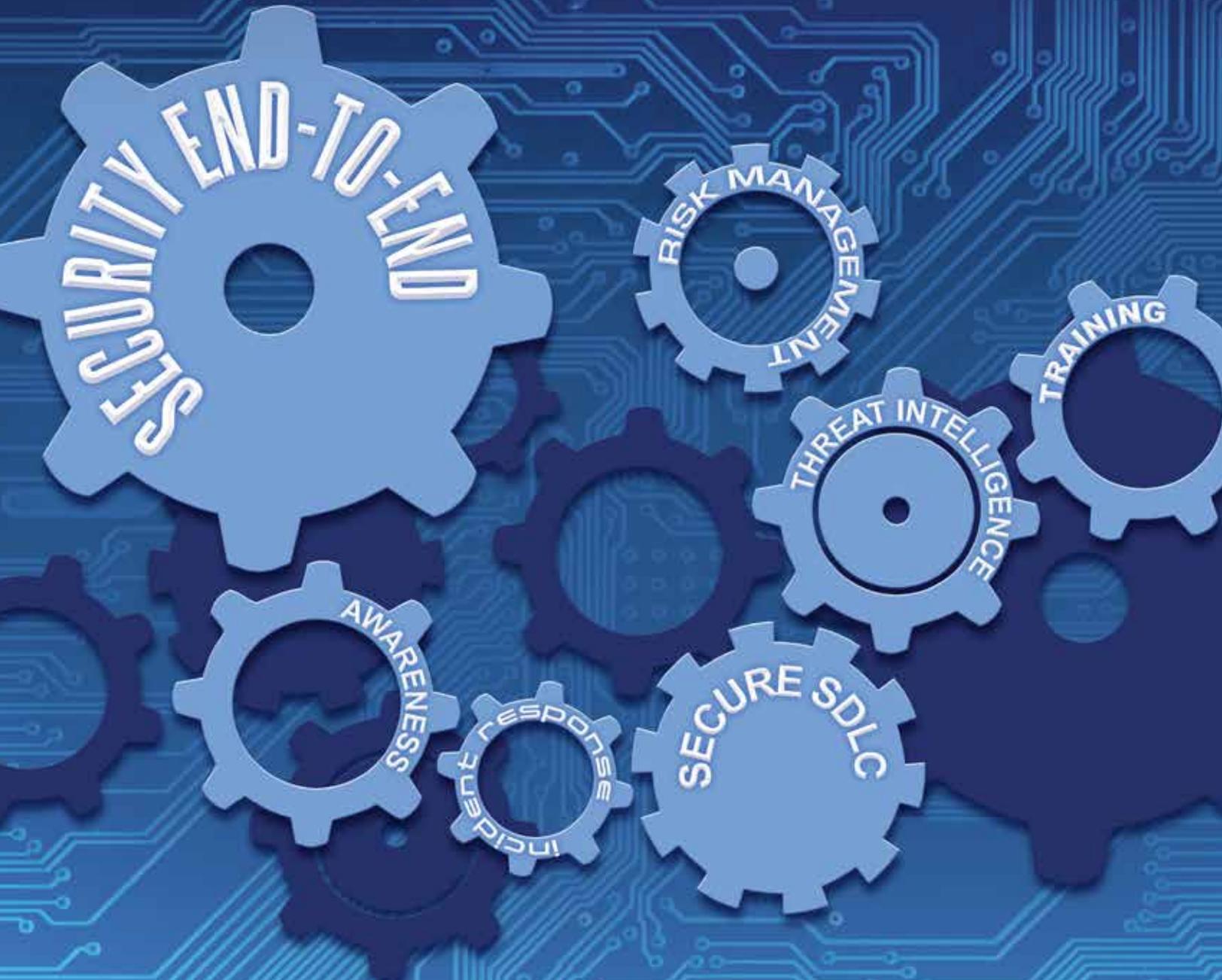


New York State
Cyber Security Conference

June 2-3, 2015



www.its.ny.gov/eiso/conference/2015

TERABYTE SPONSOR



at&t

PRESENTED BY



Office of Information
Technology Services



The NYS Forum, Inc.



UNIVERSITY
AT ALBANY

State University of New York

WWW.ITS.NY.GOV

WWW.NYSFORUM.ORG

WWW.ALBANY.EDU/IASYMPIUM

Agenda Day 1 - June 2, 2015

Conference Hours		Security Strategies					Legal Issues					Incident Response					Encryption					Risk Management					ASIA				
8:00am - 4:15pm		Securing Your Company for Today's Cyber War: A Three-Pronged Approach to a Comprehensive IT Security Strategy					Bulletproofing Your Incident Response Plan: Effective Tabletops					What would you say, ya do here? Tactical steps to perform tomorrow to meaningfully increase security					Encryption and Data Security: A Conundrum?					The Intersection of Security and Privacy					Behavioral Security				
8:00am - 9:00am		Peter Allor IBM Security					Reg Harnish GreyCastle Security					Tyler Wrightson Leet Systems					Dan Srebnick DynTek Services					Srinj Subramanian and Robert Glaser Deloitte & Touche LLP					Chair: Damira Pon, University at Albany, SUNY				
9:00am - 10:30am		Meeting Room 5					Meeting Room 4					Meeting Room 6					Meeting Room 3					Meeting Room 2					Paper: Experience Matters: The Role of Direct and Vicarious Experience in Secure Actions and Leigh A. Mutchler, University of Tennessee and Merrill Warkentin, Mississippi State University				
10:30am - 11:00am		Meeting Room 5					Meeting Room 4					Meeting Room 6					Meeting Room 3					Meeting Room 2					Paper: Two Studies on Password Memorability and Perception Delbert Hart, SUNY Plattsburgh				
11:00am - 11:50am		Meeting Room 5					Meeting Room 4					Meeting Room 6					Meeting Room 3					Meeting Room 2					Paper: A Holistic Approach for Service Migration Decision, Strategy and Scheduling Yanjun Zuo, University of North Dakota				
1:00pm - 1:50pm		Meeting Room 5					Meeting Room 4					Meeting Room 6					Meeting Room 3					Meeting Room 2					Paper: Post-audit of Service Security Investment: Using Simulation Approach Hemantha Herath and Tejaswini Herath, Brock University				
1:50pm - 2:10pm		Meeting Room 5					Meeting Room 4					Meeting Room 6					Meeting Room 3					Meeting Room 2					Paper: A Covert Channel in the Worldwide Public Switched Telephone Network Dial Plan Bryan Harmat, Jared Stroud and Daryl Johnson, Rochester Institute of Technology				
2:10pm - 3:00pm		Meeting Room 5					Meeting Room 4					Meeting Room 6					Meeting Room 3					Meeting Room 2					Paper: Crowdsourcing Computer Security Attack Trees Matt Tentilucci, Nick Roberts, Penn State University, Shreshth Kandari, Daryl Johnson, Dan Bogaard, Bill Stackpole; Rochester Institute of Technology and George Markowsky, University of Maine				
3:00pm - 3:20pm		Meeting Room 5					Meeting Room 4					Meeting Room 6					Meeting Room 3					Meeting Room 2					Paper: International Security Cooperation & Cyber Warfare Chair: Sanjay Goel, University at Albany, SUNY				
3:20pm - 4:15pm		Meeting Room 5					Meeting Room 4					Meeting Room 6					Meeting Room 3					Meeting Room 2					Paper: International Cooperation to Enhance Website Security Mamohan Chaturvedi and Srishti Gupta, Indian Institute of Technology				
		Meeting Room 5					Meeting Room 4					Meeting Room 6					Meeting Room 3					Meeting Room 2					Paper: Sharing Cyber Threat Information: Swimming in Data but Starving for Information Sanjay Goel, University at Albany, SUNY and Charles Barry, National Defense University				
		What Your Employees Don't Know, Can Hurt You: Creating the Vigilant Employee in the Cybersecurity War					Data Governance in the Era of the Data Breach					Advanced Persistent Threats - What You Need to Know					Application Security Testing - How to find software vulnerabilities before you ship code or procure code					Cyber Security: From Cost Centre to Revenue Driver					Cyber Attacks Chair: Victoria Kisseka, University at Buffalo, SUNY				
		Dane Boyd Dell Secure Works					Ron Raether Fanuki Ireland & Cox P.L.L.					Terry Hect AT&T					Hassan Radwan Anita D'Amico Secure Decisions					Igor Volovich Schneider Electric					Paper: Crowdsourcing Computer Security Attack Trees Matt Tentilucci, Nick Roberts, Penn State University, Shreshth Kandari, Daryl Johnson, Dan Bogaard, Bill Stackpole; Rochester Institute of Technology and George Markowsky, University of Maine				
		Cyber Security's Weakest Link: YOU					Government Use of Social Media - The Legal Issues					Pitfalls and Potholes of the Dark Net					We DevOps'd - Experience and Lessons Learned Securing the SDLC					"That Will Never Happen To Us": Five Ways to Make Security Risks Relevant to Your Organization					International Security Cooperation & Cyber Warfare Chair: Sanjay Goel, University at Albany, SUNY				
		Michael McCutcheon Rational Enterprise					David Menken Smith Buss & Jacobs LLP					Leonard Popyack Utica College and Anthony Martino Northeast Cyber Forensics Center					Dr. Sherly Abraham Excelsior College and Dr. Din Cox Medical Science and Computing LLC.					Todd Brasel and Vincent Hannon NYSETEC					Paper: International Cooperation to Enhance Website Security Mamohan Chaturvedi and Srishti Gupta, Indian Institute of Technology				
		Cyber Security's Weakest Link: YOU					Government Use of Social Media - The Legal Issues					Pitfalls and Potholes of the Dark Net					We DevOps'd - Experience and Lessons Learned Securing the SDLC					"That Will Never Happen To Us": Five Ways to Make Security Risks Relevant to Your Organization					Paper: Sharing Cyber Threat Information: Swimming in Data but Starving for Information Sanjay Goel, University at Albany, SUNY and Charles Barry, National Defense University				
		Michael McCutcheon Rational Enterprise					David Menken Smith Buss & Jacobs LLP					Leonard Popyack Utica College and Anthony Martino Northeast Cyber Forensics Center					Dr. Sherly Abraham Excelsior College and Dr. Din Cox Medical Science and Computing LLC.					Todd Brasel and Vincent Hannon NYSETEC					Paper: International Cooperation to Enhance Website Security Mamohan Chaturvedi and Srishti Gupta, Indian Institute of Technology				
		Cyber Security's Weakest Link: YOU					Government Use of Social Media - The Legal Issues					Pitfalls and Potholes of the Dark Net					We DevOps'd - Experience and Lessons Learned Securing the SDLC					"That Will Never Happen To Us": Five Ways to Make Security Risks Relevant to Your Organization					Paper: Sharing Cyber Threat Information: Swimming in Data but Starving for Information Sanjay Goel, University at Albany, SUNY and Charles Barry, National Defense University				
		Michael McCutcheon Rational Enterprise					David Menken Smith Buss & Jacobs LLP					Leonard Popyack Utica College and Anthony Martino Northeast Cyber Forensics Center					Dr. Sherly Abraham Excelsior College and Dr. Din Cox Medical Science and Computing LLC.					Todd Brasel and Vincent Hannon NYSETEC					Paper: International Cooperation to Enhance Website Security Mamohan Chaturvedi and Srishti Gupta, Indian Institute of Technology				

