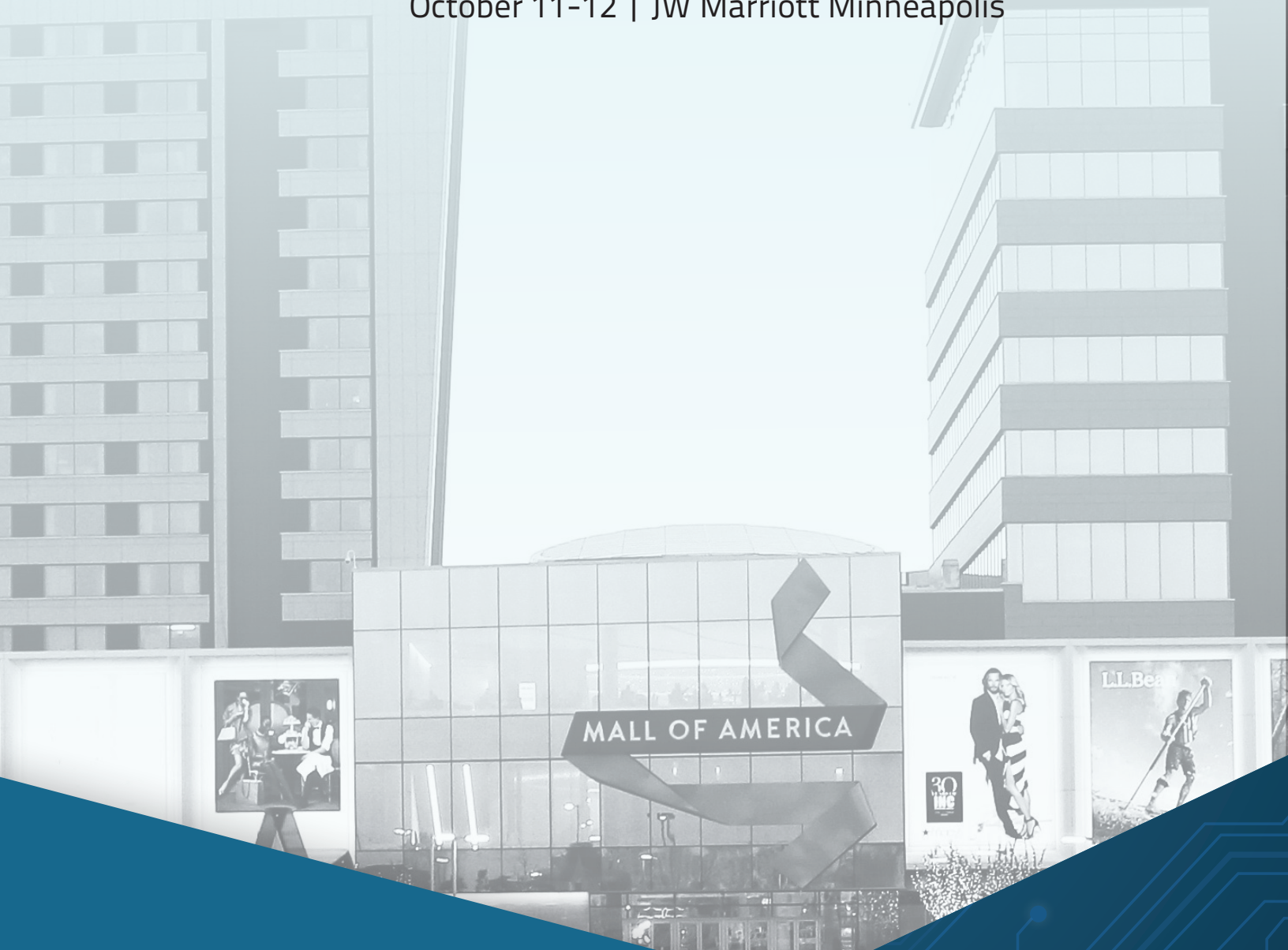


SIXTH ANNUAL EVENT



CYBER SECURITY SUMMIT 2016

October 11-12 | JW Marriott Minneapolis





TECHNOLOGICAL LEADERSHIP INSTITUTE

MASTER of SCIENCE

Security Technologies

Prevent
& Protect

tli.umn.edu

Join the Next Cohort of Security Leaders

Enhance the skills needed to prevent, protect and respond to today's security demands with an **M.S. in Security Technologies** from the University of Minnesota Technological Leadership Institute. Our proven curriculum and expert faculty will provide students with the expertise to lead in this growing career field. Attend an information session to learn how a graduate degree in Security Technologies can help advance your career!

Upcoming Information Sessions:

- Wednesday, November 9, 5:30PM - 7:00PM
- Monday, December 5, 5:30PM - 7:00PM
- Monday, January 9, 5:30PM - 7:00PM
- Wednesday, January 25, 5:30PM - 7:00PM

Contact TLI admissions at tli-info@umn.edu to register.

THANK YOU 2016 SPONSORS

Founding Partner



Printing Sponsor



Table Top Exercise Co-Sponsor



Small Business Forum Host



Presenting Sponsors



Premier Sponsors



Emergent Networks



CISO Luncheon Host



VIP Reception Sponsor



Cyber Security Exercise Sponsor



CEO Breakfast + Table Talk Co-Sponsor



Panel Sponsor



Lanyard Sponsor



MN.IT Student Breakfast Sponsor



Refreshment Sponsor



Expo Stage Participant



Exhibitors



Supporting Sponsors



Contributing Sponsor



Cooperating Entity



Conference Producer



➤ MAXIMIZE YOUR EXPOSURE

Sign up to sponsor Cyber Security Summit 2017 today and receive a FREE color logo upgrade - a \$150 value! Contact our sponsorship sales consultants: Jennifer Churchill at 763-548-1306/Jennifer.Churchill@eventshows.com or Paul TenEyck at 763-548-1308/Paul.TenEyck@eventshows.com

CONTENTS

Thank You Sponsors.....	03
Welcome.....	04
Summit Highlights.....	05
2016 Advisory Board.....	06
2016 Committees.....	07
Visionary Leader Awards.....	09
Symantec™ Cyber Security Exercise...	10
Upcoming Industry Events.....	11
Table Top Exercise.....	12-13
Small Business Forum.....	14
Full Summit Agenda.....	17-18
Keynote Speakers.....	22-23
2016 Speakers.....	24-26
Expo Floor Map.....	28
Sponsors/Exhibitors.....	29-40
Index of Cyber Terminology.....	42-45
Notes.....	47-49

WELCOME

Six years ago a few folks with a shared seed of interest got together at the University of Minnesota Technological Leadership Institute. Their goal was to gather the best people, ideas and perspectives from both public and private sectors in a forum focused on one critical topic, and nine months later the Cyber Security Summit was born.

The next two days - in keeping with the original vision - are the result of a broad collaboration from those who understand the benefits of sharing solutions and perspectives to address the increasing import and challenges at hand. As attendees, you experience the final result, but you don't get to see how an event like this comes together.

The more than 40 Summit advisors involved in the design/build effort come from health care, retail, banking, energy, legal, military, manufacturing, government and higher education. We meet monthly to brainstorm, propose, argue, agree, refine and ultimately put forth a program that prepares you for the security realities of our interconnected worlds. Here we network with others, share best practices and participate in real-world demonstrations that can reduce risk back at your workplace and at home. The content provided protects critical infrastructure interests and our national security, ultimately.

In a recent address as newly-appointed NSA Director, Admiral Michael Rogers highlighted the need to use platforms such as this Summit to help companies understand that the question is not IF a breach will happen, but how to be best prepared for the response WHEN it happens. That is an actionable point of focus in this year's agenda. In addition, you will hear about one of the most crucial and non-technical cyber challenges faced today: how to develop and retain the next generation of cyber security talent.

We are honored to have such dignitaries as Under Secretary Suzanne Spaulding, Dr. Shima Keene and Lieutenant General Ronald Burgess speak to attendees who have traveled from as far as London and Finland.

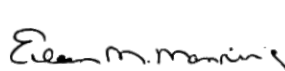
This Summit would not be possible without the support of the advisory board and speakers who volunteer their time to best arm you with content. Our sponsors are also critical to our success, so please visit with them before you leave the JW Marriott Mall of America to learn how they can support your needs.

Thank you for joining us and pulling together to make a more secure world.



Andrew Borene

2016 Honorary Co-Chair,
Cyber Security Summit



Eileen Manning

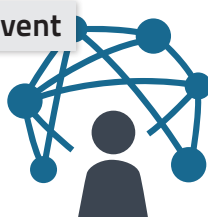
Executive Producer,
Cyber Security Summit



Elizabeth Stevens

2016 Co-Chair,
Cyber Security Summit

Pre-Event



VIP RECEPTION

Pre-Summit event by invitation only
or with purchase of VIP ALL ACCESS PASS.

Sponsored by:



Pre-Event



INVESTMENT TOWN HALL

This first-of-its-kind hyper-interactive Town Hall will engage every attendee to collaboratively investigate strategies and opportunities and obstacles in today's cyber investment market.

QUESTIONS?

Call 763.548.1313 or go to
www.cybersecuritysummit.org

09

**2016 VISIONARY
LEADER AWARDS**

This year the Cyber Security Summit is presenting two Visionary Leader Awards - one for the private sector and one for the public sector. The individuals honored have made lasting contributions to improving our nation's security.



10

CYBER SECURITY EXERCISE

This training scenario will test the sleuthing skills of tech pros and future CISOs in an immersive half-day threat management gauntlet of simulated cyber threats.

**CISO LUNCHEON**

This invite-only lunch will bring together CISOs, CIOs and CTOs from a range of organizations to network and listen to a presentation tailored for them. 12:00 p.m. - 1:15 p.m., Tuesday, Oct. 11, Ruby Room.

12

**OPTUM****TABLE TOP EXERCISE**

A team of technical experts plays out the scenario of the real-world turmoil resulting from a targeted cyber attack.

14

**BRIGGS
AND MORGAN[®]**
PROFESSIONAL ASSOCIATION**SMALL + MID-SIZE
BUSINESS FORUM**

Most small businesses can't afford a dedicated cyber team. Here they can learn about risky behaviors, preventative actions, legal issues and insurance options.

**CEO/BOD BREAKFAST**

This invite-only breakfast features Chris Mark of AT&T Security Solutions.

Sponsored by:

**EXPO RECEPTION**

Tuesday, October 11, 5:00 to 6:30 p.m.
Network with your peers at this reception in the Exhibit Area featuring appetizers.

**CLE + CEU CREDITS**

This Summit has been approved for Continuing Legal Education credits in Minnesota and Iowa. We can also provide certificates of attendance for other continuing education credits.

2016 ADVISORY BOARD

6



Jill Allison, ASIS
International



Dr. Massoud Amin,
University of MN TLI



Bonnie Anderson,
HCMC



Ken Barnhart,
Highground Cyber



Michael Benz, Kraus-
Anderson Construction



John Bonhage,
InfraGard



Andrew Borene,
Booz Allen Hamilton



Jim Brzezinski,
Tanium



Chris Buse,
MN.IT Services



Patrick Deegan,
ID3



Antonio Enriquez,
DHS



Steen Fjalstad,
MRO



Mary Frantz, Enterprise
Knowledge Partners, LLC



Joe Holmes,
Best Buy



Col. Stefanie Horvath,
MN Army National Guard



Bob Hoschka, Computex
Technology Solutions



Brian Isle,
Adventium Labs



Lisa Jemtrud, Better
Business Bureau



Mike Johnson,
University of MN TLI



Eran Kahana,
Maslon LLP



Faisal Kaleem, Metropolitan
State University



Michael Kearn, U.S.
Bank Corporation



David La Belle,
NorSec



Loren Dealy Mahler,
Dealy Mahler Strategies



Eileen Manning, The Event
Group, Incorporated



Karl Mattson,
University of MN TLI



Vicki Miller,
FICO



Jerrod Montoya,
OATI



Dave Notch,
KPMG



Stefan Pittinger,
CenturyLink



Todd Rosenblum,
IBM



James Ryan,
Litmus Logic, LLC



Glenn Sanders,
DHS



Philip Schenkenberg,
Briggs & Morgan P.A.



Melissa Seebeck,
Deluxe Corporation



Scott Singer,
PaR Systems, Inc.



Kevin Spanbauer, Intensity
Analytics Corporation



Jay Spreitzer,
Wells Fargo Bank



Elizabeth Stevens,
UnitedHealth Group



Chris Terzich,
Wells Fargo



Christophe Veltsos,
Dr. InfoSec

For complete bios of the 2016 Cyber Security Summit Advisory Board, visit www.cybersecuritysummit.org/advisors.

