

NEW YORK STATE  
CYBER SECURITY CONFERENCE

JUNE 4-5, 2013

HELPING NAVIGATE STORMY SEAS



[WWW.DHSES.NY.GOV/GO/CONFERENCE2013](http://WWW.DHSES.NY.GOV/GO/CONFERENCE2013)

TERABYTE SPONSOR



PRESENTED BY



[WWW.ITS.NY.GOV](http://WWW.ITS.NY.GOV)



[WWW.NYSFORUM.ORG](http://WWW.NYSFORUM.ORG)



UNIVERSITY  
AT ALBANY  
State University of New York

[WWW.ALBANY.EDU/IASYMPIUM](http://WWW.ALBANY.EDU/IASYMPIUM)

## Our network is your network.

Security is the most important priority with cloud services delivered on the AT&T network.

In here, state and local governments can count on AT&T's legendary reliability to provide both security and access, making it easy to implement new services and applications.

At AT&T we strive to deliver some of the world's most comprehensive cloud solutions, in ways that work for you and your budget.

In here, we share the same concerns because we share the same network.

To learn more about best practices in cloud security, hear from our experts at: [att.com/securecloud](http://att.com/securecloud)

CAUTION

CONFIDENCE

Rethink Possible®



# Welcome

3

June 4, 2013

## Dear Colleague:

On behalf of the New York State Office of Information Technology Services, Enterprise Information Security Office, the University at Albany, State University of New York and The NYS Forum Inc., we welcome you to the 16th Annual NYS Cyber Security Conference. This year's theme, *Helping Navigate Stormy Seas*, focuses on security challenges facing today's security professionals, businesses, and citizens, and the proactive steps to mitigate cyber risk. The Conference brings you the latest information on cloud security, mobility issues, technology solutions, reports and research, public-private partnerships, workforce and legal issues, incident response, and other topics.

Today, the Conference begins with *Recommended Cyber Actions for Large Enterprises: An Industry Perspective* keynote by Michael Papay, Vice President of Information Security and Cyber Initiatives for Northrop Grumman's Information Systems sector. He leads the company's strategy development to advance the company's leadership role in the cybersecurity community. Dr. Papay also serves as Northrop Grumman's Chief Information Security Officer, delivering Northrop Grumman's internal information security program.

The 8th Annual Symposium on Information Assurance (ASIA '13) will run concurrently with the main conference and present academic papers on information security topics by academic experts. On Wednesday, the day will begin with ASIA's keynote Billy Rios of Cylance. Mr. Rios returns to speak about *Why Every CSO Needs to Know Industrial Control Systems ICS*.

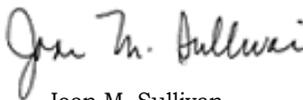
The Conference offers 48 training sessions designed for a broad audience and provides a forum to learn about emerging information security trends and solutions. The event features dynamic sessions from industry leaders, along with networking opportunities to facilitate knowledge sharing, as we all strive to enhance our cyber security posture. An Exhibit Hall featuring displays from security focused companies, including sponsors of this Conference, will also be available on site. Stop by the *NYS Kids Safe Online Cyber Security Awareness Poster Contest* display to view the winning Kindergarten through Grade 12 posters. We are very proud of all the contestants!

Thank you for your service and commitment to *Helping Navigate the Stormy Seas* in the ever-changing world of cyber security threats and attacks. Enjoy the Conference!

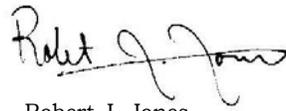
Sincerely,



Brian Digman  
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



# 4 Conference Partners

## Brian Digman

### **NYS Chief Information Officer**

### **New York State Office of Information Technology Services**

Brian Digman was named NY State Chief Information Officer (NYS CIO) and head of the Office of Information Technology Services (ITS) on January 16, 2013. ITS was created as part of the 2011-12 Budget to make government more efficient and effective by streamlining IT services in a single agency. Recently, approximately 3,500 professionals from over 37 agencies were consolidated into the new ITS. ITS will provide innovative ideas to help agencies solve problems and improve service delivery to their customers.

For nearly 10 years, Mr. Digman served as the CIO for the New York State Department of Taxation and Finance. In April 2012, Mr. Digman was named the NYS CIO of the Year by Government Technology Magazine. Mr. Digman also held positions with the former New York State Office for Technology as the Director of Enterprise Applications and Assistant Deputy Director of Operations. His experience includes a broad range of proficiencies in systems development, managerial innovation, large scale operations, and public administration. Mr. Digman entered state service in 1986 as an applications programmer for the Tax Department. He recently retired with over 30 years of honorable service in the United States Coast Guard Reserve as a Marine Science Technician - Master Chief, E9. He is a graduate of the New York State University of Albany.

## Robert J. Jones

### **President**

### **University at Albany, State University of New York**

Dr. Robert J. Jones was appointed by the State University of New York (SUNY) Board of Trustees on September 12, 2012 as the 19th president of the University at Albany. Previously, Dr. Jones had served as senior vice president for academic administration at the University of Minnesota System since 2004. Prior, Dr. 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, Dr. Jones has more than three decades of higher education leadership experience as well as academic expertise spanning plant physiology and urban and international development. He 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 focuses on the role of cytokinins in stabilizing grain yields of maize against environmental stresses and global climate change. Over 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.

Dr. Jones currently serves as Regional Council Co-Chair for the Capital Region Economic Development Council (CREDC) alongside Albany Medical Center President James J. Barba. He is a fellow of both the American Society of Agronomy and the Crop Science Society of America. He has been a visiting professor and featured speaker in North America, Europe, Asia and Africa, and from 1984 to 1994 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).

Dr. 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. Currently, he serves on the boards of the Coalition of Urban Serving Universities and the Bush Foundation, among other leadership roles. He was also a member of the Grammy award-winning Sounds of Blackness, a Twin Cities-based choral ensemble.

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

## 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.

## Fran Reiter

### **Executive Deputy Director of State Operations**



Following a 15-year career as a marketing executive in the television industry, Fran Reiter served as NYC Deputy Mayor for Planning and Community Relations and, subsequently, for Economic Development and Planning during Mayor Rudolph Giuliani's first term. Her many accomplishments include authoring and overseeing the implementation of the Lower Manhattan Revitalization Plan, negotiating passage by the City Council of the citywide Adult Use Rezoning, negotiating the community agreement that led to the first Williamsburg rezoning, founding the Crown Heights Mediation Center, and the restructuring of the Division of AIDS Services. She left government service to run Mayor Giuliani's successful 1997 re-election campaign then returned to the private sector, serving as President and CEO of the NYC Convention and Visitors Bureau (now NYC & Company) and Executive Director of the Joseph Papp Public Theater/NY Shakespeare Festival. In 2002, Ms. Reiter founded Reiter Consulting which then merged with MSB Strategies to form Reiter/Begun Associates, LLC. She served as the firm's managing partner and provided government relations, strategic advisement and nonprofit management consulting services to an array of businesses and nonprofit organizations. In 2011, Reiter/Begun merged with J. Adams Consulting to form The Reiter/Giuliani Group, LLC. In November 2012, Ms. Reiter returned to public service to serve in the administration of Governor Andrew M. Cuomo as Executive Deputy Director of State Operations.

