CYBER SECURITY SUMMIT 2014

Brought to you by Symantec™

October 21-22, 2014

The Commons Hotel
Minneapolis, Minnesota

www.CyberSecuritySummit.org

KPMG

TECHNOLOGICAL LEADERSHIP INSTITUTE
UNIVERSITY OF MINNESOTA
Driven to Discover℠

MASLON

ATOMICdata

Deloitte.

FIBERPOP SOLUTIONS
DIGITAL CONTENT AT THE SPEED OF LIGHT

TANIUM™

Xcel Energy®

transform

Title Sponsor

Symantec.

Presenting Sponsors

KPMG

TECHNOLOGICAL LEADERSHIP INSTITUTE
UNIVERSITY OF MINNESOTA
Driven to Discover

MASLON

Premier Sponsors

ATOMICdata

Deloitte.

FIBERPOP SOLUTIONS
DIGITAL CONTENT AT THE SPEED OF LIGHT

TANIUM

Xcel Energy

VIP Reception Sponsor

MASLON

Official Summit Printer

UNISYS

CEO Breakfast Sponsor

CARDINAL STRITCH UNIVERSITY

Panel Sponsors

BRIGGS
BRIGGS AND MORGAN

MASLON

Passport Sponsor

SURFWATCH CYBER SIGHT

Gold Exhibitor

milestone systems

Silver Exhibitors

Check Point
SOFTWARE TECHNOLOGIES LTD.

LogRhythm
The Security Intelligence Company

SURFWATCH CYBER SIGHT

Exhibitors

fishnet SECURITY

pwc

MNIT SERVICES

paloalto networks.

Bremer Bank

KASPERSKY lab

esp IT
Placing People First

Metropolitan State University

Jet
Defending Enterprise Mobility

Supporting Sponsors

am 1570
WALL STREET BUSINESS NETWORK
KYCR
business1570.com

mhta
Driving Innovation & Technology

robotics alley
CONFERENCE & EXPO
Robotics Sensors Advanced Manufacturing

WWTC AM1280 THE PATRIOT

BBB
bbb.org

minnesota BUSINESS magazine

UMSA
United in security leadership

INFRAGARD

ISACA
Minnesota Chapter

SecMN
MINNESOTA SECURITY PROFESSIONALS

ISSA
MINNESOTA CHAPTER

BSides MSP

Summit Producer

the EVENT GROUP incorporated

MAXIMIZE YOUR EXPOSURE

Sign up to Sponsor Cyber Security Summit 2015 TODAY and receive a FREE color logo upgrade – a $150 value!

Contact **Jennifer Churchill**, Sponsorship Sales Consultant at 763-548-1306 or Jennifer.Churchill@eventshows.com

Welcome!

Thank you for participating in the fourth annual Cyber Security Summit!

In 2011, the University of Minnesota's Technological Leadership Institute came to us with a vision. The leaders there wanted to start a dialogue on cyber security, a topic they recognized wasn't getting nearly enough attention. It's hard to believe today, but in our first year, a big part of our task was just explaining what cyber security is.

Four years later, thanks to the hard work of many people and — unfortunately — after some hard-learned lessons, awareness is growing. Yet too many organizations still adopt an 'it-won't-happen-to-me" attitude and are left scrambling when an attack comes.

Those of you here today have chosen not to sit back and wait. You get it. But until everyone gets it, we all suffer the consequences. That's why this Summit is built on the idea that cyber security is an issue where we must pull together in a spirit of collaboration, not competition. From the beginning, it has been structured as a multi-stakeholder consortium where the ultimate goal is to stay ahead of the curve in protecting your data and infrastructure.

This important dialogue is only possible with the support and guidance of our advisors, sponsors, speakers and you: the attendees. Joining us this week are delegates representing industry, government and academia traveling from throughout Minnesota, 16 states and 5 countries.

Topics covered will include what this crisis means for American businesses, a look back at what people are calling 'The Year of the Large Scale Breach," and several presenters from D.C. who will speak to how this is being addressed in Washington. We will discuss why cyber security can't just be an afterthought — it must be integrated into the decision-making process at the highest levels. And later this evening, our partners at Security B-Sides MSP will host a 'Hacker Showcase" where you can learn about encryption, 'practical paranoia," exploitation methodology, how to secure your social media and more.

By now, some type of cyber security incident has affected almost everyone. The Ponemon Institute, which does independent research on privacy, reported last month that 43 percent of companies have experienced a data breach in the past year. Yet, according to the same report, 27 percent of companies still don't have a data breach response plan or team in place. That's unfortunate because for businesses today, it's not a matter of if they'll get hit, it's a matter of when.

The problem of cyber attacks will never be completely solved, but by working together we can drastically improve the state of cyber security both in the U.S. and abroad. Once again, we thank you for your participation in this ongoing dialogue, and we look forward to the conversation that will occur during the next two days.

— The 2014 Cyber Security Summit Advisory Board

Table of Contents

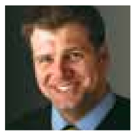
Special thanks to founding planning committee member **Ginny Levi**. Her dedication and continuous support has helped in growing this important Summit. We wish her well in retirement.

Ginny Levi, *Associate Director, External Relations/Administration, Technological Leadership Institute (TLI), University of Minnesota with* ***Mark Weatherford,*** *Principal, The Chertoff Group; Former Deputy Under Secretary for Cybersecurity, U.S. Department of Homeland Security*

Cyber Security Summit 2014 would not have been possible without the dedication and expertise of the Advisory Board and Summit Committee.

2014 Advisory Board Members

Dr. Massoud Amin, D.Sc.
Director, Technological Leadership Institute, University of Minnesota



Andrew Borene, Esq.
Chair, Cyber Security Summit 2015; Attorney, Steptoe & Johnson LLP; Adjunct Professor, American University

Christopher Buse, CISA, CISSP
Assistant Commissioner/CISO, MN.IT Services

Doug DeGrote
CISO & Director of IT Security & Risk Management, Xcel Energy

Steen J. Fjalstad, MS, CISA, CISSP, CGEIT, CRISC
Security and Mitigation, Principal & Chief Administration Officer, Midwest Reliability Organization, ISACA, InfraGard

Ron Fresquez
CEO/Founder, TOSTA Information Security Training Services

Matthew Harmon, CISSP, GSEC, GCIH, GCIA
Owner and Security Researcher, IT Risk Limited

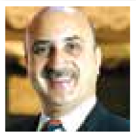
Col. Stefanie Horvath, MSS
Colonel, MN Army National Guard

Brian Isle, PE
Senior Fellow, Adventium Labs/University of Minnesota Technological Leadership Institute

Mike Johnson, MSST, CISM
Chief Information Security Officer/Operations Risk Director, Bremer Financial Services, Inc.

Eran Kahana, J.D.
Attorney, Maslon Edelman Borman & Brand, LLP

Margaret Anderson Kelliher
President & CEO, Minnesota High Tech Association



Gopal Khanna
Managing Partner, The Khanna Group, LLC

Chip Laingen
Commander, U.S. Navy (Ret.); Executive Director, Defense Alliance

Mark Lanterman, MS
Chief Technology Officer, Computer Forensic Services

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

Jerrod Montoya, Esq.
Security & Compliance Attorney, OATI; Vice President, InfraGard Minnesota Members Alliance

Kathleen Moriarty
Global Lead Security Architect, Corporate Office of the Chief Technology Officer, EMC Corporation

Dave Notch
Director, Information Protection and Business Resilience, KPMG

John Orner, MBA
Vice President, Treasurer & Chief Investment Officer, Blue Cross and Blue Shield of Minnesota

James Ryan, CSyP, CEA, PMP
Chief Strategy Officer, Cyber Security Summit; Owner & Founder, Litmus Logic, LLC

Philip Schenkenberg, J.D.
Attorney, Director, and Shareholder, Business Litigation, Briggs & Morgan, P.A.

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

2014 Summit Committee

Matt Cleghorn
Policy and Strategy Assistant, Technological Leadership Institute (TLI), University of Minnesota

Jennifer Churchill
Sponsorship Sales Manager, The Event Group, Incorporated

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

Ginny Levi
Associate Director - External Relations/Administration, Technological Leadership Institute (TLI), University of Minnesota

Doug Mroczkowski
Event, Travel & Registration Coordinator, The Event Group, Incorporated

Sarah Myers
Associate Marketing Manager and Speaker Coordinator, The Event Group, Incorporated

Nancy Skuta
IT Standards & Risk Management Division, MN.IT Services

Paulette Sorenson, CMP
Director of Events, The Event Group, Incorporated

Rhonda Zurn
Director of Communications, Office of the Dean, College of Science and Engineering, University of Minnesota

VIP RECEPTION

Sponsored By

MASLON

Stewart A. Baker, *Partner, Steptoe & Johnson LLP, Washington, D.C.; Former First Assistant Secretary of Policy, Homeland Security; and Former General Counsel, National Security Agency*

Yesterday evening, Cyber Security Summit 2014 hosted a VIP Reception attended by select sponsors, speakers, and key opinion leaders. Stewart A. Baker presented a preview of his Summit Keynote presentation on what the growing cyber security crisis means for American business — and how knowing your adversary can reveal what you have to do to defend yourself.

INTERACT WITH PRESENTERS THROUGHOUT THE SUMMIT!

Sponsored By

KPMG

KPMG is making engagement easier with its e-Brainstorming® technology. Using laptops provided at each table, Cyber Security Summit participants can ask questions or provide feedback anonymously and can view questions and other participants' answers simultaneously – in real-time!

HACKER SHOWCASE

Sponsored By

B Sides MSP

Tuesday, October 21, 2014
5:00 – 8:00 PM, Meridian Ballroom
(Check-in begins at 4:00 PM)

Want to know more about the fundamentals of encryption and how it works? Want to understand 'practical paranoia" and how to secure your social media? Or how to use GPG to securely transfer information? Then attend the 'Security B-Sides MSP Hacker Showcase" session at the Cyber Security Summit. This special event is being hosted at the end of Day One of the Summit by Security B-Sides MSP, a group that provides a launchpad for security professionals and offers hands-on security training, and is free to all registered attendees. Other topics that will be touched on include critical security controls, USB 'rubber duckies," exploitation methodology, how to pick a lock, and more.

ROUNDTABLE DISCUSSIONS AT LUNCH

Sponsored By

the EVENT GROUP incorporated

Tuesday, October 21, 2014
11:45 AM – 12:30 PM
Think Tank and Inventor Rooms

Engage fellow participants with similar interests during our topic-specific roundtable discussions on Day One of the Summit. Join your peers in exploring one of the following topics:

What is the No. 1 thing companies should be doing about cyber security that they aren't?

What should be our top public policy priority regarding cyber security?

How can organizations better integrate security professionals into decision-making at a high level?

What can small businesses do to better protect themselves against cyber attacks?

Following a cyber attack, what are the first three things an organization should do?

What are the next big cyber threats on the horizon?

Will we ever stop hearing regular announcements of large data breaches or is this the new reality?

NETWORKING RECEPTION

Tuesday, October 21, 2014
4:00 – 6:00 PM, Exhibit Area

Collaborate with fellow leaders on cyber threat issues, brainstorm innovative countermeasures, network with industry experts, and walk away with actionable solutions. Appetizers and cocktails (cash bar) will be available to enjoy.

POST-SUMMIT RECEPTION

Wednesday, October 22, 2014
5:00 PM, Beacon Public House (Commons Hotel, Lower Level)

Continue the momentum from the Summit and join colleagues at the Beacon Public House to resume the collaboration.

CLE CREDITS APPROVED IN MN AND IA!

Cyber Security Summit 2014 has been approved for 11 CLE Credits in Minnesota and 6.75 in Iowa.

For Minnesota: Visit www.mbcle.state.mn.us, search courses and use Event ID 195228

For Iowa: Visit www.iacourtcommissions.org, search courses and use Activity ID 157190

STEM EDUCATION SCHOLARSHIP FUND

CYBER SECURITY SUMMIT 2014

Support Our Youth
Cyber Security Summit is making a commitment to supporting STEM Education through its scholarship fund. Congratulations to this year's recipient **Vanessa Esaw**, who will receive $5,000 to pursue further education in Computer Science.

SCHOLARSHIP RECIPIENT

Administered By

mhta
Driving Innovation & Technology

Vanessa Esaw
Vanessa is a sophomore at the University of Minnesota majoring in computer science. This past summer, she did research in natural language processing at the University of Texas at El Paso. She was awarded fifth place for best poster presentation for her research ‘Determining the Proficiency of Bilingualism of English-Spanish Speakers.” She was also very involved on campus at her former school, Normandale Community College. She helped to establish the school's local STEM club as secretary and assistant leader of a student-driven quadcopter project. She also re-created and built a foundation for Japanese Club as club president. She has committed more than 300 hours to community service projects and volunteering through the student organization Leadership Through Service. She intends to continue doing research in artificial intelligence and natural language processing through the National Science Foundation's undergraduate program in the summer of 2015. After completing her degree, she intends to go to graduate school in computer science.