COMMITTEES

EXECUTIVE COMMITTEE

Andrew Borene, 2016 Summit Honorary Co-Chair; Federal Chief Strategist, Booz Allen Hamilton

Eileen Manning, Executive Producer & Co-Creator; CEO, The Event Group, Incorporated

Elizabeth Stevens, 2016 Summit Co-Chair; Director, Enterprise Resiliency & Response, UnitedHealth Group

REGISTRATION COMMITTEE

Jill Allison, Sr. Cybersecurity Consultant, BISO, International e-Commerce Retailer; Member, CSO Center for Leadership and Development, ASIS International

Bonnie Anderson, Information Security Officer, Hennepin County Medical Center

Mike Johnson, Senior Fellow & Honeywell James J. Renier Chair, Security Technologies Program, Technological Leadership Institute (TLI), University of Minnesota

Elizabeth Stevens, Director, Enterprise Resiliency & Response, UnitedHealth Group

Stefan Pittinger, VP Midwest Region, Business Technology Solutions, CenturyLink

Todd Rosenblum, Senior Executive, Worldwide Business Development, IBM i2 Safer Planet

INTERACTIVE TABLE TOP EXERCISE

Lisa Beury-Russo, DHS

Ken Barnhart, President & Principal Consultant, Highground Cyber

Barry Caplin, VP & CISO, Fairview Health Services

Antonio Enriquez, Cyber Security Advisor, Region V, Office of Cybersecurity & Communications, DHS

Keatron Evans, Partner and Cyber Security Lead, Enterprise Knowledge Partners, LLC

Mary Frantz, Table Top Producer; Managing Partner, Enterprise Knowledge Partners, LLC

Stefanie Horvath, Colonel, MN Army National Guard

Loren Dealy Mahler, President, Dealy Mahler Strategies

Eileen Manning, Executive Producer & Co-Creator; CEO, The Event Group, Incorporated

Melissa Seebeck, Senior Manager, Risk and Compliance Operations, Deluxe®

Scott Singer, Chief Security and Information Officer, PaR Systems, Inc.

PR/MEDIA OUTREACH

Mike Davin, Director of Marketing & Communications, The Event Group, Incorporated

Bob Hoshcka, Sr. Account Executive, Computex Technology Solutions

Loren Dealy Mahler, President, Dealy Mahler Strategies

James Ryan, Owner & Founder, Litmus Logic

CYBER SECURITY FOR THE SMALL AND MIDDLE MARKETS

Ken Barnhart, President & Principal Consultant, Highground Cyber

Jon Charles, Owner, Jon Charles Salon

Lisa Hiebert, Director Strategic Marketing, Better Business Bureau of Minnesota and North Dakota

Lisa Jemtrud, Foundation Director, Better Business Bureau of Minnesota and North Dakota

Phil Schenkenberg, Attorney and Shareholder, Briggs and Morgan, P.A.

Sarah Swenty, Public Affairs Specialist, SBA

Christophe Veltsos, Cyber Risk Strategist, Digital Trust Advisor; Dr. InfoSec

THE EVENT GROUP, INCORPORATED

Michael Border, Marketing Associate

Jennifer Churchill, Sponsorship Sales Manager

Mike Davin, Director of Marketing & Communications

Amanda Hallberg, Marketing & Registration

Doug Mroczkowski, Event Planner

Hayley Piekola, Graphic Designer

Pankti Shah, Strategic Planning & Speaker Coordination

Lana Skindelen, Student Scholarships & Financial Manager

Paul TenEyck, Sponsorship Sales

GLOSSARY OF TERMS

Mary Frantz, Managing Partner, Enterprise Knowledge Partners, LLC

David La Belle, Co-Founder, NorSec Foundation; Business Systems Analyst, US Bancorp Asset Management

Jay Spreitzer, Vice President, Cyber Threat Intelligence, Wells Fargo

THANK YOU SUPPORTERS

The 2016 Cyber Security Summit would not have been possible without the efforts, commitment and expertise of all who were involved. Thank you for your generous commitment.

Interested in getting involved? Our growing annual Summit is looking to expand our supporter community. To be considered for our 2017 Advisory Board, Committee, or speaking position please email us at: info@cybersecuritysummit.org.



VISIONARY LEADER AWARDS

2016 HONOREES

The Cyber Security Summit represents an ongoing collaboration between the public and private sectors, this year we are honoring two individuals - one from the private sector and one from the public sector. They will be formally presented with the awards at 8:30 a.m. on Day 2 of the Summit in the general session room.



Chris Buse

Chris Buse, who was named Minnesota's first CISO in 2007, will accept the Visionary Leader Award - Public Sector on behalf of his entire team at MN.IT Services, the State of Minnesota's central IT organization.

Representing one of the diverse paths that can lead to a career in cyber security, Mr. Buse started as a CPA before branching into information technology audit, which eventually led to him to a technical audit group responsible for IT audit in government. After many years working in that capacity, he became Minnesota's first CISO.

As an IT group that spans more than 70 different agencies, MN.IT faces the challenge of centralizing processes for organizations that have historically been separate. Prior to appointing a CISO, state agencies had adopted a wide variety of different technologies, making the IT infrastructure less efficient and more difficult to secure. Buse said his role has been to help lead a group that provides a holistic approach to the problem. He credits a strong team for the success MN.IT has achieved in that area.

"In government you always struggle with resource issues, but all the men and women on the MN.IT team have done a stellar job putting together services to protect the state of Minnesota," he says. "Really, the team should get the award. They do all the important work for the state, so I accept this on their behalf."

Mr. Buse is a member of the original group that helped found the Cyber Security Summit. He became involved because he saw the need for a security event geared toward thought leadership and big picture strategic issues impacting information security. Today, with a threat landscape that continues to change and a more diverse array of attacks happening increasingly quickly, he sees a greater need for collaboration than ever before.

"You can't be a successful security leader if you live in a vacuum," he says. "You need to be part of a broader cyber security ecosystem that shares information across boundaries."

As someone who has seen the growing need for security professionals firsthand, Mr. Buse is a strong advocate for workforce development and getting young people involved in cyber security. For the past two years, he has spearheaded a breakfast at the Cyber Security Summit for students interested in information security.

"Information security is a wonderful career opportunity with lots of opportunity for growth," he says. "I would encourage it as a career choice, and there is lots of opportunity in the government sector."



Brian Isle

Brian Isle was selected for the Visionary Leader Award - Private Sector for mentoring numerous technology leaders, contributing to the development of safety and security technologies, and advancing regional and national security strategies.

After earning an electrical engineering degree at the University of Minnesota, Mr. Isle began his career in the world-renowned research lab at Honeywell, where he worked on projects in diverse fields including space, industrial controls and voice recognition. After a short time, he was moved into management because, as Mr. Isle notes, "I was good at technical, but I was really good at people."

Mr. Isle spent two decades at Honeywell working on advanced technologies including optical communications and high-speed networks for both federal and commercial clients. During that time, he worked on safety-critical systems, which led to his interest in developing methodologies to reduce the complexity of very complex systems and decrease additional accidents.

During the 1990s, his focus on safety led naturally to an interest in security with the awareness that critical systems are vulnerable not only to accidental misuse but to intentional attacks as well. He and his team began working on safety and security strategies before many customers even understood the importance of having a security plan.

"Engineers were focused on accidents at the oil refineries," Mr. Isle said, "but it didn't occur to them that anyone would ever try to purposely blow up a refinery."

In 2002, Mr. Isle continued that work when he co-founded Adventium Labs, which went on to develop next generation distributed firewall technology and push technology forward in cyber security, system engineering and automated reasoning.

In addition to his business career, Mr. Isle has volunteered a huge amount of his time leading vulnerability assessments and other projects that have improved security at both the state and local levels. He has been involved at the board level in numerous security organizations, including many years supporting the InfraGard organization dedicated to improving critical infrastructure security. He has also taught at the University of Minnesota since 2010, where he has helped develop the Technological Leadership Institute's security technologies curriculum.

In his "retirement" Mr. Isle continues to coach several security companies, consult with Adventium, hold roles on numerous boards, and maintain a busy teaching schedule.



CYBER SECURITY EXERCISE

Tuesday, October 11 | 8:00AM -12:30PM

📍 **Sapphire Room** - Symantec's Cyber Security Exercises (CSEs) are technical training that simulates the latest threats and attack vectors on various industry verticals, ranging in difficulty, in a controlled, virtualized environment.

Participants will engage in a hands-on capture-the-flag training competition that casts them as attackers vying to achieve devious ends faster than others to earn recognition and win prizes. Actions will be ranked in real time, with displayed results continuously updated. Your team will experience attacker motives and tactics, and learn to mimic the adversarial methodologies in a controlled environment so realistic it's indistinguishable from a real siege.

A CSE will challenge participant's practical security knowledge, and provide training and participant progress reports for benchmarking and comparative metrics. Symantec's CSEs can be used for any organization that wants to identify new talent, build stronger security teams from within, and successfully use scenario-based cyber training to develop the skills of their most valuable assets, their people.

As the guardians who scan and protect your domains, both internal and external, security professionals face cyber threats that are constantly evolving; knowledge and battle experience confer a winning edge. Professionals who engage in CSE's formidable challenge will emerge better prepared to assure stakeholders that their data and work space are secure.

Note: Summit Attendees can participate remotely from the general session.



Upcoming Industry Events

18

OCTOBER 2016

ISSA MINNESOTA - BI-MONTHLY MEMBER MEETING

Ewald Conference Center
The Information Systems Security Association (ISSA) is a not-for-profit, international organization of information security professionals and practitioners. Doors open at 1 p.m. for networking with a 1:30 p.m. meeting start. You are welcome to join us as a guest if you're not currently an MN ISSA member!

20

OCTOBER 2016

(ISC)2 - OCTOBER MEETING, NIST CSF

The (ISC)2 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 help support the Information Security and Cyber Security Communities of the Upper Midwest.

25

OCTOBER 2016

MHTA - WOMEN LEADING IN TECHNOLOGY

Metropolitan Ballroom
Recent studies show women represent 45% of the entry level professional employee population. Yet, St. Catherine University's 2015 Minnesota Census of Women in Corporate Leadership reveals that, within Minnesota's 100 largest publicly-held corporations, women make up a mere 15.5% and 19.4% of the directors and executive officers, respectively. We've been having this conversation for years, so what's it going to really take to improve these statistics?

16

NOVEMBER 2016

MHTA - MINNESOTA TEKNE AWARDS

Minneapolis Convention Center
Each year the Tekne Awards shine a spotlight on Minnesota's technology industry. Drawing our state's most influential businesses, political leaders and individuals, the Tekne Awards honor advancement in technology areas including advanced manufacturing, information and lifesciences.

17

NOVEMBER 2016

ISACA MINNESOTA - THE FIGHT AGAINST SOCIAL ENGINEERING: DOES TRAINING AND AWARENESS REALLY WORK?

Cargill - Excelsior Crossing
Roundtable meeting. Check in: 3:00 p.m. Roundtable: 3:30-5:00 p.m. Light snacks and beverages: 5:00-5:30 p.m. CPE Credits: 1.5

21

NOVEMBER 2016

INFRAGARD MINNESOTA MEMBERS ALLIANCE - GENERAL MEMBERSHIP MEETING

The InfraGard Minnesota Members Alliance is an FBI-sponsored partnership program focused on critical infrastructure protection. To learn more about this 20-year strong partnership program or apply for membership, visit www.infragard.org.

CYBERSECURITYBUSINESS.COM

Did you know that we host a blog in addition to organizing and staging the annual Cyber Security Summit? The Summit happens once each year, but these issues are around 24/7/365. We're fortunate that organizing the Summit keeps us in touch with very smart industry leaders who contribute to our blog in addition to our writers, who regularly highlight security trends and issues.

We invite you to visit cybersecuritybusiness.com to see our work. You can scan the QR code to even make it easier. When you do and sign up for our newsletter during the Summit, you will automatically be entered into a drawing for a VIP All Access Pass to Cyber Security Summit 2017. There will also be a second drawing for a VIP Pass for members of our LinkedIn Group "Cyber Security Summit 2016."

ENTER NOW! By scanning the QR Code or visiting www.cybersecuritybusiness.com



2016 INTERACTIVE TABLE TOP EXERCISE

Tuesday, October 11 | 2:20 - 3:50PM

📍 **General Session Room** - Business leaders today need quick, actionable ideas to keep data and information safe. With so much advice flooding the market, it can be hard to know what really matters – and how it really works.