Conference Hours		Opening of the Exhibit Hall														
8:00am - 3:45pm		Convention Hall														
8:30am - 10:00am		Visit the Exhibitors (Terabyte Sponsor Demo: AT&T 10:05am-10:25am)														
10:00am - 10:30am		Forensics		Threat Landscape		Mobile/BYOD		Invasion of Technology		Cyber Potluck		ASIA				
10:30am - 11:20am	Tales from the Crypt: Fighting Ransomware	James Antonakos National Cybersecurity Institute	The Promises and Pitfalls of Public-Private Sector Cooperation in Cybersecurity	Austen Givens Utica College	The Truth about Cybersecurity: A real-world look into the current threat landscape and the business & financial impact of targeted cyber attacks	Nick Bennett Mandiant, A Fire Eye Company	Planning Mobile?! Eric Green Mobile Active Defense and Larry Whiteside, Jr. Lower Colorado River Authority	Biometrics: Who Are You? Stephanie Schuckers Clarkson University	Ahead of the Curve: Better Cyber Security through Tech Transfer Partnerships Doug Maughan Department of Homeland Security	Paper: Shot Segmentation and Compliance Andrew Pulver, <i>University at Albany, SUNY</i> , Ming-Ching Chang, <i>GE Global Research</i> and Siwei Lyu, <i>University at Albany, SUNY</i>	Meeting Room 1	Meeting Room 2	Meeting Room 3	Meeting Room 4	Meeting Room 5	Meeting Room 7
11:20am - 11:40am	Are you Tired of Hearing that the Sky is Falling when we Talk About Information Security?	Tom Brennan Proactive RISK	Information Sharing in Multi-agency Disaster and Crisis Response: Smithfield tornado disaster and DeRuyter shooter man-made crisis events discussed	Joe Treglia Syracuse University	After the Recently Publicized Events, What's Next? Michael Corby CGI Solutions and Technologies, Inc.	BYOD - Its not so hard! Kevin Wilkins iSecure LLC	The Day After Passwords Die - How Biometrics Will Usher in a New Age of Technoorepiness Thomas Keenan University of Calgary	What Makes a Good Cyber Security Policy? George Duchak Air Force Research Lab	Cloud Computing and Internet of Things Chair: Yuan Hong, <i>University at Albany, SUNY</i> Paper: Secure Audio Reverberation over Cloud Abukari Mohammed Yakubu, <i>University of Winnipeg</i> , Namunu C. Maddage, <i>University of Melbourne</i> , and Pradeep K. Atrey, <i>University at Albany, SUNY</i> Paper: Using Features of Cloud Computing to Defend Smart Grid against DDoS Attacks Anthony Califano, Ersin Dincelli, and Sanjay Goel, <i>University at Albany, SUNY</i>	Meeting Room 1	Meeting Room 2	Meeting Room 3	Meeting Room 4	Meeting Room 5	Meeting Room 7	
11:40am - 12:30pm	Lunch on your own and Visit the Exhibitors															
12:30pm - 1:40pm	The Critical Role of Netflow/PPFIX Telemetry in the Next-Generation Network Security Infrastructure	Ken Kaminski Cisco Systems	ICT Supply Chain Risk in 2015: Can the Private Sector be Engaged? Michael Aisenberg MITRE Corp	Reporting on the Current Risk landscape-The Verizon Data Breach Investigative Report Chris Novak Verizon Enterprise Solutions	Compliance Cyber Security Threats, Trends and Best Practices to Secure Your Government Organization Tim Finn and Ron Smalley First Data	From the Hobbyist's Garage to Threat From Above - Defending Against Drones George Palmer Stuart Card AX Enterprize, LLC	Cooperating in Cyber Defense: Learning Together and Sharing Knowledge NYS Forum Panel	Disasters and Incident Response Chair: Pradeep Atrey, <i>University at Albany, SUNY</i> Paper: Trust Management in Resource Constraint Networks Thomas Babbitt and Boleslaw Szymanski, <i>Rensselaer Polytechnic Institute</i> Paper: The Causal Relationships of IS Effectiveness After an Extreme Event Victoria Kisekka, Raj Sharman, H.R. Rao, Shambhu Upadhyaya, <i>University at Buffalo</i> , and Nicole Gerber, <i>Roswell Park Cancer Research Center</i>	Meeting Room 1	Meeting Room 2	Meeting Room 4	Meeting Room 3	Meeting Room 6	Meeting Room 5	Meeting Room 7	
1:40pm - 2:30pm	Next-Generation Endpoint Security: Protection, Detection and Response	Jesse Torzs Bit9	Mind the Gap: Evolving Information Sharing, Protecting U.S. Critical Infrastructure Against Growing Cyber Threats John Cassidy CenturyLink Government	The Explosion of Cybercrime - The 5 Ways IT May Be an Accomplice Mark Villinski Kaspersky Lab	Strong Medicine for HIPAA Compliance Paul Romeo GreyCastle Security	Is your Privacy Being Miced? Raj Goel Brainlink	Establishing a Prototype to Enable Usage-based Cyber Liability Insurance Steve Hamby Independent Consultant	Network Security Chair: George Berg, <i>University at Albany, SUNY</i> Paper: A Layer 2 Protocol Design to Protect the IP Communication in a Wired Ethernet Network Reiner Campillo and Tae Oh, <i>Rochester Institute of Technology</i> Paper: Proposed Terminal Device for End-to-End Secure SMS in Cellular Networks Gaurav Balawar, Neetesh Saxena, and Narendra S Chaudhari, <i>Indian Institute of Technology Indore</i>	Meeting Room 1	Meeting Room 2	Meeting Room 6	Meeting Room 3	Meeting Room 4	Meeting Room 5	Meeting Room 7	
2:30pm - 2:50pm	Visit the Exhibitors															
2:50pm - 3:45pm	Next-Generation Endpoint Security: Protection, Detection and Response	Jesse Torzs Bit9	Mind the Gap: Evolving Information Sharing, Protecting U.S. Critical Infrastructure Against Growing Cyber Threats John Cassidy CenturyLink Government	The Explosion of Cybercrime - The 5 Ways IT May Be an Accomplice Mark Villinski Kaspersky Lab	Strong Medicine for HIPAA Compliance Paul Romeo GreyCastle Security	Is your Privacy Being Miced? Raj Goel Brainlink	Establishing a Prototype to Enable Usage-based Cyber Liability Insurance Steve Hamby Independent Consultant	Network Security Chair: George Berg, <i>University at Albany, SUNY</i> Paper: A Layer 2 Protocol Design to Protect the IP Communication in a Wired Ethernet Network Reiner Campillo and Tae Oh, <i>Rochester Institute of Technology</i> Paper: Proposed Terminal Device for End-to-End Secure SMS in Cellular Networks Gaurav Balawar, Neetesh Saxena, and Narendra S Chaudhari, <i>Indian Institute of Technology Indore</i>	Meeting Room 1	Meeting Room 2	Meeting Room 6	Meeting Room 3	Meeting Room 4	Meeting Room 5	Meeting Room 7	

4 | Welcome

June 2, 2015

Dear Colleague:

On behalf of the New York State Office of Information Technology Services, the University at Albany, State University of New York and the NYS Forum, Inc., we welcome you to the 18th Annual New York State Cyber Security Conference.

This year's Conference theme, Security End-to-End, focuses on the need to provide a comprehensive approach to security, encompassing people, process, and technology. With over 50 dynamic breakout sessions to choose from, the Conference brings you the latest information on information security trends and solutions. Industry experts will speak on such topics as risk management, security strategies, the threat landscape, cyber legal issues, forensics, and incident response, and more.

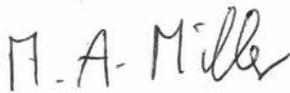
We are pleased to welcome Jane Holl Lute as this morning's keynote. Ms. Lute is the CEO of the Center for Internet Security and former Deputy Secretary of the U.S. Department of Homeland Security. An internationally recognized security expert whose career has included serving as Assistant Secretary-General of the United Nations, Ms. Lute will present an engaging keynote that dispels the myth that cyberspace is the "Wild Wild West," but is instead an environment over which we can exert significant influence.

Top researchers in academia will present their papers on information security at the 10th Annual Symposium on Information Assurance (ASIA), concurrent with the Conference.

On Wednesday, the day will begin with ASIA's keynote Bruce McConnell, Senior Vice President of the EastWest Institute (EWI) and former Deputy Under Secretary for Cybersecurity of the U.S Department of Homeland Security. Mr. McConnell manages EWI's Cooperation in Cyberspace Initiative. He will speak about the roles of individuals, the larger community, and governments in cybersecurity and how we can move from a reactive mode to a more successful offensive mode. An Exhibit Hall featuring displays from our sponsors and exhibitors will also be available on site both Tuesday and Wednesday.

Thank you for your continued commitment to cyber security. Together we truly are making a difference. Enjoy the Conference!

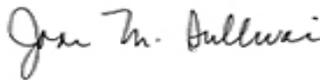
Sincerely,



Margaret Miller

NYS Chief Information Officer

NYS Office of Information Technology Services



Joan M. Sullivan

Executive Director

The NYS Forum, Inc.



Robert J. Jones

President

University at Albany

State University of New York



Margaret Miller **Chief Information Officer** **NYS Office of Information Technology Services**

Maggie Miller was appointed Chief Information Officer of the New York State Office of Information Technology Services by Governor Cuomo in December 2014. Maggie now oversees the agency's IT services to the State and government entities. This includes setting statewide technology policy for all state government agencies; and monitoring large technology expenditures in the State to find innovative ways technology can be leveraged to provide the best possible experience for the citizens of New York State. Maggie is an IT leader with more than 40 years' experience and an expert in IT strategy, innovation, business transformation, multi-channel strategies, business intelligence, and analytics.

With a proven record as an innovative, business technology leader, Maggie's public and private sector experiences makes her uniquely qualified to manage the State's IT services and help ensure state government is working for all New Yorkers.

Maggie was previously a Senior Vice President and Group Chief Information Officer at Warner Music Group, a major global record company, where she oversaw the optimization of the company's global IT systems and business processes for the digital media age.

Prior to her time at Warner Music Group, Maggie was the Chief Information Officer at a \$20 billion dollar retailer and previously for Dell Europe. She also has extensive experience as a CIO in the financial services and travel sectors.

Immediately before joining the State, Maggie was CIO for Girls Scouts USA, a Movement whose mission is to build girls of courage, confidence, and character who make the world a better place. During her time there, she was responsible for transforming the Movement-wide IT services and platforms to better support and improve the experience for nearly 3 million girl and adult members in 90 countries.

Joan M. Sullivan **Executive Director** **The NYS Forum, Inc.**

Ms. Sullivan has served as the Executive Director of the NYS Forum since November 2012 after serving over 37 years in New York State Government. Ms. Sullivan retired from government as the Executive Deputy Comptroller of Operations in the State Comptroller's Office. Appointed to that position in May 2007, she was responsible for the oversight of the Division of Payroll, Accounting, and Revenue Services and the Division of Contracts and Expenditures. Most notably during this tenure as Executive Deputy Comptroller, she oversaw the implementation of the Statewide Financial System (SFS) as well as the design and implementation of OpenBookNY, the Comptroller's premier transparency initiative.

From February 2004 through May 2007, Ms. Sullivan served as the Assistant Comptroller of the State Financial Services Group. She was responsible for managing five bureaus as well as the project to redesign the State's Central Accounting System (the predecessor to SFS) and the Vendor Responsibility initiative and system implementation (VendRep).

Ms. Sullivan joined the Comptroller's Office in January 2000 as Assistant Director of Contracts, and in September 2001 was appointed to Director of Contracts. Prior to joining OSC, she managed the Strategic Technology Assessment and Acquisition Team for the Office for Technology. Before this assignment, she spent 21 years with the former Department of Social Services, rising to the level of Director of the Office of Contract Management and later Director of Administration for the Human Services Application Service Center.

Robert J. Jones **President** **University at Albany, State University of New York**

Robert J. Jones, Ph.D. became the 19th president of the University at Albany in January 2013. He came to UAlbany following 34 years at the University of Minnesota, where he had most recently served as senior vice president for academic administration at the University of Minnesota System since 2004. Before that, Jones spent more than 15 years in key administrative leadership positions at the University of Minnesota-Twin Cities, including vice president and executive vice provost for faculty and academic programs, vice president for campus life and vice provost for faculty and academic personnel, interim vice president for student development and president of the University of Minnesota Outreach, Research and Education (UMore) Park Development, LLC.

A native of Dawson, Georgia, Jones earned a bachelor's degree in agronomy from Fort Valley State College, a master of science degree in crop physiology from the University of Georgia, and a doctorate in crop physiology from the University of Missouri, Columbia. After earning the Ph.D., he joined the University of Minnesota faculty as a professor of agronomy and plant genetics. He is an internationally recognized authority on plant physiology and has published numerous scientific papers, manuscripts and abstracts. His research focused on the role of cytokinins in stabilizing grain yields of maize against environmental stresses and global climate change. During his career, he has trained many students who have gone on to leading careers in higher education and the private and not-for-profit sectors. He is a fellow of both the American Society of Agronomy and the Crop Science Society of America.

From the outset of his career, Jones has worked to advance international education. He has been a visiting professor and featured speaker in North America, Europe, Asia and Africa. From 1984 to 1994, he served as an academic and scientific consultant for Archbishop Desmond Tutu's South African Education Program. In 2010, he was awarded a University of Minnesota endowed chair in urban and international development; he was also named a recipient of the Michael P. Malone International Leadership Award by the Association of Public and Land-Grant Universities (APLU).

Jones is nationally recognized for his work to advance university-community engagement, and at UAlbany, he is leading efforts to strengthen the University's community partnerships. He currently serves as Regional Council Co-Chair for the Capital Region Economic Development Council (CREDC) alongside Albany Medical Center President James J. Barba. In 2013, he was appointed a co-chair for Albany Mayor-elect Sheehan's transition committee. Other boards on which he serves include the Center for Economic Growth, Saratoga Performing Arts Center, Capitalize Albany and Albany Promise. At the national level, he serves on the boards of the Bush Foundation, the Coalition of Urban Serving Universities and the Scholars at Risk Network. He is a member of the Committee on Equal Opportunities in Science and Engineering, an advisory committee to the National Science Foundation.

Jones is a member of several SUNY and UAlbany-affiliated boards, including the University at Albany University Council, The University at Albany Foundation, the University at Albany Biotech Development Corporation, the University Auxiliary Services Corporation, Empire Commons Student Housing, Inc., Fuller Road Management Corporation, the University at Albany Alumni Association, RF Research Council and Rockefeller Institute.

Prior to his arrival at UAlbany, Jones held a gubernatorial appointment as a commissioner of the Midwestern Higher Education Compact and served on the board of directors for the Midwest Universities Consortium for International Activities. He was also a member of the Grammy award-winning Sounds of Blackness, a Twin Cities-based choral ensemble.

Jones and his spouse, Lynn Hassan Jones, M.D., have five children and two grandchildren

6 Keynote - Day 1

June 2, 2015

9:00 a.m. - 10:30 a.m.

