sanders  
DHS



Phil Schenkenberg  
Briggs and Morgan, P.A.



Melissa Seebeck  
Deluxe Corporation



Paul Seim  
AT&T



Scott Singer  
PaR Systems, Inc.



David Stavseth  
Akamai



Catharine Trebnick  
Dougherty & Co. LLC



Chris Veltsos  
Dr. InfoSec



Kristi Yauch  
TCF Bank

# 2017 Committees

## CISO

Mike Johnson, Technological Leadership Institute\*\*; Mary Frantz, EKP; Tina Meeker, Beacon Information Security; Dave Notch, Medtronic; Chris Olive, Vormetric/Thales

## Glossary of Terms

Steen Fjalstad, Midwest Reliability Organization; David La Belle, NorSec Foundation

## Healthcare/Med Device

Brian Isle, Adventium Labs\*\*; Bob Bennett, HealthEast; Todd Carpenter, Adventium Labs; Emily E. Duke, Amplifon Americas; Ken Hoyme, Boston Scientific; William Scandrett, Allina; Michael Seeberger, Boston Scientific; Chris Tyberg, St. Jude Medical; Kristi Yauch, TCF

## Investment Town Hall

Catharine Trebnick, Dougherty & Company LLC\*\*; Anne Bader, The International Cybersecurity Dialogue; David La Belle, NorSec Foundation; Tina Meeker, Beacon Information Security; Bill Strub, NaviLogic

## Sponsorship Committee

Jill Allison, Best Buy; Andrew Borene, Booz Allen Hamilton; Bob Hoschka, Computex Technology Solutions; Tina Meeker, Beacon Information Security; Dave Notch, Medtronic

## PR

Anne Bader, The International Cybersecurity Dialogue; Loren Dealy Mahler, Dealy Mahler Strategies; Bob Hoschka, Computex Technology Solutions; Michelle Knoll, Technological Leadership Institute; Melissa Seebeck, Deluxe Corporation

## Program & Speaker Review

Bonnie Anderson, HCMC; Anne Bader, The International Cybersecurity Dialogue; Ken Barnhart, Highground Cyber; Andrew Borene, Booz Allen Hamilton; Steen Fjalstad, Midwest Reliability Organization; Stefanie Horvath, MN Army National Guard; Mike Kearn, US Bank; Dave Notch, Medtronic; David Stavseth, Akamai; Elizabeth Stevens, UnitedHealth Group; Kristi Yauch, TCF Bank

## Registration Ambassadors

Bob Hoschka, Computex Technology Solutions; Melissa Seebeck, Deluxe Corporation

## Presentation Review

David Stavseth, Akamai; Elizabeth Stevens, UnitedHealth Group

## Registration Committee

Michele Azar, Fortune 50 Global e-Commerce Multichannel Retail Executive; Anne Bader, The International Cybersecurity Dialogue; Chris Buse, MNIT Services; Loren Dealy Mahler, Dealy Mahler Strategies; Bob Hoschka, Computex Technology Solutions; Mike Johnson, Technological Leadership Institute; Faisal Kaleem, Metropolitan State University; Michael Kearn, U.S. Bank; Eileen Manning, The Event Group, Incorporated; Jerrod Montoya, OATI; Dave Notch, Medtronic; Melissa Seebeck, Deluxe Corporation; Elizabeth Stevens, UnitedHealth Group; Chris Veltsos, Dr. InfoSec; Kristi Yauch, TCF

## Security Solutions Stage

Loren Dealy Mahler, Dealy Mahler Strategies

## Small Business

Phil Schenkenberg, Briggs and Morgan, P.A. \*\*; Loren Dealy Mahler, Dealy Mahler Strategies; Lisa Jemtrud, Better Business Bureau of Minnesota and North Dakota; Twila Kennedy, Small Business Administration; Cyrus Malek, Briggs and Morgan, P.A.

## International Committee

Anne Bader, The International Cybersecurity Dialogue; Stefanie Horvath, MN Army National Guard; Mike Johnson, Technological Leadership Institute

## Legislative & Government Outreach

Chris Buse, MNIT Services; Mary Frantz, EKP; Jack Lichtenstein, JDL Advisory, LLC; Phil Schenkenberg, Briggs and Morgan, P.A.

## Committee Meeting Hosts

November: Elizabeth Stevens, UnitedHealth Group; December: Catharine Trebnick, Dougherty & Company LLC; January: Phil Schenkenberg & Cyrus Malek, Briggs and Morgan, P.A.; February: Tina Meeker, Best Buy; March + April: Eileen Manning, The Event Group, Incorporated; May: Dave Notch, Medtronic; June: Mike Johnson, Technological Leadership Institute; July: Mary Frantz, EKP; August: Jerrod Montoya, OATI; September: Tina Meeker, Best Buy; October: Frank Ross, General Mills

\*\*Committee Chair

## Specialty Events



### VIP Reception

Oct.23 @5:15 PM



### MNIT Breakfast

Oct.24 @7:00 AM | MINNESOTA IT SERVICES



### CISO Luncheon

Oct.24 @12:15 PM | THALES



All Welcome

### FBI Breakfast

Oct.25 @7:15 AM



### CEO Breakfast

Oct.25 @7:15 AM | CenturyLink Business



# Future-Proofing Medical Device Security

Monday, October 23 | 1:00 - 5:15 PM

The Cyber Security Summit was founded in 2011 to bring together thought leaders around the important topic of security. Since that time, it has annually hosted representatives from industry, government and academic interests for a high-level strategic view of security issues.

The goal of this new event is to build awareness and bring a similar focus to the medical device industry. The Twin Cities provides a perfect venue because of its concentration of health care and medical device leaders.



## Agenda

1:00 – 1:15 PM	Welcome and Setting the Stage	3:30 – 4:00 PM	Break
1:15 – 2:15 PM	Threat Briefing: Med Device & Healthcare Delivery Organization-specific Speakers: Christopher Golomb, FBI; Ken Hoyme, Boston Scientific; Jay Radcliff, Rapid7; Billy Rios, WhiteScope	4:00 – 5:00 PM	Panel: Building the Future – Standards and Resources Speakers: Seth Carmody, FDA; Justin Heyl, Underwriters Laboratories; Ken Hoyme, Boston Scientific
2:15 – 2:30 PM	Q&A	5:00 – 5:15 PM	Concluding Remarks
2:30 – 3:30 PM	Panel: Moving Toward Future -Proofing Medical Device Security Speakers: Todd Carpenter, Adventium Labs; Stephanie Domas, Battelle DeviceSecure® Services; Dan Lyon, Synopsys Software Integrity Group		

Sponsors:



MASLON

Supporters:





# An Ounce of Prevention...

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

Maslon has extensive experience advising healthcare and medical device clients on effective data security practices and privacy law. We not only know the law, we know the industry—and we're dedicated to helping our clients avoid unnecessary complications.



**MASLON LLP**  
612.672.8200  
MASLON.COM

**MASLON**



**30** YEARS OF EXCELLENCE

hardware. software. brainware.

## AWARD WINNING SOLUTION PROVIDER

Computex Technology Solutions is an award-winning solutions provider committed to helping our clients evolve their business through technology, for the past 30 years. At our core we are architects and engineers that specialize in delivering data centers, enterprise networking, cybersecurity and cloud & managed services.



Enterprise Networking



Data Center



Cybersecurity



Cloud & Managed Services

[www.computex.net](http://www.computex.net) | 1.877.957.1001

## RELENTLESS PREPARATION.

By the time you read this, methods of cyber attack will have evolved, again. Attackers are continuously evolving their tactics to exploit vulnerabilities. Enterprises need relentless preparation in their approach to cybersecurity.

We protect our clients from the attacks of today, and prepare them for the threats of tomorrow.

[BOOZALLEN.COM/COMMERCIAL](http://BOOZALLEN.COM/COMMERCIAL)

## Mn(C)<sup>3</sup> MINNESOTA CYBER CAREERS CONSORTIUM

THE FORMULA  FOR SECURITY

[www.MnC3.org](http://www.MnC3.org)

Interested in learning more and contributing to this industry/academic partnership?

**Come meet us at booth # 508**

### Research Resource

An initiative where industry or academic experts will guide students conducting applied cybersecurity research

Learn how to become part of the MnC3 and help us achieve our goals

### Mission

To address Minnesota's cybersecurity workforce needs, and to assist Minnesota businesses in handling cyber risks.

### Goals

1. To provide Minnesota college & university students with the knowledge, skills, and abilities needed to transition into successful cybersecurity professionals.
2. To facilitate continuing education and training of the existing workforce for high-demand skills in cyber-related occupations, for employees both with and without IT/security background.
3. To raise awareness of cyber risks faced by small/medium businesses, and provide resources to improve their cybersecurity and cyber-resilience.
4. To advance awareness of cybersecurity issues (cyber safety, cyber hygiene) in the community at large.
5. To grow interest in cybersecurity careers among students in grades 7-12.
6. To conduct and support applied research to advance the field of cyber security.



# Investment Town Hall

**Monday, October 23 | 2:00 - 5:15 PM**

The 2nd Annual Investment Town Hall includes sessions on the changing threat landscape and how it impacts cyber security start-ups, the changing public market for established appliance and software vendors, and the future of the space through the lenses of internal development or acquisition. Topics span legacy vendor replacement through next-generation techniques, the emerging role of blockchain and cryptocurrencies, and insight into the strategic planning behind capital raising.

The day culminates with a panel of accredited investors and thought leaders, including hedge fund portfolio managers, sell-side research analysts, and seed investors.