## Kids Safe Online

Visit the New York State Kids Safe Online K-12 Cyber Security Awareness Contest Posters' display in the Northeast Gallery to view the 2012 winning Kindergarten through Grade 12 posters. We are very proud of all the contestants!



# 6 Keynote

June 4, 2013

Convention Hall

9:00am-10:30am

## Michael Papay

**Vice President and  
Chief Information Security Officer**

**Northrop Grumman Information Systems**



Michael Papay is vice president of Information Security and Cyber Initiatives for Northrop Grumman. He leads the company's cyber strategy development to advance the company's leadership role in the cybersecurity community. Dr. Papay also serves as Northrop Grumman's chief information security officer (CISO), delivering Northrop Grumman's internal information security program. In this role, he is responsible for strategy and vision for the company's global computer and network information security systems; defining companywide policies for information security; and enhancing the security of Northrop Grumman's products, services and infrastructures.

Dr. Papay has 27 years of experience with Northrop Grumman developing engineering solutions for the Department of Defense and intelligence community, including intercontinental ballistic missiles; missile defense systems; command and control systems; networking solutions; satellite and ground systems; airborne intelligence, surveillance and reconnaissance platforms; modeling and simulation programs; and military training tools.

Dr. Papay is a nationally recognized expert in the modeling and simulation (M&S) field. He has written numerous papers, managed large programs, developed coursework and contributes to the congressional M&S caucus. He served on the 2012 Homeland Security Advisory Council's (HSAC) Task Force on Cyber Skills and he is also on the Advisory Board for the George Mason University Volgenau School of Engineering.

Dr. Papay has a bachelor's degree and a doctorate in aerospace engineering from Virginia Tech.

Presentation:

### **Recommended Cyber Actions for Large Enterprises: An Industry Perspective**

Most large enterprises now understand the basic cyber threat landscape and find they are faced with an array of choices about integrating technology, implementing cyber defense tools, finding and keeping a qualified workforce, and defining corporate processes for topics from incident response to breach reporting. Michael Papay, Chief Information Security Officer for Northrop Grumman, will provide a perspective from the Aerospace and Defense Industry on lessons learned from setting up their internal information security program as well as tailoring cyber solutions for customers. Seeking to answer the question "What action can I take right now to get ahead of the cyber threat?" this keynote address will cover the above topics, as well as appropriate business models to consider as enterprises securely move towards cloud and mobile.



Tweet the Conference at #nyscyber

# ASIA Keynote 7

June 5, 2013

8:30am - 10:00am

Convention Hall

## Billy Rios

**Director of Consulting**

**Cylance**

Billy Rios is currently the director of consulting at Cylance and is the Chair of the Operational Security Testing panel at the NBISE. Previous to this, he was a Team Lead for Google where he studied emerging security threats and technologies. Billy was one of the primary security engineers for Google Plus, the new social network by Google. Before Google, Billy was a Security Program Manager at Microsoft where he helped secure several high profile software projects including Internet Explorer and Microsoft Online. Prior to his roles at Google and Microsoft, Billy was a penetration tester for various consulting firms.

Before his life as a penetration tester, Billy worked as an Information Assurance Analyst for the Defense Information Systems Agency (DISA). While at DISA, Billy helped protect Department of Defense (DoD) information systems by performing network intrusion detection, vulnerability analysis, and incident handling. Before attacking and defending information systems, Billy was an active duty Officer in the United States Marine Corps where he served as an OIC, Platoon Commander, and Company Executive Officer.

Billy is an accomplished public speaker and published author. He has authored and contributed to several books, most notably: "Hacking: The Next Generation" and "Inside Cyber Warfare: Mapping the Cyber Underworld", both published by O'Reilly Media. Billy has also presented at such prestigious security conferences as Black Hat, RSA, NATO CCDCOE, Microsoft's Blue Hat, DEFCON, ToorCon Seattle, and HITB Security conference. Billy is cited in numerous security advisories for research on attacking Industrial Control Systems, URI and protocol handlers, content ownership issues (such as the GIFAR attack), DNS rebinding attacks (against Flash and the Java Virtual Machine), and was previously credited for discovering vulnerabilities in Microsoft Windows and Adobe PDF Reader.



**Presentation:**

### **Why Every CSO Needs to Know Industrial Control Systems (ICS.)**

Industrial Control Systems (ICS) have introduced tremendous cost savings by automating some of the enterprise's most critical operations. Do you understand the systems that support your critical data centers and corporate campuses? Do you understand the risks associated with these technologies? Every data center large building, and corporate campus around the world plays host to environmental controls, building entry systems, safety systems, and many other automation systems that are considered ICS. In many industries these systems are a vital component to the enterprises most critical business operations. Given the complexity and specialization of these systems, many of these systems are managed and operated outside of the traditional IT sphere, leaving traditional vulnerability and risk management programs blind to their existence and the risk associated with these systems. Many of these systems are even managed and maintained by external third parties, providing a backdoor to your corporate network and hence represent a new weakest link in enterprise information security. Using the experience of a team with wide experience in critical infrastructure this session talks about strategies for understanding risk and implementing mitigating controls which need to be used to protect these vital systems.

Please remember to complete the Conference survey at  
<https://www.surveymonkey.com/s/NYSCSC13eval>



# 8 Legal Issues / Reports & Research

Tuesday June 4, 2013 – Day One

## Legal Issues Track

### 2012: The Year High Courts Get Involved in Tech Privacy Law and Make a Mess of IT

Steve Treglia  
Absolute Software Corporation

11:00am - 11:50am

Meeting Room 6

Higher-level courts have historically shied away from addressing issues having to do with the privacy of electronic communications. Starting with the U.S. Supreme Court's decision on law enforcement's use of GPS tracking issued in January of 2012, *United States v. Jones*, it appears that trend may be coming to an end. That does not mean, however, that the law is getting any clearer in this area or that the courts are starting to provide definitive and reliable precedent. For even where there was a unanimous ruling in favor of suppression, as in *Jones*, the way the Supreme Court Justices reached that ruling resulted in the issuance of three separate concurring opinions from as varied a range of interpretations as can be possibly imagined.