Convention Hall



Jane Holl Lute **Chief Executive Officer** **Center for Internet Security**

Jane Holl Lute serves as Chief Executive Officer (CEO) of the Center for Internet Security (CIS), an international nonprofit organization focused on enhancing cybersecurity readiness and response for the public and private sectors. Ms. Lute most recently served as the President and Chief Executive Officer of the Council on CyberSecurity, an independent, expert organization dedicated to the security of an open Internet. Prior to joining CIS, Ms. Lute served as Deputy Secretary for the Department of Homeland Security (DHS). As the DHS chief operating officer, Ms. Lute was responsible for the day-to-day management of the Department's efforts to prevent terrorism and enhance security, secure and manage the nation's borders, administer and enforce U.S. immigration laws, strengthen national resilience in the face of disasters, and ensure the nation's cybersecurity.

From 2003-2009, Ms. Lute served as Assistant Secretary-General of the United Nations (UN) and established the Department of Field Support, responsible for comprehensive on-the-ground support to UN peace operations worldwide, including rapid-response efforts in support of development and humanitarian operations and crises. Ms. Lute also served as Assistant Secretary-General for Peacebuilding, responsible for coordinating efforts on behalf of the Secretary General to build sustainable peace in countries emerging from violent conflict.

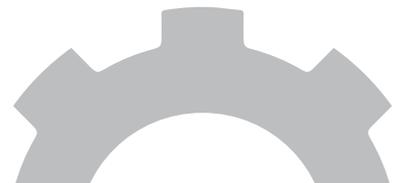
Prior to joining the UN, Ms. Lute was Executive Vice-President and Chief Operating Officer of the United Nations Foundation and the Better World Fund. From 1994-2000, she worked with David A. Hamburg, former president of the Carnegie Corporation of New York, and Cyrus Vance, former U.S. Secretary of State, on the Carnegie Commission on Preventing Deadly Conflict, a global initiative that pioneered the cause of conflict prevention.

Ms. Lute served on the National Security Council staff under both President George H.W. Bush and President William Jefferson Clinton and had a distinguished career in the United States Army, including service in the Gulf during Operation Desert Storm. She has a Ph.D. in political science from Stanford University and a J.D. from Georgetown University.

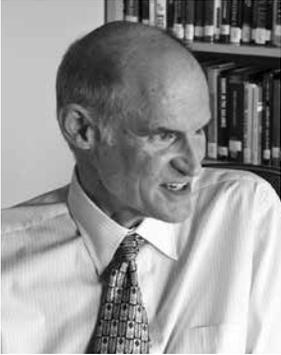
Presentation:

Cyber Security End-to-End: What Each of Us Can Do Now

Ms. Lute will present an engaging keynote that dispels the myth that cyberspace is the "Wild Wild West," but rather an environment over which we can exert significant influence. She will challenge the audience to see the powerful role each individual plays in our collective cybersecurity ecosystem, and to understand that improving cybersecurity is within our reach. Ms. Lute will discuss how the adoption of foundational cyber hygiene measures will result in immediate and measurable protections against the vast majority of cyber attacks and incidents.



June 3, 2015
8:30 a.m. - 10:00 a.m.
Convention Hall



Bruce McConnell
Senior Vice President
EastWest Institute

Bruce McConnell leads EWI's relationship-building with government and businesses around the world. He also manages the institute's Cooperation in Cyberspace Initiative.

Beginning in 2009, McConnell was a leader of the cybersecurity mission at the U.S. Department of Homeland Security. He became Deputy Under Secretary for Cybersecurity in 2013, and responsible for ensuring the cybersecurity of all federal civilian agencies and for helping the owners and operators of the most critical U.S. infrastructure protect themselves from growing cyber threats. During his tenure, McConnell was instrumental in building the national and international credibility of DHS as a trustworthy partner that relies on transparency and collaboration to protect privacy and enhance security.

Before DHS, McConnell served on the Obama-Biden Presidential Transition Team, working on open government and technology issues. From 2000-2008 he created, built, and sold McConnell International and Government Futures, consultancies that provided strategic and tactical advice to clients in technology, business and government markets. From 2005-2008, he served on the Commission on Cybersecurity for the 44th Presidency.

From 1999-2000, McConnell was Director of the International Y2K Cooperation Center, sponsored by the United Nations and the World Bank, where he coordinated regional and global preparations of governments and critical private sector organizations to successfully defeat the Y2K bug. McConnell was Chief of Information Policy and Technology in the U.S. Office of Management and Budget from 1993-1999.

McConnell is also a senior advisor at the Center for Strategic and International Studies. He received a Master of Public Administration from the Evans School for Public Policy at the University of Washington, where he maintains a faculty affiliation, and a Bachelor of Sciences from Stanford University.

Presentation:

Whose Job is it to Solve the Cyber Security Problem?

Most organizations believe that in cyberspace, offense wins, and that cyber defenders are doomed to remain forever in reactive mode. While everyone says "cybersecurity is a shared responsibility," the roles of individuals, the larger community, and governments are not agreed. How do we get out of this hole?



8 Risk Management

Tuesday, June 2, 2015
Day One

Risk Management Track

The Intersection of Security and Privacy

Srini Subramanian and Robert Glaser
Deloitte & Touche LLP
11:00 a.m. - 11:50 a.m.
Meeting Room 2

As CISOs take on more and more responsibilities, an important question arises: Have the responsibilities become too diversified for one executive to handle? If so, what priorities take a back seat? The CISO function might evolve to manage three broad areas: a) governance, risk, and compliance; b) privacy; and c) security technology and operations. While one or more positions may still report to an elevated CISO position, having leaders who specialize in each of these areas and assigning them resources can help improve program efficiency. As the role of Privacy Officer emerges across states, how can they improve collaboration on documenting potential risk to citizen and business data? Enterprise-level privacy officers can help determine which data needs to be protected and why. They also play an important role safeguarding citizen privacy and restoring trust when an incident occurs. Leading practices around how privacy officers and CISOs are working together to be better positioned to gain business leadership support for their programs and build a stronger enterprise risk management program will be discussed.

Future Trends: Why your Security Program has to Change Going Forward

Manny Morales
Independent Consultant
1:00 p.m. - 1:50 p.m.
Meeting Room 2

We have all heard of the threats to the retail business, the political actions taken by Anonymous, LulzSec, or other groups (Guardians of Peace, etc.), foreign attacks to gain money or intellectual property (Romania, China, etc.). We have also heard about the costs (millions of dollars) to address these breaches and what these businesses are trying to do. If you follow the direction these companies are taking, you will still not be addressing the bigger issue. Defense in depth is no longer the cure all, you now have to re-exam your program and take more of a risk approach. Understand that management, and not the implementation of more tools is your biggest challenge. In this session, you will be given a different approach to implementing security. Using the NIST standard, as well as others, the speaker will address the words no one wants to hear "you have been breached, now what." You will come away with a new way to address security and tell management that a good security program is not only about defenses but how to respond.

Cyber Security: From Cost Centre to Revenue Driver

Igor Volovich
Schneider Electric
2:10 p.m. - 3:00 p.m.
Meeting Room 2

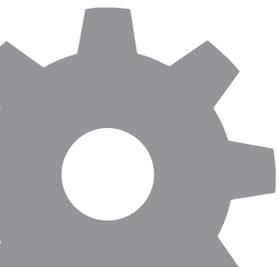
The rapidly emerging cyber regulatory climate is creating increased compliance pressures across a wide range of industries. Product and service providers now find themselves subject to new compliance and governance obligations for which they may be unprepared. Revenue generation and

cashflow are being impacted as enterprises struggle to demonstrate compliance as a condition of commercial tenders. The common tendency to view cyber governance as just another compliance activity and a cost of doing business denies enterprises the opportunity to recognize strategic value of cyber security as a business enabler and revenue driver. This session will cover the new approach to cyber security as a strategic business function, value generation through cyber maturity, and regulatory compliance as your competitive attribute.

"That Will Never Happen To Us": Five Ways to Make Security Risks Relevant to Your Organization

Todd Brasel and Vince Hannon
NYSTEC
3:20 p.m. - 4:15 p.m.
Meeting Room 2

Does your organization grasp the relevance of security risks? Is your risk management program in jeopardy because executive management does not understand its relevance? Are you developing a risk management program? Smart information security practitioners understand that all levels of an organization need to manage security risks, but it's hard to focus attention on risk when there are so many other competing business needs. Risk management programs often stumble because managers don't realize their relevance, believe it's someone else's responsibility, or don't fully understand the risks involved. In this session, you'll get practical advice on effective methods for communicating security risks that you can immediately apply to your risk management program. Through real-life examples and industry-standard practices, you'll learn to structure communication about your existing risk management program around these five concepts:



- Identifying and recruiting key allies for your risk management program
- Talking about risk assessment with your stakeholders in business terms
- Picking the right schedule of messages to keep people informed without tuning out
- Choosing the best communication channels for your messages
- Supporting the development of a risk-conscious culture

Encryption Track

Encryption and Data Security: A Conundrum?

Dan Srebnick
DynTek Services
11:00 a.m. - 11:50 a.m.
Meeting Room 3

Industry pundits talk about encryption of data as a panacea ensuring data security. But data must be decrypted in order to be processed. The issue of encryption for data security presents difficult questions for IT managers and the answers are not always obvious. This session will present the problems at hand and then methodically look at the possible answers.

Bad Cryptography

Bruce Barnett
NYSTEC
1:00 p.m. - 1:50 p.m.
Meeting Room 3

Cryptography is a key component for ensuring confidentiality and authenticity in communication. Passwords, cookies, account and session information, along with confidential information shared between sites, contain sensitive information that should be secured with encryption, but it is difficult to do this correctly. Even with the best of intentions using NIST-approved algorithms, mistakes can be made that result in unprotected information. This

presentation provides an introduction to uses of cryptography, and describes how it can be implemented incorrectly. Examples include misuse of one-time-pads, the XOR function, nonces, initialization vectors, random number generator initialization, padding oracles, use of block cipher modes, storage of confidential information, and choice of cipher suites. Some of the attacks, including some that are frighteningly trivial, will be briefly described. In conclusion, recommendations will be given on how risk can be minimized.

Secure Coding Track

Application Security Testing - How to Find Software Vulnerabilities Before You Ship Code or Procure Code

Hassan Radwan and Anita D'Amico
Secure Decisions
2:10 p.m. - 3:00 p.m.
Meeting Room 3

Most cyber security incidents can be traced back to a software vulnerability that was inadvertently put there when the code was developed. Web application attacks were the top IT security threat in 2013 according to Verizon's 2014 Data Breach Investigations Report. Of the 1,367 confirmed data breaches covered in the report, 35 percent were caused by web application attacks. Despite the high risk of attacks, it is not uncommon for software developers to wait until the development process is complete before testing for weaknesses. This goes against industry best practices which have shown that it actually costs a lot less to build security in during the software development process than to fix the vulnerabilities later in the lifecycle. Furthermore, many organizations fail to ask about the security testing that was conducted on software applications that they are procuring. Application security testing involves taking measures throughout the code's life-cycle to prevent gaps in the

design, development, deployment, upgrade, or maintenance of an application. This session will introduce the audience to a variety of application security testing techniques including:

- Manual Testing - Analyzing the code line by line
- Static Application Security Testing (SAST) - SAST tools, known as white box testing tools, analyze the application source, byte or binary code for weaknesses during the programming or testing phases of the software lifecycle
- Dynamic Application Security Testing (DAST) - DAST tools, considered black box testing tools used for application penetration testing, DAST technology analyzes applications in real-time while the application is running.

We DevOps'd - Experience and Lessons Learned Securing the SDLC

Dr. Sherly Abraham, Excelsior College
Dr. Din Cox, Medical Science and Computing
3:20 p.m. - 4:15 p.m.
Meeting Room 3

Recent massive data breaches emphasize that organizations cannot afford to take a reactive approach to security, but calls for a proactive and ground-up collaboration to security. In this presentation we discuss an emerging concept - DevOps that fosters a proactive and built into approach to software application development and deployment. We elaborate on the DevOps model including the different techniques that can be employed in order to build secure code. The presentation will highlight the adoption of a rugged approach to DevOps for building secure software where each phase of the development process involves ongoing collaboration with the IT operations, security engineering, and QA/testing teams. This includes leveraging tools such as Source Code Analysis Tools (SAST),

Dynamic Application Security Testing (DAST) and the automation of repeatable processes and best practice to reduce risk where possible. Through our DevOps strategy, we have seen reduction in application related vulnerabilities including remediation times from identification to resolution. We share lessons learned, challenges faced and best practices from the real time adoption of DevOps to secure code development and deployment, and offer recommendations on utilizing this strategy.

Incident Response Track

What Would You Say, ya do Here? Tactical Steps to Perform Tomorrow to Meaningfully Increase Security

Tyler Wrightson
Leet Systems
11:00 a.m. - 11:50 a.m.
Meeting Room 6

In this talk Tyler Wrightson reviews the chart toppers of technical security controls you can implement tomorrow to make your systems meaningfully more secure. Based on Tyler's experience penetration testing and red teaming for many diverse organizations, he focuses on the vulnerabilities that are most likely to be targeted by attackers. This talk is best suited for technical and management personnel such as systems admins, network admins, and application developers/owners.

Investigating Cyber Crime with the FBI

Michael Keller
1:00 p.m. - 1:50 p.m.
Meeting Room 6

Advanced Persistent Threats- What You Need to Know

Terry Hect
AT&T
2:10 p.m. - 3:00 p.m.
Meeting Room 6

Advanced threats and the frequency of breaches have elevated security to the executive level in organizations of every size. Additionally, nearly every new threat is now being created to be self-reliant or an "Advanced Persistent Threat" (APTs), which differ from other more simplistic attack types. The vast majority of threats that the industry is concerned with are very strategic in nature and often last for years if not discovered. By studying these attacks, we are learning that they are sometimes seen only once before their "signature" changes and they become nearly invisible again.