## Agenda

**2:00 – 2:15 PM**

**Update on Cyber Security Marketplace From IPO to Seed Funding**

Speaker: Catharine Trebnick, Dougherty & Company LLC

**2:15 – 3:00 PM**

**Discussion on Next-Generation Techniques Replacing Legacy Software Tools**

Speaker: Larry Whiteside Jr., Whiteside Security LLC

**3:00 – 3:45 PM**

**M&A Opportunities with Security**

Speaker: Joel Fulton, Splunk

**3:45 – 4:30 PM**

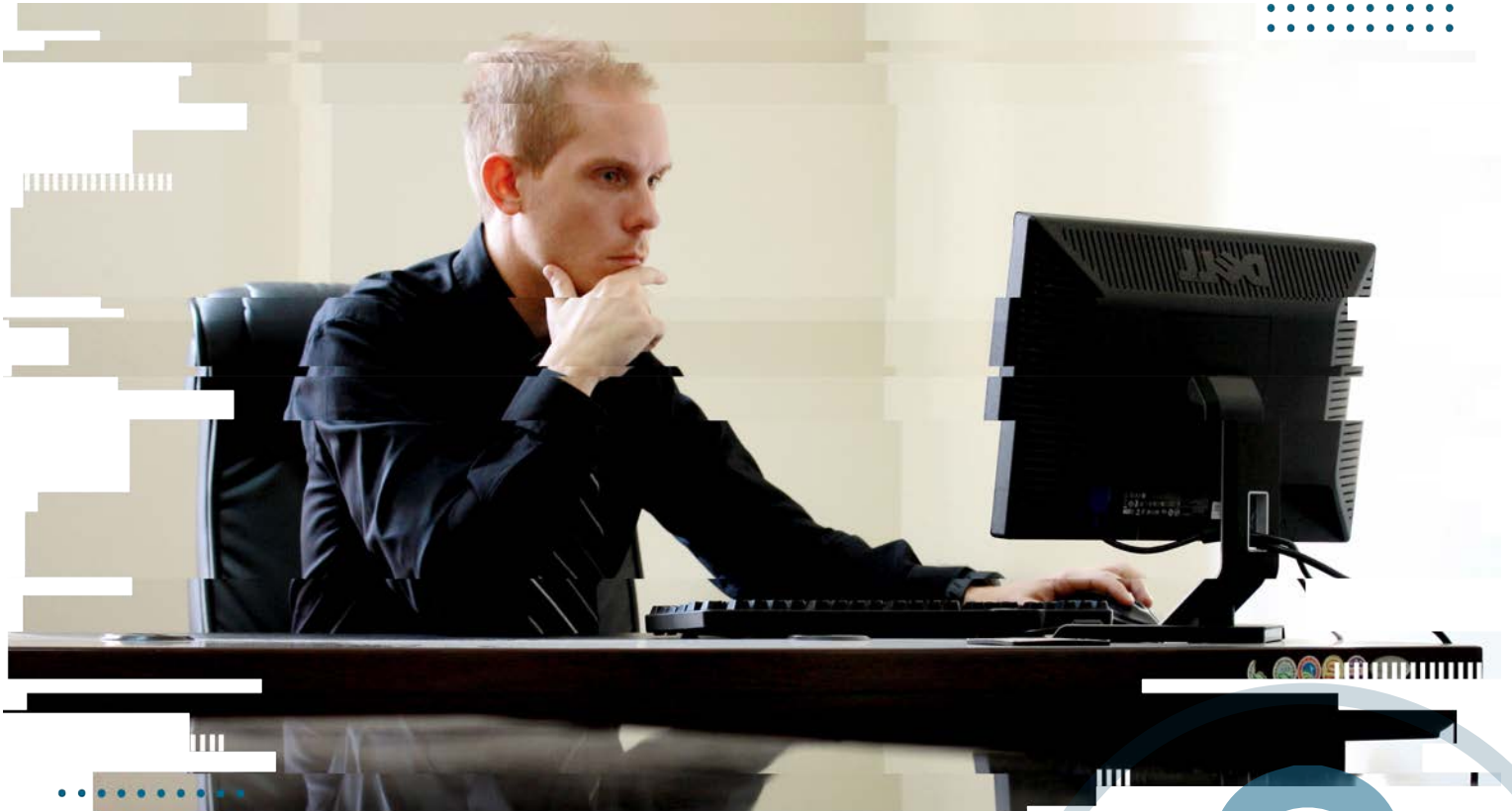
**Discussion on Defense M&A**

Speaker: Bob Kinder, SixGen, LLC

**4:30 – 5:15 PM**

**Investing Through the Lens of Accredited Investors and Thought Leaders**

Panel Moderators: Bill Strub, Navilogic; Tina Meeker, Beacon Information Security, LLC  
Panelists: Joel Fulton, Splunk; Bob Kinder, SixGen, LLC; Larry Whiteside Jr., Whiteside Security LLC



# Demystifying DevSecOps with **VERACODE**

Monday, October 23 | 2:30 - 5:15 PM

This year's Tech Talks are designed for Security & Development professionals interested in learning more about Secure DevOps and how to build security into their platforms from Day 1.

## Agenda

2:30 – 3:15 PM

**DevOps – Security's Big Opportunity**

As the shift to DevOps continues to accelerate, how can security teams harness the power of this change and build a strategic vision for their business?

Speaker: Pete Chestna, Veracode

3:15 – 4:00 PM

**Planning For A Responsive AppSec Program**

AppSec programs have had to adapt to changes in software development and management philosophies as Agile, and now DevOps, have become more popular in development organizations. As your organization moves to DevSecOps, how can you plan to be resilient and adaptable to future change?

Speaker: Darren Meyer, Veracode

4:00 – 4:15 PM

**BREAK**

4:15 – 4:45 PM

**Veracode's DevSecOps Journey**

This discussion will focus on how Veracode has worked to harness the power of DevSecOps and will include some real life examples of success with our program.

Speaker: Chris Eng, Veracode

4:45 – 5:15 PM

**Open Q+A**

Speakers: Pete Chestna, Chris Eng and Darren Meyer of Veracode



# DEVOTPS

BUILD IN SECURITY AT THE SPEED  
OF SOFTWARE DEVELOPMENT



TECHNOLOGICAL LEADERSHIP INSTITUTE



GRADUATE MINOR

## Cyber Security

DO YOU HAVE WHAT IT TAKES  
TO BEAT THE THREAT?

Gain the skills to protect the information and systems we rely on with a Cyber security graduate minor from the University of Minnesota's Technological Leadership Institute (TLI). Cyber security professionals are in greater demand than ever. Our minor provides students with the skills to adapt and lead in this critical career field. Courses are open to both U of MN students and non-degree seeking professionals looking to advance their careers.

# Start With Trust<sup>®</sup>

Promoting data privacy in the marketplace is an educational priority for Better Business Bureau. We work with both consumers and businesses to promote cyber security best practices and resources. Learn more about BBB and our free programs and services at [BBB.org](http://BBB.org).



**BBB.org**  
**800-646-6222**



**CYBER SECURITY  
SUMMIT 2017**



Protecting **Data**  
is Protecting **People**

Minnesota needs great cybersecurity professionals to protect our systems and our citizens. Join us. Visit [mn.gov/mnit/careers](http://mn.gov/mnit/careers) for opportunities.

**m** MINNESOTA  
IT SERVICES



# Cyber Security for Small and Mid-size Businesses

Tuesday, October 24 | 1:30 - 5:00 PM

Many normal business transactions can open the door to cyber theft or attack. If your business is not big enough to have dedicated resources to manage security strategies, this is the perfect opportunity to learn more about best practices for keeping your data secure and responding after you've been compromised.

## Agenda

- |                |   |                |  |
|----------------|---|----------------|--|
| 1:30 – 1:45 PM | Welcome and Available Resources<br>Speaker: Nancy Libersky, SBA   | 3:45 – 4:00 PM | Having a Cyber Communications Plan<br>Speaker: Loren Dealy Mahler, Dealy Mahler Strategies                                       |
| 1:45 – 2:15 PM | Cyber Security for Business Leaders<br>Speaker: Hala Furst, DHS   | 4:00 – 4:30 PM | What You're Up Against: Real Life Examples from a Small Business Owner<br>Speaker: Eileen Manning, The Event Group, Incorporated |
| 2:15 – 2:45 PM | Cyber Case Studies and Legal Considerations<br>Speakers: Cyrus Malek, Briggs and Morgan PA; Phil Schenkenberg, Briggs and Morgan PA | 4:30 – 5:00 PM | Q&A with Panel of Experts  |
| 2:45 – 3:15 PM | Risk Assessments and Being Prepared for an Attack<br>Speakers: Yan Kravchenko, Atomic Data; Jim Wolford, Atomic Data                |                |  |
| 3:15 – 3:45 PM | BREAK IN EXPO AREA  |                |  |


Sponsor: **BRIGGS**  
BRIGGS AND MORGAN  
PROFESSIONAL ASSOCIATION

Supporters: **BBB**  
bbb.org **SBA**  
U.S. Small Business Administration

# Monday, October 23

1:00 - 5:15 PM	Future-Proofing Medical Device Security - See page 8 for details.
2:00 - 5:15 PM	2nd Annual Investment Town Hall - See page 11 for details.
2:30 - 5:15 PM	Demystifying DevSecOps with Veracode - See page 12 for details.
5:15 - 7:00 PM	VIP RECEPTION (Invitation Only)

# Tuesday, October 24

7:00 - 7:45 AM	 <b>Student Breakfast</b> (Invitation only) <i>Chris Buse, MNIT Services, State of Minnesota</i>
8:00 - 8:30 AM	<b>Welcome and Opening Remarks</b> - <i>Michael Kearn and Elizabeth Stevens, 2017 Summit Co-Chairs</i>
8:30 - 9:00 AM	<b>Year in Review</b> /// Matt will share insights and experiences with key cyber security issues, ranging from workforce challenges and opportunities to the emerging threat landscape. <i>Matt Loeb, ISACA</i>
9:00 - 9:30 AM	<b>The Dark Web</b> /// Take a journey into the underbelly of the Internet, the Dark Web. We'll look at recent breaches, types of breaches, impacts of breaches, and motivation for breaches. The journey continues with an exploration of the "dark web" and the black markets contained in it. The simplicity and ease of access is astounding and will instill fear, uncertainty and doubt. Prepare to have some FUD. <i>Scott Sweren, AT&amp;T</i>
9:30 - 9:50 AM	<b>CYBER BYTE™ : Real-Life Lessons Learned</b> /// Hala will provide examples of how engagement with the Department of Homeland Security NCCIC and the government in general can help companies respond or recover from incidents. She will also provide a high-level overview of the threat landscape, current best practices, free tools and resources for businesses and state and local governments, the government's progress on the recent Cybersecurity Executive Order, and any potential implications for the private sector. <i>Hala Furst, Department of Homeland Security</i>
9:50 - 10:00 AM	<b>Welcome</b> - <i>Governor Mark Dayton</i>
10:00 - 10:30 AM	<b>BREAK IN EXPO AREA</b>
10:30 - 10:50 AM	<b>CYBER BYTE™ : Phishing Trends</b> /// Learn how people in your organization are targeted by cyber criminals, hackers and even state-sponsored actors. You'll also learn how email is at the heart of this evolving threat. <i>JP Blaho, Mimecast</i>
10:50 - 11:10 AM	<b>CYBER BYTE™ : Compliance – What it Really Means</b> /// Historically, Compliance ≠ Security. However, new and updated mainstream operating control frameworks such as FedRAMP dictate aggressive and downright onerous Continuous Monitoring Programs. This presentation will discuss how achieving full conformity with the letter and intent of these standards is bringing us closer to realizing the promise of Compliance = Security. <i>Rich Banta, Lifeline Data Centers</i>
11:10 - 11:50 AM	<b>Compliance is not a Cybersecurity Strategy</b> /// Does compliance make us more secure – and how do we keep innovation and creativity thriving within a compliance structure? <i>Moderator: Mike Johnson, University of Minnesota TLI</i> <i>Panelists: Rich Banta, Lifeline Data Centers; Steen Fjalstad, Midwest Reliability Organization; Kevin Johnson, Secure Ideas</i>