This year, the Cyber Security Summit is tackling that challenge and presenting a live Incident Response Table Top Exercise as a featured presentation. Executives from companies of all sizes will learn more about what really matters in the heat of the moment and leave with a greater understanding of what they can do to improve their own incident response plans.

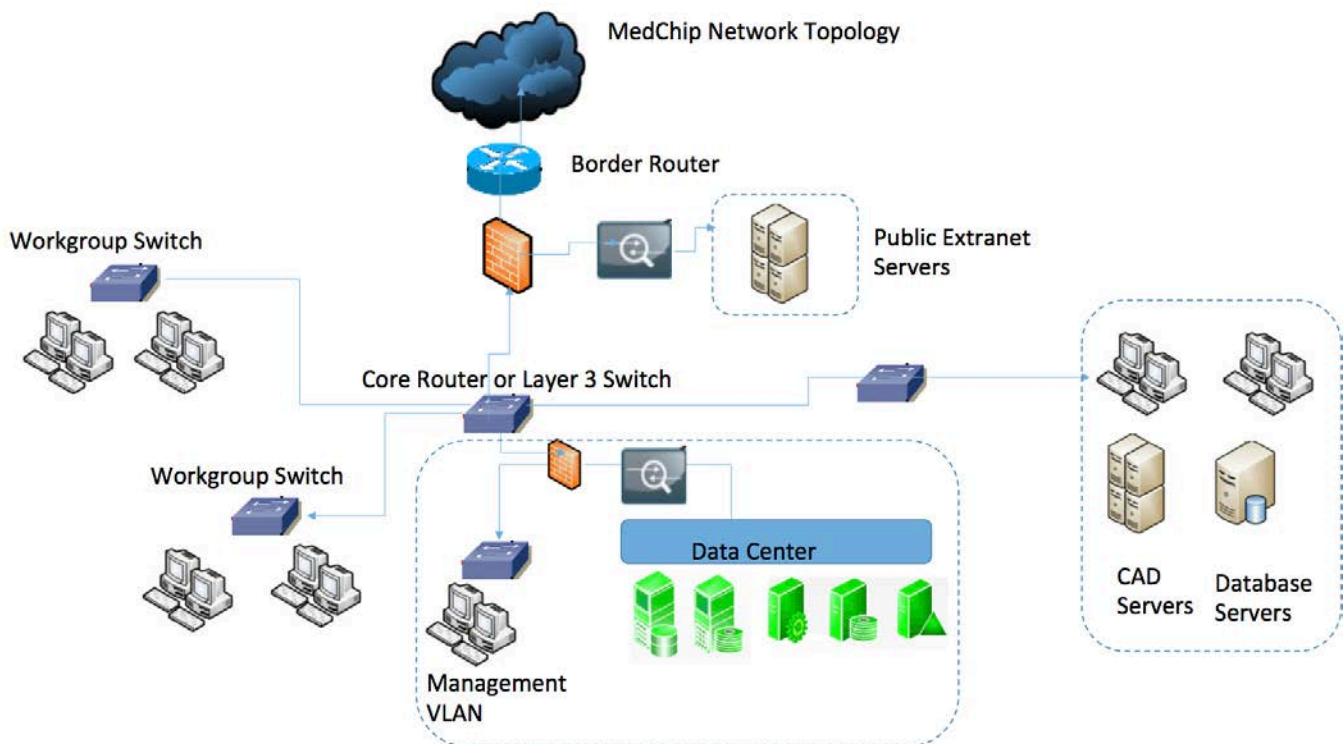
The Table Top Exercise will allow viewers to watch a cyber incident unfold and observe the forces at play in managing a response to a common cyber incident. The exercise will cover several facets of response from technical requirements to internal and external communication strategies, operational impact and leadership challenges.

Most importantly the exercise will highlight the decision making processes involved in a response and showcase how to build a reliable plan to ensure executives have the information they need to make critical decisions as quickly as possible.

After Monday's final keynote, the Table Top discussion will continue during the networking reception from 5 - 6:30 p.m.

*PLEASE NOTE: The diagrams featured here will be used and explained as a part of the interactive exercise. This activity will demonstrate the roles, responsibilities and standard response format required to effectively manage an incident.

Sponsored by:



Network Diagram: The response roles, responsibilities and forces at play.

CYBER KILL CHAIN®

Lockheed Martin's Cyber Kill Chain® and Intelligence Driven Defense® services identify and prevent cyber intrusion activity. The services monitor what the adversaries must complete in order to achieve their objective.

A : ADVANCED

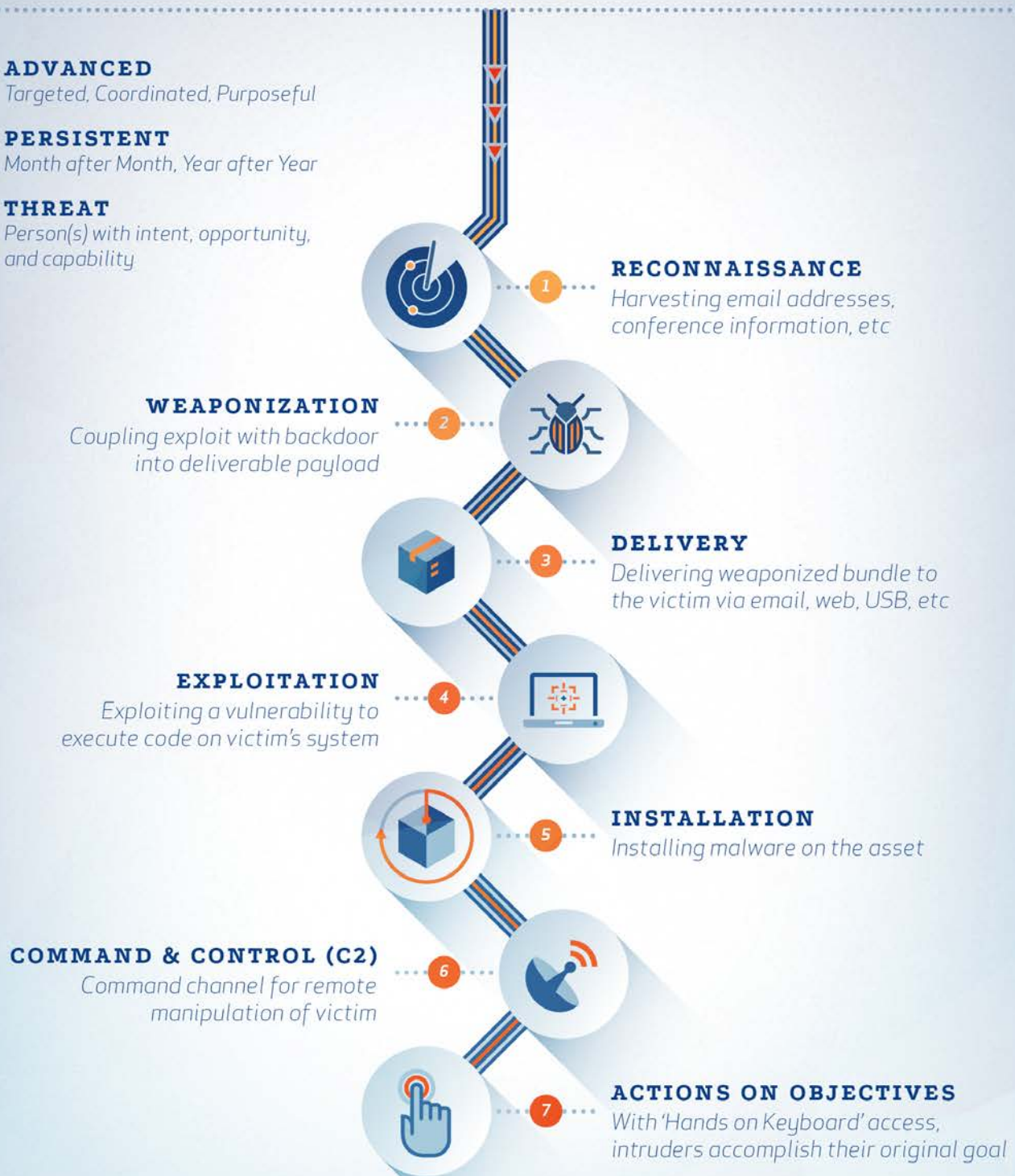
Targeted, Coordinated, Purposeful

P : PERSISTENT

Month after Month, Year after Year

T : THREAT

Person(s) with intent, opportunity, and capability



Learn how defenders have the advantage at:
lockheedmartin.com/cyber





CYBER SECURITY FOR SMALL + MID-SIZE BUSINESSES

Tuesday, October 11 | SAPPHIRE ROOM

- 2:00 – 2:10 PM** **Executive Networking & Refreshments**
- 2:10- 2:30 PM** **Thoughts on Cyber Security from the Small Business Administration**
Speaker: Nancy Libersky, District Director, U.S. Small Business Administration
- 2:30- 3:10 PM** **Cybersecurity — Seven Ways to Keep Your Small Business Running in the Era of Viruses, Scams, and Breaches**
Speaker: Chris Veltsos, Cyber Strategist, Digital Advisor; Dr. InfoSec
- 3:10- 3:30 PM** **How the FBI can Help Protect Your Company From Criminal Actions and Financial Loss**
Speaker: Lizabeth Lehrkamp, White Collar Crime, FBI
- 3:30- 3:40 PM** **BREAK**
- 3:40- 4:10 PM** **Reasons Businesses End Up Calling a Cyber Lawyer**
Speaker: Phil Schenkenberg, Attorney and Shareholder, Briggs and Morgan, P.A.
- 4:10- 4:40 PM** **Do Small Businesses Need Cyber Insurance?**
Speaker: Jake Omann, Cyber Specialist, Certified Insurance Counselor, Ahmann Martin Risks and Benefits Consulting
- 4:40- 5:10 PM** **Panel of Experts Takes Questions from the Audience**
- 5:10- 6:30 PM** **Networking Reception**

Hosted by:



Cooperating entities:



Start With Trust[®]

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.



BBB.org
800-646-6222



CYBER SECURITY
SUMMIT 2016



TECHNOLOGICAL LEADERSHIP INSTITUTE

GRADUATE MINOR

Cyber Security

DO YOU HAVE WHAT IT TAKES
TO BE A **THREAT EXPERT?**

Gain the skills to protect the information and systems we rely on with a graduate minor in Cyber Security from the University of Minnesota Technological Leadership Institute (TLI). Highly trained cyber security professionals are in demand, and TLI's Cyber Security minor provides students with the knowledge to adapt and lead in this emerging career field. Many courses are open to non-degree seeking professionals. Contact our admissions team at tli-info@umn.edu.

tli.umn.edu



Security for the cognitive era.