This lecture will analyze the major cases issued in this area by high courts in 2012 after tracing some of the history of communication privacy law which will allow these 2012 decisions to be placed in a proper historical context. Those attending this lecture may very well leave with the opinion currently held by the lecturer that just because the highest level of the judiciary is beginning to weigh in on these issues, we are still a very long way from having any clear and reliable precedent.

### From ".gov" to the Private Sector: Federal Efforts in Securing Cyber Space: 2.0

Bradley Schreiber  
Applied Science Foundation for  
Homeland Security

1:00pm - 1:50pm

Meeting Room 6

This presentation will be an update to last year's that focused on the current state of cyber, from a Federal government perspective, give an update on the current legislation and what action, if any, the White House will be taking. We will discuss, among other things, which Federal agencies have jurisdiction over the public, private and critical

infrastructure networks; ongoing challenges the Federal government faces in securing their own information technology systems and the Internet; jurisdictional battles within the government; cyber security legislation being considered by Congress; and, what role the private sector has/or will have in securing their networks.

### Data Tagging, Redaction, and the Future of Automated E-Discovery

Elton Juter  
Symantec Corporation

2:10pm - 3:00pm

Meeting Room 6

E-discovery technologies are getting smarter -- and not a moment too soon. Immense accumulations of electronically stored information (ESI) have made the efficient identification, preservation and collection of state data for legal discovery requests incredibly valuable -- yet exceedingly difficult to achieve. Compared to traditional paper files, today's electronic data stores are enormous and quite easily corrupted. States need solutions to keep pace with the information explosion. Is automation this answer? This session will explore how New York State can best achieve robust, future-proof e-discovery strategies through automation -- and how automated e-discovery can streamline the discovery process while reducing cost, time and complexity.

### Social Media and Cloud Computing: Global Threats to Privacy, Security & Liberty

Raj Goel  
Brainlink International, Inc.

3:20pm - 4:15pm

Meeting Room 6

Updated for 2013 - New case studies from 2012-2013. Social Media has quickly woven itself into the very fabric of everyday life. This boom in sharing, even the most banal of details, has had a resounding impact on how our children, employees and colleagues communicate. Using case studies from the US and around the world, we'll examine how people have lost jobs, college admissions, college degrees, fortunes and freedom through (un) social media. We'll also investigate the rampant OVERCOLLECTION of customer and subscriber data by major corporations and governments. We'll also discuss some strategies and steps we can take to protect civil liberties and privacy in the age of Social Media.

## Reports and Research Track

### You've Been Hacked, Now What?

Reg Harnish  
GreyCastle Security

11:00am - 11:50am

Meeting Room 1

The pace of databreaches 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. Developing and maintaining an effective Incident Response plan and team has never been more important.

This session will present an in-depth look at several recent databreach victims and how their incident response processes led to effective business resumption or epic failure. Attendees will learn best practices for incident response, from law enforcement, forensics and legal considerations to compliance and public relations.

### The Intersection of Cyber Security and Public Opinion: from Small Business Owners to Investors

John Zogby  
Zogby Analytics

1:00pm - 1:50pm

Meeting Room 1

Small Businesses form the backbone of the U.S. economy, yet many are not prepared for the ever changing cyber security landscape. At the same time k-12 teachers are struggling with being able to teach students about the cyber related risks they face daily. The rapidly changing cyber security threat levels are confusing many home users, resulting in many users doing nothing to protect themselves. As if that wasn't enough, now investors are making financial decisions based on the cyber security measures a company is taking.

The majority of small business owners believe Internet security is critical to their success and that their companies are safe from ever increasing cyber security threats even as many fail to take fundamental precautions, according to a new survey of U.S. small businesses sponsored by Symantec and

the National Cyber Security Alliance and conducted by Zogby Analytics. Highlights from the study include:

- A majority of Small Business owners think they're cyber secure. 40 percent of Small Businesses have suffered a security breach Surprisingly Small Businesses are unconcerned about some potentially nasty cyber attacks.
- There is a notable disconnect among teachers, administrators, and IT specialists when it comes to the success of cyber education as well as a school district's cyber education requirements.
- Findings from home user research have provided revealing insights into how digital shopping practices and behaviors have impacted online safety and the nation's collective digital infrastructure. Nearly one in five Americans report being a victim to a crime that was committed over the Internet.

The new survey shows that today's investors are more educated about the damage cyberattacks can cause to a company's brand and financial bottom line. The high cost of cyberattacks cannot be understated. While it is the consumer data breaches that are in the headlines, it is the lack of concern for intellectual property theft that shows the need for broader education about the financial risk IP theft poses to companies. The ongoing theft of trade secrets and other sensitive data is resulting in billions of dollars in lost revenue.. A new cyber security survey will be conducted to track finds from previous studies.

## 2013 Global Security Report Abstract

*Jonathan Spruill  
Trustwave SpiderLabs*

2:10pm - 3:00pm

Meeting Room 1

Today, organizations need to not only understand current trends in security threats, but also be able to identify inherent vulnerabilities within existing systems. In 2012, Trustwave tested, analyzed and discovered the top vulnerabilities and threats that have the most potential to negatively impact organizations.

What we found will show you that businesses around the world face many of the same issues – from uneducated employees, to poor breach self-detection, to threats that are purpose-built for the mobile device explosion.

Highlighting the top data security risk areas, this presentation also offers analysis on perceived

trends and tactical and strategic pursuits to help any organization reduce data security threats in 2013 and beyond.

## Investigative Response and the 2013 Data Breach Report

*Chris Novak  
Verizon Enterprise Solutions*

3:20pm - 4:15pm

Meeting Room 1

The Data Breach Report is an Internationally recognized report that brings together statistics and findings from worldwide investigative response organizations such as the Dutch National High Tech Crime Unit, the US Secret Service, the Australian Federal Police, Irish Reporting and Information Security Service and Police Central e-crime unit. Chris Novak is Managing principal on the Verizon Investigative Response team and a contributing author to the Data Breach report and is knowledgeable regarding data breaches, cyber crime and investigations world-wide.

## State Government Track

### State Governments at Risk: A Call for Collaboration and Compliance

*Moderator: Srin Subramanian  
Deloitte & Touche LLP*

*Panelist: Thomas D. Smith, NYS Office of  
Information Technology Services*

11:00am - 11:50am

Meeting Room 2

A presentation of the findings and analysis the 2012 Deloitte-NASCIO Cybersecurity Study, a survey of State Chief Information Security Officers conducted by National Association of State Chief Information Officers (NASCIO), with additional perspectives on the impact of President Obama's cybersecurity Executive Order signed on Feb. 12th.