Join the Cyber Security Summit in supporting our youth - Donate Now at the Registration Desk!

JOIN THE DISCUSSION

Experience the Summit on Twitter

We encourage all attendees to share their thoughts and feedback throughout the conference on Twitter, using the **hashtag #CSS2014MN**

You can find Cyber Security Summit on **Twitter (twitter.com/cs_summit)**

LIKE US ON FACEBOOK

Like us on Facebook to receive the latest news from Cyber Security Summit

Facebook.com/cssummit

CONNECT WITH US ON LINKEDIN

Join the discussion with industry leaders and cyber security experts on LinkedIn

Cyber Security Summit 2013 – International Cyber Security Thought Leadership

COMPLIMENTARY WI-FI

Complimentary Wi-Fi is available throughout the convention center for your use.

Use Code: CSS14

STAY CONNECTED

Visit **CyberSecurityBusiness.com** to keep up-to-date on current events and sign up for our weekly newsletter!

SECURE THE WORLD'S MOST CRITICAL ASSETS

At TLI we bridge the space where business, engineering, science, and technologies converge.

What Makes TLI Programs Stand Out?

- **MOT: Master of Science in Management of Technology** More than one-third of our graduates become executives within five to seven years. Another 50 percent become managers and senior managers.

- **MDI: Master of Science in Medical Device Innovation** With approximately half of the world's medical device companies in Minnesota, at TLI you will advance in the heart of the industry.

- **MSST: Master of Science in Security Technologies** Employers of TLI graduates appreciate their breadth of knowledge of security issues as well as the depth of understanding they bring to their field.

TECHNOLOGICAL
LEADERSHIP INSTITUTE

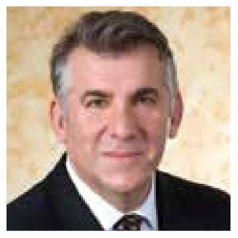
UNIVERSITY OF MINNESOTA
Driven to Discover℠

Mark Abbott

Chief Information Officer, Atomic Data

Cyber Resiliency - Preparing for the Inevitable

Since the early nineties, Mark has garnered expertise in a diverse background of IT, law and business. Working his way up from a technologist at Atomic Data's sister company, The Foundation, Mark filled the role of Director of Special Projects with Atomic Data. In addition to owning Abbott Systems, Inc., Mark is the Chief Technology Officer at The Foundation and the Chief Information Officer at Atomic Data. Mark holds a Computer Science degree from Macalester College with a J.D. and MBA from the University of Minnesota - Twin Cities.

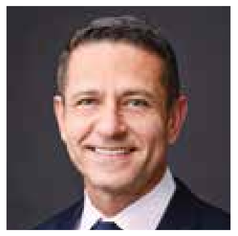


Dr. Massoud Amin, D.Sc.

Director, Technological Leadership Institute, University of Minnesota

The Year In Review and What's Ahead; Cyber Resiliency - Preparing for the Inevitable (Panelist)

Dr. Massoud Amin leads extensive projects in smart grids and infrastructure security and is considered the father of smart grid. He holds the Honeywell/H.W. Sweatt Chair in Technological Leadership at the University of Minnesota, directs the University's Technological Leadership Institute (TLI), is a University Distinguished Teaching Professor, and professor of electrical and computer engineering. Before joining the University in 2003, he held positions of increasing responsibility at the Electric Power Research Institute in Palo Alto. After 9/11, he directed all Infrastructure Security R&D and led Grid Operations/Planning and Energy Markets. Prior to 9/11, he served as head of mathematics and information sciences, led the development of more than 24 technologies that transferred to industry, and twice received the Institute's highest honor.



Souheil Badran

Senior Vice President and General Manager, Digital River World Payments

CEO Breakfast

Souheil Badran is the Senior Vice President and General Manager of Digital River, leading all aspects of the company's global payments strategy, including strategic development, sales and marketing, product management, operations, mergers and acquisitions. Today, Digital River processes more than $30 billion in online transactions and offers global payments in more than 190 countries and over 170 currencies. Souheil joined Digital River with extensive experience in high technology organizations — leading sales and marketing, product management, strategic development, mergers and acquisitions and high-growth initiatives. Prior to Digital River, Souheil was senior vice president and general manager of First Data Corporation's e-commerce solutions group, a team that focused on e-commerce and card-not-present commerce. His specialty in international e-commerce also includes previous executive leadership positions at Rebtel, VeriSign, Digital Insight (acquired by Intuit) and Metavante Corporation (acquired by FIS).

Stewart A. Baker

Keynote Speaker

Partner, Steptoe & Johnson LLP, Washington, D.C.; Former First Assistant Secretary of Policy, Homeland Security; and Former General Counsel, National Security Agency

What the Cyber Security Crisis Means for American Business

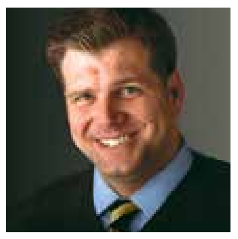
Stewart Baker is a partner in the law firm of Steptoe & Johnson in Washington, D.C. From 2005 to 2009, he was the first Assistant Secretary for Policy at the Department of Homeland Security. His law practice covers cybersecurity, data protection, and travel and foreign investment regulation. Mr. Baker has been General Counsel of the National Security Agency and of the commission that investigated WMD intelligence failures prior to the Iraq war. He is the author of 'Skating on Stilts," a book on terrorism, cybersecurity, and other technology issues, and he blogs about such topics on www.skatingonstilts.com. He also hosts a weekly podcast on technology, security, privacy and government, the Steptoe Cyberlaw Podcast. www.steptoe.com/feed-Cyberlaw.rss.

Brett Beranek

Senior Principal Marketing Manager, Nuance Communications, Inc.

Beyond Passwords: Something You Have, Something You Know, Something You Are

Senior Principal Marketing Manager, Nuance Communications, Inc.
Like you, voice biometrics expert Brett Beranek is fascinated by transformative technologies that have a real impact on our lives. With over a decade of experience in the biometrics and security space, Brett brings strategic and tactical insights to organizations wishing to deliver a better authentication experience to their customers. Prior to joining Nuance, Brett, a technologist and entrepreneur by education and passion, successfully introduced several disruptive technologies to the health-care, IT and security markets. Brett has in-depth expertise with a wide range of security technologies, including facial recognition, fingerprint biometrics, video analytics and license plate recognition technology.



Andrew Borene, Esq.

Chair, Cyber Security Summit 2015; Attorney, Steptoe & Johnson LLP; Adjunct Professor, American University

Beyond Passwords: Something You Have, Something You Know, Something You Are

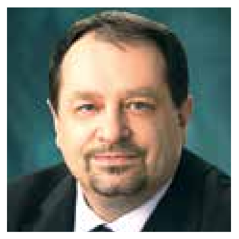
Andrew Borene is a defense industry executive, Adjunct Professor at American University, and Counselor to the international law firm of Steptoe & Johnson LLP. His corporate career includes leading corporate development at a microrobotics startup and managing federal open-source intelligence programs for a publicly-held, international big-data company. He served as a civilian Associate Deputy General Counsel at the U.S. Department of Defense and is a former U.S. Marine Corps military intelligence officer. He is active within the leadership of leading public-private initiatives for improved U.S. national security, global leadership and technology growth. Andrew is the editor of American Bar Association legal research books on human rights, humanitarian law and national security. A Minnesota native based in Washington, D.C., Andrew has published numerous policy articles and appears as a guest analyst on military, intelligence and veterans issues for several international news networks.

L. Keith Burkhardt

Vice President, Kraus-Anderson Insurance

Liability

L. Keith Burkhardt is responsible for Kraus-Anderson's agency growth strategies including product development throughout all market sectors, talent acquisition and M&A. Recently, Mr. Burkhardt has developed Cyber Risk Strategies for the agency customers that unite cyber security vendors, the FBI, and insurance. Previously, Burkhardt was regional managing director of Wells Fargo Insurance Services, leading its 22 Upper Midwest operations and Minneapolis office for nine years. During that period he led national initiatives for Wells Fargo Insurance in Healthcare, Public Entity and Higher Education. He also served as managing director of Bloomington-based Acordia, developing its agency operations and market positioning; and as senior vice president of Memphis-based Sedgwick, directing its energy, transportation and healthcare production teams. In addition to his leadership roles, his experience also includes more than 25 years working with Lloyd's of London as well as managing and consulting on large claim events in excess of $20 million. Burkhardt earned a B.A. in Economics from Southern Methodist University (SMU) and a B.B.A. in Finance from SMU - Cox School of Business.



Douglas DeGrote

CISO & Director of IT Security and Risk Management, Xcel Energy

Liability

Douglas DeGrote is the Chief Information Security Officer and director of IT Security & Risk Management at Xcel Energy. In this role, he has leadership responsibility for developing and delivering IT security, disaster recovery and business continuity strategies for a major U.S. electricity and natural gas utility with operations across eight states. DeGrote and his team have a strong record of working together with internal and external experts as well as government entities to identify, assess, respond to and defend against ever evolving cyber threats and ensuring the reliability and resiliency of the energy grid.

Matthew Harmon, CISSP, GSEC, GCIH, GCIA

Owner and Security Researcher, IT Risk Limited

Panel Introduction

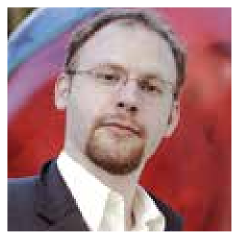
Matthew is an executive advisor, security researcher, SANS instructor and mentor, auditor, penetration tester, incident handler, security architect and security team builder as well as international standards developer. He has consulted and advocated for many Fortune, governmental, campaigns, and not-for-profit organizations and is familiar with the day-to-day challenges of businesses large and small. In addition to his role at his company, Matthew is also the President and Founder of the (ISC)2 Twin Cities Area Chapter, and sits on the board for the Upper Midwest Security Alliance (UMSA) and Whittier Business Association.

Peter J. Holbrook, Ph.D.

Dean, College of Business and Management, Cardinal Stritch University

CEO Breakfast

Peter J. Holbrook, Ph.D., is Dean of the College of Business and Management at Cardinal Stritch University and has 30 years of experience in higher education. His expertise includes board development, organizational leadership and change, program development and evaluation, service, strategic thinking and planning, succession planning, and teams. Dr. Holbrook teaches at the doctoral level and is a researcher, writer, and speaker in the area of Leadership, with an expertise in the area of Franciscan, servant and transformational leadership as well as leading for innovation and change.



Lance James

Head of Cyber Intelligence, Deloitte & Touche LLP

Year of the Large Scale Breach
'Crimeware as a Service"

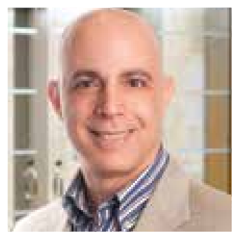
Lance James is an internationally renowned information security expert. He has fifteen years of experience in programming, network security, digital forensics, malware research, cryptography design, cryptanalysis, and attacking protocols. He has provided advisory services to a wide range of government agencies and Fortune 500 organizations, including America's top financial services institutions. Credited with the identification of Zeus and other malware, James is an active contributor to the betterment of security practices and counter-threat methods through active membership in a wide range of organizations, and through contributions to a number of industry books and publications, including Phishing Exposed (Syngress, 2005), Emerging Threat Analysis (Syngress, 2006), and Reverse Deception (McGraw Hill Professional, 2012). Publications currently in the works include The Threat Intelligence Handbook (No Starch Press) and Hacking Back: Offensive Cyber Counterintelligence (McGraw Hill). Keynote speaking engagements include the SC Congress eSymposium on Cyber Espionage, the First Asia HTCIA Conference (Hong Kong), Digital PhishNet (Germany/San Diego, CA), and SANS Conference (San Diego, CA). Prior to joining Deloitte, James was the Chief Scientist for Vigilant, Inc., co-founder and chief scientist of Secure Science Corporation, and senior threat analyst at Damballa.

Mike Johnson, MSST, CISM

Chief Information Security Officer/ Operations Risk Director, Bremer Financial Services, Inc.

CEO Breakfast

Mike Johnson has worked in financial services for over 20 years, focusing on Security, Risk Management, Compliance, and IT issues. Mike has been with Bremer Bank, a $9 Billion regional financial services firm, for 15 years and is responsible for developing and overseeing Bremer's enterprise security and operations risk management program. Prior to joining Bremer, Mike was IT Director and Compliance Officer for Dean Financial Services in St. Paul and spent eight years as an FDIC Bank Examiner. Mike holds a Certified Information Security Manager (CISM) designation from ISACA and a Master of Science degree in Security Technologies from the University of Minnesota College of Science and Engineering.