In a world where everything is connected, everything is vulnerable. IBM helps organizations create a safer planet by arming them with advanced analytics and cognitive technology. This combination helps detect millions of hidden threats from millions of sources and continuously learns how to defeat them. When your organization thinks, you can outthink threats.

outthink threats

IBM and its logo are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. See current list at ibm.com/trademark. Other product and service names might be trademarks of IBM or other companies. ©International Business Machines Corp. 2016. P31795

Learn more about the IBM Safer Planet portfolio
ibm.co/saferplanet



TUESDAY OCT. 11

7:00AM	Registration & Continental Breakfast	12:00 - 1:15PM	CISO Luncheon (Invite Only)
7:00 - 7:45AM	MN.IT Student Breakfast (Invite Only) Speaker: Chris Buse, MN.IT	1:15 - 2:15PM	KEYNOTE: How to Attract and Retain Cyber Talent It's no secret that cyber security currently has negative unemployment rates. This presents significant challenges not only because of the rarity of talent but also makes identifying good talent problematic as the space floods with ill-equipped individuals to respond to the shortfall. The good news is that you still can build a strong cyber team. In this talk we'll look at proven strategies for identifying, attracting, acquiring, growing, and retaining strong talent. Speaker: Tim Crothers, Target Corporation
8:00 - 8:25AM	Welcome	2:20 - 3:50PM	Interactive Table Top Exercise Using an interactive table-top exercise, we'll witness the real-life impact as an experienced executive team works with their technical experts to respond to a major breach of company data. It's Office Space meets 24. Moderator: Elizabeth Stevens, UnitedHealth Group Panelists: Ken Barnhart, Highground Cyber; Kate Baxter-Kauf, Lockridge Grindal Nauen P.L.L.P.; Barry Caplin, Fairview Health Services; Keatron Evans, EKP; Mary Frantz, EKP; Graham Jenich, PaR Systems, Inc.; Loren Dealy Mahler, Dealy Mahler Strategies; Tom Mills, Alert Logic; Scott Singer, PaR Systems, Inc.; Kristi Yauch, St.Jude Medical
8:25 - 8:45AM	OPENING DEBATE: Privacy vs. Security Join our Summit co-chairs for this lively debate to kick off the event. Panelists: Andrew Borene, Booz Allen Hamilton; Elizabeth Stevens, UnitedHealth Group	3:50 - 4:10PM	Break in Expo Area
8:45 - 9:15AM	KEYNOTE: 2016 Cyber Attacks by the Numbers The latest data on cyber attacks. Speaker: Kevin Thompson, FireEye	4:10 - 5:00PM	KEYNOTE: Protecting the Homeland: Collaboration Required NPPD's mission is to strengthen the security and resiliency of the nation's critical infrastructure against physical and cyber risk, securing federal facilities, building capabilities in the .gov and .com domains, and advancing identity management verification. The directorate accomplishes its mission by partnering with infrastructure owners and operators as well as Federal, State, local and territorial officials. Speaker: Suzanne Spaulding, U.S. Department of Homeland Security
9:15 - 10:00AM	KEYNOTE: The Nexus of Cybersecurity, Crime and Terrorism Dr. Shima Keene will illuminate the connections between online fraud, organized crime and the funding for terrorism, as well as how terrorist groups and criminal organizations use the cyber environment more broadly to achieve their objectives. The session will include a discussion of how enterprises can understand who is attacking them and why, as well as what can be done to make them less vulnerable. Speaker: Shima Keene, Oxford	5:00 - 6:30PM	Networking Reception in Expo Area The Interactive Table Top Discussion continues - you saw the breach during the live exercise, now learn more about some of the solutions while networking with your peers at this reception.
10:00 - 10:30AM	Training the Next Generation We face many challenges today and our task is to train the next generation to deal with them. Panelists: Brian Isle, Adventium Labs; Mike Johnson, University of Minnesota TL; Eileen Manning, The Event Group, Incorporated		
10:30 - 11:00AM	Break in Expo Area		
11AM - 12:00PM	PANEL: Assume you're Breached-Do you Know How to Respond? Given the number of high-profile companies that have been breached during the past several years, it's become clear that no one is immune. But do you know how to respond? Hear from a legal, technical, insurance, and PR expert on what to do. Panelists: Matt Danielak, Willis Towers Watson; Eran Kahana, Maslon LLP; Loren Dealy Mahler, Dealy Mahler Strategies		
12:00 - 1:15PM	Lunch in Expo Area		

Join the discussion by sharing your thoughts and feedback throughout the Summit on social media.



twitter.com/cs_summit
#CSSMN2016



facebook.com/cssummit
(Be sure to like us!)



Cyber Security Summit 2016 - International
Cyber Security Thought Leadership

WEDNESDAY, OCT. 12

7:00 - 8:30AM	Summit Breakfast	12:30 - 1:30PM	Lunch in Expo Area
7:00 - 8:15AM	CEO/BOD Breakfast (Invite Only) Speaker: Chris Mark, AT&T Security Solutions	1:30 - 2:15PM	KEYNOTE: Anatomy of an Attack: Hack Stories and How you are being Infiltrated There has been a growing trend of adversaries compromising accounts by reusing stolen credentials. This is a particularly insidious method, as it does not require any traditional "hacking," nor does it create any detectable cyber incident on the network. We will discuss the common factor exploited in the majority of intrusions, as well as how to educate end users in your organization to recognize, report and help remediate these threats. Speaker: Kevin Charest, UnitedHealth Group
8:30 - 8:45AM	Visionary Leader Awards Ceremony The Cyber Security Summit will present its second annual award honoring individuals who have made a lasting contribution to our nation's security dialogue. Speaker: Eileen Manning, The Event Group, Incorporated		
8:45 - 9:30AM	KEYNOTE: The Cyber Threat and Way Ahead A discussion on the cyber threat to the United States and our national security in an inter-connected world. The role of government, private and public companies and academia. Speaker: Lt. Gen. (Ret.) Ronald Burgess, Auburn University	2:15 - 3:00PM	KEYNOTE: Cyber After 2016: Protecting Your Network in the New Political Environment This session will provide an overview of policy and politics — particularly relevant legislation — involving cybersecurity since 2013, with an eye toward landscape shifts that will likely affect business in the next administration. It will also delve briefly into active cyber defense policy and improving cooperation between the government and companies in defending against significant cyberattacks. Speaker: Dan Paltiel, Truman Center for National Policy
9:30 - 10:15AM	KEYNOTE: Leveraging Intelligence, Visualization, and Analytics to fight advanced Cyber Threats What happens when advanced cyber actors slip past all your defenses and detection tools? Advanced threats which slip by perimeter security can live on your network for months or years using innovative ways to avoid detection. By constructing an expert team and using intelligence techniques, security operation centers can create advanced analytical algorithms to fight cyber threats. Speaker: Bob Stasio, IBM	3:00 - 3:30PM	Break and Prize Drawing in Expo Area
10:15 - 10:35AM	CYBERBYTE: Ransomware: What is it and how do I respond? Ransomware has become the attack of choice for many cyber criminals. Last year industry analysts saw a record number of these types of attacks and their prevalence has only grown in 2016. Learn more about how this malicious software works and how to protect your organization Speaker: Jay Spreitzer, Wells Fargo Bank	3:30 - 4:30PM	PANEL: The DHS Cyber Resilience Review This presentation will cover the process of executing a DHS facilitated Cyber Resilience Review. We will start by discussing resilience concepts; we will describe the CRR and its methodology; how it identifies strengths and weaknesses; maturity indicators; the comparison cross-walk of the NIST Cyber Security Framework; the process of requesting a CRR; executing a CRR; draft and final report processes; actions after the final report is delivered; and the comparison of a facilitated CRR vs. a Self-Assessment CRR. Panelists: Antonio Enriquez, DHS; Michael Rattigan, Carnegie Mellon University
10:35 - 11:00AM	Break in Expo Area		
11:00 - 11:30AM	Making Best Practice Common Practice: the CIS Controls The challenge is that you can't find those "best practices" on your own to learn from them. Walk through the CIS response to this challenge – the CIS Critical Security Controls. We'll show how a broad community comes together to understand threats, translate them into action, and sustain an ecosystem of volunteers, tools, vendors, working aids, and information to help us all improve our cybersecurity. Speaker: Tony Sager, Center for Internet Security	4:30 - 5:15PM	An Overview - Practical Takeaways We will wrap up the Summit with a summation of practical takeaways people can bring back to their organizations. Speaker: Andrew Borene, Booz Allen Hamilton; Elizabeth Stevens, UnitedHealth Group
11:30 - 12:30PM	Case Studies: What is Working in Cyber Security? Statistics about the cyber problem make it seem overwhelming. This session will focus on what is working and how to implement best practices in your business. Panelists: Jake Dewoskin, Emergent Networks; Tony Sager, Center for Internet Security; Kevin Thompson, FireEye		

Take the next step at symantec.com

With so many alerts, it's not your
security that's working hard.

You are.

KNOW THE TRUTH.

www.FireEye.com

the Only Constant is Change

As the Greek philosopher Heraclitus famously noted, “the only constant is change”. This statement was as accurate 2,500 years ago as it is now. The world around us changes constantly, often times at a somewhat frenetic pace. The field of information security is no different. Both the organizations we support and the threat landscape we face are changing and evolving constantly.

One unfortunate side effect of continual change can be what I colloquially call “shiny object syndrome” (SOS). As you might imagine, there are some organizations, and indeed some people, that seem to run continually from one “shiny object” to another, unfortunately. In other words, rather than approach security strategically, adjusting the plan in a calculated manner to account for changes to the risks and threats the organization faces, many organizations repeatedly chase after the fad of the day.

Rather than discuss why this occurs, I'd like to focus on what organizations can do to avoid falling victim to shiny object syndrome. Hype, buzz, and trends change constantly, but the fundamentals of a good security program stay the same.

While this is certainly not an exhaustive list, here are my top five ways that organizations can stay grounded and focused amidst a sea of distractions:

1. STICK TO THE PLAN:

As I and many others have previously noted, if you don't already have an incident response plan, you should. If you do already have a plan, then you are already one step ahead of the game. The trick is to stick to the plan, even when the temperature gets a little hot in the kitchen. If you've done your homework properly, or worked with qualified professionals who have helped you do it properly, you will pull through. Just as long as you don't succumb to the near constant temptation of distraction and the knee-jerk reactions it causes.

2. FOCUS ON RISK:

The best security organizations use a variety of techniques to understand the unique threat landscape they face. Those same organizations use this knowledge to help them prioritize the risks and threats that they wish to mitigate. In

addition to helping these organizations prioritize spending and mitigate risk more effectively, this approach helps them stay focused and avoid running astray in pursuit of shiny objects. When the temptation to run in a particular direction arises, the organization can evaluate this new direction against its prioritized list of risks and threats. This helps the organization understand how this potential new direction impacts the organization, specifically regarding any additional risk that it may or may not introduce. In this sense, it is fairly easy to identify distractions by understanding their lack of relevance to the risk mitigation goals of the organization.

3. PRIORITIZE HOLES TO PLUG:

In the security world, new techniques for intruding into organizations appear fairly frequently. Some of them grab big headlines, which of course can increase attention and pressure on security types from non-security types in leadership or executive positions within our respective organizations. But how firm of a grasp do we have on the primary ways in which we are being attacked and owned, as well as broader patterns and trends across the industry? It is far too easy to divert important resources away from their strategically prioritized day-to-day work and onto the hack du jour. But if today's distraction poses a minor risk to our organization, does it make sense to divert resources from mitigating risks or plugging holes that we know pose serious risk to the organization? Not particularly, although without a quantitative handle on risk that includes a robust risk register, it can be hard to justify that stance in the heat of the moment.

4. GO BEYOND THE BUZZ:

A few years ago, I remember walking around the RSA Conference vendor expo hall and seeing signs that read “big data”, “security analytics”, or “big data security analytics” everywhere. Everyone was talking about the topic, and many still are, for good reason. But let's go beyond the buzz and take a look at one of my favorite questions: So what? What will you use security analytics for? Do you have a list of risks to mitigate that will require a variety of different people, process, and technology to mitigate, including security analytics? For example, identifying stolen credentials and attackers masquerading as legitimate users? Having insight beyond the buzz allows an organization to more efficiently and effectively apply people, process, and technology to solve real world problems and challenges. Otherwise, solutions that are purchased and implemented wind up looking for a problem to solve. Not a great place to be, particularly when looking to justify expenditures and show return on investment.

5. MEASURE WHAT MATTERS:

Did your security organization open and close 500 tickets last week and handle 10,000 IDS alerts? Pardon my candor, but who cares? How do those metrics help you assess how you are or are not progressing against the prioritized list of risks and threat you're looking to mitigate? Measuring what matters allows an organization to produce metrics that actually help it assess its progress against its strategic objectives. Unfortunately, I am not able to expand on this concept in this piece, but I have written about it previously. Metrics that matter have the added benefit of allowing an organization to assess and measure whether activities (whether new or old) are adding value to the security program. You guessed it -- that helps a security organization stay focused on adding value, rather than chasing after shiny objects.

There is no shortage of distractions in the information security realm. As security professionals, we need to stay focused on managing, mitigating, and minimizing risk to our respective organizations, even as both the business and the threat landscape change around us. If we stay grounded, adapt strategically, and adjust incrementally, we stand a far better chance of successfully accomplishing our goals. Running off course on all sorts of impulsive tangents never made anyone more secure.



JOSHUA GOLDFARB

CTO of Emerging Technologies at FireEye, Inc.

Twitter: @ananalytical

Joshua Goldfarb has over a decade of experience building, operating, and running Security Operations Centers (SOCs). Before joining nPulse Technologies, which was acquired by FireEye, as its Chief Security Officer (CSO), he worked as an independent consultant where consulted and advised numerous clients in both the public and private sectors at strategic and tactical levels. Earlier in his career Goldfarb served as the Chief of Analysis for US-CERT where he built from the ground up and subsequently ran the network, physical media and malware analysis/forensics capabilities. Goldfarb holds both a B.A. in Physics and a M.Eng. in Operations Research and Information Engineering from Cornell University.