The first half will highlight the results of the second biennial 2012 Deloitte-National Association of State Chief Information Officers (NASCIO) Cybersecurity Study, which was conducted in the summer of 2012. The study assessed the security of state digital data and cyber assets administered by state chief information security officers (CISOs). CISOs from 48 states, and two US territories, participated in

the survey. 63 business official stakeholders from a broad cross-section of states responded to a parallel survey. The study addresses the challenges that states and chief information officers (CIOs)/CISOs face in protecting states' critically important systems and data. The survey results call for a greater collaboration among state CIOs/CISOs and business/program leadership of the executive branch agencies and elected officials. A copy of the study can be found at <http://www.nascio.org>.

The second part of the discussion will take a state-level view of the recently issued Executive Order and its implications for New York State. State homeland security and related agencies will play a pivotal role, given their oversight and regulation of transportation (e.g., mass transit, highways, bridges, airports), health (e.g., disease management, health information exchanges), public safety (e.g., emergency management, law enforcement) and utilities (e.g., nuclear, power, and chemical plants). However, without Federal funding, there will be a financial impact. During the session, we will provide different perspectives on the national framework, what New York agencies need to do in response, and what potential funding opportunities are available.

### Securing the Mission of Government: Prevention Rather than Reaction to the Cyber Threat

*Moderator: Slawomir Marcinkowski, NYSTEC*

*Kishor Bagul and Deborah A. Snyder, NY  
State Office of Information Technology  
Services.*

*Dr. Kamal T. Jabbour, Information Assurance,  
Information Directorate, Air Force Research  
Laboratory, Rome, NY*

1:00pm - 1:50pm

Meeting Room 2

A panel presentation and discussion with participants from the NYS Information Technology Services -- Enterprise Information Security Office, the Air Force Research Laboratory (AFRL) in Rome NY, the Griffiss Institute, and NYSTEC on cyber security threats and risks as seen from an organization (AFRL) that does world-class research in Cyber Operations and Security. The panel will discuss current approaches to confronting cyber threats, along with the perspective of the challenges faced by NYS. One of the major challenges faced by organizations, including NYS, is to ensure that the mission of government continues in the face of the ever-increasing cyber

# 10 State Government / IT Solutions I

threat. The new cyber paradigm is to prevent the “bad stuff” from happening rather than reacting to cyber threats after they occur. The panel will examine actions that organizations can take today to build a security program focusing on prevention rather than reaction by examining operational dependencies and mission vulnerabilities. The panel will look at critical NYS operations and functions and their dependence on cyber; the vulnerability of the cyber infrastructure to environmental and malicious disruptions, and the impact of these on critical services and functions; prioritization of critical infrastructure, and segmentation from office automation IT; increasing robustness, and reducing fragility to cyber disturbances; education (not to be confused with training) necessary to build a cyber-competent workforce.

## **A Moment in Time: An Outside-in Perspective of the Health and Welfare of State Government Cyber Infrastructure**

*Chris Coleman*  
*Lookingglass Cyber Solutions*

2:10pm - 3:00pm

Meeting Room 2

This session will explore the analysis, research and findings on global trends and threats that impact the networks and infrastructure associated with a collection of States Lookingglass evaluated. Chris will define and explain the research and analysis methodology, highlight the most prolific threats and vulnerabilities and demonstrate insight describing the overall wellness of state government infrastructure. This infrastructure includes the Enterprise network and supplier, provider and partner networks that make up each states cyber ecosystem. Specific details will be provided on infection rates, trends in attack patterns and assessments of how the States are responding to these threats.

## **Scalable Protocol-Based Packet Inspection for Advanced Network Threat Detection**

*Richard Lethin*  
*Reservoir Labs, Inc.*

3:20pm - 4:15pm

Meeting Room 2

Protocol-based packet inspection systems provide a means for advanced threat detection that can complement traditional string matching IDS. These

systems execute analytics written in cybersecurity domain-specific programming languages and in terms of protocol elements, and this allows for agile detection of attack behaviors that cannot be captured with string matching IDS. We will provide a quick tutorial on protocol-based packet inspection systems and their benefits for cyber security, and describe a system called R-Scope(R) that extends the open source Bro network security monitor with new analytics and that can employ advanced network processing electronics. R-Scope allows network security engineers to provide protection from evolving threats and at high network traffic rates. R-Scope is the result of Small Business Innovative Research (SBIR) performed by Reservoir Labs for the US DOE, with current installation and experimentation in DOE.

## IT Solutions Track I

### **Protection from DDoS Attacks: Observations and Protections**

*Brian Rexroad*  
*AT&T*

11:00am - 11:50am

Meeting Room 3

Distributed Denial of Service (DDoS) attacks are occurring more frequently. The attacks are getting larger and more sophisticated. Some attacks are intended to be disruptive, while others are focused on influencing our perception. For the unprepared, attacks can be crippling. This presentation will cover the latest trends seen in DDoS attacks and how organizations can prepare and protect their assets from the threat of DDoS attacks.

### **Information-Driven Cyber Security: “Why COTS Solutions Are Not Enough”**

*Bill Russell*  
*Northrop Grumman*

1:00pm - 1:50pm

Meeting Room 3

Enterprise security teams are confronted daily with a dizzying array of threats to the confidentiality, integrity and availability of the data, systems, and network infrastructures they are charged with protecting. A similarly complex eco-system of COTS security tools are available to address these threats. These COTS tools are widely available and implemented in large enterprise environments

by certified technicians supported by governance structures designed to deliver secure services and systems to corporate users. And yet, we regularly read about high-profile intrusions, data breaches, and attacks on companies who are technically sophisticated and have great public image and brand incentives to defend their systems. In government we are no longer surprised to read about breaches of government networks and loss of sensitive data (e.g., personally identifiable information, intellectual property). In fact, this problem is wider and deeper than what is publicly admitted to because government agencies and commercial companies often don't report (or publicize) these events. How is this possible with the availability of so much technology, security tools, and skilled personnel focused on combating these threats?

I believe there are three basic causes that each requires separate approaches to be successful: technology, security tools and skilled (and unskilled) people. So how do we stay ahead of those persistent adversaries who would do our data harm? What do we have to level the playing field? Fortunately, there are some things the good guys have at their disposal that can help.

### **Finding the Needle in a Stack of Needles**

*David Santeramo*  
*Logic Technology Inc.*

2:10pm - 3:00pm

Meeting Room 3

The goal of this presentation is to demonstrate that most organizations already possess the data that will help them head off security problems. Every device on the Internet today generates log data in some way. All you need to know how to do is collect and analyze the data so that it can be used to make effective decisions. You already have the data; this presentation will show you how to use it.