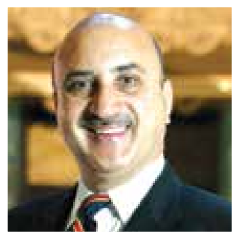


Eran Kahana, J.D.

Attorney, Maslon Edelman Borman & Brand, LLP

Liability

Eran Kahana, Special Counsel to Minneapolis law firm Maslon Edelman Borman & Brand, LLP, is an IP attorney with extensive experience advising clients in domestic and international settings. He focuses his practice on matters such as drafting and negotiating complex software, patent, and trademark licenses, joint development agreements, strategic partnerships, subcontract agreements, and service agreements. Eran has extensive experience managing and enforcing global copyright, trademark and patent portfolios, and advises clients on a wide variety of IP needs. Eran is a frequent speaker and writer on various intellectual property topics and a Research Fellow at Stanford Law School.



Gopal Kahana

Managing Partner, The Khanna Group, LLC

Keynote Introduction

Gopal Khanna is Co-Founder of the Cyber Security Summit, and served as Chair of the Board of Advisors from 2011-2013. He frequently consults, writes and speaks on Cyber Security, C-Suite strategies for information risk management and CIO strategies for securing IT Platform by drawing upon his unique expertise at the intersection of technology, government and business. Khanna is a Senior Fellow at the Technological Leadership Institute at the University of Minnesota, managing partner at The Khanna Group LLC and President & Chair of the Minnesota Innovation Lab. Earlier, Khanna served as CIO and CFO of the United States Peace Corp., and CFO for the Executive Branch of the Office of the President and Office of Administration.

Demetrios (Laz) Lazarikos, CISA, CISM, CRISC, CSLLP

Keynote Speaker

IT Security Strategist, Blue Lava Consulting, LLC

Gaining Visibility: Meaningful Information Security and Fraud Data in Seconds

Laz works with Fortune 500 companies and emerging technology companies in building IT security, IT risk, and compliance solutions. Laz is the former CISO and the visionary behind the Information Security and Compliance team for the Sears Online Business Unit. In that role, Laz drove efforts in creating an Information Security and Fraud big data platform to combat cyber criminal activities and protecting the international business unit. His work in the areas of quantifying loss exposure in dollars by implementing big data systems for Information Security and Fraud analytics have been widely praised by industry analysts at Gartner. Prior to joining the online retailer, Laz was the CISO for Silver Tail Systems, where he built the Information Security and Compliance program from the ground up. Laz was hired post Series B venture-funding from Andreessen-Horowitz to promote the growth of marquee accounts in key verticals – Financial Services, Government, and eCommerce. Laz is the inventor of several patents for controlling personally identifiable information, Information Security, and quantifying security risks. His involvement with security initiatives includes contributions for standards, policies, and frameworks regarding Information Security methodologies, Web application security, and IT risk. While enlisted in United States Air Force (USAF), Laz was decorated twice, including two USAF Achievement Awards for using his expertise in the area of operational efficiencies, information technology, computer security, and leadership qualities at two highly visible USAF bases. Laz is a Teaching Fellow at Pepperdine University's Graziadio School of Business and Management, holds a Master's in Computer Information Security (MCIS) from the University of Denver, a Master's in Business Administration (MBA) from Pepperdine University, and has earned several security and compliance certifications.

Brian L. Levine

Keynote Speaker

Trial Attorney, Computer Crime and Intellectual Property Section (CCIPS), U.S. Department of Justice

Cyber Security: A Team Effort

Brian L. Levine serves as a prosecutor in the Department of Justice's Computer Crime and Intellectual Property Section ("CCIPS"). Prior to joining CCIPS, Mr. Levine served as an Assistant Attorney General in the Internet Bureau at the New York Attorney General's Office; a county prosecutor in Detroit, Michigan; and a civil litigator in Silicon Valley. Mr. Levine has clerked for federal judges in the Southern District of Florida and on the Seventh Circuit. He earned his J.D. from New York University and his B.A. from the University of Pennsylvania.

Loren Dealy Mahler

Keynote Speaker

Vice President Corporate Communications, MWW Group

Lessons Learned; Cyber Resiliency - Preparing for the Inevitable (Panelist)

Loren Dealy Mahler is Vice President in MWW Group's corporate communications practice. She works with a number of diverse clients, including large corporations and non-profits, to accomplish their business objectives through corporate reputation building, executive visibility and influencer engagement. Prior to joining MWW, Loren spent over a decade in Washington, D.C., directing strategic communications initiatives. Most recently, Loren served as Director of Legislative Affairs on the National Security Council Staff at the White House, where she coordinated across multiple federal agencies to build support for national security, foreign policy and homeland security policy issues. Previously, Loren was Director of Communications for the Office of Legislative Affairs at the Department of Defense, where she created legislative communications strategies to win support for multiple policy initiatives across a wide range of audiences. She also worked to coordinate strategic communications and legislative outreach on crisis issues, including the publication of classified government documents by Wikileaks in 2010. Before joining DoD, Loren was Communications Director for the House Armed Services Committee, where she coordinated all communications functions, including external communications around the Committee's work on the annual defense bill. Originally from Houston, Texas, Loren graduated from Princeton University with a degree in Sociology and Georgetown's McCourt School of Public Policy with a Master's in Policy Communications.

Eileen Manning

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

Welcome and Scholarship Presentation

Eileen Manning is a 30-year executive specializing in marketing and event management. She has served with a top advertising agency and spent over a decade in management at a Fortune 100 financial institution producing hundreds of business conferences ranging in attendance from 100 to 5,000; managing marketing services including communications, public relations, business television, video production, and graphic design; and directing an $11 million corporate travel department. She holds a Bachelor of Science Degree from Cardinal Stritch University, graduating magna cum laude, and earned an Audio Visual Technology Degree from Hennepin Technical College, graduating summa cum laude. Eileen has also completed additional advanced business courses from the University of St. Thomas.

Michael C. McCarthy

Partner and Member of Firm Governance Committee, Maslon Edelman Borman & Brand, LLP

VIP Reception Keynote Introduction

Mike McCarthy is a partner in Maslon's Litigation Group and a member of the firm's Governance Committee. He represents clients in complex litigation and appeals. His practice has involved a range of substantive matters, including breach of fiduciary duty, securities and consumer fraud, environmental claims, medical-device liability, and antitrust. Mike has defended class actions in federal and state courts involving environmental claims, medical-device liability, securities and consumer fraud, constitutional rights, and antitrust violations. In addition, he has experience with and expertise in technology-related litigation (including patent infringement) and electronic discovery. Before joining Maslon, Mike served as a law clerk to Judge Gerald W. Heaney of the U.S. Court of Appeals for the Eighth Circuit and Judge Louis H. Pollak of the U.S. District Court for the Eastern District of Pennsylvania.

Jay Meier

Vice President of Corporate Development, BIO-key International, Inc.

Beyond Passwords: Something You Have, Something You Know, Something You Are

As VP Corporate Development at BIO-key, Jay is responsible for strategic and corporate development, primarily in the healthcare markets. With his extensive financial analytical experience, he also supports C-level management regarding BIO-key's operational execution, as well as manages BIO-key investor relations. Before joining BIO-key, Jay was Founder & Managing Partner of Sage Capital Advisors, which provides economic, capital market and strategic consulting services in the Security, Credentialing and Identity Management industries. Prior to that, Jay was SVP of Corporate Development for OTI-America, a leading provider of contactless smart card solutions. Previous to OTI, Jay worked as Finance Controller for a healthcare services firm and for many years as a Senior Research Analyst at various boutique investment banks. In June 2006, Jay published Secure Credentialing & Identification — Wall Street's first and most comprehensive industry research overview of the Security, Biometrics, PKI, Smartcard, Credentialing and Identity Management industries. In 2003, he ranked in the 99th percentile of all securities analysts in North America. In 2004, he ranked in the 97th percentile. In 2005, the StarMine/Forbes Magazine Securities Analyst Ranking Survey named Jay "8th Best Stock Picker in North America." Jay earned a B.S. in Economics from the University of Wisconsin-Madison in 1992.

Michael Mimoso

Editor, Kaspersky Lab – Threatpost.com

Year of the Large Scale Breach ʻCrimeware as a Service"

Michael brings more than a decade of IT security news reporting to Threatpost. As an editor of Threatpost, he covers critical security issues, research, and cyber crime affecting businesses and end-users today. Prior to joining Threatpost, Michael was Editorial Director of the Security Media Group at TechTarget and Editor of Information Security magazine where he won several ASBPE national and regional writing awards. In addition, Information Security was a two-time finalist for national magazine of the year. Michael has been writing for business-to-business IT publications for 11 years, with a primary focus on information security. Earlier in his career, Michael was an editor and reporter at several Boston-area newspapers. He holds a bachelor's degree from Stonehill College in North Easton, Mass.

Dave Notch

Director, Information Protection and Business Resilience, KPMG

CEO Breakfast

Dave has over 20 years of experience in the technology and security fields. He is currently Director of Information Protection and Business Resilience in KPMG's Advisory Services division, where he assists organizations with developing and executing business-centric information protection strategies. Prior to KPMG, Dave was President of Intensity Analytics, a security software firm that specializes in behavioral biometric authentication using keyboard input in addition to software that measures and monitors computer activity. Combined, these solutions provide real-time, continuous authentication and monitoring of all computer activity. Before Intensity Analytics, Dave was CISO of Thomson Reuters, where he was responsible for managing the corporate programs for information security, business continuity, disaster recovery and technology-related audit and compliance activities. Dave holds a Master's degree in Computer and Information Science from the University of Minnesota, Institute of Technology.

Chris Nutt

Director of Incident Response, Mandiant, A FireEye Company

Year of the Large Scale Breach ʻCrimeware as a Service"

Chris Nutt is the Director of Incident Response. Mr. Nutt has 10 years of experience in enterprise incident response, working with the federal government, defense industrial base, and Fortune 100 companies. He has extensive experience in incident response, computer forensics, and remediation planning. He has led high-visibility investigations into the theft of intellectual property as well as the theft of payment card industry information. He regularly assists organizations in developing remediation strategies designed to remove sophisticated attackers from client networks. Mr. Nutt teaches computer incident response to the public and private sectors. He is responsible for development and delivery of technical content in the incident response training courses he teaches. In these courses, he instructs students how to collect and analyze information and how to manage investigations.

Matthew Rhoades

Keynote Speaker

Director, Cyberspace & Security Program, Truman National Security Project & Center for National Policy

Cyber After Snowden: Can D.C. Help Protect Your Networks?

Matt is the Director, Cyberspace & Security Program at the Truman Project and Center for National Policy. In this role, he leads the program's Steering Committee and directs the organization's cyber security policy initiatives. Matt has been published in multiple outlets including Roll Call, Politico, The Hill, San Jose Mercury News, and Christian Science Monitor. Previously, Matt served as the Director of Legislative Affairs at the Truman National Security Project. In that capacity, he ran the Congressional Security Scholars program and was the principal author of the Truman Security Briefing Book. Matt advises Members of Congress and congressional staff on foreign affairs and defense policy.

John Rome, J.D.

Founder and CEO, Intensity Analytics Corporation

Beyond Passwords: Something You Have, Something You Know, Something You Are

Mr. Rome has a national reputation as a software architect and technology inventor. He holds a B.A. in economics with a concentration in mathematics, with honors, as well as a Juris Doctor degree from the University of Minnesota. After passing the Minnesota Bar decades ago, John sidestepped the practice of law in favor of staying with software development, his lifelong passion. He has developed large-scale computer programs to automate virtually every facet of the practice of law and several other industries. Along the way, he launched five innovative businesses, descendants of which endure today. A veteran entrepreneur, his professional happiness comes from creating high-tech jobs — not to mention entire industry segments. Fluent in Microsoft technologies, when not creating new uses for automation helpful to the non-tech world, John spends hobby time developing spherical trigonometric algorithms to further his interest in astronomy. Some of those mathematics formulas have shown up in formally patent-pending software in the cyber security area. He is a noted speaker, having made over 250 presentations and now is managing his company's activities in the area of multifactor biometric authentication by means of keystroke patterns.

Charles Ross, CISSP, CISM

Sr. Director, Technical Account Management, Tanium, Inc.