**LT. GEN. (RET.)
RONALD BURGESS**

Senior Counsel for National Security Programs, Cyber Programs and Military Affairs, Auburn University

Lt. Gen. (Ret.) Ronald Lee Burgess, Jr. was the 17th Director of the Defense Intelligence Agency. As head of the Agency and a former Acting Principal Deputy Director of National Intelligence, Burgess served as a key player within the national security arena, called upon by the President, the Secretary of Defense, the Director of National Intelligence, the Chairman of the Joint Chiefs of Staff, and Congressional leaders for his opinions, advice and expertise. He is currently Senior Counsel for National Security Programs, Cyber Programs and Military Affairs for Auburn University.

SESSIONS:

Wednesday, Oct.12 | 8:45AM
The Cyber Threat and Way Ahead



KEVIN CHAREST

Vice President, Global Cyber Defense Operations, Information Risk Management, UnitedHealth Group

Dr. Kevin Charest serves as the VP, IT Security and Cyber Defense Operations for UnitedHealth Group. He is responsible for all facets of IT security operations, continuous monitoring, and cyber defense strategy across the enterprise. Previously he served as the Chief Information Security Officer for the Department of Health and Human Services (HHS), the United States government's principal agency for protecting the health of all Americans, where he was directly responsible for the cybersecurity technology portfolio for the Department. Prior to joining the federal government Dr. Charest served in a number of entrepreneurial and senior executive positions in the private sector. His leadership in technology applications, innovation, and security were instrumental to the development of numerous products and services. Dr. Charest currently serves as a Board member for (ISC)², the largest international information security certifying body in the world.

SESSIONS:

Wednesday, Oct.12 | 1:30PM
Anatomy of an Attack: Hack Stories and How You Are Being Infiltrated



TIM CROTHERS

Senior Director, Cyber-Security, Target

Tim is a seasoned security leader with over 20 years' experience building and running information security programs, large and complex incident response engagements, and threat and vulnerability assessments. He has deep experience in cyber-threat intelligence, reverse engineering, and computer forensics. He is a recognized thought leader and author/co-author of 14 books to date as well as regular training and speaking engagements at information security conferences. Tim is Senior Director of Cyber-Security for Target. There he has built and leads the Computer Security Incident Response Team where they are working on using innovative and new techniques and technologies to achieve world class security.

SESSIONS:

Tuesday, Oct.11 | 1:15PM
How to Attract and Retain Cyber Talent



SHIMA KEENE

Director of Conflict Studies Research Centre, Oxford; Director of Security Economics Programme, Institute for Statecraft, London, United Kingdom (UK)

Dr. Shima Keene is a Director of the Conflict Studies Research Centre, Oxford; Senior Fellow at the Institute for Statecraft, London; Special Advisor to Force Intelligence and Specialist Operations, Thames Valley Police; and a Deployable Civilian Expert for the UK Government's Civilian Stabilisation Group specializing in Security and Justice. Shima advises on matters relating to National and Global Security to include terrorism, organised crime, economic crime, cyber-crime and governance. Shima is a former investment banker, Director of Security Technology and Advisor on Security and Resilience at the Defence Academy of the UK, as well as Special Advisor to the UK Ministry of Defence. She is the author of "Threat Finance: Disconnecting the Lifeline of Organized Crime and Terrorism" and holds a BSc (Hons) in Business Studies; an MPhil in Defence and Security Studies; and a Ph.D. in International Criminal Law. Dr Keene currently lectures at Sulhamstead Police Academy, BPP Law School, the University of Cambridge, and the University of St. Thomas in Minnesota.

SESSIONS:

Tuesday, Oct.11 | 9:15AM
The Nexus of Cybersecurity, Crime & Terrorism

**DAN PALTIEL****Policy Program Manager, Truman Center for National Policy**

Dan Paltiel is Policy Program Manager at the Truman Center for National Policy. In this capacity, Dan leads the organization's Cyberspace & Security programming. Prior to joining Truman, Dan was Program Coordinator and Research Assistant in the Strategic Technologies Program at the Center for Strategic and International Studies (CSIS), where he worked on cybersecurity and technology policy issues. He was lead organizer of the 2016 CSIS Cyber Policy Task Force, a commission composed of 70 leading experts in Washington, DC and Silicon Valley, to make recommendations to the 45th President on cybersecurity. His work at CSIS included developing international best practices for cybersecurity, as well as "active cyber defense" policies for private industry. Prior to CSIS, Dan lived in Amman, Jordan, where he studied Arabic and taught English. Dan holds a BA in History from Amherst College, and hails from New Haven, Connecticut. He is fluent in French and Arabic.

SESSIONS:

Wednesday, Oct. 12 | 2:15PM
Cyber After 2016: Protecting Your Network in the New Political Environment

**SUZANNE SPAULDING****Under Secretary, National Protection and Programs Directorate (NPPD), U.S. Department of Homeland Security**

Suzanne E. Spaulding oversees the coordinated operational and policy functions of the Directorate's subcomponents: office of Cybersecurity and Communications, Infrastructure Protection, Biometric Identity Management, Cyber and Infrastructure Analysis, and the Federal Protective Service. NPPD's mission is to strengthen the security and resiliency of the nation's critical infrastructure against physical and cyber risk, securing federal facilities, building capabilities in the .gov and .com domains, and advancing identity management verification. The directorate accomplishes its mission by partnering with infrastructure owners and operators as well as Federal, State, local and territorial officials. Ms. Spaulding has spent nearly 25 years working on national security issues for both Republican and Democratic Administrations and on both sides of the aisle of Congress.

SESSIONS:

Tuesday, Oct. 11 | 4:10PM
Protecting the Homeland: Collaboration Required

**BOB STASIO****Senior Product Manager, Cyber Analysis, IBM**

Prior to his role at IBM, Bob Stasio worked in the private sector standing up threat intelligence programs at Bloomberg and global financial firms. He accomplished these efforts as the owner of his own consulting firm and working internally within the enterprise. He also has deep government experience having held positions at NSA's Cyber Center, U.S. Cyber Command, U.S. Army's Signals Intelligence Corps, the FAA, and NASA. Bob served as a U.S. Army officer, and is a recipient of numerous military awards, including the Bronze Star and Global War on Terrorism Expeditionary Medal. Bob is also a Truman National Security Fellow, Brookings Institution Council on U.S. and Italy fellow, and serves on the advisory board of multiple startups. Bob is also a graduate of numerous U.S. Department of Defense professional education courses focusing on intelligence operation, and holds various technical certifications, including CISSP.

SESSIONS:

Wednesday, Oct. 12 | 9:30AM
Leveraging Intelligence, Visualization, and Analytics to Fight Advanced Cyber Threats

**KEVIN THOMPSON****Threat Analyst, FireEye**

As a Threat Analyst for FireEye, Kevin Thompson educates FireEye customers and partners on the latest cyber threats to their infrastructure. Before joining FireEye, Kevin worked as a cyber analyst for the Central Intelligence Agency in Washington DC. In that role, Kevin used digital exploitation and all source analysis to educate multiple agencies of the U.S. Government on current and future cyber threats. Kevin's analytic work has been included in Presidential Daily Briefings and became a case study used in multiple training classes.

SESSIONS:

Tuesday, Oct. 11 | 8:45AM
2016 Cyber Attacks By The Numbers

Wednesday, Oct. 12 | 11:30AM
PANEL: Case Studies: What is Working in Cyber Security?



KEN BARNHART

President & Principal Consultant,
Highground Cyber

SESSIONS:

Tuesday, Oct. 11 | 2:20PM
Interactive Table Top Exercise



MATT DANIELAK

Vice President, Willis
Towers Watson

SESSIONS:

Tuesday, Oct. 11 | 11:00AM
*PANEL: Assume You're Breached:
Do You Know How to Respond?*



KATE BAXTER-KAUF

Attorney, Lockridge Grindal
Nauen P.L.L.P.

SESSIONS:

Tuesday, Oct. 11 | 2:20PM
Interactive Table Top Exercise



JAKE DEWOSKIN

Security Practice Director,
Emergent Networks

SESSIONS:

Wednesday, Oct. 12 | 11:30AM
*PANEL: Case Studies: What is
Working in Cyber Security?*



ANDREW BORENE

Honorary Co- Chair, Cyber Security
Summit 2016; SETA Advisor to IARPA,
Booz | Allen | Hamilton

SESSIONS:

Tuesday, Oct. 11 | 8:25AM
Opening Debate: Privacy vs. Security
Wednesday, Oct. 12 | 4:45PM
An Overview – Practical Takeaways



ANTONIO ENRIQUEZ

Cyber Security Advisor – Region
V, Office of Cybersecurity &
Communications, Department of
Homeland Security

SESSIONS:

Wednesday, Oct. 12 | 3:30PM
*PANEL: The DHS Cyber
Resilience Review*



CHRIS BUSE

Assistant Commissioner/
CISO, MN.IT Services

SESSIONS:

Tuesday, Oct. 11 | 7:00AM
*MN.IT Student Breakfast
(Invite Only)*



KEATRON EVANS

Partner and Cyber Security Lead,
Enterprise Knowledge Partners, LLC

SESSIONS:

Tuesday, Oct. 11 | 2:20PM
Interactive Table Top Exercise



BARRY CAPLIN

Vice President + Chief Information
Security Officer, Fairview Health
Services

SESSIONS:

Tuesday, Oct. 11 | 2:20PM
Interactive Table Top Exercise



MARY FRANTZ

Founder & Managing Partner,
Enterprise Knowledge Partners, LLC

SESSIONS:

Tuesday, Oct. 11 | 2:20PM
Interactive Table Top Exercise



BRIAN ISLE

Co-Founder, Adventium Labs;
Senior Fellow, University of
Minnesota Technological
Leadership Institute

SESSIONS:

Tuesday, Oct.11 | 10:00AM
Training the Next Generation



LIZABETH LEHRKAMP

Special Agent, U.S. Federal Bureau
of Investigation (FBI)

SESSIONS:

Tuesday, Oct.11 | 3:10PM
*How the FBI Can Help Protect
Your Company From Criminal
Actions and Financial Loss
(Small Business Forum)*



GRAHAM JENICH

Mechanical Engineer, PaR
Systems, Inc.

SESSIONS:

Tuesday, Oct.11 | 2:20PM
Interactive Table Top Exercise



NANCY LIBERSKY

Minnesota District Director, U.S.
Small Business Administration

SESSIONS:

Tuesday, Oct.11 2:10PM
*Thoughts on Cyber Security
from the Small Business
Administration
(Small Business Forum)*



MIKE JOHNSON

Senior Fellow & Honeywell James J.
Renier Chair, Security Technologies
Program, Technological Leadership
Institute (TLI), University of
Minnesota

SESSIONS:

Tuesday, Oct.11 | 10:00AM
Training the Next Generation



LOREN DEALY MAHLER

President, Dealy Mahler Strategies

SESSIONS:

Tuesday, Oct.11 | 11:00AM
*PANEL: Assume You're Breached: Do
You Know How to Respond?*
Tuesday, Oct.11 | 2:20PM
Interactive Table Top Exercise



ERAN KAHANA

Attorney, Maslon LLP; Research
Fellow, Stanford Law School;
General Counsel and Member of
the Board of Directors, InfraGard

SESSIONS:

Tuesday, Oct.11 | 11:00AM
*PANEL: Assume You're Breached:
Do You Know How to Respond?*



EILEEN MANNING

Executive Producer, Cyber Security
Summit; President & CEO, The
Event Group, Incorporated

SESSIONS:

Tuesday, Oct.11 | 8:00AM
Welcome & Opening Remarks
Wednesday, Oct.12 | 8:30AM
Visionary Leader Awards



DAVID LA BELLE

Co-Founder, NorSec Foundation;
Business Systems Analyst, US
Bancorp Asset Management

SESSIONS:

Monday, Oct.10 | 5:30PM
*VIP Reception – Keynote
Introduction*



CHRIS MARK

PCI Practice Director- Security
Consulting, AT&T Security Solutions

SESSIONS:

Wednesday, Oct.12 | 7:00AM
CEO Breakfast (Invite Only)



TOM MILLS

Solutions Engineer, Alert Logic

SESSIONS:

Tuesday, Oct.11 | 2:20PM
Interactive Table Top Exercise



SCOTT SINGER

Captain, United States Navy Reserve;
Chief Security and Information
Officer, PaR Systems, Inc.