### **Enterprise Security on a Budget: Deciding What Gets Done First and What Doesn't Get Done At All**

*Kristine Briggs and Andy Hubbard*  
*Neohapsis, Inc.*

3:20pm - 4:15pm

Meeting Room 3

Whether you run a government IT organization, a non-profit, or an under-funded enterprise IT or security group, managing a broad range of

operational controls, emerging threats, and compliance requirements can be a hugely daunting task. Effective security requires a risk management mindset, so you are making appropriate budget trade-offs. Neohapsis' top consultants will revisit the most critical controls that make up your security program (which are not necessarily the most expensive ones), as well as the best practice tools, practices, and organizational approaches needed to provide practical protection against common and even advanced threats.

## Mobile Issues Track

### **Mobile SECURITY (not just MDM): Understanding the Real Risk**

*Eric Green*

*Mobile Active Defense*

11:00am - 11:50am

Meeting Room 4

A hype free discussion about where the real mobile risk lies. Where the threat is, how BYOD fits in, why so many 'solutions' are far from security to protect organizations against the perfect storm, and finally what's really happening out there as this market for mobile devices and mobile security matures. Then right back to the basics - managing the risk.

### **The BYOD (Bring Your Own Device) Wave: Policy, Security, and Wireless Network Infrastructure**

*Ken Kaminski*

*Cisco Systems*

1:00pm - 1:50pm

Meeting Room 4

This presentation will focus on the Bring Your Own Device Wave currently hitting all major enterprises and the required policy, security, and wireless network infrastructure changes needed to accommodate and securely absorb user owned wireless devices such as Apple iDevices such as iPads and iPhones along with Android devices. A basic model for BYOD absorption will be introduced. Topics include the needed changes to the wireless network infrastructure, device on-boarding technology including how Apple's Over-the-Air (OTA) functionality assists in this process, Mobile Device Management (MDM) agents, integration with existing authentication methods and device profiling, and how various functions such as device on-boarding, Radius AAA, device profiling, and

MDM agents are all stitched together in various vendor technologies using both proprietary and standards based methods such as Radius Change of Authorization.

### **Future Shock: How Mobility is Forcing Enterprises to Completely Rethink Security**

*Michael Sutton*

*Zscaler*

2:10pm - 3:00pm

Meeting Room 4

No single change in enterprise computing will have a greater impact on end-user security than the rapid adoption of mobile devices. Users are increasingly working outside of the office, doing so on smartphones and tablets. Despite this fact, the majority of enterprises continue to employ traditional security solutions that rely on appliances or host based software – solutions that cannot consistently inspect mobile traffic and are often not permitted to run on mobile ecosystems. Enterprises need to completely rethink their approach to end user security in this new paradigm. Zscaler ThreatLabZ has spent considerable time researching security and privacy risks in mobile applications and the results are frightening. Popular apps that have been blessed by the app stores and downloaded millions of times are blatantly exposing users to security and privacy risks by insecurely collecting and transmitting data while freely sharing it with third parties. In this talk, discuss our findings and share our thoughts on how enterprises should rethink security in this new paradigm.

### **Breaking the Mobile Mold**

*Mark Vondemkamp*

*F5 Networks*

3:20pm - 4:15pm

Meeting Room 4

The iPhone hit IT by storm just a few short years ago, driven by end-user pressure to allow enterprise use of these devices. Android smartphones, then tablets soon followed and the BYOD era was upon us - along with an additional business risk to manage: sensitive intellectual property on personal devices. Driven by tight timelines, many organizations reached for MDM solutions and device-level VPNs. Today's BYOD point solutions focus on managing and connecting devices that belong to the user, not the organization. This approach can cause conflicts with end users who

might not want IT touching their personal data and applications. Simultaneously, it made a lot of personal data and applications a security risk for the enterprise. The risk introduced is not just an IT problem: multiple organizational departments like Finance, HR and Legal must all be included in any BYOD initiative.

In 2013, the enterprise BYOD focus has hit the mainstream, and new capabilities allow for a more sophisticated enterprise admin to more closely meet the needs of both the organization and the employee. BYOD 2.0 could shrink the enterprise jurisdiction on a mobile device to just the enterprise data and applications on that device, allowing IT to focus on the new mobile enterprise footprint, reducing the mobile security concerns in order to allow BYOD.

Attendees will get a clear strategy to improve availability, performance, and security for their BYOD strategy. They will learn how BYOD has evolved over these first couple of years, and about the challenges of what the industry currently provides. Key approaches discussed will be mobile application SDKs, dynamic post-compile security wrappers, application-level VPNs, and enterprise application store (distribution and management) capabilities. The presentation will also look at the next set of concerns on the horizon as more enterprise applications move to cloud-based infrastructures.

## Threat Landscape Track

### **Is End Point Control Going the Way of the Dodo?**

*Matthew R. Schwartz*

*General Electric*

11:00am - 11:50am

Meeting Room 5

Historically, defense in depth alone has protected enterprise networks. However, the logic of security within the confines of one's enterprise leaves vulnerabilities in today's world. Most enterprise systems have fallen to a flat security model, soft on the inside, and hard on the outside. Additionally, with loss of control of the endpoint, numerous devices, and constant connectivity to the enterprise; networks security posture is based on upon 3rd party marketing claims. For true security posture it is vital to implement hunting teams and intelligence

# 12 Threat Landscape

collection. Thereby identifying the attacker's tactics and draw a conclusion of their methods and logic; additionally technologies such as honeypots has been utilized in research but seldom used in product in environments mainly due to their high level of overhead to maintain them. Honeypots on the other hand if implemented correctly can help to alert system maintainers to reconnaissance on the network. Active defense technologies such as honeypots provides more analysis of attacker behavior, increase their time spent on a meaningless service and more thoroughly disguise the true nature of the honeypot.

## Cyber Warfare: The Reality Is That We Are All Under Attack

*Matthew Lane*  
*JANUS Associates*

1:00pm - 1:50pm

Meeting Room 5

This non-advertorial session explores the technical and business perspectives of Cyber Warfare. Modern warfare has always been governed by rules of engagement including the Geneva and Hague conventions. Humanitarian interests during conflicts have been clearly spelled out as far back as the Old Testament. Cyber Warfare is different. There are no conventions, norms, or protections for governments, industry or private citizens. Every system and individual is fair game and at risk.

The purpose of this presentation is to clearly define the who, what, when, where of a Cyber attack, how it will affect your organization and how to prepare and respond should you come under attack.