11:50 AM - 12:10 PM	<p><b>Breaches &amp; Sensitive Documents – Prepare, Respond, and Protect Yourself</b> /// Cybersecurity – and how to prepare and respond to a breach and protect sensitive documents under a company’s control – has become a critical consideration for corporate executives in managing risk. Evan Wolff, partner and co-chair of Crowell &amp; Moring’s Privacy &amp; Cybersecurity Group, will walk you through the anatomy of a data breach and describe legally compliant industry best practices and government standards that may help mitigate the potential risks. Mr. Wolff will also highlight the top ten steps that executives may take, in working with other key personnel, to improve their companies’ cybersecurity and privacy posture.</p> <p><i>Evan Wolff, Crowell &amp; Moring LLP</i></p>
12:15 - 1:15 PM	<p><b>THALES CISO Luncheon</b> (Invite Only; Must be a CISO, CIO or CTO to attend)</p> <p><i>Brent Lassi, Carlson Wagonlit Travel; Chris Olive, Thales e-Security; Kathy Orner, Carlson Wagonlit Travel</i></p>
12:15 - 1:15 PM	<b>LUNCH IN EXPO AREA</b>
1:30 - 5:00 PM	<b>Cyber Security for Small and Mid-size Businesses</b> - See page 15 for details.
1:30 - 2:00 PM	<p><b>Anatomy of an Attack</b> /// Brad Antoniewicz leads Cisco Umbrella’s security research analyst team. He is an adjunct professor teaching Vulnerability Analysis and Exploitation and a Hacker in Residence at NYU’s Tandon School of Engineering. Brad is also a contributing author to both the “Hacking Exposed” and “Hacking Exposed: Wireless” series of books.</p> <p><i>Brad Antoniewicz, Cisco</i></p>
2:00 - 2:45 PM	<p><b>Got Spies in Your Wires?</b> /// This talk will discuss the ever-evolving cyber threat landscape from the speaker’s perspective as an incident responder. The talk will discuss some of the more significant threat groups and activities from a handful of countries as well as the professionalization of the hacking industry as a whole. The threats the security community face today are quite different from the threats we faced even five years ago. We’ve witnessed a natural evolution to a more professional cyber criminal landscape based on both monetary and political factors.</p> <p><i>Marshall Heilman, FireEye</i></p>
2:45 - 3:15 PM	<p><b>CYBER BYTE™ : Common Attack Vectors with Quick-Win Mitigations</b> /// This brief talk will discuss the most common ways our penetration testing team gains privileged access both internally and externally along with simple mitigations which would prevent access over 90% of the time.</p> <p><i>Slade Griffin, Contextual Security Solutions</i></p>
3:15 - 3:45 PM	<b>BREAK IN EXPO AREA</b>
3:45 - 4:15 PM	<p><b>CYBER BYTE™ : The Intersection of the Connected Worker and the Internet of Things</b> /// The smartphone is the primary communication and computing device for many of today’s consumers. This dependency on mobile devices will translate into a majority of enterprise computing outside of traditional PC computing. This will have the greatest impact with on campus (non-office-based) and off campus mobile workers who are becoming increasingly connected by rich real time communications powered by mobile applications running on wearable devices such as smart glasses. The rise of IoT in the enterprise, or the Enterprise of Things, will allow these workers to instantly connect with assets in the field to gain immediate understanding of the situation around them.</p> <p><i>Chris Greco, BlackBerry</i></p>
4:15 - 4:45 PM	<p><b>Securing Critical Infrastructure in an Uncertain World</b> /// A look at how to protect our critical infrastructures.</p> <p><i>Dr. Massoud Amin, University of Minnesota TLI</i></p>
4:45 - 5:00 PM	<p><b>Securing Meet the Threat Review &amp; Beat the Threat Preview</b> /// Review key points from Day 1, preview Day 2 and promote the value of building your network over cocktails at the Networking Reception</p> <p><i>Michael Kearn and Elizabeth Stevens, 2017 Summit Co-Chairs</i></p>
5:00 - 6:00 PM	<b>NETWORKING RECEPTION IN EXPO AREA</b>

# Wednesday, October 25

7:15 - 8:15 AM	 <b>CEO Breakfast (Invitation-Only; Complimentary for VIP Access Pass Holders)</b> <i>Mark Lanterman, Computer Forensic Services</i>
7:15 - 8:15 AM	<b>SUMMIT BREAKFAST</b>
7:15 - 8:15 AM	<b>FBI Career Opportunities Breakfast</b> /// Have you ever considered a career with the FBI? Join us for this special breakfast during the 2017 Cyber Security Summit. Representatives from the Bureau will be on hand to speak about the application process, IT, cyber and tech careers in the FBI. They will also take any questions people have. <i>Mike Krause, FBI</i>
8:30 - 8:45 AM	<b>Welcome and Opening Remarks</b> - <i>Eileen Manning, Summit Executive Producer</i>
8:45 - 9:30 AM	<b>Combating Short- and Long-Term Cyber Threats</b> /// Dr. Stacey Dixon joined the Intelligence Advanced Research Projects Activity (IARPA) as its Deputy Director in January 2016. She will speak on near-term cyber issues such as supply chain security, trusted component manufacturing, and cyber threat forecasting and long-term issues like super computing, artificial intelligence and the coming era of digital/biological threats. <i>Dr. Stacey Dixon, IARPA</i>
9:30 - 10:00 AM	<b>When the Levee Breaks</b> /// The shiny new product is not always the most effective solution to mitigate risk. In fact, more companies are breached because they had fundamental vulnerabilities in their security posture and were exposed due to those cracks in their foundation. This presentation will discuss what many of us in our profession consider the basic building blocks of an effective security program, in addition examining how current technologies can help create the stronger foundation all of us are seeking. A house of sand will never stand and layering next gen solutions on top of a program with a weak foundation won't either. Learn how accurate risk assessments, threat modeling and layering controls appropriately can help you set a firm foundation to build your own program on. We don't always need a new set of tools, but sometimes a new or different perspective can make the biggest difference in securing our organizations. <i>Michael Kearn, U.S. Bank; 2017 Summit Co-chair</i>
10:00 - 10:30 AM	<b>BREAK IN EXPO AREA</b>
10:30 - 11:00 AM	<b>Maintaining Cyber Readiness in an Evolving Threat Landscape</b> /// It's a fact. Threat actors are becoming more advanced—and more successful. And your attack surface is rapidly expanding through the cloud, mobile, and the Internet of Things (IoT). Prevention-based tactics are no longer enough to keep your company safe. <i>Brent Benson, LogRhythm</i>
11:00- 12:00 PM	<b>Incident Response Panel</b> /// Panelists from industry as well as government will lead this discussion of the federal incident response protocol. The discussion will be moderated by Lou Stephens, who prior to his current role was special agent in charge for the U.S. Secret Service in Minneapolis from 2011 to 2017 and managed the agency's protective and investigative operations throughout Minnesota, North Dakota and South Dakota. <i>Moderator: Lou Stephens, Sea Foam Corporation</i> <i>Panelists: Michael J. Krause, FBI; Lisa Beth Lentini, Deluxe Corporation; Brad Maiorino, Booz Allen Hamilton; Timothy Rank, U.S. Attorney's Office</i>
12:00 - 1:15 PM	<b>LUNCH IN EXPO AREA</b>
1:15 - 2:00 PM	<b>The Greatest Gift – Making Attacks Expensive</b> /// How many times have you heard the phrase "Defenders have to get security right every time, an attacker only has to get it right once"? In this presentation, we will explore the phases of a cyber attack, identifying and taking advantage of those stages that are more expensive for the attacker than the defender. By changing our perceptions and understanding of the inevitable attack, defenders can develop capabilities to gain an upper hand against the attackers. This presentation will demonstrate actionable processes to shift the power to the defense, and making attacking expensive and difficult for attackers. <i>Bill Swearingen, CenturyLink</i>

2:15 - 3:00 PM	<p><b>Strengthen Your Cyber Security Posture: What to Look for in an MSSP</b> /// Faisal Bhutto, VP of Cybersecurity for one of the nation's most recognized Cloud &amp; Managed Services Provider, explains how a cybersecurity program conversation should go beyond compliance and regulations. He will walk through the type of discipline needed to have an effective cybersecurity program for CIOs and CISOs and explore build vs. buy scenarios when it comes to holistic cybersecurity program implementation.</p> <p><i>Faisal Bhutto, Computex Technology Solutions</i></p>
3:00 - 3:30 PM	<p><b>BREAK IN EXPO AREA</b></p>
3:30 - 4:00 PM	<p><b>CYBER BYTE™ : Information Sharing to Better Protect Companies in the U.S.</b> /// Drew Evans of the Minnesota Department of Public Safety will discuss cyber security, what it means for our state, and provide tips on identifying threats and sharing information.</p> <p><i>Drew Evans, The Bureau of Criminal Apprehension</i></p>
4:00 - 4:45 PM	<p><b>Running the Defense: Securing the Super Bowl</b> /// Analytics brings the ability for both offensive and defensive cyber protection: Think football. The 2017 Summit brings forward a central theme around what analytics can do for cyber security. The very concept of using intelligence, big data and analytics brings a new thought process and has a new set of buzz words and concepts to learn. In fact, it really is a lot like football. We will break down the concepts of analytics and illustrate them in terms of the most watched game in the world. We will also share real life examples, planning and results from securing Super Bowl 50 in San Francisco.</p> <p><i>Jim Libersky, Barrier1</i></p>
4:45 - 5:00 PM	<p><b>An Overview – Practical Takeaways</b> /// After two days of in-depth presentations, our co-chairs share some of the takeaways from the 2017 Summit.</p> <p><i>Michael Kearn and Elizabeth Stevens, 2017 Summit Co-Chairs</i></p>

## Upcoming Industry Events



### MHTA - MINNESOTA TEKNE AWARDS

[Minneapolis Convention Center @4:30 PM](#)  
Each year the Tekne Awards shine a spotlight on Minnesota's technology industry. Drawing our state's most influential business, political leaders and individuals, the Tekne Awards honor advancement in technology.



### ISACA MINNESOTA - BUSINESS OF SECURITY PRESENTATION

[Land O'Lakes Conference Center @3:00 PM](#)  
Attendees will learn how to measure and communicate security program performance and associate this performance with identified risks.



### INFRAGARD MINNESOTA MEMBERS ALLIANCE MEMBERSHIP MEETING

[Cargill - Hopkins Location](#)  
The Infragard Minnesota Member Alliance is an FBI-sponsored partnership program focused on critical infrastructure protection. Apply for your membership at [www.infragard.org](http://www.infragard.org).



### ISSA MINNESOTA - CHAPTER MEETING

[Ewald Conference Center @1:00 PM](#)  
The Information Systems Security Association is a not-for-profit, international organization of information security professionals and practitioners. Doors open at 1:00PM for networking with a 1:30PM meeting start.



### NEW 2018 SERIES - CYBER SECURITY FOR MED-DEVICE + HEALTHCARE

Medical device security is such an important topic that we are launching a series of events in 2018 to discuss the issues and explore possible solutions

[Check cybersecuritysummit.org](http://Check cybersecuritysummit.org) for updates



#### ABOUT THE AUTHOR:

**ERAN KAHANA** is a cybersecurity and intellectual property lawyer as well as a Fellow at Stanford Law School. He counsels clients on a wide variety of matters related to cybersecurity, technology law, trademarks, patents, and copyright issues. Eran also serves in a variety of cybersecurity thought-leadership roles and works closely with the FBI, Department of Justice, Secret Service, and colleagues from the private and academic sectors to set, promote, and sustain cybersecurity best practices. Eran serves as both general counsel and as a director on the Executive Board of InfraGard (MN Chapter).

[eran.kahana@maslon.com](mailto:eran.kahana@maslon.com)

**MASLON LLP** is a full-service commercial law firm in Minneapolis, offering a depth of experience in the areas of Business & Securities, Litigation, and Financial Services, with a supporting practice focused on Cyber Security Law.

Maslon's Cybersecurity Law counselors offer deep knowledge and experience regarding legal, regulatory, and industry standards. Clients receive proactive, practical advice that will help protect their company's data as well as ensure legal compliance.

**MASLON**

## Effective Leadership: The Key to Building and Maintaining a Reasonable Cybersecurity Regime

Healthcare sector cyber incidents seem to garner less media attention than the headline-grabbing breaches featuring powerful malware (Stuxnet), spies (China, Russia), and malicious state actors (North Korea), but that in no way reflects the severity of the problem. In 2015, Anthem got hit with the largest attack to date, one in which 78.8 million patient records were compromised. The most significant damage, however, is caused by the steady stream of small cyber incidents that impact both individual patients and the entire health sector ecosystem.

One way to gauge the magnitude of these breaches is to examine the relevant statistics. The Department of Health and Human Services' Office of Civil Rights (OCR), which is tasked with enforcement of healthcare breaches, identifies healthcare cyber incidents reported to and investigated by OCR on a rolling 24-month basis on its website. There have been 348 incidents collected over the past two years—nearly half (41%) of the incidents were classified as a "Hacking/IT incident" and 36% as "Unauthorized Access/Disclosure." Following in third place was "Theft," garnering 18% of the incidents. In terms of data-breach localization, the "Network Server" category bore 27% of the cyber-attacks and email accounted for 18%.