Year of the Large Scale Breach 'Crimeware as a Service"

Charles is the Sr. Director, Technical Account Management at Tanium, Inc. In this role, Charles is responsible for leading an engineering team that empowers Fortune 500 organizations with visibility and control of their endpoint environments at scale. The Technical Account Management team that Charles leads helps assess ongoing threats, define customer requirements/use cases, and deploy solutions to respond to the most complex IT problems in real-time. Prior to joining Tanium, Charles was the Vice President of North America Technical Operations at McAfee. Charles led an organization chartered with helping McAfee customers and partners develop a strategic vision for security, compelling business cases, and the efficient positioning of products and services to achieve their critical security and business initiatives. Charles has also served as a Security Consultant for Deloitte & Touche in their Enterprise Risk Services group. There he consulted with Fortune 500 companies to assess, develop, and implement world-class security programs.

Renault Ross, CISSP, MCSE, CHSS, CCSK, VCP5

Keynote Speaker

U.S. Technical Architect, Information Protection, Public Sector Strategic Programs, Symantec Corporation

The Ever Changing Threat Landscape

Renault Ross is a United States Technical Architect for security and privacy supporting Public Sector strategic state, local and education department at Symantec. In this role, Ross provides information security and privacy thought leadership messaging and strategy, increasing Symantec's presence in the health IT, education and state consolidation verticals. He joined Symantec in 2007. Ross represents Symantec on panel discussions as well as at industry conferences and state CxO briefings around the country. His expertise lies in virtualization, mobility, cloud and cyber security, including enterprise security management best practices to address cyber security risk and drive up efficiencies. Prior to Symantec, Ross worked as a global security architect and security engineer at a private company located in Atlanta, Ga. His duties included establishing the organization's first security program (Compliance, Vulnerability Management and Incident Response). Ross holds many certifications including, Certified Information Systems Security Professional (CISSP), Certified HIPAA Security Specialist (CHSS), Microsoft Certified Systems Engineer (MCSE), Symantec Certified Specialist (SCS), Certificate of Cloud Security Knowledge (CCSK), and VMware Certified Professional (VCP5).

Dr. Ron Ross

Keynote Speaker

Fellow, National Institute of Standards and Technology (NIST), Information Technology Laboratory, Computer Security Division

The National Conversation No One Wants to Have: A New Paradigm for Cyber Resiliency

Dr. Ron Ross is a Fellow at the National Institute of Standards and Technology (NIST). He currently leads the Federal Information Security Management Act (FISMA) Implementation Project, which includes the development of key security standards and guidelines for the federal government, contractors, and the United States critical infrastructure. Dr. Ross has authored numerous cyber security publications and is the principal architect of the NIST Risk Management Framework. Dr. Ross also leads the Joint Task Force Transformation Initiative Working Group, a joint partnership with NIST, the Department of Defense, and the Intelligence Community, to develop a unified information security framework for the federal government. A graduate of the United States Military Academy at West Point, Dr. Ross served in a variety of leadership and technical positions during his 20-year career in the United States Army. He is a three-time recipient of the Federal 100 award and has been inducted into the Information Systems Security Association Hall of Fame. During his military career, Dr. Ross served as a White House aide and as a senior technical advisor to the Department of the Army. Dr. Ross holds both Master's and Ph.D. degrees in Computer Science from the United States Naval Postgraduate School.

Bradley Rossiter, MS, CISSP, CRISC, CISA

Principal Security Architect, Verizon

Year of the Large Scale Breach 'Crimeware as a Service"

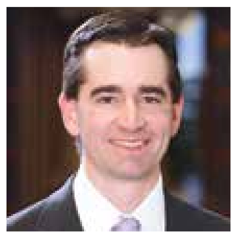
Bradley Rossiter, an innovative expert in enterprise information security and business protection strategies, is currently providing thought leadership in the cyber security services industry. His primary responsibility is delivering the necessary technological and risk management leadership that allows global 1000 organizations to safely sustain a competitive marketplace advantage. Throughout Operation Ababil, Mr. Rossiter was invited to speak about global network attacks to the USSS, DHS, and many business leaders across the globe. Mr. Rossiter received his M.S. in Management of Technology at the University of Minnesota's Technological Leadership Institute and also holds a B.S. in Computer Science and industry gold-standard certifications in information security and technology.

James Ryan, CSyP, CEA, PMP

Chief Strategy Officer, Cyber Security Summit; Owner & Founder, Litmus Logic, LLC

Panel Introduction

James is a cyber defense strategy implementation expert and author with over 15 years of experience delivering transformational business results for U.S. federal agencies and critical infrastructure companies. In 2008, James worked with NASA, HP/EDS, TSCP, and others to define game-changing identity and credential management strategies — then pioneered the first implementations for early adopters. These strategies have evolved into Personal Identity Verification Interoperability (PIV-I) and the Identity, Credential, and Access Management (ICAM) Segment Architecture. James holds a MSEE from Virginia Tech and is a Chartered Security Professional (CSyP), Certified Enterprise Architect (CEA), and Project Management Professional (PMP).



Philip Schenkenberg, J.D.

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

Cyber Resiliency - Preparing for the Inevitable

Phil is co-chair of Briggs and Morgan's Business Litigation Section and serves on the firm's board of directors. He is a member of the firm's Privacy and Data Security Group, which offers a full range of services to help clients prevent, prepare for and minimize the impact of data security breaches and cyber attacks. Phil practices principally in data security, telecommunications and general business litigation. He also serves as the firm's Data Security Manager and chairs the firm's Information Security Committee. In his practice, Phil represents clients in federal and state courts, and before the FCC and public utilities commissions.

Scott Singer

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

Liability

Since assuming his role in 2010, Scott has been responsible for information systems, global quality, export control, security, and continuous process improvement. Before PaR, Scott spent 16 years with Medtronic in various leadership positions, and in his last IT position at Medtronic, he was head of IT for a billion dollar division. In 2003, Scott transitioned into quality at Medtronic where he drove a company-wide systems development and validation methodology for IT systems. In his last two years at Medtronic, Scott led the global security function. Capt. Singer is active in the Navy Reserve and has been involved in the Gulf War and Operations Enduring Freedom/Noble Eagle. Currently he is the Navy Emergency Preparedness Liaison Officer (NEPLO) for the state of Minnesota. In his most previous role he was the Executive Officer for Commander Pacific Fleet Maritime Operations Center responsible for supporting the communications and cybersecurity needs of the Pacific Fleet. Scott has an undergraduate degree in Meteorology from the University of Wisconsin and a Master's in Business Administration from the University of Minnesota.

Jeremy Wunsch

Founder & CEO, LuciData, Inc.

Cyber Resiliency - Preparing for the Inevitable

Jeremy Wunsch is the founder and CEO of LuciData Inc. With almost two decades of forensics, internal threat management and e-discovery experience, he is a leading authority in the development of internal threat management and data forensic solutions for companies and their legal counsel. In addition, he has served as an IP protection consultant for organizations of all sizes and across multiple industries. Most recently, he directed the creation of HelioMetrics to help transform data breach identification. Jeremy is the author of numerous industry-related articles, a frequent national lecturer and quoted source, and is an adjunct professor teaching digital evidence analysis.

SECURE.
ROCK SOLID.
BULLETPROOF.

CYBER SECURITY SUMMIT 2014

WORDS PEOPLE USE TO DESCRIBE THE EVENTS WE MANAGE.

Events. Marketing. Strategy. Meetings. Branding. Website Design.

the EVENT GROUP incorporated

Producers of the 2014
Cyber Security Summit

PlanToAstound.com

Federal Bureau of Investigation

Addressing Threats to the Nation's Cybersecurity

As the primary investigative agency of the federal government for more than a hundred years, the responsibilities of the Federal Bureau of Investigation (FBI) have kept pace with ever-emerging threats and crime trends affecting the United States. From the notorious gangsters of the early 20th century, to espionage and sabotage during World War II, through the Cold War years and the global war on terrorism, the FBI has protected our nation. The 21st century brings with it entirely new challenges, in which criminal and national security threats strike from afar through computer networks, with potentially devastating consequences. While the FBI must adapt to meet these challenges, addressing the broad range of threats to the nation's cybersecurity is squarely within its mandate. *Why the FBI?*

It's our job.

The FBI has a unique dual responsibility, to prevent harm to national security as the nation's domestic intelligence agency and to enforce federal laws as the nation's principal law enforcement agency. These roles are complementary, as threats to the nation's cybersecurity can emanate from nation-states, terrorist organizations, and transnational criminal enterprises; with the lines between sometimes blurred.

The FBI's unified mission brings all lawful investigative techniques and legal tools together in combating these threats. This approach facilitates information sharing and ensures responsible stewardship of resources by collocating talent, tools, and institutional knowledge in a single organization.

- **Domestic Coordination within the U.S. Intelligence Community**

  As a member of the U.S. Intelligence Community (USIC), the FBI leads the National Cyber Investigative Joint Task Force (NCIJTF). Located in the Washington, D.C. metro area, the NCIJTF serves by Presidential Directive as the national focal point for coordinating cyber threat investigations. Representatives from the USIC member agencies, as well as select federal law enforcement partners, are present at the center and collaborate in identifying, mitigating, and disrupting cybersecurity threats.

- **Support to the Homeland Security Enterprise**

  As part of the homeland security enterprise, the FBI supports the Department of Homeland Security's (DHS) mission by investigating threats and incidents which affect the security of protected computers and networks. The results of these investigations increase collective knowledge which can be leveraged to improve the nation's security posture, such as providing effective mitigation strategies to potential victims. Additionally, actions taken by the FBI have succeeded in disrupting and dismantling threats. With the entire homeland security enterprise working together, and through a balanced approach employing both defensive measures and directed action against adversaries, our nation is safer.

Roles and Authorities in Brief

The FBI has the authority and responsibility to investigate and enforce all violations of federal law that are not exclusively assigned to another federal agency.
- Title 28, USC Section 533 & 28 CFR 0.85

"The Department of Justice and the FBI lead the national effort to investigate and prosecute cybercrime."
- The President's National Strategy to Secure Cyberspace, 2003

"The FBI is vested by law with the primary role in carrying out investigations within the United States of threats to the nation's security. This includes the lead domestic role in the investigation of international terrorist threats…and in the conduction of counterintelligence activities against foreign espionage and intelligence efforts directed against the U.S."
- Attorney General Guidelines for Domestic FBI Operations

"Intelligence elements of the FBI…shall collect (including through clandestine means), analyze, produce, and disseminate foreign intelligence and counterintelligence…"
- Executive Order 12333 and pursuant to Title 50, USC Section 401

- **Leadership within U.S. Law Enforcement**

  The FBI's capacity to respond to cyber incidents and emergencies in communities nationwide is enhanced through task force partnerships with other law enforcement agencies. Key federal, state, and local cyber investigative and forensic personnel, sworn and civilian, are teamed together in this endeavor. The FBI is enhancing the capabilities of each of its cyber task forces to address the full range of cybersecurity threats and function as extensions of the NCIJTF. No other agency can match this broad and robust presence, which is crucial for timely and effective incident response.

In the U.S. and abroad, we are where you need us.

Domestic — Whether you live and work in a large city or small town, chances are that the FBI has an office nearby. FBI field offices are located in 56 cities, with satellite offices in some 380 additional locations. Cyber agents at each field office are equipped to respond to events ranging from a significant data breach to a national cyber emergency. And, to supplement this standing capability, the FBI also maintains a rapid deployment team of highly specialized cyber agents.

International — Not only does 21st century technology enable global communication and commerce, it enables threat actors to apply their craft from anywhere in the world. For nearly 70 years, the FBI has stationed personnel overseas to build relationships that protect Americans at home. Today, the FBI maintains legal attaché offices within 75 U.S. Embassies globally, covering over 200 countries. Additionally, cyber agents have been embedded with foreign law enforcement partners in several key countries, fulfilling a liaison role to foster cooperation and mutual legal assistance.

We acknowledge the unique capabilities of private industry and academia, and the need for constant collaboration.

The U.S. Government cannot address cybersecurity threats alone. Ongoing collaboration with affected industries, security researchers, and academia is indispensible. The FBI maintains a presence and close partnership with the National Cyber Forensics and Training Alliance (NCFTA), and shares intelligence with the private sector through FBI-led InfraGard chapters and through various industry-specific Information Sharing and Analysis Centers (ISACs). In partnership with the National White Collar Crime Center (NW3C), the FBI offers the Internet Crime Complaint Center (IC3) as a means to receive cyber crime complaints from consumers and businesses for action by authorities, and to disseminate fraud alerts to the public.

FBI Headquarters, J. Edgar Hoover Building

We defend the Constitution by upholding the law, while protecting privacy and civil liberties.

Roles and responsibilities within the Executive Branch agencies are divided to ensure mission focus and clarity in regard to authorities. As a component of the Department of Justice, the FBI is responsible for investigations and intelligence collection within the territorial jurisdiction of the United States and relating to U.S. persons overseas.