## The Ever-evolving Threat Landscape

*Jeff Multz*  
*Dell SecureWorks*

2:10pm - 3:00pm

Meeting Room 5

Attacks on government organizations far exceed those on banking, healthcare and retail industries, yet it is only ranked No. 3 of organizations that are attacked the most. While the rankings change from year to year, the point is this: No industry is secure without providing the proper measures to secure its network, and following compliance guidelines alone are not enough. Monitoring more than 30 billion events a day for organizations of all sizes around the world, Dell SecureWorks does more than watch over customers. Its threat intelligence team secretly spies on underground communities to create countermeasures for the latest threats to protect customers. Hacking has gone from a sport to a high-income business where criminals in the underground net millions of dollars a year. The days of just needing anti-virus and firewalls are long gone as security threats can double in a year and have become so sophisticated and stealthy that hackers could be inside a network for years without notice.

Jeff Multz will show you how the threat landscape has changed in the past decade, and what malware can do to you today that was unheard of just a few years ago. You'll see why the regulatory agencies continue to increase their security guidelines and why just having firewalls and IDS/IPS systems are not enough. Dell SecureWorks, which sells no products, will teach you about the latest threats and vectors for attacks to help you understand what you need to do to block them.

## Ensuring Software Security Even in Imperfectly Protected or Hostile Environments

*Dan Stickel*  
*Metaforic*

3:20pm - 4:15pm

Meeting Room 5

Most software today is written to expect and depend upon a perfectly protected operating environment. These programs require a hothouse environment, a "Software Garden of Eden", that can no longer be realistically expected. Cisco's own SVP for Security states that we should expect the perimeter to be porous, and the former Director of US National Intelligence has stated that in examining systems 'of consequence', he has yet to encounter one computer that has not been compromised by an advanced persistent threat.

Faced with these daunting odds, it seems prudent that people responsible for mission critical software – whether that means nuclear power plant operations, mobile banking apps, or even just software running onboard a public bus – should ensure that that software can defend itself from attack when its environment inevitably becomes corrupted.

This talk will review the common ways that software programs can defend themselves and protect their own integrity, from simple techniques such as code signing to modern software immune systems.



### Afternoon Cookie Breaks

June 4 at 3:00pm-3:20pm and June 5 at 2:30pm-2:50pm

Re-energize with a beverage and a snack!

*Continuing Legal Education (CLE) credits are sponsored by the Albany County Bar Association.*

## Meeting Room 7

### **SYMPOSIUM SESSION 1: Behavioral Security I**

*Chair: Raj Sharman  
University at Buffalo, SUNY, NY*

11:00am - 11:50am

*Paper: **What Drives Perceptions of Threats to Your Facebook Friends' Information?***

Stephane Collignon, Tabitha James, Virginia Tech, VA; Merrill Warkentin, Mississippi State University, MS; and Byung Cho Kim, Korea University, South Korea

*Paper: **Impact of Security and Privacy Concerns among Medicare Patients on Sharing Health Information Online***

Wencui Han, Rohit Valecha, and Raj Sharman, University at Buffalo, SUNY, NY

### **SYMPOSIUM SESSION 2: Behavioral Security II**

*Chair: Bill Stackpole  
Rochester Institute of Technology, NY*

1:00pm - 1:50pm

*Paper: **Customized Behavioral Normalcy Profiles for Critical Infrastructure Protection***

Andrey Dolgikh, Zachary Birnbaum and Victor Skormin, Binghamton University, NY

*Paper: **Consumer Acceptance of Smart Metering Technology***

Merrill Warkentin, and Philip Menard, Mississippi State University, MS; and Sanjay Goel, University of Albany, SUNY NY.

### **SYMPOSIUM SESSION 3: Risk Assessment**

*Chair: Sanjay Goel  
University at Albany, NY*

2:10pm - 3:00pm

*Paper: **Quantifying e-risk for Cyber-insurance Using Logit and Probit Models***

Arunabha Mukhopadhyay, Indian Institute of Management, Lucknow, India.

*Paper: **Performance Evaluation of Classification Techniques used for Data Theft Detection***

Pratik C. Patel and Upasna Singh, Defence Institute of Advanced Technology, India

### **SYMPOSIUM SESSION 4: Handheld and Wireless Device Security**

*Chair: Anil Somayaji  
Carleton University, Canada*

3:20pm - 4:15pm

*Paper: **Malware Analysis for Android Operating System***

Kriti Sharma, Trushank Dand, Tae Oh and Bill Stackpole, Rochester Institute of Technology, NY

*Paper: **Security Analysis of Certified Wireless Universal Serial Bus Protocol***

Rishabh Dudheria and Wade Trappe, Rutgers university, NJ

*Paper: **Android Malware Research Environment***

Ben Andrews, Bill Stackpole and Tae Oh, Rochester Institute of Technology, NY

**Cyber Showcase Table**  
located near Meeting Room 7  
opens at 8:30am.

# 14 Cloud Security / Workforce/Human Factor

Wednesday June 5, 2013 Day Two

## Cloud Security Track

### No More Trade-Offs: How to Secure Cloud Data Without Compromise

Gerry Grealish  
PerspecSys

10:30am - 11:20am

Meeting Room 1

With security remaining the number one inhibitor to cloud adoption, enterprises are faced with a lot of options regarding how best to protect their data. While technologies like encryption are often regarded as prevailing choice, they're not always the best choices. Using the wrong solution can force companies to make compromises in application functionality, user experience, compliance, and their ability to future-proof. In this session, Gerry Grealish of PerspecSys will examine a variety of technologies and share best practices in choosing cloud data security solutions that provide maximum protection and minimum exposure. He'll review recommendations from the National Institute of Standards & Technology (NIST) regarding compliance (i.e., what you need to know about standards like FIPS 140-2 to ensure your company is protected). And, he'll outline the baseline requirements organizations need to meet, and what to watch out for when traditional methods of protection – like encryption – aren't enough.

### Weathering the Storm: Clouds and Critical Infrastructure Protection

Greg Metzler  
SRC, Inc.

11:40am - 12:30pm

Meeting Room 1

Cloud and critical infrastructure. What features of the cloud enable our confidentiality, integrity and availability objectives? What capabilities they good for supporting? More importantly, what don't they do (or do well)? This talk cuts through the fog of the marketing hype and gives you an unvarnished, vendor-neutral look at how (or if) the cloud is right for your business or mission.

### Cloud Security Pros Unite - PCI DSS for 2014 and Beyond: Upcoming Revisions Mean Now is the Time to Collaborate and Foster Positive Change within the SSC

Kurt Hagerman  
FireHost

1:40pm - 2:30pm

Meeting Room 1

As a group, we all work to promote the use of best practices for providing security within the cloud computing industry. And compliance plays an important part of helping us all succeed in meeting this goal. The challenge we face together is that the current Payment Card Industry Data Security Standard (PCI DDS) tries to be a 'one-size-fits-all' standard, for all types of service providers.