So, what is the problem here? These statistics are not the product of a dearth of regulations, nor the lack of standards—there are plenty of both. It's not even the case that the law makes compliance difficult. It does not. Bullet-proof security is not a legal precondition for avoiding liability. In *United States ex rel. Sheldon v. Kettering Health Network*, for example, the court held that being compliant with healthcare data security regulations "does not equate with having impenetrable cybersecurity defenses."

The vast majority of cybersecurity breaches, including those tracked by the OCR, are rooted in: 1) dysfunctional leadership; 2) lack of relevant corporate wherewithal and knowledge (a close relative to the first item); 3) absence of proper policies and procedures; 4) sporadic, non-existent, or ineffective training of all relevant users (not just employees); and 5) negligent or malicious employees. It is perhaps no surprise

then that building and maintaining an effective cybersecurity regime is a task that often stubbornly evades effective execution, despite regulations and industry standards.

An integral part of the solution is to properly understand the "how-to" component of building and maintaining a legally-reasonable cybersecurity regime. This begins with recognizing that this it is not a journey from A to B, but a continuous cycle, one that involves a complex eco-system. The cycle includes countless efforts, some big, some small—some take a long time to work through and some are just a quick shot. Technology, business processes, best practices, and legal principles must sync to enable this regime to work through its life cycle in a consistent way, every time.

To illustrate this a bit further, consider the benefits of implementing emerging technologies with current cybersecurity best practices. For example, blockchain sports cryptographic controls along with decentralized verification that uses a consensus-based, transaction-entry voting system to guaranty data integrity like no other database. As such, blockchain promises to play a key role in reducing fraud. Though HIPAA makes no mention of it, the case for implementing blockchain-enabled applications and business processes can be gleaned from it in § 164.312(c)(1), which requires identifying what can be done to protect the data integrity. Its use-case becomes even more compelling because blockchain is not necessarily limited to wealthy, large healthcare players—Azure, Amazon Web Services, and IBM offer it as a service.

The initial listing of "dysfunctional leadership" among the problems causing cybersecurity breaches was intentional. Without effective leadership, any effort is doomed and the cyber incident story told by the breach data on the OCR's website may never change. While courts have traditionally provided corporate directors with a wide operational berth, the relentless plague of healthcare cybersecurity breaches and pervasive noncompliance will invariably alter that approach. Fixing the leadership problem is the key to curbing the steady stream of healthcare sector cyber incidents.

# Security Solutions Stage



Moderated by:  
**Loren Dealy Mahler**  
President, Dealy Mahler  
Strategies LLC

This year the **NEW Security Solutions Stage** will feature a mix of interviews with security leaders and brief presentations from a variety of solution providers.

The stage is located within the Expo Area and will be active throughout the Summit. A complete schedule of presenters will be posted outside the Security Solutions Stage entrance.

Presentations will focus on tools attendees can utilize to improve their organization's security.

Moderating the interviews will be Loren Dealy Mahler, a seasoned strategic communications and crisis management expert and author of the "Communications War Room" blog at [csoonline.com](http://csoonline.com).

Be sure to stop by during the Summit to check out this new resource.

Presented by:



Supported by:

**BLACKDUCK**



**COLLIER**

**crowell**  **moring**



**PLURALSIGHT**

**RSA**

  
**Synack**

## Stay Connected

Join the discussion by sharing your experience throughout the Summit on social media!



# THE BREACH STOPS HERE™

90% of all enterprises are moving to the cloud, billions of users are accessing data across millions of applications. All accessed by one simple permission. The password.

The results? Two thirds of enterprises have been breached due to compromised passwords. Until now.

Centrify is a massive rethink in security, defending today's boundaryless hybrid enterprise through the power of identity services.

**THIS IS  
NEXT DIMENSION SECURITY**

 **Centrify**

Free trial: [www.centrify.com/free-trial](http://www.centrify.com/free-trial)

Learn more: [www.centrify.com/resources](http://www.centrify.com/resources)

Contact us at +1 (669) 444-5200 or [sales@centrify.com](mailto:sales@centrify.com)

# Featured Speakers



**Mark Dayton**  
Governor, State of Minnesota

Tuesday, October 24 | 9:50AM  
Welcome /// Mark Dayton is Minnesota's 40th Governor. He is a strong proponent of the importance of cybersecurity, and earlier this month he signed a proclamation declaring October "Cybersecurity Awareness Month" in Minnesota. At this year's Summit, he will help welcome attendees.

Gov. Dayton is among 38 governors who pledged at a meeting of the National Governors Association this summer to make cybersecurity a top priority. He has said, "Strong cybersecurity is critical to protect our citizens, our businesses, and our state from attacks online. As these threats increase in volume and sophistication, we must invest in critical upgrades, technology, and talent to keep Minnesotans safe and secure online."



**Dr. Stacey Dixon**  
Deputy Director, IARPA

Wednesday, October 25 | 8:45AM  
Combating Short- and Long-Term Cyber Threats /// Dr. Stacey Dixon joined the Intelligence Advanced Research Projects Activity (IARPA) as its Deputy Director in January 2016. Dr. Dixon joined IARPA from the National Geospatial-Intelligence Agency (NGA) where she most recently served as Deputy Director of InnoVision and oversaw geospatial

intelligence research and development. Prior to InnoVision, she served as NGA's Chief of Congressional and Intergovernmental Affairs. From 2007 to 2010 she worked on the U.S. House of Representatives Permanent Select Committee on Intelligence (HPSCI) staff. From 2003 to 2007 she worked for the Central Intelligence Agency (CIA) assigned to the National Reconnaissance Organization (NRO)'s Advanced Systems and Technology Directorate. Dr. Dixon holds doctorate and master's degrees in mechanical engineering from the Georgia Institute of Technology, and a bachelor's degree in mechanical engineering from Stanford University.



**Matt Loeb**  
CEO, ISACA

Tuesday, October 24 | 8:30AM  
Year in Review /// Matt Loeb is chief executive officer of ISACA. Prior to joining ISACA, he completed a 20-year career as staff executive for the Institute of Electrical and Electronics Engineers (IEEE) and as the executive director of the IEEE Foundation. His experience includes enterprise strategy, corporate development, global business operations,

governance, publishing, sales, marketing, product development and acquisitions functions in a variety of for-profit and nonprofit organizations. He is a member of ISACA, CESSE and NACD, and a senior member of IEEE. Additionally, he is an ASAE Fellow and serves on ASAE's board of directors.



**Dr. Massoud Amin**  
Director and Professor,  
Technological Leadership  
Institute and ECE, University  
of Minnesota

Tuesday, Oct. 24 | 4:15PM  
Securing Critical Infrastructure  
in an Uncertain World



**Brad Antoniewicz**  
Head of Security Research  
Analyst Team, Cisco

Tuesday, Oct. 24 | 1:30PM  
Anatomy of an Attack



**Rich Banta**  
Managing Member, Lifeline Data  
Centers

Tuesday, Oct. 24 | 10:50AM  
Compliance: What it Really Means  
Tuesday, Oct. 24 | 11:10AM  
Compliance is not a Cybersecurity  
Strategy



**Brent Benson**  
Enterprise Sales Engineer,  
LogRhythm

Wednesday, Oct. 25 | 10:30AM  
Maintaining Cyber Readiness in an  
Evolving Threat Landscape



**Faisal Bhutto**  
VP of Enterprise Networking,  
Cloud & Cybersecurity, Computex  
Technology Solutions

Wednesday, Oct. 25 | 2:15PM  
Strengthen Your Cyber Security  
Posture



**JP Blaho**  
Senior Director, Product  
Marketing, Mimecast

Tuesday, Oct. 24 | 10:30AM  
Phishing Trends



**Christopher Buse**  
Chief Information Security  
Officer & Assistant  
Commissioner, MNIT  
Services, State of Minnesota

Tuesday, Oct. 24 | 7:00AM  
Student Breakfast

## Learn More About Our Speakers

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



**Seth Carmody**  
Cybersecurity Program  
Manager, FDA

Monday, Oct. 23 | 4:00PM  
Building the Future –  
Standards and Resources



**Steen Fjalstad**  
Security and Mitigation  
Principal, Midwest Reliability  
Organization

Tuesday, Oct. 24 | 11:10AM  
Compliance is not a  
Cybersecurity Strategy



**Justin Heyl**  
Solutions and Cybersecurity  
Business Development  
Director, UL

Monday, Oct. 23 | 4:00PM  
Building the Future –  
Standards and Resources



**Todd Carpenter**  
Chief Engineer and Co-Owner,  
Adventium Labs

Monday, Oct. 23 | 2:30PM  
Moving Toward Future-  
Proofing Medical Device  
Security



**Joel Fulton**  
Chief Information Security  
Officer, Splunk

Monday, Oct. 23 | 3:00PM  
M&A Opportunities with  
Security  
Monday, Oct. 23 | 4:30PM  
Investing Through the Lens  
of Accredited Investors and  
Thought Leaders



**Ken Hoyme**  
Director, Product Security,  
Boston Scientific

Monday, Oct. 23 | 1:15PM  
Threat Briefing: Medical  
Device & Healthcare Delivery  
Organization-Specific  
Monday, Oct. 23 | 4:00PM  
Building the Future – Standards  
and Resources



**Pete Chestna**  
Director of Developer  
Engagement, Veracode

Monday, Oct. 23 | 2:30PM  
DevOps – Security's Big  
Opportunity  
Monday, Oct. 23 | 4:45PM  
Open Q+A



**Hala V. Furst**  
Cybersecurity and Technology  
Business Liaison, U.S.  
Department of Homeland  
Security

Tuesday, Oct. 24 | 9:30AM  
Real-Life Lessons Learned  
Tuesday, Oct. 24 | 1:45PM  
Cyber Security for Business  
Leaders



**Kevin Johnson**  
CEO, Secure Ideas

Tuesday, Oct. 24 | 11:10AM  
Compliance is not a  
Cybersecurity Strategy



**Loren Dealy Mahler**  
President, Dealy Mahler  
Strategies LLC

Tuesday, Oct. 24 | 3:45PM  
Having a Cyber  
Communications Plan



**Christopher Golomb**  
Supervisory Special  
Agent, Federal Bureau of  
Investigation

Monday, Oct. 23 | 1:15PM  
Threat Briefing: Medical  
Device & Healthcare Delivery  
Organization-Specific



**Mike Johnson**  
Senior Fellow, Technological  
Leadership Institute (TLI),  
University of Minnesota

Tuesday, Oct. 24 | 11:10AM  
Compliance is not a  
Cybersecurity Strategy



**Stephanie Domas**  
Lead Medical Security  
Engineer, Battelle  
DeviceSecure® Services

Monday, Oct. 23 | 2:30PM  
Moving Toward Future-  
Proofing Medical Device  
Security



**Chris Greco**  
Senior Director of Solution  
Development, BlackBerry

Tuesday, Oct. 24 | 3:45PM  
The Intersection of the  
Connected Worker and the  
Internet of Things



**Eran Kahana**  
Attorney, Maslon LLP

Monday, Oct. 23 | 1:15PM  
Threat Briefing: Medical  
Device & Healthcare Delivery  
Organization-Specific



**Chris Eng**  
VP of Security Research,  
Veracode

Monday, Oct. 23 | 4:15PM  
Veracode's DevSecOps  
Journey  
Monday, Oct. 23 | 4:45PM  
Open Q+A



**Slade Griffin**  
Director of Security  
Assessments, Contextual  
Security Solutions

Tuesday, Oct. 24 | 2:45PM  
Common Attack Vectors with  
Quick-Win Mitigations



**Michael Kearn**  
Co-Chair, Cyber Security Summit  
2017; Vice President, Information  
Security Officer, U.S. Bank

Tuesday, Oct. 24 | 8:00AM  
Welcome & Opening Remarks  
Tuesday, Oct. 24 | 4:45PM  
Meet the Threat Review & Beat  
the Threat Preview  
Wednesday, Oct. 25 | 9:30AM  
When the Levee Breaks  
Wednesday, Oct. 25 | 4:45PM  
An Overview – Practical  
Takeaways



**Drew Evans**  
Superintendent, Bureau of  
Criminal Apprehension

Wednesday, Oct. 25 | 3:30PM  
Information Sharing to Better  
Protect Companies in the U.S.