Bound by the U.S. Constitution, relevant laws, and guidelines provided by the Attorney General, the FBI is governed by the principle of employing the least intrusive method necessary to further an investigation. When an investigative method would infringe upon an individual's reasonable expectation of privacy, approval and oversight by a U.S. District Court or the Foreign Intelligence Surveillance Court is required.

In its role as a protector and defender of the U.S. Constitution and enforcer of federal law, the FBI regularly takes action on behalf of victims whose privacy has been violated, such as through a computer intrusion or identity theft.

We care.

In the last decade, the FBI has assembled a team of hundreds of cyber experts with diverse and highly skilled information technology backgrounds. Our people are committed to serving the public by meeting cyber challenges head on and imposing consequences on those who victimize the American people through the misuse of computers and networks.

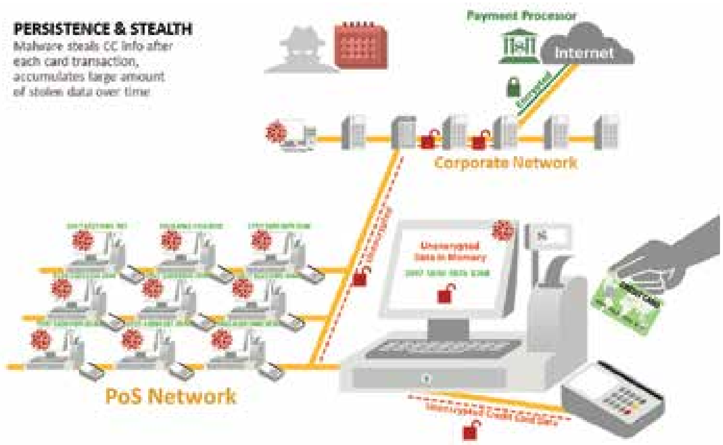
Backoff Trojan Is Back:

Protect Your Business From The Next POS Breach

By Solange Deschatres

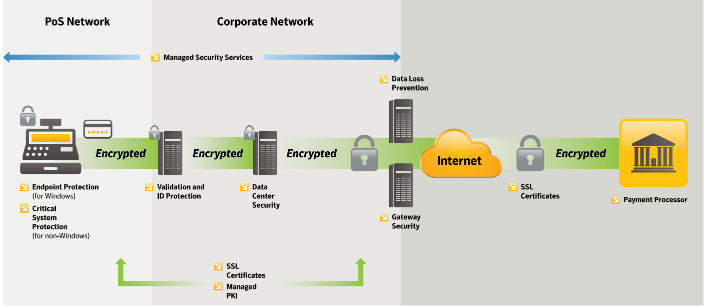
The New York Times has reported that the Department of Homeland Security has expanded its estimate of businesses affected by the Trojan.backoff Point of Sale malware. Over 1000 total businesses in the U.S. are reported to have been affected, up from around 600, which was reported earlier this month. Dubbed "Backoff", this Trojan malware steals customer payment details through remote access applications.

This kind of activity appears to be growing. Identity theft, according to the Bureau of Justice Statistics, affected 16.6 million people in 2012. Hackers sell credit card data in underground markets. Credit card data is used to produce fake credit cards, or make online purchases.


PERSISTENCE & STEALTH
Malware steals CC info after each card transaction, accumulates large amount of stolen data over time
Payment Processor
Internet
Corporate Network
Unencrypted Data in Memory
PoS Network

How Can Retailers Protect Customers?

According to Symantec security expert, Kevin Haley, a properly configured endpoint protection product can block even the most dogged attacker, especially when it comes to a POS system. As a device with limited functionality, a POS is easier to secure than a PC with email and web-browsing capabilities.



Multi-Layered Protection

Multi-layered protection, including encryption, anti-virus, intrusion protection, application control and device control capabilities, is vital to maximizing security. Invest in a product that provides the right tools to allow you to minimize the attack surface by limiting the specific applications running on the system, as well as regulate which devices and applications are allowed to access the network. Limiting applications and network accessibility on the machines can render malware useless.

Existing Symantec Endpoint Protection customers can optimize their POS protection by following our guide, available here.

How Can Customers Protect Their Information?

Most customers no longer carry cash everywhere they go, so it is important that they are equipped with the information to help them to keep their finances safe.

Here are a few key tips for consumers:

- Sign up for online access to credit card accounts via the credit card company's website, or download the app.
- Track online transactions and regularly verify purchases.
- Report any suspicious transactions to a credit card company immediately. In most cases, fraudulent charges can be reversed, and the account frozen to prevent any further theft.

For more important links to help safeguard your business, please visit:

- Upgrading to SEP 12
- How To Secure your Mobile POS Devices
- Secure Your Point Of Sale System

Solange Deschatres is blogger, journalist, and storyteller with expertise in covering enterprise security and technology.

AM 1280 The Patriot

SUPPORTING SPONSOR

AM 1280 The Patriot is the Twin Cities Intelligent radio station. Since its launch in March of 2001 it has been a movement and the voice of the silent majority. Our hosts include Bill Bennett, Dennis Prager, Mike Gallagher, Michael Medved, Hugh Hewitt, and Mark Levin. Patriot listeners are loyal, affluent and influential.

Mike Murphy
2110 Cliff Road
Eagan, MN 55122
651.289.4418
mike.murphy@salemtc.com
www.am1280thepatriot.com

Atomic Data

PREMIER SPONSOR

Atomic Data is a SOC 3 certified IT services company, dedicated to providing safe, simple and smart technology solutions to meet the needs of business. From The Atomic Cloud™, to enterprise-grade colocation, to custom software development and much more, Atomic Data truly is a one-stop-shop for all things IT. Safe. Simple. Smart. That's Atomic Data.

Scott Evangelist
615 North 3rd Street
Minneapolis, MN 55401
612.466.2100
info@atomicdata.com
www.atomicdata.com

Better Business Bureau

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.

Better Business Bureau of Minnesota and North Dakota
220 S. River Ridge Cir
Burnsville, MN 55337
651.699.1111
ask@thefirstbbb.org
www.thefirstbbb.org

Bremer Financial Corporation

EXHIBITOR

Bremer Financial Corporation is a privately held, $8.7 billion regional financial services company jointly owned by the Otto Bremer Foundation and Bremer employees. The company provides a comprehensive range of banking, investment, trust and insurance products and services throughout Minnesota, North Dakota and Wisconsin.

Michael Johnson
8555 Eagle Point Boulevard
Lake Elmo, MN 55042
mpjohnson@bremer.com
www.bremer.com

Briggs and Morgan, P.A.

PANEL SPONSOR

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

Phil Schenkenberg
2200 IDS Center
80 South 8th Street
Minneapolis, MN 55402
612.977.8400
pschenkenberg@briggs.com
www.briggs.com

Business 1570

SUPPORTING SPONSOR

Business 1570 is the only full-time business radio station in the Minneapolis/St. Paul metropolitan area. With our broadcast partners Bloomberg and CNBC, Business 1570 covers financial news, events, and topics from Wall Street to Main Street. Business 1570 listeners are the movers and shakers in the Twin Cities business community.

Mike Murphy
2110 Cliff Road
Eagan, MN 55122
651.289.4418
mike.murphy@salemtc.com
www.business1570.com

Cardinal Stritch University

CEO BREAKFAST SPONSOR

Cardinal Stritch University, Milwaukee, WI provides transformative, value-centered education to students of all faiths and ages in four colleges: Arts and Sciences, Education and Leadership, Business and Management, and Nursing. Stritch is the largest Catholic, Franciscan institution of higher education offering undergraduate and graduate degrees across Wisconsin, Minnesota, and Illinois.

Amie Engels
6801 N Yates Rd
Milwaukee, WI 53217
800.347.8822
admityou@stritch.edu
www.stritch.edu

Check Point Software Technologies

SILVER EXHIBITOR

Check Point Software is the worldwide leader in securing the Internet, provides customers with uncompromised protection against all types of threats, reduces security complexity and lowers total cost of ownership.

Andrew Fox
763.218.3500
afox@checkpoint.com
www.checkpoint.com

Deloitte & Touche LLP

PREMIER SPONSOR

Deloitte & Touche LLP provides audit and enterprise risk services that help organizations build value by taking a Risk Intelligent approach to managing financial, technology and business risks.

Bethany Larson
50 S 6th St.
Suite 2800
Minneapolis, MN 55402
612.397.4000
cyberiskinfo@deloitte.com
www.deloitte.com/us/cyberrisk

ESP IT

EXHIBITOR

A Minneapolis-based IT consulting and Direct Hire placement firm, ESP IT has consistently exceeded expectations by delivering candidates with the technical skills and culture fit our clients need. Since 1968, we've been committed to finding our clients their greatest assets, advancing IT Pros' careers, and always placing people first.

Denise Morelock
527 Marquette Ave
Suite 600
Minneapolis, MN 55402
careers@esp.com
www.esp.com

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.

Doug Mroczkowski
2815 Wayzata Blvd.
Minneapolis, MN 55405
763.548.1313
Doug.Mroczkowski@eventshows.com
www.Eventshows.com

FiberPop Solutions, Inc.

PREMIER SPONSOR

Our mission is to deliver unlimited digital content at the speed of light. We develop, engineer, build and manage open access, high capacity Fiber to the Premise (FTTP) networks and data centers for communities in the Upper Midwest.

Jim Louks
3703 West Highway 14
Owatonna, MN 55060
507.451.3326
jmlouks@fiberpops.com
www.fiberpops.com

TUESDAY, OCTOBER 21

7:00 – 8:00 AM

Registration Opens and Continental Networking Breakfast

8:00 – 8:15 AM

The Year In Review and What's Ahead *(Welcome)*

Sponsored by TECHNOLOGICAL LEADERSHIP INSTITUTE UNIVERSITY OF MINNESOTA Driven to Discover

Dr. Massoud Amin, Director of the Technological Leadership Institute, will provide an overview the past year, which has included the disclosure of some of the most high-profile breaches and vulnerabilities in history. In addition, he will discuss what can be done going forward and how the cyber security profession is expected to grow in the coming years.

Dr. Massoud Amin, D.Sc., Director, Technological Leadership Institute, University of Minnesota

8:15 – 8:30 AM

Measuring Audience Perceptions of Today's Cyber Security Threat Landscape

Sponsored by KPMG

8:30 – 9:25 AM

The Ever Changing Threat Landscape 🔑

Sponsored by Symantec.

In today's ever changing threat landscape, you want your IT environment to be secure. We will walk you through various security vectors and how cyber criminals obtain access to your valuable data, which can mean disaster for your brand's reputation. Learn what the latest and most popular threats are and how you can avoid them. Gain knowledge and understanding that one security product can only protect you at specific entry points. In order to create a fortress for your IT environment you will need multiple layers of security defense to keep cyber criminals out. From managing increased IT workloads that continue to transform the business to adopting new mobile devices and applications that live in the cloud to securing a 'borderless" border with an ever-changing threat landscape, IT professionals are faced with a daunting task: Making information readily available while keeping it secure. By adopting an intelligent, information-centric approach to your organization's data, you can be confident your critical information is secure.

Renault Ross, CISSP, MCSE, CHSS, CCSK, VCP5, U.S. Technical Architect, Information Protection, Public Sector Strategic Programs, Symantec Corporation

9:25 – 10:10 AM

What the Cyber Security Crisis Means for American Business 🔑

The headlines are full of new breaches, and Washington seems intent on punishing the victims. Stewart Baker will talk about what the growing cyber security crisis means for American business. From direct regulation to indirect influence on negligence suits, the government is doing what it can to change network security practices around the country. But regulation alone will not solve the problem. Instead, Baker thinks, we need to focus on the attacker. Knowing your adversary tells you what you have to do to defend yourself, and perhaps how to deter future attacks.

Stewart A. Baker, Partner, Steptoe & Johnson LLP, Washington D.C.; Former First Assistant Secretary of Policy, Homeland Security; and Former General Counsel, National Security Agency

10:10 – 10:30 AM

Break and Book Signing by Keynote Stewart A. Baker

10:30 – 11:45 AM

Year of the Large Scale Breach – "Crimeware as a Service" *(Panel Discussion)*

Large-scale criminal cyber activity has reached new levels of sophistication with malware vendors providing malicious code for targeted use. This 'Crimeware as a Service" provides well-designed, configurable malware complete with customer support and periodic upgrades and bug fixes. The customers for this malicious code are sophisticated criminals, organized crime, and nation states intent on stealing funds and critical intellectual property.

Introduction: **Matthew Harmon, CISSP, GSEC, GCIH, GCIA**, Owner and Security Researcher, IT Risk Limited

Moderator: **Lance James**, Head of Cyber Intelligence, Deloitte & Touche LLP

Panelists: **Michael Mimoso**, Editor, Kaspersky Lab - Threatpost.com

Chris Nutt, Director of Incident Response, Mandiant, A FireEye Company

Charles Ross, CISSP, CISM, Sr. Director, Technical Account Management, Tanium, Inc.