Attackers, regardless of their origin are a national security issue. Nation states, terrorists, organized crime and social hackers are all utilizing the same kinds of weapons and frequently the same cyber mercenaries. There are only so many ways to identify attackers and fewer ways to stop them.

Pitfalls and Potholes of the Dark Net

Leonard Popyack, Utica College
Antony Martino, Northeast Cyber Forensics Center (NCFC)
3:20 p.m. - 4:15 p.m.
Meeting Room 6

This session will examine some of the inner workings of the Dark Net. The Dark Net is an encrypted anonymous overlay network, such as Tor. We will highlight current activity and showcase some properties of the Dark Net of which you should be aware. Furthermore, we will show how unique cyber operations can be conducted with the use of specialized routers that can make use of Dark Nets and their unique properties.

Legal Issues Track

Bulletproofing Your Incident Response Plan: Effective Tabletops

Reg Harnish
GreyCastle Security
11:00 a.m. - 11:50 a.m.
Meeting Room 4

The pace of data breaches has reached epic proportions. Organizations large and small, in every industry are falling victim to hackers, hacktivists and nation states. Your intellectual property, data and bank accounts have never been at greater risk - it's not if, but when your organization will be victimized. Testing and maintaining an effective Incident Response plan has never been more important.

Join GreyCastle Security for an interactive table top exercise, and put your Incident Response Plan to the test. This session will raise awareness to the importance of the IR plan while exposing attendee's processes, policy and procedure to the various cyber threats every organization is currently facing. Attendees will take away actionable information for performing effective table top exercises and testing their own Incident Response programs.

GRC (Governance, Risk Management, Compliance) -- Why All the Recent Commotion, What are the Consequences, and What Can You Do to Comply?

Stephen Treglia
Absolute Software Corporation
1:00 p.m. - 1:50 p.m.
Meeting Room 4

This presentation will cover the evolution of the laws and regulations (HIPAA, Sarbanes Oxley, Gramm Leach Bliley, state breach notification, FERPA, FISMA, PIPEDA, and the EU's Data Protection Regulation), some recent case law starting to address civil damages for breaches, and a few suggested solutions.



Data Governance in the Era of the Data Breach

Ron Raether
Faruki Ireland & Cox P.L.L.
2:10 p.m. - 3:00 p.m.
Meeting Room 4

Ripped from today’s headlines in which company after company is reporting breaches of their information security, this session will provide a fresh perspective on some tried and true information security practices. While companies rush to spend dollars on improved technologies and contracting with third parties to build bigger fortresses around their data, many of them fail to address information security at the fundamental level through sound data governance and the implementation of layered security. Information security technology is only as good as the people using that technology and the policies under which such technology is implemented. Ron Raether will speak on the importance of an enterprise-wide data governance policy, to include real-world examples of policy driving technology selection and implementation. Ron will also discuss the importance of security in depth and how such data governance should serve as but one of many layers in an enterprise-wide information security plan, tying these concepts into various regulatory regimes.

Government Use of Social Media - The Legal Issues

David Menken
Smith Buss & Jacobs LLP
3:20 p.m. - 4:15 p.m.
Meeting Room 4

This session will explore how local governments use social media. The session will first identify the many benefits of using social media in government (i.e., Facebook, Twitter, LinkedIn, Instagram), including improved government transparency, increased collaboration, enhanced citizen participation, and improved efficiency. The session will then identify two important issues relating to government use of social

media, free speech issues, and compliance by government entities with new legal requirements.

The presentation will touch on the First Amendment, the application of the First Amendment to local government and limitations on speech in the public forum by the public and governmental employees. The presentation will review evolving laws relating to government use of social media, specifically the Freedom of Information Act, the Open Meetings Law, Record Retention Laws and the NYS Personal Privacy Protection Law. The session will then discuss social media policies which are appropriate for a local government entity to adopt, such as the type of information/opinion to be permitted, how sites are moderated and an acceptable use policy for government entities.

Security Strategies Track

Securing Your Company for Today’s Cyber War: A Three-pronged Approach to a Comprehensive IT Security Strategy

Peter Allor
IBM Security Security Strategist Federal Sector, Critical Infrastructure Group
11:00 a.m. - 11:50 a.m.
Meeting Room 5

In 2014, we saw more major cyber attacks than ever before which continued to put pressure on organizations in every industry to have the right measures in place to protect both themselves and their customers. While most organizations already have some sort of security practices in place, it does not mean they have a complete security strategy for end-to-end coverage. In fact, a recent study found 80 percent of CISOs feel they are not properly prepared for today’s cyber war. In this talk, Pete Allor will detail three critically important aspects to building a complete, end-to-end security strategy. The first,

integrate your organization’s operations and security leaders. By doing so, security leaders gain visibility into operation partners, vendors, and practices which allows them to have a complete view of the ecosystem that needs protection. Second, adopt security intelligence/situational awareness processes. Most companies lack the ability to understand where potential threats many be in their infrastructure which means attacks can go unnoticed for extended periods of time before they receive a proper response. Third, make your security strategy your own. No security strategy is the same, because every organization has different business critical data and different operations. Each organization needs to take the understanding of their operations and security needs and then apply it to the necessary security steps appropriate for their company.

Cybersecurity: A Shared Responsibility

Erin Meehan
Department of Homeland Security’s Office of Cybersecurity and Communications
1:00 p.m. - 1:50 p.m.
Meeting Room 5

The world is more interconnected today than ever before; with more connectivity comes more responsibility. The Federal government is committed to raising cybersecurity awareness across the Nation and is working across all levels of government, with the private sector, and internationally to defend against and respond to cyber incidents, while protecting individual privacy, civil rights, and civil liberties. During this presentation, you will learn about the U.S. Department of Homeland Security’s free cybersecurity resources including the Stop. Think. Connect.TM Campaign. As a partner in the Campaign, the State of New York is part of a national public awareness effort to empower the American public to be more vigilant about practicing safer online behavior. Learn more at www.dhs.gov/stopthinkconnect (link is external) or www.dhs.gov/cyber (link is external).

What Your Employees Don't Know, Can Hurt You: Creating the Vigilant Employee in the Cybersecurity War

Dane Boyd

Dell Secure Works

2:10 p.m. - 3:00 p.m.

Meeting Room 5

Social engineering has become a choice tactic for today's cyber-threat actors. Learn how vital security awareness is for your organization and see what methods are necessary to change employee behavior to result in a stronger security posture. This session can also include how to talk to senior management about needing a security awareness program.

Cyber Security's Weakest Link: YOU

Michael McCutcheon

Rational Enterprise

3:20 p.m. - 4:15 p.m.

Meeting Room 5

All companies have a baseline of security, which typically includes firewalls, proxy servers, intrusion detection, data loss prevention, spam filtering, and anti-virus. However, even prominent organizations that spend huge budgets on data security and have significantly more than baseline protections still lose massive volumes of data. Cyber security is only as strong as its weakest link: You. This presentation will explore the end user's role in cyber security and the need to mitigate that risk with technology that allows organizations to be more content aware. Automated, content-based classification of organizational data enhances cyber security protections by providing definitive answers to the troubling questions that arise following a data breach: "what data did we lose?" and "what is our exposure?" Moreover, a content aware organization can proactively defend against cyber security threats by moving sensitive data to the most secure storage locations.

Training Track

Attendees must be pre-registered

Tuesday, June 2, 2015

Information Security Risk Analysis

Sanjay Goel and Damira Pon

University at Albany, SUNY

10:30 a.m. - 12:30 p.m.

Meeting Room 7

Analyzing the information security risks in an organization is a fundamental task of security management in an organization. Yet, organizations continue to struggle to conduct risk analysis and make the right decisions on security investments in the organization. This tutorial takes the attendees through the process of organization's risk analysis. The tutorial provides a broad overview of the risk analysis process and then delves deep into the actual process through cases and examples. The first part of the risk analysis process is the identification of assets, vulnerabilities, and threats. The second part of the process involves determining the exposure of the organization to cyber security risks. The third part of the process is identifying the controls to mitigate the risk to an acceptable level. The tutorial will use excel spreadsheets and take the users through the entire thread of the risk analysis process. The tutorial discusses the differences between qualitative and quantitative risk analysis, as well as some advanced risk analysis methodologies based on attack trees and probabilistic analysis.

360-degree Global Cyber Threat Analysis

Peter Stephenson, PhD

Norwich University

1:15 p.m. - 4:15 p.m.

Meeting Room 7

From malware to open source intelligence to threat actor identification, analyzing a large cyber-attack is tedious work. By analyzing pre-existing attacks before they target your organization you can be more proactive. If you are reacting to an attack against your enterprise you can be more effective. This half-day tutorial will begin with dynamic analysis and profiling of a malware sample. From the information extracted we will identify domains, functionality, similar attacks and, finally, the threat actor responsible. Using the latest tools for malware analysis, open source intelligence, domain identification and threat actor identification we will create an attack profile that can be used either proactively or reactively to protect your enterprise or respond to attacks. The tutorial will be conducted live from our cyber threat analysis platform and will provide a complete recipe for global cyber threat analysis.

Continuing Legal Education (CLEs)

credits are sponsored by the Albany County Bar Association for the following June 2 sessions:

- GRC (Governance, Risk Management, Compliance) -- Why All the Recent Commotion, What are the Consequences, and What Can You Do to Comply?
- Data Governance in the Era of the Data Breach
- Government Use of Social Media - The Legal Issues

Tuesday, June 2, 2015
Meeting Room 1

SYMPOSIUM SESSION 1: Behavioral Security

Chair: Damira Pon, University at Albany, SUNY, NY
 11:00 a.m. - 11:50 a.m.

Paper: Experience Matters: The Role of Direct and Vicarious Experience in Secure Actions

Leigh A. Mutchler, University of Tennessee and Merrill Warkentin, Mississippi State University

Paper: Two Studies on Password Memorability and Perception

Delbert Hart, SUNY Plattsburgh

SYMPOSIUM SESSION 2: Service Security

Chair: Justin Giboney, University at Albany, SUNY, NY
 1:00 p.m. - 1:50 p.m.

Paper: A Holistic Approach for Service Migration Decision, Strategy and Scheduling

Yanjun Zuo, University of North Dakota

Paper: Post-audit of Service Security Investment: Using Simulation Approach

Hemantha Herath and Tejaswini Herath, Brock University

SYMPOSIUM SESSION 3: Cyber Attacks

Chair: Victoria Kisseka, University at Buffalo, SUNY, NY
 2:10 p.m. - 3:00 p.m.

Paper: Crowdsourcing Computer Security Attack Trees

Matt Tentilucci, Penn State University, Nick Roberts, Penn State University, Shreshth Kandari, Daryl Johnson, Dan Bogaard, Bill Stackpole; Rochester Institute of Technology, NY, and George Markowsky, University of Maine

Paper: A Covert Channel in the Worldwide Public Switched Telephone Network Dial Plan

Bryan Harmat, Jared Stroud and Daryl Johnson, Rochester Institute of Technology, NY

SYMPOSIUM SESSION 4: International Security Cooperation & Cyber Warfare

Chair: Sanjay Goel, University at Albany, SUNY, NY
 3:20 p.m. - 4:15 p.m.

Paper: International Cooperation to Enhance Website Security

Manmohan Chaturvedi and Srishti Gupta, Indian Institute of Technology, Delhi

Paper: Sharing Cyber Threat Information: Swimming in Data but Starving for Information

Sanjay Goel, University at Albany, SUNY, NY and Charles Barry, National Defense University



Afternoon Cookie Breaks

June 2 at 3:00 p.m. - 3:20 p.m. and

June 3 at 2:30 p.m. - 2:50 p.m.

Re-energize with a beverage and a snack!



Wednesday, June 3, 2015
Day Two

Forensics Track

Tales from the Crypt: Fighting Ransomware

James Antonakos
National Cybersecurity Institute
10:30 a.m. - 11:20 a.m.
Meeting Room 1

Ransomware, such as Cryptolocker and Cryptowall, does not bother to steal your critical files as it is much easier to just encrypt them in place and give you a ransom note. This session describes the forensic analysis of a ransomware attack and describes the vulnerabilities exploited to infect the victim computer, the damage done to the system's files, other actions taken by the ransomware, and the lessons learned during the investigation of different incidents. Ransomware requires that we take a fresh look at access control, intrusion detection, and backup strategies.

Are you Tired of Hearing that the Sky is Falling When we Talk About Information Security?

Tom Brennan
ProactiveRISK
11:40 a.m. - 12:30 p.m.
Meeting Room 1

It is time for tactical and practical suggestions. Attend this proactive session and learn how to identify issues before they become headline news. Learn about practical and many times overlooked system configurations changes that could have stopped many breaches and where to start when investigations of computer crime are needed. Discuss, debate and ask your hypothetical questions.