**Marshall Heilman**  
VP of Mandiant Consulting  
and Executive Director of  
Incident Response and Red  
Team Operations, FireEye

Tuesday, Oct. 24 | 2:00PM  
Got Spies in Your Wires?



**Bob Kinder**  
President, SixGen, LLC

Monday, Oct. 23 | 3:45PM  
Discussion on Defense M&A  
Monday, Oct. 23 | 4:30PM  
Investing Through the Lens  
of Accredited Investors and  
Thought Leaders



**Michael Krause**  
Supervisory Special Agent,  
Federal Bureau of Investigation  
Wednesday, Oct. 25 | 7:15AM  
FBI Career Opportunities  
Breakfast  
Wednesday, Oct. 25 | 11:00AM  
Incident Response Panel



**Dan Lyon**  
Principal Consultant,  
Synopsis Software Integrity  
Group  
Monday, Oct. 23 | 2:30PM  
Moving Toward Future-  
Proofing Medical Device  
Security



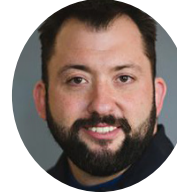
**Kathy Orner**  
Vice President, Chief Risk  
Officer, Carlson Wagonlit  
Travel  
Tuesday, Oct. 24 | 12:15PM  
CISO Luncheon  
(Invitation Only)



**Yan Kravchenko**  
Chief Information Security  
Officer, Atomic Data  
Tuesday, Oct. 24 | 2:45PM  
Risk Assessments and Being  
Prepared for an Attack



**Brad Maiorino**  
Executive Vice President,  
Booz Allen Hamilton  
Wednesday, Oct. 25 | 11:00AM  
Incident Response Panel



**Jay Radcliffe**  
Senior Security Consultant,  
Rapid7  
Monday, Oct. 23 | 1:15PM  
Threat Briefing: Medical  
Device & Healthcare Delivery  
Organization-Specific



**Mark Lanterman**  
Chief Technology Officer,  
Computer Forensic Services  
Wednesday, Oct. 25 | 7:15AM  
CEO/BOD Breakfast  
(Invitation Only)



**Cyrus Malek**  
Associate, Briggs  
and Morgan P.A.  
Tuesday, Oct. 24 | 2:15PM  
Cyber Case Studies and Legal  
Considerations



**Timothy Rank**  
Assistant United States  
Attorney, Deputy Criminal Chief,  
Fraud & Public Corruption  
Section, United States  
Attorney's Office  
Wednesday, Oct. 25 | 11:00AM  
Incident Response Panel



**Brent Lassi**  
VP of Information Security,  
CISO, Carlson Wagonlit Travel  
Tuesday, Oct. 24 | 12:15PM  
CISO Luncheon  
(Invitation Only)



**Eileen Manning**  
President and CEO, The Event  
Group, Incorporated  
Tuesday, Oct. 24 | 8:00AM  
Welcome & Opening Remarks  
Tuesday, Oct. 24 | 4:00PM  
What You're Up Against: Real  
Life Examples from a Small  
Business Owner  
Wednesday, Oct. 25 | 8:30AM  
Welcome & Opening Remarks



**Billy Rios**  
Founder, WhiteScope, LLC  
Monday, Oct. 23 | 1:15PM  
Threat Briefing: Medical  
Device & Healthcare Delivery  
Organization-Specific



**Lisa Beth Lentini**  
Assistant General Counsel –  
Compliance, Deluxe Corporation  
Wednesday, Oct. 25 | 11:00AM  
Incident Response Panel



**Tina Meeker**  
Owner & Principal, Beacon  
Information Security, LLC  
Monday, Oct. 23 | 4:30PM  
Investing Through the Lens  
of Accredited Investors and  
Thought Leaders



**Philip Schenkenberg**  
Attorney and Shareholder,  
Briggs and Morgan P.A.  
Tuesday, Oct. 24 | 2:15PM  
Cyber Case Studies and Legal  
Considerations



**Jim Libersky**  
President, Barrier1  
Wednesday, Oct. 25 | 4:00PM  
Running the Defense:  
Securing the Super Bowl



**Darren Meyer**  
Principal Security Researcher,  
Veracode  
Monday, Oct. 23 | 3:15PM  
Planning For A Responsive  
AppSec Program



**Lou Stephens**  
Vice President of Operations and  
Security, Sea Foam Corporation  
Wednesday, Oct. 25 | 11:00AM  
Moderator - Incident  
Response Panel



**Nancy Libersky**  
Minnesota District Director,  
U.S. Small Business  
Administration  
Tuesday, Oct. 24 | 1:30PM  
Small Business Forum  
Welcome



**Chris Olive**  
Senior Channel Engineer,  
North America, Thales  
e-Security  
Tuesday, Oct. 24 | 12:15PM  
CISO Luncheon  
(Invitation Only)



**Elizabeth Stevens**  
Co-Chair, Cyber Security Summit  
2017; Director, Enterprise  
Resiliency & Response,  
UnitedHealth Group  
Tuesday, Oct. 24 | 8:00AM  
Welcome & Opening Remarks  
Tuesday, Oct. 24 | 4:45PM  
Meet the Threat Review & Beat  
the Threat Preview  
Wednesday, Oct. 25 | 4:45PM  
An Overview – Practical  
Takeaways





**Bill Strub**  
 Founder & CEO, NaviLogic  
 Monday, Oct. 23 | 4:30PM  
 Panel Moderator: Investing  
 Through the Lens of  
 Accredited Investors and  
 Thought Leaders



**Bill Swearingen**  
 Director of Cyber Defense,  
 CenturyLink  
 Wednesday, Oct. 25 | 1:15PM  
 The Greatest Gift – Making  
 Attacks Expensive



**Scott Sweren**  
 Senior Security  
 Consultant, AT&T  
 Tuesday, Oct. 24 | 9:00AM  
 The Dark Web



**Catharine Trebnick**  
 Vice President, Equity Capital  
 Markets, Dougherty &  
 Company LLC  
 Monday, Oct. 23 | 2:00PM  
 Update on Cyber Security  
 Marketplace From IPO to  
 Seed Funding



**Larry Whiteside Jr.**  
 CEO, Whiteside Security LLC  
 Monday, Oct. 23 | 2:15PM  
 Discussion on Next-Generation  
 Techniques Replacing Legacy  
 Software Tools  
 Monday, Oct. 23 | 4:30PM  
 Investing Through the Lens  
 of Accredited Investors and  
 Thought Leaders



**Evan Wolff**  
 Partner, Crowell  
 and Moring LLP  
 Tuesday, Oct. 24 | 11:50AM  
 Breaches and Sensitive  
 Documents – How to Prepare,  
 Respond, and Protect  
 Yourself



**Jim Wolford**  
 CEO/Co-Owner, Atomic Data  
 Tuesday, Oct. 24 | 4:30PM  
 Small Business Forum Q&A



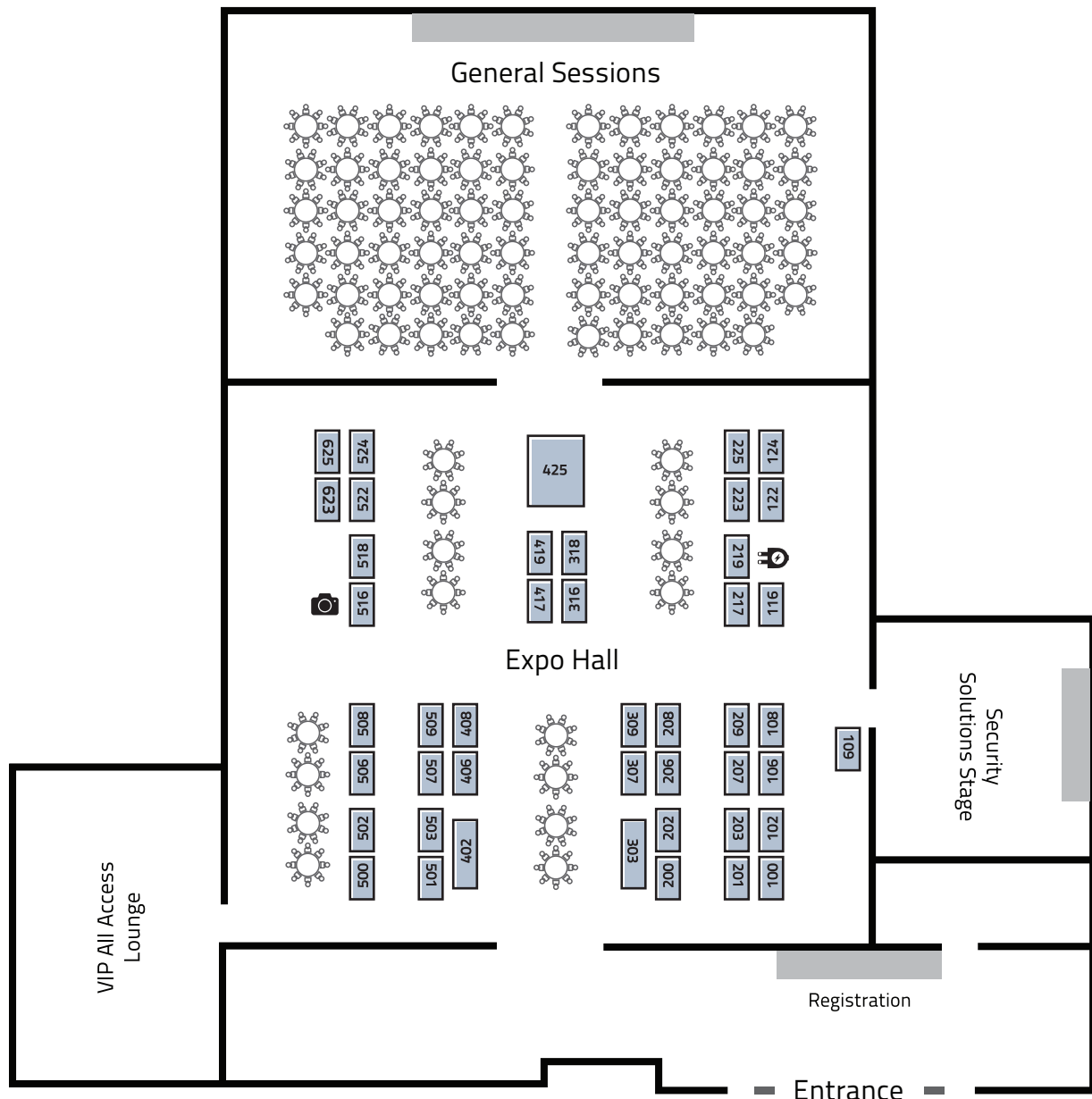
# STAY AHEAD OF THE CYBER SECURITY CURVE

Today, your organization is caught between an ever-growing number of smart, sophisticated cyber attacks and an army of hyper-connected customers, employees, suppliers and partners who simply expect access to information any time, from anywhere.