The current PCI DDS service provider Attestation of Compliance (AOC) lets cloud hosting providers make bold PCI claims, when, in reality, they are likely only achieving some of the more easily met controls and requirements. This weak AOC means that service providers can meet minimal requirements while still promoting themselves as wholly (or at least more vaguely) compliant. For merchants regulated to meet compliance, the AOC does not provide a way to differentiate between service providers that have taken a minimalist approach to PCI DDS compliance and those that have upped the ante to take on more risk and responsibility for security.

In this presentation, Kurt Hagerman, director of information security at FireHost, will outline what the current PCI DDS AOC covers, what it doesn't and how we, cloud security advocates, can use our voices to amend the standard when it comes up for review and amendment in October 2013.

### Cloud Security: Focusing on Automation and Thwarting APTs

Derek Tumulak  
Vormetric, Inc.

2:50pm - 3:45pm

Meeting Room 1

Security concerns continue to be the number one inhibitor of cloud adoption. The easier we can make it to securely embrace the cloud, the more readily businesses will adopt it. Cloud servers need to be protected immediately as they get spun up. The best way to do this is through automation – especially for Cloud Service Providers (CSPs) who need to

provide quick deployment in order to meet the needs of their customers at scale. Automation is key to creating a cloud security ecosystem in which CSPs and enterprises can be more agile, lower costs, and improve their security posture.

The need to meet compliance requirements is a major factor in cloud adoption. However, compliance does not equal security; it is necessary, but not sufficient, to achieve it — especially in the cloud. As recent breach news has demonstrated, sophisticated hackers are getting into all kinds of supposedly secure systems and stealing sensitive, valuable data. So really the question becomes this: how do you best thwart APTs and attackers already inside your network perimeter? The answer is data-centric security, utilizing encryption, key management, strong access control policies and advanced security intelligence so you can see — at a root level — who is accessing your data and what they're doing with it.

## Workforce / Human Factor Track

### We See the Future...And It Isn't Pretty"

Chris Eng  
Veracode

10:30am - 11:20am

Meeting Room 2

In this session Veracode presents research findings from the State of Software Security Report, which offers a before the breach look at security, by examining the flaws commonly found in applications of all kinds. The company also examines what the research findings mean for security, predicts how these flaws could cause history to repeat itself, and discusses how security pros can help change the future.

## Strategies for Improving Workers Cyber Security Engagement

*Joseph Treglia  
Syracuse University – iSchool*

11:40am - 12:30pm

Meeting Room 2

Strategies and processes have been identified that improve the human performance and acceptance of security related activities and habits; engagement. Tools and technology are available which can stop cyber-attacks and malicious incidents within agencies and also reduce losses and speed recovery. The greatest failure of these systems, however, lies in the human elements. This session highlights current work in this area so agencies may implement policies and practices that will more likely be adopted and continued by the people within the organization. A multidimensional approach for cyber security policy that incorporates promotional (including positive reinforcement) as well as proscriptive and prevention focused means (including sanctions) is explained. Actions that foster and promote ongoing integrity and policy compliance within the organization are presented.

## Is Security Awareness a Waste of Time?

*Scott Greaux  
PhishMe, Inc.*

1:40pm - 2:30pm

Meeting Room 2

The continued uptick in successful spear phishing attacks against high-profile targets like The White House has security 'pundits' debating whether security awareness efforts are a waste of time. People, we believe, are a critical part of an organization's security posture. Reliance on technology alone to combat a threat that its core targets humans is a recipe for disaster. PhishMe's Scott Greaux will present his arguments, lessons learned from well and ill-developed programs, and discuss a holistic strategy for thwarting the advanced threat actors and cyber criminals in their tracks, and how enterprise-wide security awareness programs that focus on behavior modification can play a key role.

## Virtual Learning Tools in Cyber Security Education

*Dr. Li-Fang Shih and Dr. Sherly Abraham  
Excelsior College*

2:50pm - 3:45pm

Meeting Room 2

The presentation will address how the core competencies of Cyber Security are attended to in an online virtual environment. Our discussion will explain how the affordances provided by technology can be explored to create a seamless learning environment for supporting Cyber education. The presentation will primarily emphasize two themes. First, we will provide information on the interactivity tools employed to educate students by promoting a learning environment of feedback and interactivity. We will demonstrate a number of the interactivity activities that we have developed in the Cyber security context to enhance the learning process of students in identifying threats, relating to core concepts in security and other technical domains.

Secondly, we will explain how we have been able to create virtual labs in online environments to provide hands-on-experience to students on the concepts of Cyber Security. The demonstration will focus on network vulnerability detection, network attacks and defenses, securing network devices, server level operating system hardening and setting up honeypots. The demonstration will show how we setup these lab activities in a virtual environment. We will elaborate on the course –Communications Security for our demonstration. The technical topics covered include device hardening, encryption, proxies, firewalls, VPN and remote access design, NAT, DHCP, and VoIP. Students learn how to implement a security plan, itemize security threats, and list the elements of security in networked and mobile systems. Honeypots, sinkholes, and other network defenses are examined. This presentation will not only demonstrate how virtual tools can be used to educate students on Cyber security but also show how the affordances of technology can be explored to overcome the limitations of distance and time in developing a workforce proficient in Cyber security.

## Audit Track

### Security Audits: How to Fail Them Big Time

*James L. Antonakos  
WhiteHat Forensics*

10:30am - 11:20am

Meeting Room 6

In this presentation James provides examples from actual security audits that raised red flags in terms of security violations from many different areas of the audit process, including physical security, system administration, network security, user and data security, and security policies and procedures. If your company has never undergone a security audit or is actively preparing for one, this presentation may prove useful in enhancing your protection and security and avoiding red flags of your own.

### Beyond the Checklist: Designing an Internal Audit Framework for Better Security

*Randy Rose  
NYS Office of the State Comptroller*

11:40am - 12:30pm

Meeting Room 3

We live in at a time when everything is pre-washed, pre-cooked, pre-heated, pre-screened, pre-approved, pre-packaged, post-dated, freeze-dried, double-wrapped, vacuum-packed, fully equipped, factory authorized, hospital tested, and clinically proven. In other words, there is a template for everything and we have a tendency to shape our worlds to these templates, rather than the other way around. This session will look at moving away from those templates and building an internal audit program that makes sense for your organization, so you can stay behind the eight ball and ahead of the curve.