The Critical Role of Netflow/IPFIX Telemetry in the Next-Generation Network Security Infrastructure

Ken Kaminski
Cisco Systems
1:40 p.m. - 2:30 p.m.
Meeting Room 1

More and more we have seen the security perimeter of the network breached with attackers taking up an increasing number of footholds inside of the network. This session takes an in-depth look at NetFlow/IPFIX with the goal of leveraging this technology to provide heightened visibility and context into network traffic in order to identify attackers and accelerate incident response. Use of this technology is recognized as one of the most effective ways to combat Advanced Persistent Threat penetrations. Design and deployment of technology utilizing Netflow/IPFIX as a collection and analysis system will be presented. Use cases include using Network Identity Management systems as an additional telemetry source, integration with SIEM vendors, and using Netflow/IPFIX to identify an attacker's presence on the network.

Next-Generation Endpoint Security: Protection, Detection and Response

Jesse Torzs
Bit9
2:50 p.m. - 3:45 p.m.
Meeting Room 1

A new generation of threats is attacking your endpoints and servers—you need to a modern defense. Today's attackers are after the data and intellectual property on your endpoints and servers. If you're only relying on traditional endpoint security, such as antivirus, or network security, you're putting your organization at risk. AV doesn't see or stop targeted attacks, nor does it help you respond to an incident. And if an attack bypasses your network security, your endpoints will be compromised. Do you know what's happening on your endpoints

and servers—right now? Most security teams have no way of knowing. If you suspect malware is in your environment, how can you tell what machines it's on? Is it executing? What is it doing? In this content-rich presentation you'll learn how to solve these problems – now!

Collaboration Track

The Promises and Pitfalls of Public-private Sector Cooperation in Cybersecurity

Austen Givens
Utica College
10:30 a.m. - 11:20 a.m.
Meeting Room 2

This talk examines the advantages and challenges of closer public-private sector cooperation in cybersecurity. The presentation content comes from a three year research project examining the dynamics of public-private sector coordination in homeland security and cybersecurity. While some believe that "public-private partnership" is little more than a feel-good buzzword, these partnerships have actually yielded tangible benefits for firms and government agencies since 2001. However, closer ties between the government and business sectors have also introduced new challenges that must be navigated carefully. This talk is ideal for senior government leaders, business managers, IT security professionals, law enforcement personnel, and owner/operators of critical infrastructure.

Information Sharing in Multi-agency Disaster and Crisis Response: Smithfield Tornado Disaster and DeRuyter Shooter Man-Made Crisis Events Discussed

Joe Treglia
Syracuse University
11:40 a.m. - 12:30 p.m.
Meeting Room 2

This discussion focuses on how information is shared within and across boundaries

of government and non-government stakeholder agencies at natural and man-made crisis incidents that involve multiple agencies and jurisdictions. This session is based on evaluation of actual incidents and debriefings from recent incidents in central New York State. Various types of technologies and processes for communication and sharing are identified and discussed in terms of their strengths and encountered challenges reflecting on actual incidents. Current research on centralized versus decentralized information types of sharing is considered in this area. Formal and informal information channels are discussed along with attendant security and privacy concerns. Best practices and lessons learned from these current disaster crisis events are presented for consideration in future incidents and for policy and procedure development.

Critical Infrastructure Track

ICT Supply Chain Risk in 2015: Can the Private Sector be Engaged?

Michael Aisenberg
MITRE Corp/ABA Information Security Committee
1:40 p.m. - 2:30 p.m.
Meeting Room 2

While new statutory and agency authorities to address ICT Supply Chain Risk in the defense and intelligence agencies have been developed, 2014 Congressional authority to DHS to reach out to private sector critical infrastructure operators is new and untested. This session will review the "As Is" state of SCRM among the key critical infrastructure sectors in banking/finance, power, oil and gas, transportation and communications, the state of supply chain threats in hardware/components, software and services, and the path on which DHS is setting to engage these companies to address the continuing estimated \$1 trillion threat to the U.S. domestic economy from potential exploits against these and other CI sectors. Past DHS outreach measures,

the Cyber Framework and new proposals will be summarized, and areas of potential green field efforts, such as improved product testing and software code analysis will be outlined, along with discussion of the legal/liability risks remaining for CI businesses.

Mind the Gap: Evolving Information Sharing; Protecting U.S. Critical Infrastructure Against Growing Cyber Threats

John Cassidy
CenturyLink Government
2:50 p.m. - 3:45 p.m.
Meeting Room 2

Private companies operate our nation's most critical infrastructure including our electrical grid, water utilities, hospitals, and financial institutions. Well-funded nation state and organized cyber crime organizations are aggressively attacking U.S. critical infrastructure every minute of every day. Ensuring that these private companies are able to protect themselves from these sophisticated attacks is deemed a matter of national security by the U.S. government. As such, the U.S. government is interested in arming these private entities with sensitive and classified government vetted cyber threat intelligence to assist in thwarting these attacks. This session will focus on how the U.S. government utilizes creative information sharing programs to protect private critical infrastructure companies and federal civilian agencies from infiltration and attack. The session will highlight two Department of Homeland Security Programs - Enhanced Cybersecurity Services (ECS) and Einstein 3 Accelerated (E3A) - as key tools used to combat against the evolving cyber threat.

Threat Landscape Track

The Truth about Cybersecurity: A Real-World Look into the Current Threat Landscape and the Business and Financial Impact of Targeted Cyber Attacks

Nick Bennett
Mandiant, A Fire Eye Company
10:30 a.m. - 11:20 a.m.
Meeting Room 6

Cybersecurity is a critical consideration for today's government and business leaders alike. Considering the high-profile breaches making headlines almost daily, it is clear that the financial and business repercussions can be devastating. In fact, the aftermath of these exploits strike at the heart of leadership, including technology, line-of-business and financial teams. In this presentation we will provide a first-hand, inside look into these attacks and the related risks cybercrime creates for leadership and their organizations.

Organizations around the world of all shapes and sizes are being targeted by advanced cybercriminals who have become experts in morphing their appearance and tactics faster than it takes your team to configure a new endpoint. While defense-in-depth architecture has been the de facto cybersecurity standard, the newfound speed of attackers has led to this architecture seeing 97 percent of "secure" companies breached over the last year*. Diving into global attack data, and his learnings from responding to decades of breaches, Nick Bennett will provide insights on the best answer to today's threats: making security faster in responding to incidents. Nick will dissect recent campaigns that have seen even the "basic" cybercriminal adopting advanced attack techniques to bypass defense layers, and present case studies that demonstrate why having an architecture that makes incident response a 10-minute, not 10-month, cycle is critical.

Nick will address how these developments are reshaping the cybersecurity focus of agency leadership -- how they and their financial teams are stepping up the battle against these threats, and how the agency leadership is playing an increasingly significant role in advocating for and pursuing critical security investments that promote long-term business enablement.

* FireEye, Inc. Advanced Threat Intelligence data

After the Recently Publicized Events, What's Next?

Michael Corby

CGI Solutions and Technologies, Inc.

11:40 a.m. - 12:30 p.m.

Meeting Room 4

Sony Pictures, Target, Staples, Home Depot, etc. What's happening and where are we going? The recent rash of widely publicized security events have given us plenty of opportunities for party discussions, but what's behind this? This session will explore some interesting background behind the recent frequent release of plenty of these stories. At best, we get to have a budget discussion, but is there more that we can learn from these events?

Reporting on the Current Risk Landscape - The Verizon Data Breach Investigative Report

Chris Novak

Verizon Enterprise Solutions

1:40 p.m. - 2:30 p.m.

Meeting Room 4

The Verizon Data Breach Investigations Report is an internationally recognized report that brings together statistics and findings from worldwide investigative response organizations around the globe, as of 2014 there were 50 contributing organizations and more are being added yearly. The contributors include: The Dutch National High Tech Crime Unit, U.S. Secret Service, Australian Federal Police, Irish Reporting and Information Security Service,

and Police Central e-crime unit. Chris Novak is the Global Managing Principal of the Verizon Investigative Response team and a contributing author to the Data Breach report. He is knowledgeable regarding data breaches, cybercrime and investigations worldwide. In this session Chris will discuss the current DBIR as well as how to apply the data to shape your own risk modeling in order to address the most real and credible threats that are resulting in breaches for organizations every day.

The Explosion of Cybercrime - The 5 Ways IT may be an Accomplice

Mark Villinski

Kaspersky Lab

2:50 p.m. - 3:45 p.m.

Meeting Room 6

Mobile devices, social media sites, and the exponential growth of cybercriminals are threatening your users and your data every day. Can your IT department become an unwitting accomplice to cybercrime? Mark Villinski, Kaspersky Lab Marketing Manager, sheds light on the growing challenges facing IT today and discusses the 5 ways that IT departments may be unknowingly enabling cybercrime in their organizations. During this session, you will hear:

- A comprehensive overview of the current state of the cybercrime threat landscape
- Several real life examples and stories of attacks; where they come from and ways to detect them
- Examples of current IT policies and procedures that may be exposing your network to attacks

Mobile/BYOD Track

Planning Mobile?!

Eric Green, Mobile Active Defense

Larry Whiteside Jr., Lower Colorado River Authority (LCRA)

10:30 a.m. - 11:20 a.m.

Meeting Room 3

The value and need for proper research and planning to both take your organization mobile, and periodically re-evaluate that strategy and direction cannot be underscored enough. "We bought a Mobile Device Management product so we have it under control" is the farthest thing from true as this dynamic, ever changing environment needs constant care. This topic may not be as flashy as hacking Android or trash talking iOS - BUT - without this critical piece, in the end none of the flashy stuff matters. Okay, so maybe we will demonstrate using a trojanized app to gain full command and control of an iOS device....and....demonstrate a Man-in-the-Middle attack.

BYOD - It's Not so Hard!

Kevin Wilkins

iSecure LLC

11:40 a.m. - 12:30 p.m.

Meeting Room 3

Bring Your Own Device (BYOD) is one of the biggest challenges in IT today. As opposed to engaging in the very complex issue of MDM technology, it may be possible to look at it from a standpoint of remote access. Remote access has been an IT deliverable since the age of the modem, and can be looked upon for guidance in facing this contemporary need.

Compliance Track**Cyber Security Threats, Trends and Best Practices to Secure Your Government Organization**

Tim Finn and Ron Smalley

First Data

1:40 p.m. - 2:30 p.m.

Meeting Room 3

First Data will describe and dissect the information security challenges facing organizations in both public and private sectors. Security experts will discuss the concepts, strategies, and best practices as part of an overall security strategy, including encryption and tokenization, protection of data in motion, at rest and in flight and cyber threats, cyber crimes and cyber trends.

Strong Medicine for HIPAA Compliance

Paul Romeo

GreyCastle Security

2:50 p.m. - 3:45 p.m.

Meeting Room 3

Join us as we journey into the world of healthcare cybersecurity to uncover why your medical information and electronic health records are arguably the most sought after information on the black market today. Learn actionable information on what healthcare organizations can do to protect your data while improving security posture, better aligning with the HIPAA security rule and reducing overall cybersecurity risks.

Invasion of Technology Track**Biometrics: Who Are You?**

Stephanie Schuckers

Clarkson University

10:30 a.m. - 11:20 a.m.

Meeting Room 4

In our society with the ubiquity of electronic mediums, there is a need to establish a trusted relationship between individuals, and between individuals and organizations, in order to support: electronic commerce (including mobile transactions); worker and employer interactions; delivery of benefits from governments; movement of individuals across international borders; social connections; and delivery of quality healthcare. Ways to establish a trusted relationship include:

- What you have? (birth certificates, drivers licenses, credit cards, passports, key)
- What you know? (passwords, PINs, mother's maiden name, address, email, phone number, Social Security Number)
- Who you are? (personal traits, biometrics)

Biometrics is defined as "automated methods of recognizing an individual based on measurable biological (anatomical and physiological) and behavioral characteristics." The addition of biometrics adds another dimension of security which promotes security and reduces the burden on individuals to provide additional information. As with other personal information such as demographic information, biometric data must be protected. Combinations of security mechanisms, as well as enhancing the protections of the biometrics and other security mechanisms are critical to keeping personal information safe, while ensuring the free flow of data for the right people at the right time. This talk will give an overview of biometrics systems and give some examples of emerging privacy enhancements including template protection, cancelable biometrics, and liveness detection.

The Day After Passwords Die - How Biometrics will Usher in a New Age of Technocreepiness

Thomas Keenan

University of Calgary

11:40 a.m. - 12:30 p.m.

Meeting Room 6

As companies and government agencies scramble to recover from wholesale credential thefts, thought leaders are suggesting that we need to bury the password once and for all. As explained in my book, Technocreep, Google's Regina Dugan has mused publicly about magnetic ink tattoos or daily password pills that broadcast from your tummy. Others think your fingerprints, ear shape, DNA, microgestures, heart rhythm, brainwaves, iris scan or even breath or body odor will be used to identify you. These techniques all bring their own creepy problems. You can change your password. But if your biometric credentials are stolen by a hacker, what do you do, change your face or heartbeats? This presentation will showcase the real, planned, and "day after tomorrow" technologies that can be used to identify us, and assess their social implications, particularly in the area of privacy. After all, Target famously found out that a teenage girl was pregnant, before her father knew, from her purchase history. What if they also grabbed your DNA as you typed on the checkout keypad and sent it out for analysis? "We notice you are pre-diabetic" might pop up on the display the next time you shop. "We have a special coupon for you." As explained on Gizmodo, "Your Fuelband Knows When You're Having Sex" (you burned 150 calories at 2 a.m. and took zero steps.) This demonstrates that biodata grabbed innocuously for one purpose can be analyzed and used to draw conclusions about us. Only time will tell if consumers think biometric identification is cool or creepy. However, now is the time to think about the implications of sharing some of our most intimate and personal data, just to prove who we are.