[centurylink.com/enterprise](http://centurylink.com/enterprise)

**Reduce risk. Fill the expertise gap.  
 Complement staff resources.  
 Satisfy security requirements.  
 Visit us at booth 307.**





## Exhibitor Directory

419 Atomic Data	318 Computex	625 Mimecast	522 Securonix
425 AT&T	518 Datashield	202 Mitchell Hamline	108 Signal Sciences
201 Backbone Consulting	501 FBI	508 MNC3	116 Sirius
200 Barrier1	309 FireEye	507 MN State IT Center of Excellence	219 Skyhigh Networks
102 BBB	509 Gurucul	223 Navilogic	209 Synack
203 Black Duck Software	503 InfraGard	124 Okta	208 Target
303 BlackBerry	506 ISACA	207 Pluralsight	217 Thales
524 Booz Allen Hamilton	500 (ISC)2	122 Proofpoint	402 University of Minnesota (TLI)
109 Centrifry	502 ISSA	516 RSA	408 Veracode
307 CenturyLink	316 Lifeline Data Centers	100 SBA	406 Wipfli
417 Cisco	225 LogRhythm	206 Security B-Sides MSP	
623 Colliers IT	106 Metropolitan State University		



Connected

Protected

The more data and insights a company has, the better it is for business. And the more vulnerable they become to threats. At AT&T, we secure our entire network to help keep your business protected.





# CYBERSECURITY

## NATIONAL FOCUS SECTION

**November 20, 2017**

BridgeTower Media editors take a close look at how market dynamics, legislation, competitive trends & new technologies in the cybersecurity sector affect the business & practices of the over 300,000 readers of BridgeTower Media Brands.

### TOPICS INCLUDE:

- » Holding back - CEOs, CFOs, & CIOs each perceive different reasons for companies' IT security deficiencies
- » The four growing threats: Nuisance hacking; hacking for dollars; intellectual property theft; hacktivism
- » The increasing sophistication of cyber attacks
- » The risks of employee & customer mobile devices: They must be considered on par with laptop computers that have their own powerful peer-to-peer networks
- » Security in the cloud: As security of the cloud model improves, organizations are entrusting more sensitive data to cloud providers

**REACH INDUSTRY LEADERS IN MORE THAN 20 MARKETS!**

BridgeTower's **27** print & digital **publications** cover legal, financial, real estate & government news in over **20** different **markets.**

Our subscribers are affluent, well-educated **decision makers.**

### PACKAGE RATES (ALL PRICES ARE NET RATES):

✓ **Half or full page advertisement or native article to run across all publications, in print & digital format:**

- \$15k for full page advertisement or advertorial in all publications & native online
- \$10k for half page advertisement or advertorial in all publications & native online

✓ **A National webinar marketed to over 200k permissioned names across BridgeTower Media**

- Add \$8k to any package above
- \$15k as standalone item

✓ **Finance & Commerce and Minnesota Lawyer Combo special**

- Reach our entire audience with one simple buy
- 1/2 pg ad, Co-branded Email and 2 weeks online ad \$1,500

**Demonstrate your thought leadership & expertise by participating in this focus section!**

David Seawell: (612) 584-1545 dseawell@finance-commerce.com  
Troy Williams: (612) 584-1524 twilliams@finance-commerce.com

SAINT PAUL LEGAL LEDGER  
**MINNESOTA LAWYER**  
**FINANCE & COMMERCE**



SUPPORTING  
SPONSOR

The Association for the Advancement of Medical Instrumentation (AAMI) is a nonprofit organization founded in 1967. It is a diverse community of approximately 7,000 professionals united by one important mission—the development, management, and use of safe and effective healthcare technology.

4301 N. Fairfax Drive, Suite 301  
Arlington, VA 22203  
703.525.4890

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



PLATINUM  
SPONSOR

At AT&T, we believe the best approach to securing your digital assets from cyberthreats is an integrated multilayer approach that offers end-to-end protection. Our cybersecurity solutions provide you with the tools to prevent, detect, and respond to threats. Our network security solutions deliver unparalleled visibility, responsive analytics, and strategic alliances. AT&T cybersecurity solutions provide a revolutionary security experience, so you can focus on the business opportunities that technology brings.

[www.business.att.com](http://www.business.att.com)



SUPPORTING  
SPONSOR

Better Business Bureau of Minnesota and North Dakota is proud to be known as "the first BBB!" We're a non-profit organization founded by ethical business owners in the Twin Cities in 1912. The BBB is supported today by more than 7,000 locally Accredited Businesses that believe in our mission.

220 S. River Ridge Circle  
Burnsville, MN 55337  
651.699.1111  
ask@thefirstbbb.org

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

Adventium Labs

CONTRIBUTOR

Adventium Labs is an award-winning research and development company that blends automated reasoning, systems engineering, and cyber security to solve challenges of national importance. Adventium recently announced Magrana® Server, its robust, high-security server virtualization product which provides strong isolation to meet strict separation requirements with commodity commercial servers.

111 Third Ave South, Suite 100  
Minneapolis, MN 55401

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

Backbone Consultants

SILVER  
SPONSOR

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

50 South 6th Street, Suite 1360  
Minneapolis, MN 55402  
Lauren Carlson / 612.568.7167  
info@backboneconsultants.com

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



SUPPORTING  
SPONSOR

The Business Continuity Planners Association (BCPA), based in Minneapolis-St. Paul, has supported business professionals with a non-profit, mutual benefit association for those participating in business recovery, crisis management, emergency management, contingency planning, disaster preparedness planning, or a related professional vocation since 1994.

P.O. Box 390394  
Edina, MN 55439  
info@bcpa.org

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

Atomic Data

SILVER  
SPONSOR

Atomic Data works with your IT department or acts as your IT department to design, equip, and maintain the solutions for today's challenging IT environments. Atomic Data's areas of expertise include: The Atomic Cloud® private virtualization, data center colocation, disaster recovery consulting, compliance as a service, security consulting, private connectivity, 24x7 network monitoring and Service Desk support, on-site support, custom software development, voice solutions and more.

615 North 3rd Street  
Minneapolis, MN, 55401

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

Barrier1

BRONZE  
SPONSOR

Barrier1 is a cyber security company that was designed a Patented Real Time AI-Neural Network platform that identifies and stops the known cyber attack within sub second time. Our patented approach has proven to be far more Effective, Accurate, Faster and Affordable than any other approach and has been validated by various 3rd parties. Barrier1 has been recognized by SC Mag as Innovator of the Year for 3 straight years and then selected into the SC Mag Hall of Fame.

Jim Libersky / 763.230.1041

[www.barrier1.com](http://www.barrier1.com)



SUPPORTING  
SPONSOR

Security B-Sides MSP is the Minneapolis-St. Paul chapter of the global Security B-Sides community, which focuses on providing a launch pad for security professionals and hands-on, engaging security training.

info@bsidesmsp.org

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



PRESENTING  
SPONSOR

BlackBerry is a mobile-native security software and services company dedicated to securing people, devices, processes and systems for today's enterprise. Based in Waterloo, Ontario, the company was founded in 1984 and operates in North America, Europe, Asia, Middle East, Latin America and Africa. The Company trades under the ticker symbols "BB" on the Toronto Stock Exchange and "BBRY" on the NASDAQ.

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



GOLD  
SPONSOR

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

2200 IDS Center, 80 South 8th Street,  
Minneapolis, MN 55402  
Phil Schenkenberg / 612.977.8246  
pschenkenberg@briggs.com

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



SUPPORTING  
SPONSOR

CIOReview provides influential IT and business executives with in-depth coverage of the topics most critical to their organization's IT infrastructure. CIOReview is where senior-level IT buyers and decision-makers come to learn about and share their experiences with other technology executives regarding products, technologies and technology trends.

44790 S. Grimmer Blvd. #202  
Fremont, CA 94538  
510.565.7624  
editor@cioreview.com

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

Black Duck Software

SILVER  
SPONSOR

Organizations worldwide use Black Duck Software's industry-leading products to automate the processes of securing and managing open source software, eliminating the pain related to security vulnerabilities, open source license compliance and operational risk. Black Duck is headquartered in Burlington, MA, and has offices in San Jose, CA, London, Frankfurt, Hong Kong, Tokyo, Seoul and Beijing.

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



DIAMOND  
SPONSOR

Centrify redefines security from a legacy perimeter-based approach, to protecting millions of connections in a boundaryless hybrid enterprise. As the only industry recognized leader in both Privileged Identity Management and Identity-as-a-Service, Centrify provides a single platform to secure access to apps and infrastructure through the power of identity services.

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



Cisco Security

PLATINUM  
SPONSOR

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

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

Booz | Allen | Hamilton

PRESENTING  
SPONSOR

Booz Allen brings expertise hardened by experience in the most formidable environments to deliver intelligence-driven cybersecurity. We protect the most sensitive national security organizations, and are the trusted defender of global companies. We protect our clients against the attacks of today, and prepare them for the threats of tomorrow.

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



DIAMOND  
SPONSOR

CenturyLink (NYSE: CTL) is a global communications and IT services company focused on connecting its customers to the power of the digital world. CenturyLink offers network and data systems management, big data analytics, managed security services, hosting, cloud, and IT consulting services. The company provides broadband, voice, video, advanced data and managed network services over a robust 265,000-route-mile U.S. fiber network and a 360,000-route-mile international transport network.

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



PLATINUM  
SPONSOR

Computex Technology Solutions is an award-winning solutions provider committed to helping our clients evolve their business through technology, for the past 30 years. At our core we are architects and engineers that specialize in delivering data centers, enterprise networking, cybersecurity and cloud & managed services.

[www.computex-inc.com](http://www.computex-inc.com)

# Investigate attacks like never before

Attackers can pivot through your infrastructure,  
now you can pivot through theirs.



Learn more at

**BOOTH 417**



Cisco Umbrella

# The Difference

## What's the difference between acting and reacting to threats?

---

It's about being in **control of the new**, not just the hidden.

The **difference** is **FireEye**.

---

Interested in further discussion?  
Please visit us at booth #309





**Crowell & Moring LLP**SILVER  
SPONSOR

Crowell & Moring LLP is an international law firm with approximately 500 lawyers representing clients in litigation and arbitration, regulatory, and transactional matters. The firm is internationally recognized for its representation of Fortune 500 companies in high-stakes litigation, as well as its ongoing commitment to pro bono service and diversity. The firm has offices in Washington, DC, New York, Los Angeles, San Francisco, Orange County, London, and Brussels.

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

SUPPORTING  
SPONSOR

Cyber Defense Magazine is by ethical, honest, passionate information security professionals for IT Security professionals. Our mission is to share cutting edge knowledge, real world stories and awards on the best ideas, products and services in the information technology industry.

PO Box 8224,  
Nashua, NH 03060  
800.518.5248  
[info@cyberdefensemagazine.com](mailto:info@cyberdefensemagazine.com)

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

**Datashield**BRONZE  
SPONSOR

Datashield provides customers with true 24x7x365 SOC capabilities that go beyond log management to understand the full scope of an incident from the network to the endpoint. As a Managed Detection and Response provider our primary objective is to properly monitor, detect, investigate and communicate critical incidents in our customer's environments.

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

**FINANCE & COMMERCE**SUPPORTING  
SPONSOR

Minneapolis-based Finance & Commerce, which publishes Tuesday through Saturday, focuses on commercial real estate, construction, economic development, regional planning, transportation and transit. Finance and Commerce Inc. is also the publisher of the Minnesota Lawyer weekly and the St. Paul Legal Ledger.