Bradley Rossiter, MS, CISSP, CRISC, CISA, Principal Security Architect, Verizon

TUESDAY, OCTOBER 21

11:45 AM – 12:30 PM

Networking Lunch with Roundtable Discussions in the Think Tank and Inventor Rooms

Sponsored by the EVENT GROUP incorporated

12:35 – 1:15 PM

Cyber After Snowden: Can D.C. Help Protect Your Networks? 🔑

This session will discuss the impact the materials leaked by Edward Snowden had on the cyber security debate in Congress; the prospects for cyber security legislation in a lame duck year — 2015 — and beyond; and a case study: 'legislating after a crisis — what that may mean for cyber."

Keynote Introduction by **Andrew Borene, Esq.**, Chair, Cyber Security Summit 2015; Attorney, Steptoe & Johnson LLP; Adjunct Professor, American University

Matthew Rhoades, Director, Cyberspace & Security Program, Truman National Security Project & Center for National Policy

1:30 – 2:45 PM

Liability *(Panel Discussion)*

Sponsored by MASLON

Case Study – Learn firsthand from what one company experienced when they filed for reimbursement following a cyber security incident.

Mitigating Risk – How do you approach a Board of Directors with incident/breach without creating liability for CEO and Directors? How do you protect management?

Insurance – Exclusions and triggers organizations do that result in denied coverage.

Moderator: **Eran Kahana, J.D.**, Attorney, Maslon Edelman Borman & Brand, LLP

Panelists: **L. Keith Burkhardt**, Vice President, Kraus-Anderson Insurance

Douglas DeGrote, CISO & Director of IT Security and Risk Management, Xcel Energy

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

3:00 – 4:00 PM

Cyber Security: A Team Effort 🔑

Brian Levine, a prosecutor with the Computer Crime and Intellectual Property Section of the U.S. Department of Justice, will discuss recent trends in cybercrime and the current cyber threat environment. He will address how the private sector can work collaboratively with law enforcement to reduce the cyber threat, catch the criminals, and mitigate loss. He will also provide examples of successful strategies to help minimize risk from hackers and insider threats.

Brian L. Levine, Trial Attorney, Computer Crime and Intellectual Property Section (CCIPS), U.S. Department of Justice

4:00 – 6:00 PM

Opening of Exhibit Area, Networking Reception and Check-in Opens for Hacker Showcase

5:00 – 8:00 PM

Hacker Showcase

Sponsored by B Sides MSP

Want to know more about the fundamentals of encryption and how it works? Want to understand 'practical paranoia" and how to secure your social media? Or how to use GPG to securely transfer information? Then attend the 'Security B-Sides MSP Hacker Showcase" session at the Cyber Security Summit. This special event is being hosted at the end of Day One of the Summit by Security B-Sides MSP, a group that provides a launchpad for security professionals and offers hands-on security training, and is free to all registered attendees. Other topics that will be touched on include critical security controls, USB 'rubber duckies," exploitation methodology, how to pick a lock, and more.

WEDNESDAY, OCTOBER 22

7:15 – 8:15 AM **CEO Breakfast**

(Invitation Only)

Sponsored by CARDINAL STRITCH UNIVERSITY

As senior management, how do you develop the next generation of information security leaders who will protect your company from an increasing number of cyber security threats? Currently, many who rise through the information technology ranks have the necessary technical background to succeed but lack awareness of the broader business issues that today's IT leaders must contend with. This panel of current IT executives will discuss the issues they face today and the qualities that will be required for the leaders of tomorrow. They will also explain why business professionals must start to understand that cyber security is not just an IT issue, it is an important factor that needs to be woven into everyday management practices.

Moderator: **Peter J. Holbrook, Ph.D.**, Dean, College of Business and Management, Cardinal Stritch University

Panelists: **Souheil Badran**, Senior Vice President and General Manager, Digital River World Payments

Mike Johnson, MSST, CISM, Chief Information Security Officer/Operations Risk Director, Bremer Financial Services, Inc.

Dave Notch, Director, Information Protection and Business Resilience, KPMG

7:30 – 8:30 AM **Registration Opens and Continental Networking Breakfast**

8:30 – 8:40 AM **Welcome and Scholarship Presentation**

Congratulations Cyber Security Summit STEM Scholarship Recipient ***Vanessa Esaw***

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

8:40 – 9:40 AM **Gaining Visibility: Meaningful Information Security and Fraud Data in Seconds** 🔑

A big data case study on using a risk-based approach for Information Security and Fraud analytics to protect a company brand, intellectual property, and customer data. This case study is based on four years of experience as a CISO for a Fortune 100 retailer. Laz will discuss the build out of the Information Security program in an agile environment while using big data for Information Security and Fraud Analytics to make better decisions faster. This case study has been referred to by Gartner in their areas of research with Big Data analytics.

Demetrios (Laz) Lazarikos, CISA, CISM, CRISC, CSSLP, IT Security Strategist, Blue Lava Consulting, LLC

9:40 – 10:40 AM **Networking Break in Exhibit Area**

10:40 AM – 12:00 PM **Beyond Passwords: Something You Have, Something You Know, Something You Are** *(Panel Discussion)*

When a cyber security breach occurs, often one of the first questions asked is, 'Did they get any passwords?" The reason is simple: a password is frequently the only thing that stands between criminals and our confidential data, financial information or other sensitive online documents. For years, passwords have provided a sense of security online, but today the question is whether a password alone is enough. A panel of experts will address that question. Advances in biometrics and security tokens can offer an additional layer of security and are already being embraced by some large financial institutions.

Introduction: **James Ryan, CSyp, CEA, PMP,** Chief Strategy Officer, Cyber Security Summit; Owner & Founder, Litmus Logic, LLC

Moderator: **Andrew Borene, Esq.**, Chair, Cyber Security Summit 2015; Attorney, Steptoe & Johnson LLP; Adjunct Professor, American University

Panelists: **Brett Beranek**, Senior Principal Marketing Manager, Nuance Communications, Inc.

Jay Meier, Vice President of Corporate Development, BIO-key International, Inc.

John Rome, Esq., Founder and CEO, Intensity Analytics Corporation

12:00 – 1:00 PM **Networking Lunch in the Pinnacle Room**

WEDNESDAY, OCTOBER 22

1:15 – 2:15 PM

The National Conversation No One Wants to Have: A New Paradigm for Cyber Resiliency

The United States has developed over the years an incredibly powerful and complex information technology (IT) infrastructure — an infrastructure that is inexorably linked to the economic and national security interests of the nation. The total dependence on IT infrastructure for mission and business success in both the public and private sectors, including the critical infrastructure, has left the nation extremely vulnerable to hostile cyber-attacks and other serious threat events, including natural disasters, structural/component failures, and errors of omission and commission. The susceptibility to the cyber threat is a concern for both public and private networks. In light of the current state of the IT infrastructure, it will be important going forward to build an effective response to measurably increase confidence in the IT systems we depend on (public and private) and at the same time, decrease a would-be attacker's confidence in the effectiveness of their capabilities to compromise our systems.

Keynote Introduction by **Gopal Khanna**, Managing Partner, The Khanna Group, LLC

Dr. Ron Ross, Fellow, National Institute of Standards and Technology (NIST), Information Technology Laboratory, Computer Security Division

2:15 – 3:30 PM

Cyber Resiliency - Preparing for the Inevitable

Sponsored by BRIGGS

(Panel Discussion)

There appears to be an attempt in the industry to shift the focus from cyber security to cyber resiliency. The idea is that, at some inevitable point in time, a vulnerability will be exploited by a threat and that companies must be prepared to absorb the impact of these events by being resilient. Whereas cyber security tends to focus on mitigating the likelihood of an attack in the first place, cyber resiliency would focus on how to recover from a realized attack. This idea started gaining traction prior to the massive Target breach but has since gained more attention. The question is what happens to security (prevention-side) if cyber resiliency (recovery-side) becomes the new hot trend? Are we just going to throw up our hands and give up trying to prevent attacks?

Moderator: **Philip Schenkenberg, J.D.,** Attorney, Director, and Shareholder, Briggs and Morgan, P.A.

Panelists: **Mark Abbott,** Chief Information Officer, Atomic Data

Dr. Massoud Amin, D.Sc., Director, Technological Leadership Institute, University of Minnesota

Loren Dealy Mahler, Vice President Corporate Communications, MWW Group

Jeremy Wunsch, Founder & CEO, LuciData, Inc.

3:30 – 4:15 PM

Networking Break in Exhibit Area

4:15 – 4:25 PM

2015 Vision

Andrew Borene, Esq., Chair, Cyber Security Summit 2015; Attorney, Steptoe & Johnson LLP; Adjunct Professor, American University

4:25 – 5:00 PM

Lessons Learned

It seems that nearly every day, the headlines announce a new security breach impacting yet another company. With such a steady stream of incidents, why do some stories seem to grow legs and drag on long after the incident has occurred, while others are mere blips on the radar? The answer oftentimes has to do with the company's own reaction. Whether in the strategic development of an incident response plan or in the frantic aftermath of a breach, it's often easy to overlook the potential damage to your most valuable asset — your corporate reputation. How then can you take steps both before and after to mitigate that impact, even while you're throwing all your resources at preserving more tangible assets? Loren will walk through key lessons learned from recent high-profile data breaches, and discuss how you can apply them to your own preparation and response planning.

Loren Dealy Mahler, Vice President Corporate Communications, MWW Group

5:00 PM

Post-Summit Networking at Beacon Public House *(Commons Hotel, Lower Level)*

IS IT SAFE?

Deloitte.

Top 10 considerations for building an insider threat mitigation program

Introduction

Organizations continue to face a variety of insider threats, as demonstrated by a string of high profile cases where employees in pursuit of validation or affirmation have used their knowledge and access to physical and/or information systems to cause significant damage. These cases highlight vulnerabilities and underscore a historical perception that insider threat mitigation is predominately a cyber-security challenge, and categorized as a strictly information technology responsibility. This approach will leave the organization vulnerable to existing and emerging insider threats. Deloitte takes a fundamentally different view that insider threats are more effectively addressed as part of a holistic and risk-based program with broad participation required (e.g., legal, information assurance, human resources, physical security, information technology, etc.) and sponsorship by executive leadership. Deloitte has developed a top ten list for leaders to consider as they design, build and implement a formal insider threat mitigation program. At a time when accountability is a primary leadership responsibility, an insider threat mitigation program can bolster deterrence and provide an early detection, prevention and response mechanism assuring the business, protecting employees, and safeguarding critical data, systems and facilities. This guidance was informed by the development of insider threat programs across a diverse range of organizations in the commercial and public sector.

Key considerations

1. **Define your insider threats** — Don't be surprised if your organization hasn't defined what an insider threat is. The reality is few organizations have a specific internal working definition as security and IT budgets have historically prioritized external threats. An insider can be an employee, a contractor, or a vendor that commits a malicious, complacent or ignorant act using their trusted and verified access. Defining the threats for your organization and specific business environment is a critical first step to formulating a program, which will inform the size, structure, scope, and phasing plan for the program, aligned to business risk priorities.

2. **Define your risk appetite** — Define the critical assets (e.g., facilities, source code, IP and R&D, customer information) that must be protected and the organization's tolerance for loss or damage in those areas. Identify key threats and vulnerabilities in your business and in the way you do business. Tailor the development of the program to address these specific needs, threat types and take into account your organization's unique culture.

3. **Leverage a broad set of stakeholders** — The program should have one owner but a broad set of invested stakeholders. Establish a cross-disciplinary insider threat working group that can serve as change agents and ensure the proper level of buy-in across departments and stakeholder (e.g., legal, physical security, policy, IT security, human resources, ethics, etc.). The working group's support will be critical to building the insider threat mitigation capability and securing data needed for the program. It should assist in addressing common concerns (e.g., privacy and legal) and support the development of messaging to executives, managers and the broader employee population.

4. **Technology, alone, won't solve the problem** — The insider threat challenge is not a purely technical one, but rather a people-centric problem that requires a holistic and people-centric solution. Organizations should avoid the common pitfall of focusing on a technical solution as the silver bullet. An insider threat mitigation program should include key business processes (e.g., segregation of duties for critical functions), technical and non-technical controls (e.g., policies), organizational change management components, and security training programs needed to promote an environment of security awareness and deterrence.

As used in this document, "Deloitte" means Deloitte LLP and its subsidiaries. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Fishnet Security

EXHIBITOR

As the leading provider of information security solutions that combine technology, services, support and training – FishNet Security enables clients to manage risk, meet compliance requirements and reduce costs while maximizing security effectiveness and operational efficiency. We are committed to information security excellence and delivering quality solutions to thousands of clients worldwide.