From the Hobbyist's Garage to Threat From Above - Defending Against Drones

George Palmer and Stuart Card
AX Enterprize, LLC
1:40 p.m. - 2:30 p.m.
Meeting Room 6

Out of the workshops of hobbyists an unsuspected threat has arisen. Unmanned Air Vehicles or UAV's have been under development and in use by the military for quite some time, but there has been a parallel development effort underway by thousands of hobbyists whose only intent was to create an inexpensive Unmanned Aerial System (UAS) for personal use. In recent years this massively distributed development has been commercialized and many "personal" UAV's have flooded the consumer market. The cost of these systems has become so low that practically anyone can afford one. Therein lies the threat. The small UAV's on the market today have non-trivial payload capacities. Many are capable of lifting 5-10 lbs over considerable distances. The autopilot control systems can be nearly as accurate as a military guided bomb. It is only a matter of time until persons of mal intent attempt, and most likely succeed, at using a small UAV to deliver a harmful payload upon an unsuspecting target. There are an astoundingly large number of ways a UAV could be used maliciously. Possible uses range from physical energy attacks to psychological attacks to cyber warfare attacks. A relevant example would be the use of a UAV to transfer a payload over physical security installations (fences, walls, etc.) in order to place it within range of a supposedly "safe" wireless network it wishes to monitor or exploit. This presentation attempts to identify and classify the various possible methods of attack using small UAV's. We go on to describe some of the techniques which may, after significant development, be used to detect and mitigate against these attacks.

Is your Privacy Being Mickey Moused?

Raj Goel
Brainlink
2:50 p.m. - 3:45 p.m.
Meeting Room 4

This presentation distills 11 years of research in online threats, 4th amendment cases, ECPA enforcement, FTC actions, cloud applications, vendors, criminals, Internet of Things, Government Actions, user behavior and human psyche to develop a picture of where we are, where society is heading and what we can do to preserve and protect privacy, security and civil society.

Cyber Potluck Track

Ahead of the Curve: Better Cybersecurity through Tech Transfer Partnerships

Dr. Douglas Maughan
Department of Homeland Security
10:30 a.m. - 11:20 a.m.
Meeting Room 5

There's no shortage of great ideas, tools and technologies in cybersecurity - much of it in our national labs and universities, especially in New York. But new ideas will only make a difference if they are deployed and used. The challenge is putting these new concepts into practice. This tough task requires contributions from all sources including researchers and developers, security practitioners and end users, both public and private. This talk will illustrate how the cybersecurity research and development program at the U.S. Department of Homeland Security, Science and Technology Directorate (DHS S&T) seeks to address this challenge and harness new ideas for meeting the cybersecurity challenges of today and tomorrow.

What Makes a Good Cyber Security Policy?

George Duchak
Director of the Air Force Research Lab
11:40 a.m. - 12:30 p.m.
Meeting Room 5

The development of cyber security policy is informed by a broad spectrum of inputs ranging from strategic direction through knowledge of best practices. This talk will address the process of developing IT policies as they are influenced and derived from strategic vectors, industry best practices, and localized factors. References to available DoD and Air Force guiding documents will be shared for attendee use.

Cooperating in Cyber Defense: Learning Together and Sharing Knowledge

Deb Snyder, New York State Office of Information Technology Services
Nancy Mulholland, New York State Office of Information Technology Services
Kim McKinney, New York State Office of Information Technology Services
Leo Pfohl, GENESYS
Mark Spreitzer, CGI Federal

1:40 p.m. - 2:30 p.m.
Meeting Room 5

Protecting cyber space is a huge challenge for both public and private organizations. Despite massive investments in cyber security, breaches continue to occur. Organizations struggle to make decisions on security and IT investments since the return on investment is not clear. It is a colossal waste of national resources when neophyte organizations struggle and learn on their own rather than benefiting from experience of others who have established their programs. A forum for sharing best practices and concerns of organizations is very instrumental in creating a broad coalition working collectively towards a shared goal of protecting information and networks.

During this session we discuss the various initiatives and directives on information and knowledge sharing in cyber security. We also talk about the NYS Forum which is one such organization that supports knowledge sharing in cyber security. Learn how you can participate in this forum and learn from the collective wisdom and experience of other participants.

Establishing a Prototype to Enable Usage-based Cyber Liability Insurance

Steve Hamby
Independent Consultant
2:50 p.m. - 3:45 p.m.
Meeting Room 5

Cyber liability insurance is a rapidly growing tool that organizations use to transfer risks from threats and vulnerabilities associated with cyberspace operations. However, the cyber liability insurance premiums are very volatile, and increasing continuously. This session describes a prototype using existing enterprise IT tools that organizations can implement to enable usage-based insurance (UBI) for their cyber liability insurance policies. The implementation of UBI in other insurance markets has been successful in reducing premiums for the insured, while providing the insurer with increased awareness of the risks associated with a specific insured entity. This UBI prototype provides a semi-automated tool to establish cyber situational awareness of threats and vulnerabilities, based on prioritized organizational missions, coupled with continuous monitoring of security controls that mitigate cyber liability risk.

View the Conference agenda and your schedule with the Conference Mobile Event Guide:
<https://www.regonline.com/register/m/?eventid=1694164>

**Wednesday, June 3, 2015
Meeting Room 7**

SYMPOSIUM SESSION 5: Digital Forensics

Chair: Fabio Auffant, University at Albany, SUNY, NY
10:30 a.m. - 11:20 a.m.

Paper: Shot Segmentation and Grouping for PTZ Camera Videos Compliance

Andrew Pulver, University at Albany, SUNY, NY, Ming-Ching Chang, GE Global Research and Siwei Lyu, University at Albany, SUNY, NY

SYMPOSIUM SESSION 6: Cloud Computing and the Internet of Things

Chair: Yuan Hong, University at Albany, SUNY, NY
11:40 a.m. - 12:30 p.m.

Paper: Secure Audio Reverberation over Cloud

Abukari Mohammed Yakubu, University of Winnipeg, Canada, Namunu C. Maddage, University of Melbourne, and Pradeep K. Atrey, University at Albany, SUNY, NY

Paper: Using Features of Cloud Computing to Defend Smart Grid against DDoS Attacks

Anthony Califano, Ersin Dincelli, and Sanjay Goel, University at Albany, SUNY, NY

SYMPOSIUM SESSION 7: Disasters and Incident Response

Chair: Pradeep Atrey, University at Albany, SUNY, NY
1:40 p.m. - 2:30 p.m.

Paper: Trust Management in Resource Constraint Networks

Thomas Babbitt and Boleslaw Szymanski, Rensselaer Polytechnic Institute, NY

Paper: The Causal Relationships of IS Effectiveness After an Extreme Event

Victoria Kisekka, Raj Sharman, H.R. Rao, Shambhu Upadhyaya, University at Buffalo, and Nicole Gerber, Roswell Park Cancer Research Center, Buffalo, NY

SYMPOSIUM SESSION 8: Network Security

Chair: George Berg, University at Albany, SUNY, NY
2:50 p.m. - 3:45 p.m.

Paper: A Layer 2 Protocol Design to Protect the IP Communication in a Wired Ethernet Network

Reiner Campillo, Rochester Institute of Technology, NY and Tae Oh, Rochester Institute of Technology, NY

Paper: Proposed Terminal Device for End-to-End Secure SMS in Cellular Networks

Gaurav Balaiwar, Neetesh Saxena, and Narendra S Chaudhari, Indian Institute of Technology Indore



When managing security in an all-IP network,
it helps to see the big picture.

AT&T security experts analyze more than 310 billion flow records each day for anomalies that indicate malicious activity. It's what makes us uniquely qualified to help state and local government agencies address the security challenges they face. Our proactive network-based approach to managed security delivers some of today's most powerful weapons to combat cyber security attacks – helping to safeguard all the elements of your IP infrastructure. To learn more, download the CIO Security Guide at att.com/govsecurity





Threat-Centric Security.

Continuous threat protection
against continuous attacks
for faster time to detection
and time to remediation.

WHAT WILL
YOU
DO
WHEN
YOUR
BUSINESS IS
HACKED?



SECURITY BREACH HOTLINE
(800) 403-8350



Our commitment to New York State

For more than 100 years, Deloitte has worked with New York State government and business leaders to assist them with their business challenges and think through potential opportunities.

We have teamed with more than 100 not-for-profit organizations to help those less fortunate and provide skills to those in need.

We have collaborated with New York-based colleges and universities to educate our future workforce and help them be successful in their chosen professions.

And for more than 100 years, we have called New York home.

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.

Copyright © 2015 Deloitte Development LLC. All rights reserved.
Member of Deloitte Touche Tohmatsu Limited

Deloitte.

TOGETHER WE DO
**AMAZING
 THINGS**



CSC

CSC is doing amazing things to help New York reduce healthcare costs, improve healthcare and save lives.

csc.com

BUSINESS SOLUTIONS | TECHNOLOGY | OUTSOURCING

Protect More.



Address the Cyber-Security Landscape:

- + Secure Perimeter
- + Secure Data
- + Secure Services

Proud to Partner with:



e⁺

Where Technology Means More™

18 Corporate Woods Blvd., 2nd Floor, Albany, NY 12211
www.eplus.com



©2015 ePlus inc. All rights reserved. ePlus, the ePlus logo, and all referenced product names are trademarks or registered trademarks of ePlus inc. All other company names, logos, and products mentioned herein are trademarks or registered trademarks of their respective companies.



Security is a process.
Built in, not bolted on.

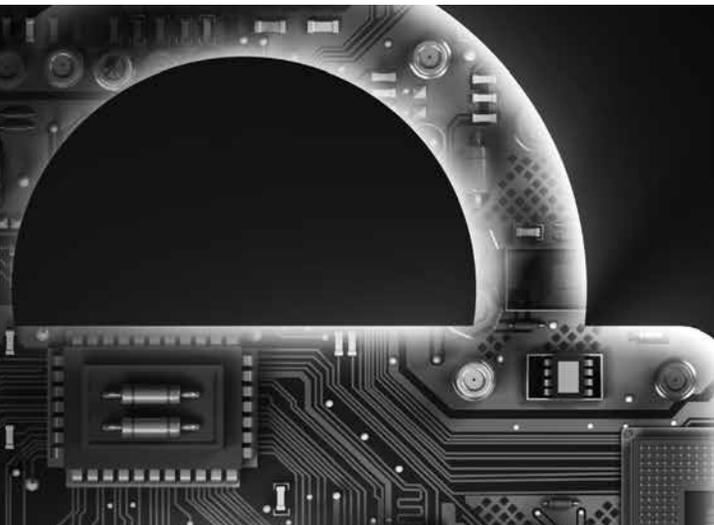
*NYSTEC can help you
build security into your
networks and systems*



Bringing Clarity
To Complex Technology Projects

www.nystec.com

PRESIDIO
Practical thinking for a connected world.



ENSURING REGULATORY COMPLIANCE AND PROTECTING INFORMATION ASSETS
AGAINST THE EVER-CHANGING THREAT LANDSCAPE.

Presidio Albany Office
20 Corporate Woods Blvd, Suite 306
Albany, NY 12211
518.213.9310 | www.presidio.com



empower

From providing a soldier secure access to mission-critical data in the field to providing citizens services across the web, the federal government demands the most innovative and scalable IT solutions available. Symantec information management and security solutions help government agencies empower their employees to achieve their goals. When you can do it simply, safely, and quickly, you can do it all. Start doing more at go.symantec.com/federal

#GoEmpower

Go ahead, you've got  **Symantec**™

Copyright © 2015 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, and the Checkmark Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.



Terabyte Sponsor

A fully connected network brings it all together.

Government transformation is the new normal from consolidation and modernization of voice and data networks to the essential need to mobilize field workers and citizen services.

With cyber security risk a reality, the need to protect information, infrastructure and citizen data is a top priority. As government continues to find new ways to unite and serve constituents, technology has the power to help.

Across the country, dedicated AT&T professionals are working with state and local governments to transform their networks and accomplish more in less time. With our comprehensive suite of solutions, agency operations are now more agile, cost efficient and highly secure. To learn more, visit www.att.com/stateandlocal



Cisco is the worldwide leader in networking that transforms how people connect, communicate, and collaborate. Cisco's network-centric platform is changing the nature of work and the way we live.

Founded in 1984, Cisco pioneered the development of Internet Protocol (IP)-based networking technologies. This tradition continues with the development of routing, switching, and other networking-based technologies such as application networking services, collaboration, home networking, security, storage area networking, telepresence systems, unified communications, unified computing, video systems, and wireless. All of these technologies are made possible due to the evolution of the network.

As an innovator in the communications and information technology industry, Cisco and our valued partners sell Cisco hardware, software, and services to businesses of all sizes, governments, service providers, and consumers.