SESSIONS:

Tuesday, Oct.11 2:20PM
Interactive Table Top Exercise



JAKE OMANN

Cyber Specialist, Certified Insurance
Counselor, Ahmann Martin Risks
and Benefits Consulting

SESSIONS:

Tuesday, Oct.11 | 4:10PM
*Do Small Businesses Need Cyber
Insurance? (Small Business Forum)*



JAY SPREITZER

Vice President, Cyber Threat
Intelligence, Wells Fargo Bank

SESSIONS:

Wednesday, Oct.12 | 10:15AM
*CYBER BYTE: Ransomware: What
Is It and How Do I Respond?*



MICHAEL RATTIGAN

Senior Member of the Engineering
Staff, Cyber Security Assurance
Directorate CERT Program, Software
Engineering Institute (SEI), Carnegie
Mellon University

SESSIONS:

Wednesday, Oct.12 | 3:30PM
*PANEL: The DHS Cyber
Resilience Review*



ELIZABETH STEVENS

Co- Chair, Cyber Security Summit
2016; Director, Enterprise Resiliency
& Response, UnitedHealth Group;
Past President at InfraGard
Minnesota Members Alliance

SESSIONS:

Tuesday, Oct.11 | 8:25AM
Opening Debate: Privacy vs. Security
Tuesday, Oct.11 | 2:20PM
Interactive Table Top Exercise
Wednesday, Oct.12 | 4:45PM
An Overview – Practical Takeaways



TONY SAGER

Senior VP & Chief Evangelist, Center
for Internet Security

SESSIONS:

Wednesday, Oct.12 | 11:00AM
*Making Best Practice Common
Practice: the CIS Controls*
Wednesday, Oct.12 | 11:30AM
*PANEL: Case Studies: What is
Working in Cyber Security?*



CHRIS VELTSOS

Cyber Risk Strategist, Digital Trust
Advisor; Dr. InfoSec

SESSIONS:

Tuesday, Oct.11 | 2:30PM
*Cybersecurity — Seven Ways
to Keep Your Small Business
Running in the Era of Viruses,
Scams, and Breaches
(Small Business Forum)*



PHILIP SCHENKENBERG

Attorney and Shareholder,
Briggs & Morgan, P.A.

SESSIONS:

Tuesday, Oct.11 | 3:40PM
*Reasons Businesses End Up
Calling a Cyber Lawyer
(Small Business Forum)*

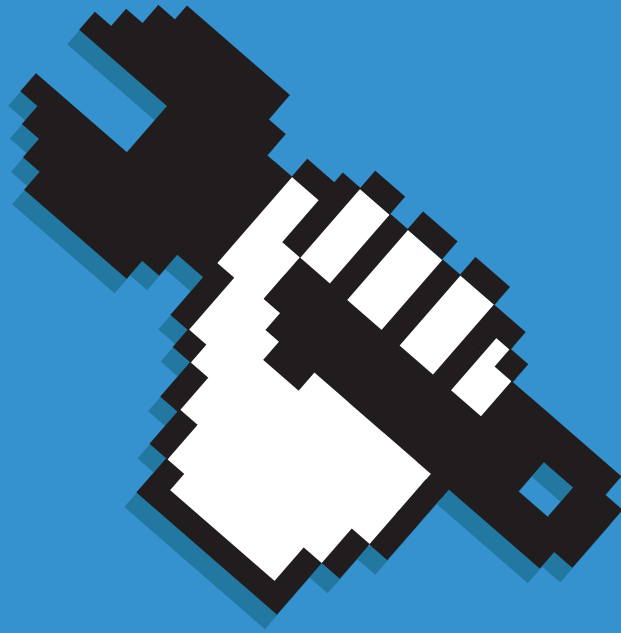


KRISTI YAUCH

Senior Security Engineer,
St. Jude Medical

SESSIONS:

Tuesday, Oct.11 | 2:20PM
Interactive Table Top Exercise



Building the tools to respond to cyber risk in real-time.



NorSec creates tools, educates and conducts security research to protect national security.

For information on becoming a member, email info@norsec.org. Members get access to real-time feeds, quarterly threat briefings and actionable intelligence information. **norsec.org**



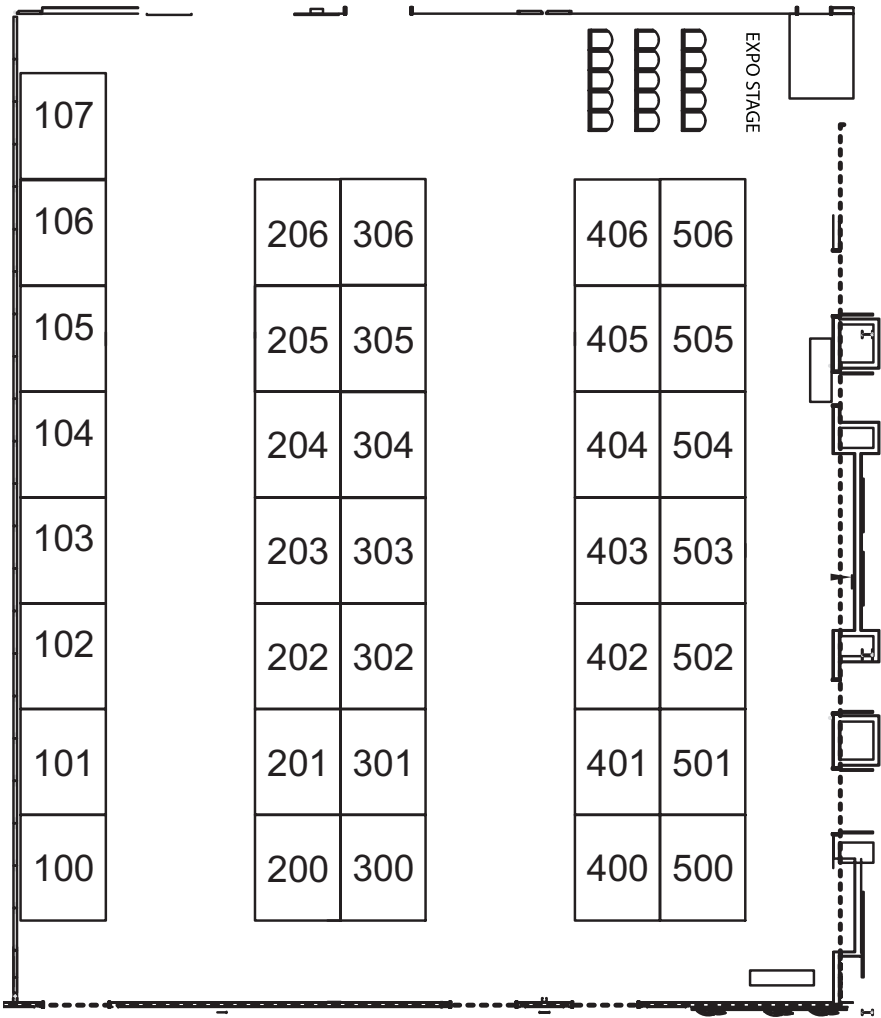
IT'S NO LONGER A QUESTION OF IF, IT'S A QUESTION OF WHEN

Cyber threats are growing and your security efforts are aimed at a moving target—one that's getting harder to hit thanks to mobile devices, outsourcing, and cloud computing that come with new business risks. It's only a matter of time before thieves and hackers strike.

Ensure your security strategy and solutions are as fluid and agile as the evolving cyber landscape with expert assistance from Wipfli. Wipfli's 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.

EXPO FLOOR MAP



DIRECTORY

105	Alert Logic	500	FireEye	203	Newberry Group	505	Target
306	AT&T	502	Guidance Software	405	NorSec Foundation	400	Technological Leadership
104	Bitsight Tech	300	IBM	304	Nucleon		Institute University of MN
107	B-Sides MSP	204	ISACA MN Chapter	102	OPTIV	201	ThreatQuotient, Inc
202	Carbon Black	100	ISSA MN Chapter	206	RSA	504	TrapX
103	CenturyLink	200	LogRhythm	402	SailPoint	106	U.S. Small Business
205	Digital Defense, Inc.	303	Metropolitan State University	101	Sila Solutions		Administration
301	Emergent Networks	503	Mitchell Hamline School of Law	401	Symantec	406	Vormetric
203	Fidelis	305	MN.IT Services	506	Tanium	302	Wipfli

ADVANCE IT MINNESOTA - Supporting Sponsor

Advance IT Minnesota is a Minnesota State Colleges and Universities (MnSCU) Center of Excellence whose mission is to engage employers, educators, and learners to develop a more robust IT Workforce in Minnesota. Their vision is to position Minnesota as a top-ten regional economy for information technology careers.

Suite 104 Energy Park Place, 1380 Energy Lane, St. Paul, MN 55108
612.659.7221/advanceitmn@metrostate.edu
www.advanceitmn.org



ALERT LOGIC - Exhibitor

AlertLogic's Security-as-a-Service solution delivers deep security insight and continuous protection for cloud, hybrid, and on-premises data centers. Providing application, system, and network protection from the cloud, the Alert Logic solution analyzes over 450 million events and identifies 60,000 security incidents monthly for over 3,000 customers worldwide.

1776 Yorktown St., Suite 700, Houston, TX 77056
877.960.3383/Info@alertlogic.com
www.alertlogic.com

ASIS INTERNATIONAL - Supporting Sponsor

ASIS International is a global community of security practitioners, each of whom has a role in the protection of assets - people, property, and/or information. Our members represent virtually every industry in the public and private sectors, and organizations of all sizes. From entry-level managers to CSOs to CEOs, from security veterans to consultants and those transitioning from law enforcement or the military, the ASIS community is global and diverse.

1625 Prince Street, Alexandria, VA
asis@asisonline.org/703-519-6200
www.asisonline.org



AT&T- CEO Breakfast Sponsor & Table Top Exercise Co-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



BETTER BUSINESS BUREAU OF MINNESOTA AND NORTH DAKOTA - Supporting Sponsor

The mission of Better Business Bureau is to be the leader in advancing marketplace trust by championing an ethical marketplace where buyers and sellers can trust each other. Founded in Minneapolis in 1912, and supported today by 6,400 local Accredited Businesses throughout Minnesota and North Dakota, BBB offers free programming and resources to both consumers and businesses.

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



BITSIGHT TECH - Exhibitor

BitSight Security Ratings are a measurement of an organization's security performance. Much like credit ratings, BitSight Security Ratings are generated through the analysis of externally observable data. Armed with daily ratings, organizations can proactively identify, quantify and manage cyber security risk throughout their ecosystem. With BitSight Security Ratings, organizations can shift towards a continuous outcome based model that is both effective and efficient.

125 Cambridge Park Drive, Suite 204, Cambridge, MA 02140
617.245.0469/info@bitsighttech.com
www.bitsighttech.com

BRIGGS AND MORGAN - Small Business Forum Host

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



B-SIDES MSP - 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



BUSINESS CONTINUITY PLANNERS ASSOCIATION - 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. BCPA membership is open to any and all professionals interested in the vocations identified above, or related vocations.

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



CARBON BLACK - Exhibitor

Carbon Black's endpoint security platform defends organizations of all sizes from modern-day attacks with its unique zero-gap protection. The Cb Endpoint Security Platform helps organizations of all sizes replace legacy antivirus technology, lock down systems, and arm incident response teams with advanced tools to proactively hunt down threats.

1100 Winter Street, Waltham MA 02452
Kelly McShane/781.786.7969/kmcshane@carbonblack.com
www.carbonblack.com



CENTURYLINK - Exhibitor

CenturyLink (NYSE: CTL) is a global communications, hosting, cloud and IT services company enabling millions of customers to transform their businesses and their lives through innovative technology solutions. CenturyLink offers network and data systems management, Big Data analytics and IT consulting, and operates more than 55 data centers in North America, Europe and Asia. The company provides broadband, voice, video, data and managed services over a robust 250,000-route-mile U.S. fiber network and a 300,000-route-mile international transport network.

Andrew Cain/612.655.6074/Andrew.Cain@centurylink.com
www.centurylink.com

CIOREVIEW - Supporting Sponsor

Published from Fremont, California, CIOReview (www.cioreview.com) 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



CONCORD - Contributing Sponsor

Concord is a consulting firm driving business value through use of technology. Our expertise is centered on data. Our execution is backed by our proven process of ALIGN, DEFINE, DELIVER. We focus on the following capabilities: Data Experience, Data in Motion, Data at Rest, Data Analytics and Data Privacy & Protection.

509 2nd Avenue South, Hopkins, MN 55343
www.concordusa.com



CYBER DEFENSE MAGAZINE - 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/marketing@cyberdefensemagazine.com
www.CyberDefenseMagazine.com



DIGITAL DEFENSE, INCORPORATED - Exhibitor

Digital Defense, Inc. (DDI) is a leader of managed security risk assessments that help organizations across the globe defend data and keep reputations secure. Offering Vulnerability Management as a Service (VMaaS™), DDI helps mitigate risk with a combination of leading-edge patented technology and support from a team of security analysts.