Ramsey Self
6130 Sprint Pkwy, Suite 400
Overland Park, KS 66211
816.556.3520
Ramsey.self@fishnetsecurity.com
www.fishnetsecurity.com

Information Systems Security Association (ISSA), MN Chapter

SUPPORTING SPONSOR

The Information Systems Security Association (ISSA)® is a not-for-profit, international organization of information security professionals and practitioners. It provides educational forums, publications, and peer interaction opportunities that enhance the knowledge, skill, and professional growth of its members.

ISSA
MINNESOTA CHAPTER

Betty Burke
1000 Westgate Drive
Suite 252
St. Paul, MN 55114-1067
866.349.5818
president@mn.issa.org
www.mn.issa.org

InfraGard

SUPPORTING SPONSOR

InfraGard is a partnership between the FBI and the private sector. It is an association of persons who represent businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the U.S.

www.infragard.org

ISACA MN Chapter

SUPPORTING SPONSOR

With approximately 1000 members from over 100 organizations, the Minnesota chapter of ISACA provides a gateway to a global organization offering security, risk, control, and governance certifications. Additionally, ISACA offers a new security knowledge platform and professional program Cybersecurity Nexus (CSX).

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

JET

EXHIBITOR

More than 28% of corporate data exists only on mobile devices living outside your corporate firewall, creating unparalleled mobile-centric security issues. Your data has left the building. Employees are increasingly using their mobile devices in non-traditional settings, putting intellectual property at risk and possibly making you liable for data breaches. JET exists to help businesses with endpoint security, cloud security, device management, data protection and productivity tools for end users.

Robert X. Casserly
6110 Golden Hills Drive
Minneapolis, MN 55416
612.578.5104
bob@jetrev.com
www.jetrev.com

Kaspersky Lab

EXHIBITOR

Kaspersky Lab is one of the fastest growing IT security vendors in the world. Firmly positioned as one of the top four vendors of security solutions for endpoint users, today it is the world's largest privately held vendor of endpoint protection solutions.

Brent Graham
500 Unicorn Park
Woburn, MA 01801
339.234-8211
Brent.graham@kaspersky.com
www.kaspersky.com

KPMG

PRESENTING/TECHNOLOGY SPONSOR

Along with today's greater flow of information comes greater risk of unauthorized access, disclosure or misuse of that information. KPMG Information Protection and Business Resilience services can help organizations effectively manage and control corporate information assets against an evolving spectrum of threats and scenarios.

Dave Notch
90 South 7th Street
4200 Wells Fargo Center
Minneapolis, MN 55402
612.305.5194
dnotch@kpmg.com
www.kpmg.com

LogRhythm

SILVER EXHIBITOR

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

U.S. Headquarters
4780 Pearl East Circle
Boulder, CO 80301
303.413.8745
866.384.0713
info@logrhythm.com
www.logrhythm.com

Maslon Edelman Borman & Brand, LLP

PRESENTING SPONSOR
VIP RECEPTION SPONSOR
PANEL SPONSOR

Maslon Edelman Borman & Brand, LLP is a full-service commercial law firm in Minneapolis, MN, offering a depth of experience in the areas of Business & Securities, Litigation, and Financial Services. We are actively involved in the area of cyber security, helping clients navigate complex issues and respond to concerns as they arise. We author articles, present at conferences, and hold leadership positions within organizations focused on this area of practice - all of which enhance our service to clients.

Eran Kahana
90 South Seventh Street
3300 Wells Fargo Center
Minneapolis, MN 55401
612.672.8385
eran.kahana@maslon.com
www.maslon.com

Milestone Systems, Inc.

GOLD EXHIBITOR

Milestone Systems, the nation's fastest growing information security and infrastructure provider, focuses on securing enterprise networks, the lifeblood of business – from cyber-attacks and other modern threats that can put businesses at risk. Along with providing leading-edge hardware and software, Milestone helps organizations across the U.S. with support services including: certified training, consulting, managed services, security assessments, infrastructure architecture design, and 24x7x365 technical support.

U.S. Headquarters
120400 Whitewater Drive
Suite 100
Minneapolis, MN 55343
866.646.9211
info@milestonesystems.com
www.milestonesystems.com

NOBODY ELSE GIVES MINNESOTA BUSINESS SO MUCH ONLINE, OFFLINE, AND ON THE PODIUM.

WHAT ARE YOU WAITING FOR? CONTACT:

SARA FERDEN | ADVERTISING DIRECTOR
sara.ferden@tigeroak.com **o.** 612.548.3884

@mnbizmag

- » Nearly **900,000** decision makers are reached through *Minnesota Business* magazine's platform
- » **55,000** engaged business executives read *Minnesota Business* magazine every month
- » Over **7,900** page views are consumed through our digital edition every month
- » **7,900** business authorities receive our e-newsletter weekly
- » **96%** of readers are in a position to make purchasing decisions
- » **60%** of readers have made a purchase due to an ad in *Minnesota Business* magazine
- » **3,000** business professionals connect with us annually at our signature events

minnesota
BUSINESS
magazine

WHERE MINNESOTA BUSINESS
COMES TO FLOURISH.

Minnesota Business Magazine

SUPPORTING SPONSOR

Minnesota Business magazine, a Tiger Oak Media property, provides insight and information for growing companies across Minnesota through the power of print, digital offerings and signature events. Subscription and digital editions online at Minnesotabusiness.com.

Sara Ferden
900 S Third Street
Minneapolis, MN 55415
612.423.5627
Sara.ferden@tigeroak.com
www.minnesotabusiness.com

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.

Kathleen Marsh
400 South 4th Street
Suite 416
Minneapolis, MN 55415
952.230.4555
kmarsh@mhta.org
www.mhta.org

MN.IT Services

EXHIBITOR

MN.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.

Jenna Bergmann
658 Cedar St.
St. Paul, MN 55155
651.201.2277
MNIT.Recruitment@state.mn.us
www.mn.gov/oet

Palo Alto Networks

EXHIBITOR

Palo Alto Networks is leading a new era in cybersecurity by protecting thousands of enterprise, government, and service provider networks from cyber threats. Because of our deep expertise, commitment to innovation and game-changing security platform, thousands of customers have chosen us and we are the fastest growing security company in the market.

4401 Great America Parkway
Santa Clara, CA 95054
408.753.4000
866.320.4788
contact_sales@paloaltonetworks.com
www.paloaltonetworks.com

PwC LLP

EXHIBITOR

PwC US helps organizations and individuals create the value they're looking for. We're a member of the PwC network of firms in 157 countries with more than 184,000 people. We're committed to delivering quality in assurance, tax and advisory services. Tell us what matters to you and find out more by visiting us at www.pwc.com/US. Gain customized access to our insights by downloading our thought leadership app: PwC's 365™ Advancing business thinking every day.

Colee Schroeder
225 South Sixth Street
Suite 1400
Minneapolis, MN 55402
612.596.6000
colee.c.schroeder@us.pwc.com
www.mn.gov/oet

Robotics Alley

SUPPORTING SPONSOR

Robotics Alley is an initiative founded by ReconRobotics and the Minnesota High Tech Association meant to spur public-private partnerships in the business, research, and development of world-leading robotics and automation systems. Robotics Alley hosts an annual conference and exposition in Minnesota's Twin Cities, which is on pace to become one of the world's leading robotics conferences.

robotics alley
CONFERENCE & EXPO
Robotics Sensors Advanced Manufacturing

Doug Mroczkowski
2815 Wayzata Blvd.
Minneapolis, MN 55405
763.548.1313
Doug.Mroczkowski@eventshows.com
www.RoboticsAlley.org

Sec.MN

SUPPORTING SPONSOR

Sec.MN is a local security group that provides security-focused meetings, demonstrations and seminars; as well as an online communications. Our members come primarily from the Twin Cities metropolitan area. Membership is always free to the general public, and is open to anyone interested in information security.

SecMN
Minnesota Security Professionals

Patrick Tatro
Patrick.Tatro@sec.mn
www.sec.mn

Security 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.

BSides MSP

info@bsidesmsp.org
www.bsidesmsp.org

SurfWatch Labs, Inc.

PASSPORT SPONSOR
SILVER EXHIBITOR

SurfWatch Labs delivers cyber risk intelligence solutions that help organizations understand the potential for cyber-attacks, determine the impact to their business and proactively address threats head on. SurfWatch automatically aggregates, standardizes and analyzes raw cyber data into risk intelligence that allows organizations to zero in on their unique cyber risk profile and ensure the most effective risk management in complete business context.

SURFWATCH
CYBER IN SIGHT

Sam Erdheim
45610 Woodland Road, #350
Sterling, VA 20166
866-855-5444
Sam.erdheim@surfwatchlabs.com
www.surfwatchlabs.com

UMSA

United in security leadership

UMSA is an alliance of security-related organizations. As a nonprofit founded in 2004, UMSA serves business, government and education professionals in the upper Midwest, collaborating with professional associations, educators and industry-leading companies to provide professional development opportunities that contribute to a stronger security foundation for organizations. UMSA is the proud host of the premier Secure360 Conference conducted every year in Saint Paul, Minnesota. Our member and affiliate organizations include:

- Advance IT Minnesota
- ASIS Minnesota
- Business Continuity Planners Association
- Cloud Security Alliance
- Information Systems Security Association
- InfraGard Minnesota
- MN ISACA
- SecMN (formerly NAISG)
- Open Web Application Security Project

Our mission is to unite upper Midwest security-related organizations in a trusted community for interdisciplinary collaboration and education. For more information, please contact **president@umsa-security.org**.

Save the Date! Celebrating a Decade of Guiding Security Professionals

Join us **May 12-13, 2015** for the **10th Annual Secure360 Conference** at the RiverCentre in Saint Paul, Minnesota. More than 80 education breakout sessions and the chance to network with over 1,000 attendees and 70+ exhibitors. Call for presentations is now open. For more information, visit: **www.Secure360.org**.

www.UMSA-Security.org

twitter.com/UMSAorg

facebook.com/UMSAorg

BSides MSP

Engaged, Happy Hackers, Protecting Planet Earth!

Attend the Security B-Sides MSP "Hacker Showcase" from 5-8 p.m. on Day 1 of the Summit.

To learn more about Security B-Sides MSP, go to **bsidesmsp.org**.

Symantec Corporation

TITLE 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.

Symantec.™

Worldwide Headquarters
350 Ellis Street
Mountain View, CA 94043
650.527.8000
www.symantec.com

Tanium

PREMIER SPONSOR

Tanium is a systems and security management company that gives enterprises the unique power to control, manage, and secure hundreds of thousands of endpoints within seconds. Serving as the 'central nervous system" for enterprises, Tanium prevents downtime and attacks that can cripple organizations and lead to costly business interruptions.

TANIUM™

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

Technological Leadership Institute (TLI), University of Minnesota

PRESENTING SPONSOR

The Technological Leadership Institute (TLI) is an interdisciplinary center at the University of Minnesota. TLI offers three Master of Science programs tailored to empower executives and leaders in their strategic vision to leverage technology to drive business development. These include the MS in Management of Technology, MS in Medical Device Innovation, and MS in Security Technologies. TLI's mission is develop local and global leaders for technology enterprises.

TECHNOLOGICAL
LEADERSHIP INSTITUTE
UNIVERSITY OF MINNESOTA
Driven to Discover℠

Jenna Egan
200 Oak Street S.E., Suite 290
Minneapolis, MN 55455
612.624.4380
egan0056@umn.edu
www.tli.umn.edu

UMSA/Secure 360

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 Conference held in May each year.

UMSA
United in security leadership

Patrick Tatro
St. Paul, Minnesota
president@umsa-security.org
www.umsa-security.org
www.secure360.org

Unisys

OFFICIAL SUMMIT PRINTER

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.

UNISYS

Scott Johnson
Stealth Portfolio Management by Unisys
404.931.1028
Scott.Johnson@unisys.com
www.unisys.com

Xcel Energy

PREMIER SPONSOR

Xcel Energy is a major U.S. electric and natural gas company with regulated operations in eight Western and Midwestern states. Based in Minneapolis, Minn., Xcel Energy provides a comprehensive portfolio of energy-related products and services to approximately 3.5 million electricity customers and 1.9 million natural gas customers through four operating companies.

Xcel Energy®

Doug DeGrote
414 Nicollet Mall, 7th Floor
Minneapolis, MN 55401
612.330.7614
Douglas.E.DeGrote@xcelenergy.com
www.xcelenergy.com

Additional Exhibitor as of 9/25/2014

Metropolitan State University

EXHIBITOR

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

13th St & Harmon Place
Minneapolis, MN 55403
612.659.7250
www.metrostate.edu

THE RISE OF CREDIT CARD DATA BREACHES: THE THIEVES AMONG US

If it can happen to Target, it can happen to your business: tech-savvy thieves hack into a supposedly secure company computer system, steal identity and credit card data, and leave the company to clean up (and pay for) the mess. The December 2013 Target breach by "an amorphous group of Eastern European hackers"[1] compromised personal information of as many as 100 million people and cost the company $148 million in related costs to date.[2]

Even if your business is smaller than Target, the costs of data breaches are significant. The average cost to a business in 2013 was $5.4 million.[3] The largest costs from these crises come from customer notification, governmental fines, legal and public relations costs, and lost business.