An integral part of Cisco's business strategy is strong corporate social responsibility. Beyond our investments in social programs and commitment to environmentally conscious operations and products, we are proactively engaged with global governmental, scientific, and social leaders to develop solutions to climate change, to create economic and educational opportunities, and to address other pressing social and environmental issues. Learn more at www.cisco.com



Kilobyte Sponsor

ePlus engineers transformative security solutions for visionary organizations. Through our security architects, engineers, and consultants, we see our clients' horizons and craft sustainable IT roadmaps. Our deep partnerships with top manufacturers, keep us immersed across the IT ecosystem. ePlus addresses the cyber-security landscape through:

- Secure Perimeter Solutions: Securing the access and transmission of electronic data
- Secure Data Solutions: Fortifying data centers and securing data where it resides
- Secure Services: Aligning seasoned experts in building a tailored security program

For more information visit www.eplus.com, or contact Kevin Manning, Regional Security Sales, (781) 615-1331, kmanning@eplus.com; Dave VanLeeuwen Sales Manager (518) 362-2501, dvanleeuwen@eplus.com



Kilobyte Sponsor

Presidio is the leading provider of professional and managed services for advanced IT solutions. By taking the time to deeply understand how our clients define success, we architect enduring technology solutions that address their business needs. Our approach blends the credibility to deliver practical results today, with the creativity to drive the business visions of tomorrow. More than 2,400 Presidio IT professionals, 1,500 of which are engineers with over 2,000 industry leading certifications, are based in 50+ offices across the US. We serve our clients through a unique, local delivery model while capitalizing on our scale as a multi-billion dollar industry leader. We are passionate about driving results for our clients and delivering the highest quality of service in the industry. For more information visit: www.presidio.com.

**Kilobyte Sponsor**

Symantec is a global leader in providing security, storage and systems management solutions to help our customers – from consumers and small businesses to the largest global organizations – secure and manage their information-driven world against more risks at more points, more completely and efficiently. As the world’s fourth largest independent software company, our unique focus is to eliminate risks to information, technology and processes independent of device, platform, interaction or location. Our software and services protect completely, in ways that can be managed easily and with controls that can be enforced automatically – enabling confidence wherever information is used or stored.

**Kilobyte Sponsor**

Tanium gives the world’s largest enterprises and government organizations the unique power to secure, control and manage millions of endpoints across the enterprise within seconds. Serving as the “central nervous system” for enterprises, Tanium empowers security and IT operations teams to ask questions about the state of every endpoint across the enterprise in plain English, retrieve data on their current state and execute change as necessary, all within seconds. Organizations now have complete and accurate information on the state of endpoints to more effectively protect against modern day threats and realize new levels of cost efficiency in IT operations. www.tanium.com

Sponsor Demonstration Schedule

Terabyte Sponsor **AT&T**

June 2 at 10:35 a.m. - 10:55 a.m. and
June 3 at 10:05 a.m. - 10:25 a.m.
Booth #33-35

Megabyte Sponsor **Cisco Systems**

June 2 at 1:55 p.m. - 2:05 p.m. and
June 3 at 11:25 a.m. - 11:35 a.m.
Booth #14-15





With Tanium you can answer critical questions about the current state of your endpoints & take immediate action as needed.

All within 15 seconds.

KNOW IN  SECONDS



How many laptops are missing critical security patches?



How many unmanaged machines are on my network?



What versions of Java are out of date in my environment?

Let us show you the magic of Tanium at booth #16.

Learn more at www.tanium.com

The 2015 NYS Cyber Security Conference would like to thank all of our sponsors, exhibitors, speakers, volunteers, and attendees for making this another successful year!

Please remember to complete the Conference survey at <https://www.surveymonkey.com/s/NYSCSCeval15>



The Graduate School at Bay Path University offers over 20 career oriented online and on-campus graduate programs and certificates, including, MS in Cybersecurity Management, MBA, MS in Communication and Information Management, MS in Forensics, MS in Nonprofit Management and Philanthropy, MS in Strategic Fundraising, MS in Leadership and Negotiation and many others. Our programs are designed for working women and men and tailored for the adult student seeking convenience, flexibility and a professional edge.

Contact Information:

The Graduate School at Bay Path University
588 Longmeadow Street, Longmeadow, MA 01106,
800.782.7284 x1332
www.graduate.baypath.edu



A new generation of threats is attacking your endpoints and servers—you need a modern defense.

Today's attackers are after the data and intellectual property on your endpoints and servers. If you're only relying on traditional endpoint security, you're putting your organization at risk. Anti virus doesn't see or stop targeted attacks, nor does it help you respond to an incident. And if an attack bypasses your network security, your endpoints will be compromised.

You need to arm your endpoints so that you can easily see and immediately stop advanced threats. The answer is Bit9 + Carbon Black.



Our expert staff will analyze organizational IT infrastructure needs to propose unique solutions ensuring maximum uptime and business continuity. We are committed to providing a relationship you can count on now, and well into the future, with best in class service before and after the sale, quality products, and proactive recommendations for stable IT environments.



CenturyLink is a choice of Fortune 500 companies, government and education organizations nationwide offering a comprehensive portfolio of data, voice, security, cloud and networking communications solutions through its high-quality network and multiple data centers. CenturyLink is the third largest telecommunications company in the United States, and has one of the largest fiber footprints serving customers in Worldwide. www.centurylink.com



Core Security offers vulnerability management and penetration testing software and services. We help more than 1,000 customers worldwide identify the most vulnerable areas of their IT environments in order to improve remediation efforts and better secure their businesses www.coresecurity.com

Tweet the Conference at #nyscyber

32 | Exhibitors



CounterSnipe Systems are a leading developer of Network Security Software which includes Intrusion Prevention System(IDS/IPS), malware protection, asset discovery plus port scanning, end point detection/scanning and intelligent alert management.

Our software is well suited to and deployed by medium to large enterprises, financial institutions, government departments and health organizations that are looking to satisfy HIPAA , PCI-DSS and other compliance while achieving comprehensive enterprise security. The ROI by implementing CounterSnipe for network security is often very attractive due to the software licensing model we offer.

CounterSnipe tops it all up by offering free of charge installation, configuration and on-going management services.



CSC is a global leader in providing technology-enabled business and government solutions and services. Leveraging our 50-year legacy of supporting the government and commercial best practices, CSC's North American Public Sector unit works closely with the federal, state and local government health and human services organizations to provide the solutions that achieve their missions and improve the quality of government services to citizens. CSC innovates with next-generation technologies such as cloud computing, big data analytics, shared services, mobility, cybersecurity and application modernization.



Air Force Research Laboratory Information Directorate/Griffiss Institute/Cyber Research Institute/CYBER NY Alliance

Air Force Research Laboratory Information Directorate at the Griffiss Business & Technology Park, Rome, NY has the mission to explore, prototype and demonstrate high-impact, game changing Command, Control, Communications, Computers, and Intelligence (C4I) and Cyber science technologies that enable the Air Force and Nation to maintain its superior technical advantage. AFRL is partnered with Griffiss Institute, the NYS Cyber Research Institute and the CYBER NY Alliance to transfer the technologies, in particular cyber security to other domains including financial, infrastructure and health care and to develop the CNY high tech-ecosystem. For more information, go to www.cybernyalliance.org



Recognized as an industry leader by top analysts, Dell SecureWorks provides world-class information security services to help higher education, local and state institutions of all sizes protect their IT assets, comply with regulations and reduce security costs.



DynTek, Inc. provides professional IT consulting services, end-to-end IT solutions, managed IT services and IT product sales to mid-market commercial businesses, state and local government agencies, and educational and healthcare institutions. At DynTek, we specialize in architecting solutions beyond any single vendor or subsystem. We design, build, operate and support cloud solutions that encompass our client's entire infrastructure - from the data center to the desktop. From virtualization and cloud computing to unified communications and collaboration, DynTek architects professional technology solutions across the core areas of your technical environment: Infrastructure/Data Center, Microsoft Platforms and End Point Computing.



"Excelsior College is a private, regionally accredited, nonprofit institution of higher education that began as part of the State University of New York. For the past forty years our purpose has been to award college credit to adults for confirmed subject knowledge, no matter how it was learned. Excelsior provides accessible online instruction and supported independent study options such as credit by exam for degree-seeking adults around the world."



FireEye protects the most valuable assets in the world from those who have them in their sights. Our combination of technology, intelligence, and expertise — reinforced with the most aggressive incident response team — helps eliminate the impact of security breaches. We find and stop attackers at every stage of an incursion. With FireEye, you'll detect attacks as they happen. You'll understand the risk these attacks pose to your most valued assets. And you'll have the resources to quickly respond and resolve security incidents. The FireEye Global Defense Community includes over 3,100 customers across 67 countries, including over 200 of the Fortune 500. For more information, please visit www.FireEye.com.



As consumer technology evolves, constituents demand more convenient access to government services. First Data helps federal, state, and local agencies deliver the same high levels of service as private industry while ensuring security and controlling costs.

For more than 25 years, we've helped governments plan, procure, and manage IT projects that support health care, human services, tax, transportation, labor, education, criminal justice, and public safety. Whether it's making payments such as benefits and payroll or receiving payment for taxes, licenses and other government services, First Data handles all your payment processing needs with safe, secure and reliable solutions.



GreyCastle Security is a cybersecurity consulting firm focused on risk management, awareness and operational security. Our company was established to counter rapidly evolving cybersecurity threats and manage risks in people, process and technology. GreyCastle Security is comprised exclusively of highly certified professionals with prior security experience in healthcare, education, retail and gaming. Our team members are all former CISOs, ISOs, security specialists and operators. We bring a client perspective to everything we do.

We provide assessments, training, testing and response capabilities to organizations of all sizes, types and industries. We bring passionate practicality to cybersecurity.

Visit us at www.greycastlesecurity.com for more information, and let GreyCastle Security redefine cybersecurity for you.

Interface Masters

TECHNOLOGIES

Innovative Network Solutions

Interface Masters Technologies is a leading vendor in the network monitoring and high speed networking markets. Based in the heart of the Silicon Valley, Interface Masters' expertise lies in Gigabit, 10 Gigabit and 40 Gigabit Ethernet network access and network connectivity solutions that integrate with monitoring systems, inline networking appliances, IPS, UTM, Load Balancing, WAN acceleration, and other security appliances. Flagship product lines include hardware load-balancers, specialized 10GE internal server adapter cards, switches, 10 Gigabit external intelligent Network TAP and Bypass and failover systems that increase network visibility capabilities, network reliability and inline appliance availability. <http://www.interfacemasters.com/>



iSECURE is a woman-owned, IT Security company based in upstate New York. Founded in 1995 as an ISP, iSECURE has extensive knowledge and practice in information technology, and has evolved into being experienced and trusted IT Security Solutions Provider, partnering with cutting-edge manufacturers and security experts in the community.

Our engineers hold a CISSP certification or are manufacturer-certified on our current solutions. Our staff is not only trained to install and support the technologies that we offer, but is also skilled and experienced in multiple facets of IT Security services, ranging from penetration testing and vulnerability assessments to end-user-awareness training.



On April 1, 2015 MAC Source was proud to announce our merger with our affiliate, Meridian IT. Our new name reflects our commitment to the future of your business. As Meridian IT, we offer an increased portfolio of products, services, and financial options to help your business reach new levels of performance. Through collaborative consulting and solution driven technologies, we can help your business grow, mitigate risk, enhance workforce productivity, and reduce costs. Discover our new combined company at www.meridianitinc.com

- Cloud Service • Data Center • Security & Risk Management • Unified Workspace•



NYSTEC is a vendor-neutral, independent advisor to clients. We understand that security is not a product but rather a process that must address threats with multiple layers of controls. We have in-depth experience with Federal and NYS government regulations and policies and are uniquely positioned to help you develop a layered security strategy that will increase the integrity, confidentiality and availability of your IT systems. Information security must be a continuous effort encompassing policy, process, procedure, education, monitoring and enforcement to address evolving threats. NYSTEC can help you secure your networks and systems.



The Cyber Security and Information Systems Information Analysis Center (CSIAC) is a Department of Defense (DoD) Information Analysis Center (IAC) sponsored by the Defense Technical Information Center (DTIC). It performs the Basic Center of Operations (BCO) functions necessary to fulfill the mission and objectives applicable to the DoD Research, Development, Test and Evaluation (RDT&E) and Acquisition communities' needs. These activities focus on the collection, analysis, synthesizing/processing and dissemination of Scientific and Technical Information (STI). It leverages best practices and expertise from government, industry, and academia on cyber security and information technology. The CSIAC is operated by Quanterion Solutions Incorporated. www.quanterion.com



Our Mission: To provide cost effective secure environmental solutions for idle, obsolete and non-working high technology products; while emphasizing environmentally sound processing methods for maximizing value and recovery while minimizing and/or eliminating disposal of electronics in landfills. www.ewaste.com



The Sage Colleges is a dynamic institution of higher education with more than 3,000 students enrolled in bachelor's, master's, and doctoral programs on two campuses located in Albany and Troy, N.Y., as well as through online programs.

Sage College of Albany offers their BS in Information Technology and Cybersecurity through Russell Sage Online. The program trains students to be practitioners in the field of cybersecurity, and prepares students for successful careers as security analysts, intrusion detection specialists, cryptologists, cryptanalysts, vulnerability assessors and related IT careers. The Certificate in Cybersecurity and the Certificate in Information Technology are both offered online as well.