9000 Tesoro Drive, San Antonio, TX 78217
888.273.1412/sales@ddifrontline.com
www.digitaldefense.com

EMERGENT NETWORKS - Premier Sponsor

Emergent Networks is a full-service technology consulting company and trusted advisor to organizations for 30+ years that offers our clients complete IT Strategy, Solutions and Support. We help our clients use technology as a competitive advantage, which has set us apart as a premier IT services company in the Midwest.

3600 Minnesota Drive, Suite 150, Edina, MN 55435
612.213.2600/info@emergentnetworks.com
www.emergentnetworks.com



Emergent Networks

SECURE360

COLLABORATION FOR AN INTERCONNECTED WORLD.

IMPROVE BUSINESS, INCREASE KNOWLEDGE AND BUILD STRATEGIES TO
PROTECT YOUR GREATEST ASSETS.

Twin Cities | Iowa | Wisconsin

www.secure360.org



The Secure360 Conferences are produced by UMSA (Upper Midwest Security Alliance) which serves to unite Upper Midwest security-related organizations in a **trusted community** for **interdisciplinary collaboration** and **education**. Member affiliates include: Advance IT Minnesota, ASIS Minnesota, BCPA, ISACA-MN, ISSA-MN, InfraGard Minnesota, ISC²-MN, OWASP and SecMN. For more information: www.umsa-security.org

They Will Get In, They Can Be Stopped

 **LogRhythm**[®]
The Security Intelligence Company

LogRhythm's Security Intelligence Platform unifies SIEM, log management, file integrity monitoring, network forensics & host forensics to help detect and respond to breaches and the most sophisticated cyber threats - faster and with greater accuracy than ever.

To learn more or schedule a demo, visit www.LogRhythm.com



Security Solutions

Protecting clients against
325 million security events
each day.

- Winner of the 2015 American Technology Cyber Award
- Winner of the 2015 Frost and Sullivan New Product Innovation Award

www.unisys.com/security

UNISYS

FIDELIS - Exhibitor

Fidelis Cybersecurity protects the world's most sensitive data. We reduce the time it takes to detect attacks and resolve security incidents. With Fidelis you'll know when you're being attacked; you can retrace attackers' footprints and prevent data theft.

4416 East West Highway, Suite 310, Bethesda, MD 20814
Ron Bachman/Ron.Bachman@fidelissecurity.com
www.fidelissecurity.com



FIREEYE - Premier Sponsor

FireEye – 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.

1440 McCarthy Blvd., Milpitas, CA 95035
John Chase/651.491.8952/John.chase@fireeye.com
www.fireeye.com



GUIDANCE SOFTWARE - EXHIBITOR

As the makers of EnCase security products, Guidance Software helps legal & HR teams, law enforcement and security professionals find and neutralize threats and bring digital chaos under control with lightning fast intervention. Our Endpoint Security product delivers complete visibility into network endpoints and speeds incident response. We integrate seamlessly with top alerting tools, structured data repositories and threat intelligence platforms to enhance breach detection, prioritization and remediation.

1055 E. Colorado Blvd., Pasadena, CA 91106
626.229.9191/info@guidancesoftware.com
www.GuidanceSoftware.com

IBM - Presenting Sponsor

With shrinking budgets and limited resources, organizations need now, more than ever, intelligent solutions that will enable them to make better-informed decisions and take confident, effective action, in real time. IBM continues to invest in developing cost-effective 'fit for purpose' solutions that will help organizations achieve their missions effectively and efficiently. IBM i2 is committed to our investment in big data and advanced analytics capabilities, and will continue to provide you with next-generation solutions that will help accelerate the data to decision process, support your mission and ensure a safer planet.

www.ibm.com



INFRAGARD - 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



ISACA MN CHAPTER - Supporting Sponsor

With approximately 1100 members from over 100 organizations, the Minnesota chapter of ISACA provides a gateway to a global organization offering security, risk, control, and governance certifications. Additionally, ISACA offers a growing security knowledge platform and professional program Cybersecurity Nexus (CSX).

1360 University Ave W, #352, Saint Paul, MN 55104
vpmembership@mnisaca.org
www.mnisaca.org



(ISC)² TWIN CITIES - 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.

Mike Janes/President@isc2tc.org
www.isc2tc.org



ISSA MN CHAPTER - Supporting Sponsor

The Minnesota chapter of the Information Systems Security Association (ISSA) is a not-for-profit organization of information security professionals and practitioners. Our goal is to be the community of choice for cybersecurity professionals dedicated to advancing individual growth, managing technology risk and protecting critical information and infrastructure. We provide educational forums, publications, and peer interaction opportunities that enhance the knowledge, skill, and professional growth of our members.

Kyle Nesgood/612.467.9621/marketing@mn.issa.org
mn.issa.org



LOGRHYTHM - Panel Sponsor

LogRhythm, the leader in security intelligence and analytics, empowers organizations around the globe to rapidly detect, respond to and neutralize damaging cyber threats. The company's patented and award-winning platform uniquely unifies next-generation SIEM, log management, network and endpoint forensics, and advanced security analytics.

4780 Pearl East Circle, Boulder, CO 80301
Steve Lerach/651.219.4591/Steve.Lerach@logrhythm.com
www.Logrhythm.com



MASLON LLP - Presenting Sponsor

No business, regardless of size, is immune to the threat of a data breach. Assuring that your data is both accessible and safe is critical—and current regulatory requirements have made cybersecurity readiness one of the biggest compliance challenges companies face. Maslon's informed and experienced counselors can assess the cybersecurity risk profile of your business and provide proactive, practical advice to help protect your data and ensure legal compliance.

3300 Wells Fargo Center, Minneapolis, MN 55401
Pamela Roemer/612.672.8252/pamela.roemer@maslon.com
www.maslon.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.

1300 Harmon Place Minneapolis, MN 55403
Aud Wengronowitz/612.659.7306
Anongsri.wengronowitz@metrostate.edu
www.metrostate.edu

MINNESOTA HIGH TECH ASSOCIATION (MHTA) - Supporting Sponsor

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

400 South 4th Street, Suite 416, Minneapolis, MN 55415
Ted Modrich/952.230.4555/tmodrich@mhta.org
www.MHTA.org



MN.IT SERVICES - MN.IT 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
<https://mn.gov/mnit/>



MINNESOTA LAWYER - Media Sponsor

Minnesota Lawyer is the only weekly newspaper serving the law community in Minnesota. Minnesota Lawyer is dedicated to providing current news and information, expert opinions, advertising, and is the only newspaper discussing case law beyond the basics. We are trusted by our readers, the key decision makers in the legal community.

222 S. Ninth St., Suite 2300, Minneapolis, MN 55402
Bill Gaier/612.584.1537/bill.gaier@finance-commerce.com
www.minnlawyer.com



MITCHELL HAMLINE SCHOOL OF LAW - Exhibitor

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.

875 Summit Ave, St. Paul, MN 55105
Holly Noble/651.695.7669/holly.noble@mitchellhamline.edu
www.mitchellhamline.edu/cybersecurity

NEWBERRY GROUP - Exhibitor

Newberry Group is an employee owned IT firm specializing in Cyber Security, Digital Forensics, & Incident Response solutions & services. Our experienced team provides consulting, integration, and reseller services that include Insider Threat Protection, Continuous Visibility & Monitoring, SIEM, Enterprise Malware Protection, End Point Security, Data Protection.

2510 Old Highway 94 South, Suite 200, St. Charles, MO 63303
Jerry Kennedy/314.973.3693/gkennedy@thenewberrygroup.com
www.thenewberrygroup.com



SOCIAL SECURITY NUMBER
HOME ADDRESS
INCOME TAX RETURNS
BIRTH DATE
HEALTH RECORDS
PASSWORDS
PHONE NUMBER
LICENSE PLATE NUMBER
INCOME DATA
DRIVER'S LICENSE NUMBER
CREDIT CARD DATA
MENTAL HEALTH RECORDS
EMAIL ADDRESS

Works hard for her living.
Supporting a hacker isn't part of her 5-year plan.

October is National Cyber Security Awareness Month. Learn how the State of Minnesota is working to protect your data | mn.gov/mnit



Showcase your knowledge by earning a Cybersecurity Fundamentals Certificate!

A Cybersecurity Fundamentals Certificate—part of ISACA's **Cybersecurity Nexus™ [CSX]**—is an ideal and inexpensive way to earn a certificate that demonstrates your knowledge and skills in this increasingly in-demand field. The Certificate is perfect for students, recent grads, entry-level professionals and career-changers—and is a great way for organizations to train employees in this rapidly changing field.

Visit www.mnisaca.org for more information.



Online Course Now Available:
Cybersecurity Fundamentals



Nobody Delivers Digital Marketing Like We Do.

Propel connects businesses with the people who matter most -
their customers.

Propel Marketing is a one-stop shop for all your online marketing services. We help our customers improve their bottom line by providing cutting-edge digital solutions and industry best practices.

With a full array of online marketing solutions, we can create the perfect mix suited to boost your business.

Some of our services include:

- *Responsive Website Design*
- *Social Media Management*
- *Centralized Dashboard*
- *Call Tracking*
- *Reputation Monitoring*
- *OnTarget - Display Advertising*
- *Search Engine Marketing*



CALL TODAY! (612) 584-1539

WEBSITES. MOBILE. SOCIAL. LISTINGS. SEARCH. SEO. REPUTATION.

MINNESOTA LAWYER

Partnered with

PROPEL
MARKETING

Visit our
Cybersecurity
Roundtable
special section at
minnlawyer.com

www.propelmarketing.com

NORSEC FOUNDATION - VIP Reception Sponsor

The mission of the NorSec Foundation is to support the NorSec ISAO (Information Sharing Analysis Organization) program, and to advance all aspects of privacy, security, technology, and organizational resiliency.

Info@NorSec.org
www.NorSec.org



NUCLEON - Refreshment Sponsor

Nucleon brings focused targeted cyber intelligence to sensitive networks. Nucleon is based on innovative technology with tools built to work autonomously on the internet, identifying and learning the most dangerous threats on the internet 24/7. Nucleon offers the most comprehensive botnet solution available today, based on 3 Patents.

Moran Zavdi/+972-54-2000417/moranz@nucleon.sh
www.nucleon.sh

OPTIV - Exhibitor

Optiv is the largest holistic pure-play cyber security solutions provider in North America. The company's diverse and talented employees are committed to helping businesses, governments and educational institutions plan, build and run successful security programs through the right combination of cyber security products, services and solutions.

1125 17th Street, Suite 1700, Denver, CO 80212
www.optiv.com

OPTUM - Table Top Exercise Co-Sponsor

Optum is a leading health services and innovation company dedicated to helping make the health system work better for everyone. With more than 100,000 people collaborating worldwide, Optum combines technology, data and expertise to improve the delivery, quality and efficiency of health care.

11000 Optum Circle, Eden Prairie, MN 55344
www.optum.com



RSA - Exhibitor

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



SAILPOINT - Lanyard Sponsor

SailPoint is the fastest-growing, independent identity and access management (IAM) provider and helps the world's largest organizations securely and effectively deliver and manage user access from any device to data and applications residing in the datacenter, on mobile devices, and in the cloud.

11305 Four Points Drive, Austin, TX 78726
888.472.4578
www.sailpoint.com



SILA SOLUTIONS - Exhibitor

Sila Solutions Group (Sila) is a national management and technology consulting firm that offers IAM and PAM consulting and system integration services as part of its Information Security practice. Partnering with BeyondTrust, we leverage their best-in-class PAM platform to provide complete visibility and control over all privileged accounts and users.

www.silasg.com

SYMANTEC - Cyber Security Exercise Sponsor

Symantec Corporation is an information protection expert that helps people, businesses and governments seeking the freedom to unlock the opportunities technology brings – anytime, anywhere. Founded in April 1982, Symantec, a Fortune 500 company, has provided leading security, backup and availability solutions for where vital information is stored, accessed and shared.

350 Ellis Street, Mountain View, CA 94043
www.symantec.com



TANIUM - CISO Luncheon Sponsor

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

1625 Shattuck Avenue, Suite 200, Berkeley, CA 94709
Jim Brzezinski/651.335.3241/jim.brzezinski@tanium.com
www.tanium.com



TARGET CORPORATION - Exhibitor

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.