222 South Ninth Street, Suite 2300  
Minneapolis, MN 55402  
Bill Gaier / 612.584.1537  
[bgaier@finance-commerce.com](mailto:bgaier@finance-commerce.com)

[www.finance-commerce.com](http://www.finance-commerce.com)

TYPE OF  
SPONSORSHIP

The Premiere Cyber Security Company – protects both large and small organizations committed to stopping advanced cyber threats, data breaches, and zero-day attacks. Organizations across various industries trust FireEye to secure their critical infrastructure and valuable assets, protect intellectual property and avoid bad press, costly fixes, and downtime.

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

**Gurukul**SILVER  
SPONSOR

Gurukul helps enterprises protect themselves against cyber fraud, insider threats and external intruders on-premises and in the cloud. User and entity behavior analytics (UEBA) and identity analytics (IdA) from machine learning anomaly detection and predictive risk-scoring algorithms reduces the attack surface for accounts, unnecessary access rights, and to identify, predict and prevent breaches.

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

SUPPORTING  
SPONSOR

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)

SUPPORTING  
SPONSOR

Nearing its 50th year, ISACA is a global association helping individuals and enterprises achieve the positive potential of technology. Today's world is powered by technology, and ISACA equips professionals with the knowledge, credentials, education and community to advance their careers and transform their organizations.

3701 Algonquin Road, Suite 1010  
Rolling Meadows, IL 60008  
847.253.1545

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

SUPPORTING  
SPONSOR

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

Scott Stone  
[President@isc2tc.org](mailto:President@isc2tc.org)

[www.isc2tc.org](http://www.isc2tc.org)



SUPPORTING  
SPONSOR

The Minnesota chapter of the Information Systems Security Association (ISSA) is a not-for-profit organization of information security professionals and practitioners focused on promoting a secure digital world. Our goal is to be the community of choice for cybersecurity professionals dedicated to advancing individual growth, managing technology risk and protecting critical information and infrastructure.

Aaron Molenaar  
communications@mnessa.org

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



AV PARTNER

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

4923 Boone Ave N  
Minneapolis, MN 55428  
Rob McCarthy / 763.478.8184  
rmccarthy@maplelanemedia.com

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

Metropolitan State  
University

EXHIBITOR

Metropolitan State University offers many graduate programs such as Master of Management Information Systems (MMIS), Master in Computer Science, MBA and DBA. These programs are high quality, practical and flexible to accommodate your busy lifestyle.

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



PLATINUM  
SPONSOR

Since 2001, Lifeline Data Centers has helped companies lead in security and compliance, improve uptime and control data center facilities operating expense. Lifeline is an innovator in Cloud and wholesale colocation by continually finding ways to reduce downtime risks while driving down costs.

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

MASLON

GOLD  
SPONSOR

Maslon LLP offers a depth of experience in the principal areas of Business & Securities, Financial Services, and Litigation—with nationally recognized practices in a variety of areas. To further support our clients, we have focused practices in Intellectual Property, Employee Benefits, Labor & Employment, Mergers & Acquisitions, Tax, Estate Planning, Bankruptcy, Corporate Trust Representation, Real Estate, Advertising & Marketing, Insurance Litigation and Cybersecurity Law.

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



SUPPORTING  
SPONSOR

Minnesota Cyber Careers Consortium (MnC3) is a program of Minnesota Innovation Lab (MNI Lab), a 501(c)(3) non-profit organization which empowers entities to foster commercial vitality and collectively impact the public good by leveraging their assets and connecting the dots in new ways. As a part of MNI Lab, MnC3 is envisioned as one key grassroots educational collaboration strategy to grow a Cyber Innovation Cluster (CiC) in Minnesota.

[www.mnc3.org](http://www.mnc3.org)



The Security Intelligence Company

PLATINUM  
SPONSOR

LogRhythm is the largest and fastest growing independent security intelligence company in the world. The company's patented and award-winning Security Intelligence Platform, unifies SIEM, log management, file integrity monitoring, network forensics and host forensics, empowering organizations around the globe to detect and respond to breaches and the most sophisticated cyber threats.

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



SUPPORTING  
SPONSOR

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

1333 H Street NW, Suite 400 West  
Washington, DC 20005  
202.354.7171

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



STUDENT  
BREAKFAST  
SPONSOR

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

658 Cedar Street  
St. Paul, MN 55155

[www.mn.gov/mnit](http://www.mn.gov/mnit)

# No data breaches

**We're authorized to store top-secret government data.**

**Can your cloud and data provider say that?**



Our FedRAMP compliance prevents breaches due to our processes, architecture and physical security. We provide this exact design and controls to corporate America as well.

We are the only FedRAMP authorized data center in the Midwest and the only one in the country that provides EMP-shielding protection.

Indiana facilities and Indiana employees.



SECURE • COMPLIANT • SIMPLE

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

# How quickly can your team detect and respond to a cyberthreat?



## DO IT FASTER WITH THREAT LIFECYCLE MANAGEMENT.

We can help. The LogRhythm Platform empowers your team to detect and respond to cyberattacks—fast. Work more efficiently and effectively to protect your organization from today's most advanced threats.

See LogRhythm in action: [logrhythm.com/demo](https://logrhythm.com/demo)



SUPPORTING  
SPONSOR

Minnesota State IT Center of Excellence, formerly Advance IT Minnesota, works with employers, educators, and learners to develop a more robust IT Workforce in Minnesota. The Center has engaged with thousands of secondary students, funded dozens of new curriculum efforts, and led numerous other efforts aimed at increasing the quantity and quality of IT talent in the state.

1380 Energy Lane, Suite 104  
St. Paul, MN 55108  
612.659.7221  
advanceitmn@metrostate.edu

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

Okta

SILVER  
SPONSOR

Okta is the leading provider of identity for the enterprise. The Okta Identity Cloud connects and protects employees of many of the world's largest enterprises. It also securely connects enterprises to their partners, suppliers, and customers. With deep integrations to over 5,000 apps, the Okta Identity Cloud enables simple and secure access from any device for thousands of customers, including Experian, 20th Century Fox, LinkedIn, and Adobe.

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

RSA

SILVER  
SPONSOR

RSA provides more than 30,000 customers around the world with the essential security capabilities to protect their most valuable assets from cyber threats. With RSA's award-winning products, organizations effectively detect, investigate, and respond to advanced attacks; confirm and manage identities; and ultimately, reduce IP theft, fraud, and cybercrime.

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



MITCHELL | HAMLINE  
School of Law

BRONZE  
SPONSOR

Cybersecurity and Privacy Law Certificate at Mitchell Hamline School of Law – Learn from industry experts in this 13-week online program studying complex legal, policy and compliance challenges associated with cyber threats. Professionals watch lectures from nationally recognized experts, participate in discussions, and complete practical hands-on exercises.

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

Pluralsight

SILVER  
SPONSOR

For enterprises building their digital future, Pluralsight is the only technology learning platform that gives you a true competitive advantage. With Pluralsight, companies attract and grow talent, ship better products faster and improve performance. Our platform evaluates the technical abilities of your teams, aligns learning to key business objectives, and closes skills gaps in critical areas like cloud, mobile, security and data.

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

Securonix

BRONZE  
SPONSOR

Securonix is re-defining the next generation of cyber-threat detection using the power of entity context, machine learning, and big data. Our purpose-built security analytics platform enriches, analyzes and scores events into actionable intelligence. Using machine learning techniques, Securonix detects insider threat, cyber threat and fraud attacks in real-time.

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



GOLD  
SPONSOR

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

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

Proofpoint

SILVER  
SPONSOR

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

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

Signal Sciences

BRONZE  
SPONSOR

Signal Sciences is revolutionizing application security with the industry's first Web Protection Platform (WPP), bringing real-time protection to both security and engineering teams. Signal Sciences WPP provides comprehensive threat protection and security visibility for web applications, microservices, and APIs on any platform.

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

Sirius

GOLD  
SPONSOR

Sirius is a national integrator of technology-based business solutions that span the enterprise, including the data center and lines of business. Built on products and services from the world's top technology companies, Sirius solutions are installed, configured and supported by our dedicated teams of highly certified experts.

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

WIFI  
SPONSOR

**In a hectic world,  
we provide peace of mind.**

Smart City is the nation's most experienced and versatile provider of utilities, technology and telecommunications services for the meeting and convention industry. With more than 30 years of experience, we operate in more than 35 convention and meeting facilities nationwide.

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

THALES

DIAMOND  
SPONSOR

Thales e-Security is the leader in advanced data security solutions and services that deliver trust wherever information is created, shared or stored. Security professionals around the globe rely on Thales to confidently accelerate their organization's digital transformation. Thales e-Security is part of Thales Group.

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

Skyhigh Networks

SILVER  
SPONSOR

Skyhigh Networks, the world's leading Cloud Access Security Broker (CASB), enables enterprises to safely adopt SaaS, PaaS and IaaS cloud services, while meeting their security, compliance and governance requirements.

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

Synack

SILVER  
SPONSOR

Synack's hacker-powered security platform arms clients with hundreds of the world's most skilled, highly vetted ethical hackers who provide a truly adversarial perspective of clients' IT environments. Synack's confidential client base is comprised of some of the largest F500/G500 enterprise organizations across banking and financial services, healthcare, consumer goods and retail, manufacturing, technology and the U.S. Federal Government.

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

 TECHNOLOGICAL  
LEADERSHIP INSTITUTE
FOUNDING  
PARTNER

The Technological Leadership Institute (TLI) bridges the knowledge gap between business and technology by taking bright individuals and producing global leaders. Founded in 1987, TLI is an interdisciplinary center created with an endowment from the Honeywell Foundation. TLI's endowed faculty chairs and more than 40 faculty members from across eight University of Minnesota colleges, government, and industry bring an exceptionally rich learning environment for the career development needs of its students and technical professionals.

[www.tli.umn.edu](http://www.tli.umn.edu)

SUPPORTING  
SPONSOR

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

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

Target

BRONZE  
SPONSOR

Minneapolis-based Target Corporation serves guests at 1,797 stores and at Target.com. Since 1946, Target has given 5 percent of its profit to communities, which today equals more than \$4 million a week. For more information, visit Target.com/Pressroom. For a behind-the-scenes look at Target, visit Target.com/abullseyeview or follow @TargetNews on Twitter.

[www.target.com/abullseyeview](http://www.target.com/abullseyeview)

 UNISYS | Securing Your  
Tomorrow™
PRINTING  
SPONSOR

At Unisys, we assess, design, develop, and manage mission-critical solutions that secure resources and infrastructure for governments and businesses. Our approach integrates resource and infrastructure security, creating the most effective and efficient security environment possible and freeing our client to focus on best serving its citizens and customers.

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

# Securing your digital transformation

Wherever safety and security matter, we deliver

PCI DSS EXPERTISE

SECURING CRITICAL DATA

ENCRYPTION, TOKENIZATION

MEETING REGULATORY COMPLIANCE

CENTRALIZED KEY MANAGEMENT

LEADING TECHNOLOGY PARTNERSHIPS

# THALES

Together • Safer • Everywhere

Search: Thales eSecurity



## SECURE360

May 15-17, 2018  
Minneapolis Convention Center  
Minneapolis, MN

EARLY-BIRD REGISTRATION NOW OPEN

REGISTER TODAY:

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

80+  
sessions

100+  
exhibitors

1500  
attendees



## Unisys Security Solutions

Unisys Security Solutions combines experienced consulting, advanced products and managed services for the entire security lifecycle: prediction, prevention, detection, and remediation of advanced threats.