SANS is the most trusted source for information security training and security certification. SANS provides intensive, immersion training designed to help your staff develop the skills necessary for defending systems, networks, and software against the most dangerous threats. SANS offers more than 40 courses that address both security fundamentals and awareness, and the in-depth technical aspects of the most crucial areas of IT security. Training can be taken in a classroom setting in cities around the world, self-paced, or over the Internet. SANS partnership programs offer state and local government and higher education institutions affordable training options to improve their security posture. www.sans.org



Splunk Inc. (NASDAQ: SPLK) provides the leading software platform for real-time Operational Intelligence. Splunk® software and cloud services enable organizations to search, monitor, analyze and visualize machine-generated big data coming from websites, applications, servers, networks, sensors and mobile devices. More than 9,000 enterprises, government agencies, universities and service providers in over 100 countries use Splunk software to deepen business and customer understanding, mitigate cybersecurity risk, prevent fraud, improve service performance and reduce costs. Splunk products include Splunk® Enterprise, Splunk Cloud™, Splunk Storm®, Hunk®: Splunk Analytics for Hadoop and premium Splunk Apps. To learn more, please visit <http://www.splunk.com/company>.



Utica College offers regionally accredited Online Bachelor's and Master's degrees in Cybersecurity and Cyber Policy with concentrations in Intelligence, Investigations, Computer Forensics, Cyber Operations, and Information Assurance taught by highly experienced faculty. The NSA and DHS have designated Utica College as a National Center of Academic Excellence in Information Assurance/Cyber Defense Education (CAE IA/CD) for academic years 2014-2019. With the renowned Economic Crime & Cybersecurity Institute, and the Center for Identity Management and Information Protection, the College collaborates with industry and government to develop innovative curriculum and provide students with unique credentials and career opportunities. Call 315-732-2640 or visit <http://programs.online.utica.edu/programs/> for more information.



Securing your data and network is a bigger, more challenging, and more critical job than ever. Expert guidance can help you achieve your unique security requirements. Vandis has assembled a team of architects and engineers with broad experience, extensive training, and reliable judgment to provide you with the assistance you need.

Our professional services team will work alongside your organization, from Design Consultation through Implementation and Support to ensure that you achieve your goals. Vandis' high-level relationships and expertise with both market leading and specialty security products allow us to always act as your trusted advisor.

Securing production environments requires a full understanding of the infrastructure behind them. Headed up by top-echelon architects and staffed with experienced engineers, our network, mobility, cloud, and virtualization practices are focused on helping our clients build secure and stable systems.

36 | Conference Co-Hosts

Deborah Snyder

Deputy Chief Information Security Officer
NYS Office of Information Technology Services
Enterprise Information Security Office

Deborah A. Snyder serves as Deputy Chief Information Security Officer (CISO) for the New York State Office of Information Technology Services (ITS). In her role, she directs the Enterprise Information Security Office's comprehensive governance, risk management and compliance program. She is responsible for providing strategic leadership and vision, and assuring business-aligned, risk-based investments to maximize business opportunity and minimize risk.

Ms. Snyder has extensive experience in government program administration, information technology and cyber security policy. She is a recognized industry thought-leader and active contributor to the security profession. She serves on the NYS Forum Board of Directors, and is a member of the Project Management Institute, InfraGard, Information Systems Security Association (ISSA), Information Systems Audit and Control Association (ISACA), and the Institute of Internal Auditors (IIA). She has published numerous articles, and co-authored the book entitled "SECURE – Insights From The People Who Keep Information Safe," which offers industry leadership insights and perspective. She has been recognized for excellence in government services and outstanding contributions to the field of cyber security. She is a highly regarded speaker on topics critical to executive-level business and IT professionals.

Sue R. Faerman

Dean of the College of Computing and Information
University at Albany, State University of New York

Sue Faerman is Dean of the College of Computing and Information at the University at Albany, State University of New York. As Dean, Faerman serves as the chief administrative and academic officer of the College, which hosts a variety of academic and research programs related to computing and information. In addition to traditional computer science and an information science program that is accredited by the American Library Association, the College is home to an innovative Informatics department that partners with other units on campus to offer interdisciplinary programs related to computing and information. This year the college launched a new BS in Informatics degree, which includes an option for students to take their entire undergraduate degree on line. The College is affiliated with a number of nationally-recognized research centers at the University that investigate the use of information technologies in the regulation of financial markets, homeland security, and government.

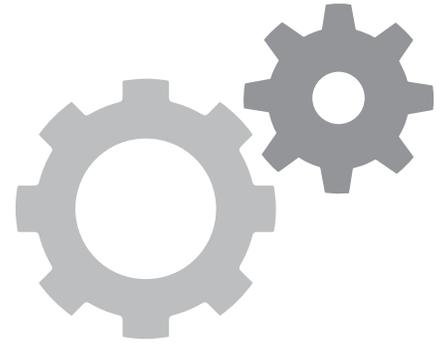
Dean Faerman is a Distinguished Teaching Professor in the Department of Public Administration and Policy at UAlbany and has served as Affiliate Faculty Member of the College of Computing and Information's Information Sciences Doctoral Program. Prior to being asked to serve as interim dean, Faerman served for 14 years as UAlbany's Vice Provost for Undergraduate Education. Her teaching and research interests are in managerial leadership, focusing particularly on the paradoxical elements of leadership performance, and on how individuals working in professional, scientific and technical fields make the transition from being an individual contributor to being manager. More recently, she has focused her research on issues related to women and leadership, and she currently serves as the Academic Chair of the University's Center for Women in Government & Civil Society's Women's Leadership Academy. Faerman received her B.S. in Applied Mathematics and Statistics from Stony Brook University, her M.S. in Applied Mathematics, with a Statistics concentration, from George Washington University, and her Ph.D. in Public Administration from UAlbany.



Donald Siegel

Dean of the School of Business and
Professor of Management
University at Albany, State University of New York

Dr. Donald Siegel is Dean of the School of Business and Professor of Management at the University at Albany, State University of New York. He received his bachelor's degree in economics and his master's and doctoral degrees in business economics from Columbia University. He then served as a Sloan Foundation post-doctoral fellow at the National Bureau of Economic Research. Don has taught at SUNY-Stony Brook, Arizona State University, the University of Nottingham, RPI, where he was Chair of the Economics Department, and the University of California-Riverside, where he served as Associate Dean for Graduate Studies. Dr. Siegel is an editor of *Academy of Management Perspectives*, *Journal of Management Studies*, and the *Journal of Technology Transfer*, an associate editor of the *Journal of Productivity Analysis*, and serves on the editorial boards of *Academy of Management Review*, *Academy of Management Learning & Education*, *Journal of Business Venturing*, *Corporate Governance: An International Review*, and *Strategic Entrepreneurship Journal*. He has also co-edited 38 special issues of leading journals in economics, management, and finance. Don was recently ranked #2 in the world for research on university entrepreneurship and #760 in the world among academic economists. He has published 105 articles and 10 books on issues relating to university technology transfer and entrepreneurship, the effects of corporate governance on performance, productivity analysis, the economic effects of gambling, and corporate and environmental social responsibility in leading journals in management, economics, and finance. His most recent books is the *Chicago Handbook of University Technology Transfer and Academic Entrepreneurship* (University of Chicago Press). He has received grants or fellowships from the Sloan Foundation, NSF, Kauffman Foundation, NBER, American Statistical Association, W. E. Upjohn Institute for Employment Research, and the U.S. Department of Labor. He has also served as a consultant or advisor to the UN, the National Research Council (NRC), the Council on Competitiveness, the U.K., Italian, and Swedish governments, the Department of Justice, the Environmental Protection Agency, Chase Manhattan, Securities Industry Association, Morgan Stanley, Goldman Sachs & Co, Deloitte and Touche, and the National Association of Manufacturers. He is chair of the NRC Committee on "Best Practice in National Innovation Programs for Flexible Electronics" and an advisor to the NRC on the Small Business Innovation Research (SBIR) Program.



**Please remember to complete
the Conference survey at
[https://www.surveymonkey.com/s/
NYSCSeval15](https://www.surveymonkey.com/s/NYSCSeval15)**



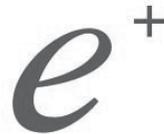
Terabyte Sponsor



Megabyte Sponsor



Kilobyte Sponsors



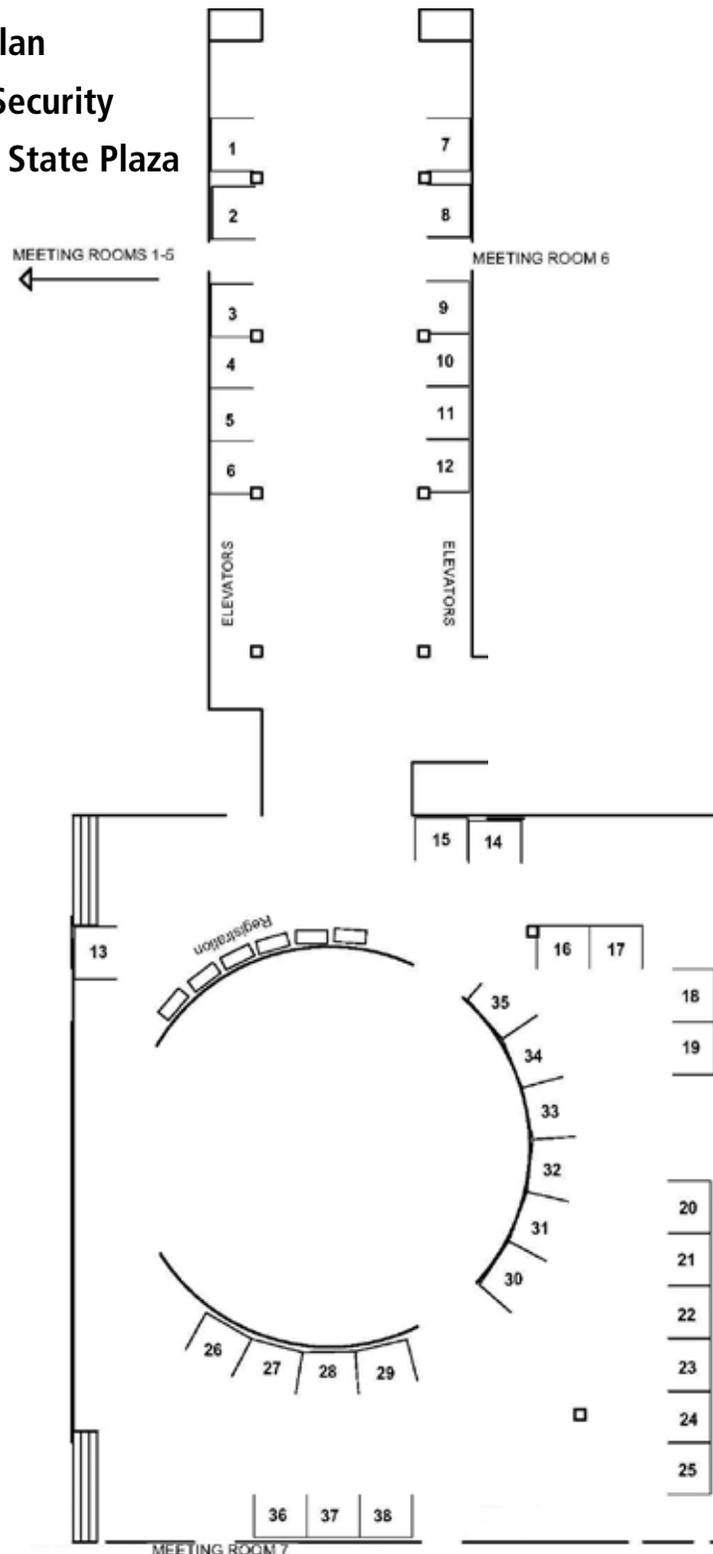
PRESIDIOTM
Practical thinking for a connected world.



Booth Assignments:

- 1 Core Security
- 2 SANS Institute
- 3 NYSTEC
- 4 Interface Masters
- 5 Vandis
- 6 Splunk
- 7 Griffis Institute/ CYBER NY Alliance
- 8 Griffis Institute/ CYBER NY Alliance
- 9 CSC
- 10 Quanterion
- 11 University at Albany
- 12 The NYS Forum, Inc.
- 13 NYS Office of Information Technology Services
- 14 **Cisco** (Megabyte Sponsor)
- 15 **Cisco** (Megabyte Sponsor)
- 16 **Tanium** (Kilobyte Sponsor)
- 17 GreyCastle Security
- 18 CenturyLink
- 19 Bay Path University
- 20 Regional Computer Recycling & Recovery (RCR&R)
- 21 **ePlus Technologies** (Kilobyte Sponsor)
- 22 **Symantec** (Kilobyte Sponsor)
- 23 Brite Computers
- 24 Excelsior University
- 25 iSecure
- 26 Bit9
- 27 Utica College
- 28 Meridian
- 29 Dyntek Services
- 30 **Presidio** (Kilobyte Sponsor)
- 31 FireEye
- 32 Dell SecureWorks
- 33 **AT&T** (Terabyte Sponsor)
- 34 **AT&T** (Terabyte Sponsor)
- 35 **AT&T** (Terabyte Sponsor)
- 36 First Data
- 37 Counter Snipe
- 38 Sage College

Floor Plan Cyber Security Empire State Plaza



Passport Drawing: Visit our participating sponsors (Tanium, Presidio, ePlus Technologies, Symantec) and these exhibitors (DELL, Brite Computers, Bay Path University) for a chance to win! All you need to do is bring the Exhibitor passport to the listed booths and have it stamped, it's that easy! Once the passport is stamped please bring it to the registration table. Drawings will be held on Tuesday, June 2 – 3:10 p.m. - 3:20 p.m. and Wednesday, June 3 – 1:30 p.m. - 1:40 p.m. Prizes must be picked up by the end of the day.