1000 Nicollet Mall, Minneapolis, MN 55403
www.target.com/careers

TECHNOLOGICAL LEADERSHIP INSTITUTE, UNIVERSITY OF MINNESOTA - Founding Partner

How can a master's degree in security technology grow your career and yield business results? Come hear stories from recent TLI graduates as they share their experiences, lessons learned, and business impact since completing a master's degree from the Technological Leadership Institute. This panel discussion will allow the audience to interact and participate as the graduates offer insight on how to change the game and achieve a positive return on investment.

200 Oak Street SE, Suite 290, Minneapolis, MN 55455
Eric Thornton/612.624.8826 /ethornton@umn.edu
www.tli.umn.edu



THE EVENT GROUP, INCORPORATED - Summit Producer

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

2815 S Wayzata Blvd., Minneapolis, MN 55405
763.548.1313/Doug.Mroczkowski@eventshows.com
www.PlantoAstound.com



THE NETWORK CONNECT - Supporting Sponsor

The Network Connect is a network of angel investors, groups and funds; including mentors and advisors. The Network Connect is an initiative to connect investors with companies seeking to raise capital and provide resources for businesses. Our network of service providers and business partners can support any company. We help fuel business growth and success by helping businesses expand their networks.

www.thenetworkconnect.com



THREATQUOTIENT, INC - Exhibitor

ThreatQuotient Inc. (TQI) is dedicated to revolutionizing cyber defense capabilities by building analyst-driven applications, helping organizations manage threat intelligence and therefore defending against sophisticated cyber attacks. Our product, ThreatQ allows analysts to spend more time on high-value processes rather than transferring intelligence across multiple cloud solutions and internal platforms.

1881 Campus Commons Drive, Suite 101, Reston, VA 20191
Michelle Mattear/michelle.mattear@threatq.com
www.threatq.com

TRAPX - Exhibitor

TrapX Security™ is the leader in deception technology. Our solution rapidly detects, analyzes and defeats new zero-day, and APT attacks in real-time. The TrapX customer base includes Forbes Global 2000 commercial enterprises and government agencies around the world in sectors that include defense, healthcare, finance, energy, and other key industries.

1875 South Grant Street, Suite 570, San Mateo, CA 94402
Marcela Ortiz/415.756.8022/Marcela@trapx.com
www.trapx.com

UPPER MIDWEST SECURITY ALLIANCE - Supporting Sponsor

UMSA (Upper Midwest Security Alliance) is an alliance of security and risk-related organizations that serves business, government and education professionals in the upper Midwest. UMSA collaborates with professional associations, educators and industry-leading companies to provide professional development opportunities including the Secure360 events in the Twin Cities, Iowa and Wisconsin and a soon-to-be student learning event in 2017.

1360 University Avenue W., Suite 461, St. Paul, MN 55104
info@umsa-security.org
www.umsa-security.org



THINK YOU KNOW WHAT'S ON YOUR NETWORK?

YOU CAN'T PROTECT WHAT YOU CAN'T SEE.



HEALTHIER IS HERE

At Optum, Healthier goes way beyond a feeling. Quite simply, it's our passion and our purpose. As a health services and innovation company, we power modern health care by combining data and analytics with technology and expertise. Our insights quickly lead to better outcomes for hospitals, doctors, pharmacies, health plans, governments, employers and the millions of lives they touch. Which, come to think of it, is a pretty good feeling as well.

optum.com



People. Technology. Data. Action.

© 2016 Optum, Inc.

HEALTHIER
ISN'T JUST A FEELING
—
FOR US, IT'S A
MISSION

UNISYS - Print 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.unisys.com/security



UNITED STATES CYBERSECURITY MAGAZINE - Supporting Sponsor

This magazine is published quarterly to help raise the level of awareness of the ever-increasing amount of Cyber crimes taking place right here in the United States of America and how to defend against these crimes through information provided here-in and by our Cyber crime-fighting advertisers displaying prevention and protection strategies in Cybersecurity.

Karen Austin/443.453.4784/karen.austin@uscysecurity.net
www.uscybersecurity.net



U.S. SMALL BUSINESS ADMINISTRATION - Cooperating Entity

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.

www.sba.gov



VORMETRIC - Expo Stage Participant

Vormetric is the industry leader in data security solutions that protect data-at-rest across physical, big data and cloud environments. Vormetric helps over 1500 customers, including 17 of the Fortune 30, to meet compliance requirements and protect their sensitive data from both internal and external threats.

www.vormetric.com

WIPFLI - Exhibitor

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

7601 S. France Ave., Suite 400, Minneapolis, MN 55435
Jeff Olejnik/952.230.6488, jolejnik@wipfli.com
www.wipfli.com/cybersecurity

THANK YOU 2016 SPONSORS + EXHIBITORS

The Cyber Security Summit would not be possible without our sponsors and exhibitors. Please take a moment during the Summit to join us in thanking them for their support and learning about the services they provide.

Interested in becoming a 2017 Sponsor or Exhibitor?

Sign up for Cyber Security Summit 2017 today and receive a FREE color logo upgrade - a \$150 value! Contact our sponsorship sales consultants: Jennifer Churchill at 763-548-1306/Jennifer.Churchill@eventshows.com or Paul TenEyck at 763-548-1308/Paul.TenEyck@eventshows.com

BIG IDEAS

BIG EVENTS

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

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

www.PlantoAstound.com

20th  the
**EVENT
GROUP**
incorporated
ANNIVERSARY

This list of terms was originally adapted from the glossary maintained by the National Initiative for Cybersecurity Careers and Studies (NICCS), a part of the Department of Homeland Security. The list has been added to by numerous industry experts.

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 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

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).

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 block unauthorized inbound and/or outbound 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 (adverse effects on) (poses a threat to) an information system or the information that the system processes, stores, or transmits and that may require a response action to mitigate the consequences.

INCIDENT HANDLER (CYBER SECURITY)

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

INDUSTRIAL CONTROL SYSTEM

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

INTEGRITY

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

INTRUSION DETECTION

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

KEYLOGGER

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

MACRO VIRUS

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

MALWARE

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

MITIGATION

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

MOVING TARGET DEFENSE

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

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.

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 search 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 non-native 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 [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*).

United States {**CYBERSECURITY**} Magazine

FREE SUBSCRIPTION

Subscribe Today to Our Digital Magazine!

**Receive complete online access
to our quarterly magazine and
full magazine archive!**

**Subscribe at
www.uscybersecurity.net/subscribe**

**443.453.4784
www.uscybersecurity.net**



Emergent Networks



Seasons change. Our commitment to **reliable IT** does not.

Emergent Networks serves our clients as a **trusted technology advisor** by offering complete IT Strategy, Solutions and Support. We seek to understand our clients' needs, environments and industries in order to **create the right business solutions** every time.

The Emergent Networks team strives to **make IT easy and transparent** so that our customers can focus on their business.

emergentnetworks.com / 612.213.2600

connections made simple.

[illegible]

[illegible]

[illegible]



Discover Minnesota's **flagship organization**
for the **science and technology community**

Learn

about emerging
technology and
innovation through
Lunch & Learns,
Member Innovation
Crawls and more



Connect to the
entrepreneurial and
investor community
at the **Minnesota**
Venture Conference

Support
STEM education
through the
SciTechsperience
Internship Program,
the **getSTEM** web
portal, and **STEM**
scholarships

Develop

your network and
professional skills
through
ACE Leadership,
Women Leading
in Technology and
networking events

There's so much
happening at the
Minnesota High Tech
Association.

Visit mhta.org

Trying to stay one move ahead?

Protecting your company's data in a world of
increasing threats is no easy game. Skilled legal
counsel is critical to managing risk, meeting
regulatory requirements, and keeping your goals
in check.

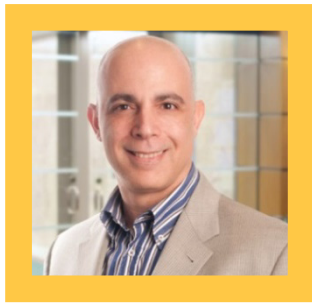
Maslon has extensive experience advising clients
on effective data security practices and privacy
law. We not only know the law, we know
business—across the board—and we're masters
at helping our clients advance.



ADVERTISING & MARKETING
BUSINESS & SECURITIES
ESTATE PLANNING
FINANCIAL SERVICES
LABOR & EMPLOYMENT
LITIGATION
REAL ESTATE

MASLON
60th ANNIVERSARY

MASLON LLP | 612.672.8200 | MASLON.COM



ABOUT THE AUTHOR:

ERAN KAHANA is a technology and intellectual property attorney with extensive experience advising clients in domestic and international settings. His practice focuses on cyber security, patent, trademark, and copyright law. Eran serves as general counsel and on the Board of Directors for the Minnesota Chapter of InfraGard, a nonprofit partnership between the FBI and the private sector dedicated to the protection of critical infrastructure, and is a Research Fellow at Stanford Law School, where he writes and lectures on the legal aspects of using artificial intelligence.

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 Cyber Security Law counsellors 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

MASLON LLP | MASLON.COM

Building a Healthy Cyber Security Ecosystem: A Three-Part Discipline

Data security breaches, legal requirements, customer obligations, demands by shareholders and boards of directors—these are but some of the variables that fuel enterprise concern with cyber security. It is a complex area, littered with critical, dynamic variables that can significantly impact or cripple (individually and collectively) every single aspect of your company's operations. Building and maintaining a healthy cyber security ecosystem is complex, but certainly achievable once the proper resources and discipline are put into place.

A "healthy" cyber security ecosystem is synonymous with one that is "reasonable." But what does that really mean? The implementation challenge begins with a definitional gap—the fact that there is no single law on point. This creates a partial legal and regulatory vacuum, one in which organizations need to build their own cyber security policies and procedures.

The good news is that regardless of the sector in which your organization belongs or the laws which directly apply to it, the reasonable cyber security ecosystem is defined as the product of three disciplines: (i) a thorough understanding of all the relevant laws, regulations, and industry standards; (ii) existence of information technology best practices, and (iii) syncing items (i) and (ii) with your corporate culture. Any gap in any of these components will dilute the effort and render the end result "unreasonable."

A key deliverable from a proper implementation of items (i) through (iii) is an Information Security Policy (ISP). Its importance cannot be overstated. The ISP serves both as a formal recordation of your company's cyber security posture and as the guiding operational principles that need to be systematically followed in order to ensure the "reasonableness" status is maintained.

Further good news here is that a reasonable cyber security ecosystem is not required to be flawless. Finding a defect is not fatal; it does not automatically render it "unreasonable." For example, a company that effectively implements monitor-test-validate data security processes can continue and maintain a "reasonable" status even when a system defect is identified.

Put differently, the law's focus is not solely on the existence of a "flaw." The law is more concerned with how it was patched. If it was completed promptly, and effective controls were adjusted to minimize recurrence, that is typically sufficient.

Maintaining post-breach operational resiliency is another important feature of maintaining a reasonable cyber security ecosystem. While this requirement is not driven by law, it is frequently driven by contract, even if not explicitly stated. For that to be in place you need to have good insurance.

"Good" insurance means your policy focuses on cyber security and is tailored to your specific operations. Relying on legacy, general instruments, such as Comprehensive General Liability (CGL), is a risky proposition as courts have yet to establish a good track record of providing clarity on data breach CGL coverage. Even favorable rulings (e.g., *Travelers v. Portal Health Solutions*) are not binding on other jurisdictions, and the fact patterns tend to be so specific as to render precedent to academic value.

Once the cybersecurity policy is provided, the real work begins and a diligent analysis is required prior to its purchase. Such policies are typically riddled with coverage exclusions. Failing to remove/amend them so they fit your company's distinct operational needs renders the policy irrelevant because your chance of recovering on a claim is less than slim.

To be effective, the diligent analysis requires experienced counsel. The attorney tasked with this review must: (i) possess a solid understanding of cyber security attack vectors; (ii) have an intimate familiarity with your ISP; and (iii) combine and leverage items (i) and (ii) to spot and remove or amend the problematic exclusions.

Data security breaches, customer demands, and management demands will continue to plague and test companies of all sizes and sectors. Legal, regulatory, and industry standards will also continue to become more complex. Fortunately, there is a solution: maintaining a reasonable cyber security ecosystem.

SIXTH ANNUAL EVENT



CYBER SECURITY
SUMMIT 2016

October 11-12, 2016 | JW Marriott Minneapolis

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.

SAVE THE DATE

October 23-25, 2017
📍 Minneapolis

To follow updates on the 2017 Cyber Security Summit, visit: cybersecuritysummit.org