SUPPORTING  
SPONSOR

UMSA (Upper Midwest Security Alliance) is an alliance of security and risk-related organizations. As a nonprofit founded in 2004, UMSA 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.

8014 Olson Memorial Hwy., Suite 234  
Minneapolis, MN 55427  
director@umsa-security.org

[www.umsa-security.org](http://www.umsa-security.org)



BRONZE  
SPONSOR

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

[www.wipfli.com/cybersecurity](http://www.wipfli.com/cybersecurity)



DIAMOND  
SPONSOR

Veracode is a leader in securing web, mobile and third-party applications for the world's largest global enterprises. By enabling organizations to rapidly identify and remediate application-layer threats before cyberattackers can exploit them, Veracode helps enterprises speed their innovations to market – without compromising security.

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

## Cyber Security Summit 2018

Stay connected to  
[cybersecuritysummit.org](http://cybersecuritysummit.org)  
to follow updates on next  
year's event!



# SAVE THE DATE

October 22-24, 2018

@ The Minneapolis Convention Center

# Cyber Security Terminology

## ACCESS CONTROL

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

## ADVANCED PERSISTENT THREAT (APT)

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

## AIR GAP

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

## ATTACK PATH

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

## ATTACK PATTERN

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

## ATTACK SIGNATURE

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

## AUTHENTICATION

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

## AUTHORIZATION

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

## BACKDOOR

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

## BEHAVIOR MONITORING

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

## BLACKLIST

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

## BLUE TEAM

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

## BOT

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

## BUG

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

## BUILD SECURITY IN

A set of principles, practices, and tools to design, develop, and evolve information systems and software that enhance resistance to vulnerabilities, flaws, and attacks.

## CHECKSUM

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

## CIP

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

## CIPHERTEXT

Data or information in its encrypted form.

## CLOUD COMPUTING

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

## COMPUTER (DIGITAL) FORENSICS

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

## CONTINUITY OF OPERATIONS PLAN

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

## CRITICAL INFRASTRUCTURE

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

## CRYPTANALYSIS

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

**CSIRT**

Cyber Security Incident Response Team

**CYBER MUNITIONS**

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

**DATA BREACH**

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

**DATA LOSS PREVENTION**

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

**DATA MINING**

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

**DENIAL OF SERVICE (DOS)**

An attack that prevents or impairs the authorized use of information system resources or services.

**DIGITAL FORENSICS**

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

**DIGITAL RIGHTS MANAGEMENT (DRM)**

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

**DIGITAL SIGNATURE**

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

**DISTRIBUTED DENIAL OF SERVICE (DDOS)**

A denial of service technique that uses numerous systems to perform the attack simultaneously.

**DMZ**

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

**DOXING**

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

**DYNAMIC ATTACK SURFACE**

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

**ELECTRONIC SIGNATURE**

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

**ENTERPRISE RISK MANAGEMENT**

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

**EVENT LOGS**

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

**EXFILTRATION**

The unauthorized transfer of information from an information system.

**EXPLOIT**

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

**EXPOSURE**

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

**FIREWALL**

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

**HASH VALUE**

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

**HASHING**

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

**IDENTITY AND ACCESS MANAGEMENT**

The methods and processes used to manage subjects and their authentication and authorizations to access specific objects.

**INCIDENT**

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

**INCIDENT HANDLER (CYBER SECURITY)**

The person assigned to lead a team of subject matter experts in cyber security and how to respond to adverse security events.

**INDUSTRIAL CONTROL SYSTEM**

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

**INTEGRITY**

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

**INTRUSION DETECTION**

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

**KEYLOGGER**

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

**MACRO VIRUS**

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

**MALWARE**

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

**MSSP**

Managed Security Service Provider

**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.

**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 TOOLS**

Tools that are made with open source code.

**OPEN SOURCE INTELLIGENCE**

Intelligence collected from publicly available sources

**OPERATIONAL EXERCISE**

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

**PACKET CAPTURES**

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

**PENETRATION TESTING (PEN TEST)**

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

**PHISHING**

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

**PRIVATE KEY**

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

**PUBLIC KEY**

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

**RDP**

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

**RECOVERY**

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

**RED TEAM**

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

**REDUNDANCY**

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

**RESILIENCE**

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

**RESPONSE**

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

**RISK MANAGEMENT**

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

**ROAMING PROFILE**

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

**ROOTKIT**

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

**SCRIPTKIDDIE**

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

## SECURITY AUTOMATION

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

## SECURITY POLICY

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

## SIEM

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

## SIGNATURE

A recognizable, distinguishing pattern.

## SITUATIONAL AWARENESS

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

## SOFTWARE ASSURANCE

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

## SPEARPHISHING

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

## SPOOFING

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

## SPYWARE

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

## TABLETOP EXERCISE

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

## THREAT AGENT

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

## THREAT ASSESSMENT

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

## TICKET

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

## TOPOLOGY DIAGRAM

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

## TRAFFIC LIGHT PROTOCOL

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

## TROJAN HORSE

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

## VIRUS

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

## VULNERABILITY

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

## WHITE TEAM

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

## WHITELIST

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

## WORK FACTOR

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

## WORM

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

## ZERO DAY

The Zero Day is the day a new vulnerability is made known. In some cases, a zero day exploit is referred to an exploit for which no patch is available yet. (Day one is day at which the patch is made available).

# Breaches, Breaches + More Breaches



**Mike Johnson**

*Senior Fellow, Technological Leadership Institute (TLI), University of Minnesota*

In the last month alone, we have learned that Yahoo! actually lost \$3 billion of our account records; trusted cybersecurity consultancy Deloitte announced a breach of their internal systems; the U.S. Securities and Exchange Commission shared that the EDGAR database had been compromised (more than a year ago); and Equifax finally told us that they lost 145 million of our most sensitive personal and financial records earlier this year.

These shocking revelations have made announcements of data breaches from retailers like Sonic Drive-Ins and Whole Foods appear almost mundane and barely worthy of news coverage compared to the current state of the larger cybersecurity problem.

If you are a seasoned security professional, most breach announcements have tended to roll off our backs. We are familiar with the challenges of security systems and networks, and the constantly evolving threat environment, and we understand that there is no such thing as 100 percent secure. Our days are consumed with trying to keep up with the endless patching and systems management that is a foundation of what we hope is an effective information security risk management program; and with implementing better tools to monitor an improved process to manage our dynamic and interconnected environments. We fight for resources and funding against a myriad of other business priorities, including activities that actually generate revenue and increase the stock price, something in which senior management and boards of directors are pretty interested.

So how do cybersecurity professionals battle these priorities? After all, increased business success is a good thing for everyone at a company, since we all want our businesses to still be here so we can come back to work tomorrow and earn a paycheck. When will the reality of the potential impact from a cyber event be enough to finally get the attention of the right leaders in your company and how can we attain this basic goal?

While improved cybersecurity awareness activities and possibly stronger regulations may help, I believe the problem starts with leadership. Both business and security leaders hold some of the blame for the state we are in. The world needs more business leaders that understand all the risks facing their organizations — including risks to data and systems from cyber threats — and realize that we have an ethical and moral obligation to protect to the best of our abilities the sensitive data entrusted to us by our customers (or in the case of Equifax, by the population in general). We must do what is right and make sure that taking those actions works for both the business bottom line and the expectations of the people who are impacted by our failures.

Security leaders need to be better communicators who are more effective at sharing the message of cyber risk. We need to make the business case for comparing risks and investments for cyber security with priorities from all areas of the organization. We need to build enterprise plans that incorporate the right people, policies and procedures to make cybersecurity capabilities' successes and weaknesses transparent to business leadership, and to help them understand the repercussions of the lack of success in this area. Leading cyber security cannot be only about acquiring the newest tools and technology that promise to solve our security problem. Communications and influence skills take practice, and security leaders need to always be learning, about security risks and technologies, as well as business needs and drivers. Security leadership can and must be the facilitator that will hopefully help organizations do the right thing and turn the corner on improving the security of our most important asset, our personal data, before there is nothing left to protect.









# 3 KEYS TO EFFECTIVE INCIDENT RESPONSE

Cyber incidents impact business operations and manifest themselves in various forms and levels of severity. They can touch every facet of your business, which can have a tremendous effect on your reputation and the trust you've established. An effective cyber incident response plan considers and involves the whole enterprise. A business, in its entirety, can be ready to respond more diligently if it takes into account the following tips.



## Create a Holistic Plan

Create an incident response plan to prepare your company for two distinct, but interconnected, incident response purposes: Technical containment and resolution of the issue, and broader corporate risk mitigation. Effective cyber incident management extends beyond incidents. Your steady state—planning/preparing and post-incident improvement activities—are equally important. The response plan should reflect enterprise-wide roles and may address specific scenarios and how to mitigate their impact to the business. Drafting an initial plan requires effort to determine how people, processes, and technology work together across business functions. Consider both technical and corporate response roles. Once the plan is created, disseminate it to relevant stakeholders to ensure awareness and familiarity. The C-suite should communicate consistent support and encourage working relationships between business units and the IT department. This way, IT is empowered to share and enforce basic cyber security measures among staff, and staff will turn to the IT department when suspicion arises.



## Test the Plan and Know the Roles

The most effective way to know how prepared you are for a cyber incident is to simulate one through an exercise to gauge your response. Testing not only gives you an assessment, but it can also help in keeping your plan updated to evolve with changes in threats, tools, and resources. These practice scenarios, often called “wargaming”, can provide clarity on strengths and gaps within the organization, help you identify sufficient tools and resources, establish and clarify lines of authority, and designate response roles. This testing entails more than just making sure employees are trained on tools and procedures; they must be able to detect and remediate an incident—real or fictional. Wargaming serves to manage realistic situations and bring together the diverse set of groups that need to work collaboratively to respond.



## Increase Awareness

Once the plans have been written and tested, keep up momentum and continued awareness about cyber risks. Engage your corporate communications or training department to help staff learn about cyber security in a way that is meaningful to their roles. In addition to internal messaging, make sure cyber incidents are incorporated into your organization's crisis communications capability. Organizations can benefit from having a crisis communications plan for a cyber incident, as well as designated spokespersons who are media-trained prior to an incident. You can also prepare in non-crisis times by setting up a responsible disclosure portal or by incorporating cyber information into your marketing materials.

## KEY TAKEAWAY:

Have a cyber incident response plan that is enterprise-wide and uses a tested, all-staff approach to help resolve cyber incidents quicker and more transparently. Given that cyber threats are omnipresent, an incident may be all but inevitable. Fortunately, smart and proactive incident response planning can minimize the impact to your business.

---

For more information, contact:

**Jason Escaravage**  
Senior Vice President  
Escaravage\_Jason@bah.com  
+1-703-984-2200

[www.BoozAllen.com/cyber](http://www.BoozAllen.com/cyber)

---

About Booz Allen Hamilton

Booz Allen Hamilton has been at the forefront of strategy, technology, and engineering for more than 100 years. Booz Allen partners with public and private sector clients across the globe to solve their most difficult challenges. To learn more, visit [www.boozallen.com](http://www.boozallen.com). (NYSE: BAH)



***BlackBerry® Secure™***

---

# **CYBERATTACKS ARE ON THE RISE**

---

**Are your Data, Apps and  
Users Secure?**

**Are You BlackBerry Secure?**

[www.blackberry.com/secure](http://www.blackberry.com/secure)



CELEBRATING

20 YEARS 1997-2017



the  
**EVENT  
GROUP**  
incorporated

After two decades of event production, marketing and strategic planning, we've got some stories to share.

Read some of our lessons learned at [plantoastound.com/milestones.html](http://plantoastound.com/milestones.html)