No company that relies on electronic networks to do business is immune to the threat of a data breach, regardless of whether it operates a transactional website or merely accepts credit card payments. Worse, in most cases you won't find out there is a problem until it's too late. First notice of a data breach may come from your credit card processing company, informing you that your business has been identified as a likely source of fraudulent credit card activity.

You then may be required to retain a computer forensic investigator to confirm whether a theft occurred. The incident could be anything from onsite theft by an employee to hacking of your wireless network or electronic intrusion into your computer network by a hacker nearby or abroad.

If a theft occurred, the credit card entity may demand that your business reimburse it for a share of the fraudulent activity that resulted from the theft. You will not obtain much by way of due process, but rather will most likely be told what sum your credit card processor will withhold from the payments that were otherwise due.

You can also forget about successfully keeping the situation under wraps and handling it internally. The laws of most states (including Minnesota) require you to notify the affected customers of the loss of their credit card data. After that, the banks that issued the affected credit cards may sue you; the Federal Trade Commission may investigate you; and the customers whose data was compromised may file a class-action lawsuit. At a minimum, you can expect the news of the theft to adversely affect your standing with customers. Target reported that its 2014 Q2 earnings were down 46% from the year prior—gently acknowledging that "[r]esults softened meaningfully following our December announcement of a data breach."[4]

What can you do to avoid such liability and lost business? First, you should attempt to comply with Payment Card Industry ("PCI") standards, which aim to reduce the risk of loss in the first place and to favorably affect the calculation the credit card entity uses to determine what share of the fraudulent activity you are required to pay.

Next, you should make sure that your business insurance package covers such losses. Unfortunately, you can't assume that your standard policies do the trick. Since data breach losses may take the form of fines and third-party liability to consumers, it is likely that neither your standard commercial general liability policy, nor the computer fraud portion of your property insurance policy, will cover such losses. Or, if your policy does provide such coverage, it probably has sublimits that are paltry compared to the fines or other damages your company can face in such circumstances.

A safer bet is purchasing a separate Cyber Liability or Network Risk policy specifically designed to cover both a direct financial loss due to theft by hacking, as well as any third-party liability for a data breach, including defense costs and the costs of the data breach investigation. Look for a policy that includes Crisis Management/Identity Theft Expenses coverage for such costs as notification, credit monitoring, and public relations expenses resulting from a data breach. Work with your insurance broker to make sure that the policy covers liability for fines and contains limits of liability ample enough to cover a significant data breach. While Target had cyber insurance before its breach,[5] it recently reported that only $38 million of the $148 million (and counting) breach-related costs are offset by its policies.[6]

The expense for a separate Network Risk policy may also be worthwhile—many shrewd contractors and customers are refusing to do business with firms that do not carry the specialized insurance required to cover the effects of data breaches. It is also possible that a data breach can arise from the negligent installation of software by a computer consultant or vendor. And while you may be able to recover some of your losses through legal action, most vendor contracts contain provisions limiting the vendor's liability for a data breach that prevent you from holding them responsible. Nonetheless, if you experienced a breach or are facing a substantial loss, it will probably be worth your while to have a lawyer help you take the necessary steps to mitigate your risk.

Data breaches are so common these days that it is prudent to think of them in the context of "when," not "if" they will occur. The thieves involved in a data breach are seldom caught, but the affected businesses rarely escape scot-free. The only questions will then be, how much are you liable for, how you will reduce your exposure, and who will bear that cost?

By Margo Brownell, Mike McCarthy, & Joe Ceronsky
Maslon Edelman Borman & Brand, LLP

Margo Brownell focuses her practice on insurance coverage counseling and litigation, and has extensive experience representing policyholders in complex insurance disputes.

margo.brownell@maslon.com

Mike McCarthy represents business entities and individuals in appellate and complex business litigation (principally class actions) in areas such as consumer and securities fraud, fiduciary breach, antitrust, and environmental contamination.

mike.mccarthy@maslon.com

Joe Ceronsky practices in the area of general commercial litigation with a focus on insurance litigation and product liability.

joseph.ceronsky@maslon.com

[1] http://www.nytimes.com/2014/01/18/business/a-sneaky-path-into-target-customers-wallets.

[2] http://www.nytimes.com/2014/08/06/business/target-puts-data-breach-costs-at-148-million.html html?action=click&contentCollection=Business%20Day&module=RelatedCoverage&region=Marginalia&pgtype=article

[3] http://www.symantec.com/content/en/us/about/media/pdfs/b-cost-of-a-data-breach-us-report-2013.en-us.pdf

[4] http://investors.target.com phoenixzhtml?c=65828&p=irol-newsArticle&ID=1903678&highlight=

[5] http://www.businessinsurance.com/article/20140119/NEWS07/301199973#

[6] http://www.nytimes.com/2014/08/06/business/target-puts-data-breach-costs-at-148-million.html

Protecting the Future

Douglas DeGrote is Xcel Energy's chief information security officer and director of IT Security & Risk Management. His responsibilities for the major U.S. electricity and natural gas utility include leading, developing and delivering IT security, disaster recovery and business continuity strategies. DeGrote and his team work with both internal and external experts, as well as government entities, to identify, assess, respond to and defend against ever evolving cyber threats to ensure energy grid reliability and resiliency.

Electricity will play a much greater role in global society in the coming years. In the face of numerous public pressures – environmental protection, regulatory requirements, renewable energy, "smart" grids – the cyber security landscape is also changing. Protecting critical infrastructure is becoming much more complex, as are threats to its security. Utility companies like Xcel Energy now face a constant quest to maintain the right level of critical infrastructure protection. The following issues shed some light on why today's cyber security efforts have become more complex:

Vendor Management – Is it the new risk management?

As companies expand the use of third parties to provide specialized products and services, the landscape of our security and risk management needs to expand as well. It's hard not to notice all the recent breaches, and the way third party providers have been targeted as vehicles to hack into the larger companies.

Vendor Management used to be about identifying and decreasing the potential business uncertainties and legal liabilities. This approach is no longer good enough. Today, we need to account for the complete risk of using third parties by creating a risk-based vendor management program. One that encompasses identification, reduction and management of the risk inherited as a result of the hiring, use and termination of these providers. This won't be your average "one time" validation of their security, but rather a program that manages security and data risk continuously throughout the complete lifecycle of relationship.

Distributed Generation – Expanding infrastructure to the customer

In the past, customers never had the ability to generate their own energy and sell what they didn't need back to the utility company. Consumer energy generation devices, such as solar panels, have made this practice, known as distributed generation, a reality. The resale of self-generated power is quickly growing in acceptance.

Although distributed generation has lots of benefits, it also means utility companies will need to expand their security programs to encompass protecting a quickly expanding "smart" critical infrastructure. The amount and complexity of security efforts and technology will need to be expanded to a degree that has never been seen before. End consumer infrastructure will quickly become a new target for critical infrastructure breach attempts.

Companies now need to secure two-way communications between centralized company infrastructure and consumer energy generation devices, while also protecting the energy usage information as if it were private data. Both prevention and detection capabilities will be necessary on a very wide scale to ensure the risk is maintained at a level acceptable to support the resiliency and reliability of the electric grid.

The Growing Complexity of Attacks – Partnering physical and cyber security

There have been multiple reports in recent years of criminals shooting at electric substations after cutting communications to the site, giving them more time to cause damage. It's true that physically attacking critical infrastructure equipment and locations could cause damage and affect the flow of electricity. Hacking into a control system would also produce the same result. However, in both cases there are redundancies and processes that will quickly route around the problem resulting in very little disruption.

The bigger risk we face today is the orchestration of a multi-faceted attack affecting both the control network and physical infrastructure, which could indeed cause a more serious situation that takes longer to remediate.

This is why today's utility operators need to form a partnership between their physical and cyber security. The ability to protect on all layers of threat, and work together to identify and remediate them, is imperative to ensuring the security and reliability of critical infrastructure.

SHARE OUR PRIDE

in

BEING PART

of something

GREAT

Xcel Energy is proud to be part of the 2014 Cyber Security Summit, working with industry leaders to discuss cyber security threats and collaborate on solutions. Together, we can protect this critical space and make our community a better place to live and do business.

xcelenergy.com

Xcel Energy®

RESPONSIBLE BY NATURE®

Friends,

Thanks for joining us again at this year’s Cyber Security Summit in Minnesota’s Twin Cities!

As your incoming Chairman for 2015, I am honored to have been asked to help communicate the global leadership of cyber security solutions, policy and providers from within America’s heartland. Addressing the increasing cyber challenges for companies, governments and individuals requires strong public-private partnerships for cooperation and communication. Because Minnesota is home to an extraordinary number of Fortune 500 companies (Minneapolis-St. Paul ranks first among the 30 largest metropolitan areas in the number of Fortune 500 companies per capita), we are uniquely situated to share the best practices and cyber security lessons learned among our sponsors, board members and attendees from around the nation and around the world.

In 2015, we will build upon the important cyber security leadership initiatives that have begun in the past five years. We will continue building the national scope of our conference with additional outreach to federal officials and corporate leaders from around the country. We will seek expert updates on the President’s cyber security and critical infrastructure protection initiatives. We will also explore the potential for success of cyber security legislation efforts on Capitol Hill in Washington.

We recognize that any security solutions to the challenges of crime, fraud and other risks in cyberspace will require public-private partnerships and collaborative approaches. As Minnesota Secretary of State Mark Ritchie has said ‘Cyber security is an extremely important topic everywhere, but Minnesota in particular has taken a lead role in this area because of the many global companies located in the state. These companies face this stuff on a daily basis, and the Summit provides a chance for them, along with government and security professionals, to collaborate on ways to address the growing problem.”

I know I speak for the Board of Advisors and all of our sponsors when I say thank you for your time, input and participation this past year. We all look forward to an increasingly national and international impact in 2015!

Sincerely,

Andrew Borene

Andrew Borene, Esq.
2015 Cyber Security Summit Chair

For information on applying to join our team of Advisors to get involved in the leadership and growth of our initiative, please contact: Eileen Manning, Executive Producer
eileen.manning@eventshows.com

OUR 2015 ADVISORY BOARD IS TAKING SHAPE...

Dr. Massoud Amin, D.Sc.
Director, Technological Leadership Institute, University of Minnesota

Ken M. Barnhart
CEO, Occam Group, Ltd

Andrew Borene, Esq.
Summit Chair; Attorney, Steptoe & Johnson LLP; Adjunct Professor, American University

Jarret Brachman
VP, Threat Intelligence Manager, Wells Fargo

Christopher Buse, CISA, CISSP
Assistant Commissioner and Chief Information Security Officer, MN.IT Services

Doug DeGrote
CISO & Director of IT Security & Risk Management, Xcel Energy

Laura Elan, P.E.
Global Service Leader - eHealth, UL LLC

Steen J. Fjalstad, MS, CISA, CISSP, CGEIT, CRISC
Security and Mitigation, Principal & Chief Administration Officer, Midwest Reliability Organization

Ron Fresquez
CEO/Founder, TOSTA Information Security Training Services

Matthew Harmon, CISSP, GSEC, GCIH, GCIA
Owner and Security Researcher, IT Risk Limited

Col. Stefanie Horvath, MSS
Colonel, MN Army National Guard

Brian Isle, PE
Senior Fellow, Adventium Labs/University of Minnesota Technological Leadership Institute

Mike Johnson, MSST, CISM
CISO/Operations Risk Director, Bremer Financial Services

Chip Laingen
Commander, U.S. Navy (Ret.); *Executive Director*, Defense Alliance

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

Jerrod Montoya, Esq.
Security & Compliance Attorney, OATI; *Vice President*, InfraGard Minnesota Members Alliance

Kathleen Moriarty
Global Lead Security Architect, Corporate Office of the Chief Technology Officer, EMC Corporation

Dave Notch
Director, Information Protection and Business Resilience, KPMG

James Ryan, CSyp, CEA, PMP
Chief Strategy Officer, Cyber Security Summit; *Owner & Founder*, Litmus Logic

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

Phil Schenkenberg, J.D.
Attorney, Director, and Shareholder Business Litigation, Briggs and Morgan, P.A.

SAVE THE DATE

CYBER SECURITY SUMMIT

OCTOBER 20-21, 2015

www.CyberSecuritySummit.org