# 16 Audit / Public Private Partnerships

## Hunting Attackers with Network Audit Trails

*John Pierce  
Lancope, Inc.*

1:40pm - 2:30pm

Meeting Room 6

Sophisticated, targeted attacks have become increasingly difficult to detect and analyze. Attackers can employ 0day vulnerabilities and exploit obfuscation techniques to evade detection systems and "fly under the radar" for long periods of time. Reports cataloging trends in data breaches reveal a systematic problem in our ability to detect that they ever occurred. Gartner estimates that 85% of breaches go completely undetected and that 92% of the detected breaches are reported by third parties. New strategies for identifying network attack activity are needed.

The purpose of this session is to review how network logging technologies such as NetFlow and IPFIX can be applied to the problem of detecting sophisticated, targeted attacks. These technologies can be used to create an audit trail of network activity that can be analyzed, both automatically and by skilled investigators, to uncover anomalous traffic. We will demonstrate how these records can be used to discover active attacks in each phase of the attacker's "kill chain." We will also cover how these records can be utilized to determine the scope of successful breaches and document the timeline of attacks.

## Security Information Event Monitoring (SIEM): Wasted Dollars or The Golden Goose

*Scott Sattler and Igor Volovich  
Secure Labs*

2:50pm - 3:45pm

Meeting Room 3

During the session I will be discussing the last decade implementing various vendor SIEM platforms in large global environments to detect insider threats, data breaches, corporate espionage and nation state effects to penetrate corporate, government and military networks.

We will look at the pitfalls, successes and realistic expectations in architecting, deploying and managing

SIEM platforms. The session case studies discuss what security events security sensors can detect and which events should be collected. Further discussions cover how events are correlated and most importantly how not to drop the ball on actionable security intelligence.

This is a valuable sessions for both management and technically minded persons as the session covers staffing problems, engineering personalities and the formidable challenges in managing day to day operations.

## Public Private Partnerships Track

### Researching the Nature of Stormy Seas: The Importance of Public-Private Collaboration in Cyber Research

*Stephen Korns, L-3 Communications  
Kurt Becker, Polytechnic Institute of New York University*

10:30am - 11:20am

Meeting Room 4

L-3 Communications and the Polytechnic Institute of New York University (NYU-Poly) have formed a strategic, collaborative partnership in cyber research. Investments in these types of industry-academia cooperative efforts are essential to the overall security ecosystem in advancing a "research renaissance" focused on solving technically challenging problems in cyber security. NYU-Poly introduced one of the nation's first master's programs in cybersecurity in 2009. The University is designated as a National Security Agency/Department of Homeland Security (NSA/DHS) Center of Academic Excellence in information assurance education and research. It is also home to the National Science Foundation-funded Information Systems and Internet Security (ISIS) Laboratory. NYU-Poly's pioneering research in cybersecurity has led to technology advancements and innovative solutions. L-3 Communications and NYU-Poly are currently focused on the specific area of virtualization and hypervisor security. Creative public-private collaborative partnerships are an important element in evolving a better understanding of the fundamental nature of cyber security threats, and researching new solutions to rapidly emerging security issues.

NYU-Poly's faculty engages in continual discovery in the context of our i2e (invention, innovation, and entrepreneurship) continuum that shapes our research environment. Research breakthroughs often start in the classroom, grow in the laboratory and come to life in the marketplace. Partnerships with industry have proved to be an invaluable tool to shape the research agenda of our faculty. Our strategic industrial partners include industry leaders in telecommunication, cyber security, next generation wireless networks, big data, power distribution and smartgrid implementation, and the chemical and biomedical industries. A few examples of how industry-university collaborations can be structured to create win-win-win situations for the industrial partner, the university, and its faculty and students will be discussed briefly.

### Targeting Emerging Cyber Threats Through Information Sharing

*Ron Plesco  
KPMG*

11:40am - 12:30

Meeting Room 4

APT's, DDos attacks, mobile threats, botnet take-downs, counterfeit goods and organized crime cyber infrastructures will be featured as the speaker discusses real case examples from 2011-present in which intelligence sharing through a private-public model have combined efforts to combat next gen. cyber crimes with a focus on ROI.

### Roadmap of Federal and State Cybersecurity Policy: Will the Public-Private Partnership Survive?

*Robert Mayer  
USTelecom*

1:40pm - 2:30pm

Meeting Room 4

The session will examine the recent releases of the White House Cybersecurity Executive Order, the accompanying Presidential Directive 21, and the National Institute of Standards and Technology (NIST) Cyber Framework that is currently being developed. These initiatives are likely to have a significant impact on government and industry

organizations as cybersecurity standards are developed and critical infrastructure risk assessments are conducted by Sector-Specific Agencies.

The session will examine the major federal and state entities involved in developing and implementing Cybersecurity policy and the implications for government and industry. The presentation will also provide insights into how information sharing is evolving and the constraints under existing law as well as concerns from privacy and civil liberties advocates.

## Using "Big Data" to Build an Intelligence Driven Security Strategy

*Seth Geftic  
RSA, the Security division of EMC*

2:50pm - 3:45pm

Meeting Room 4

"Big Data" is being touted as the silver bullet that will solve all security problems we have today. Sadly this is not the case. While Big Data is an important step, it is only impactful if it is used to work towards an intelligence driven security strategy. This session will help you understand what an intelligence driven security strategy is, how big data can help and how it can hurt and why this is the best strategy to defend against advanced and targeted attacks. Additionally, it will outline other key requirements to be able to build an effective security management program.

## IT Solutions Track II

### Security Organization on a Budget

*Michael Corby  
CGI Inc.*

10:30am - 11:20am

Meeting Room 5

Financial austerity has prevailed for quite some time now. Security programs that were relevant a while ago are becoming obsolete. Attrition has cost many security departments their experienced management, and, at best, security is now viewed as a "necessary obligation" and handled on an incident basis. The gains made to treat security aggressively as an advanced strategy are quickly slipping away.

This session will highlight how a competent security program can be established on a limited budget, while still enabling the organization to recognize and respond to security challenges successfully without compromising the demands of compliance and good business practices.

A good benchmark session for security organizations of all sizes and maturities.

### The Future of PCI: Securing Payments in a Changing World

*Bob Russo  
PCI Security Standards Council*

11:40am - 12:30pm

Meeting Room 5

This session will provide an update on PCI Standards, guidance and new programs for 2013 and strategies for how organizations can take advantage of new technologies and advances in payments to secure cardholder data in the future.

The presentation will address the following key elements:

- The relationship between PCI DSS and EMV
- Today's mobile payment environment and associated risks and challenges when it comes to securing payment card data
- New technologies available to reduce security risks by making payment data inaccessible or devaluing the data and how to take advantage of these when planning for PCI in your business
- What's ahead with the new version of the PCI Standards and how to utilize new PCI SSC resources and training programs for addressing payment security challenges.

### Managing the Data Explosion

*Samuel Chun  
HP*

1:40pm - 2:30pm

Meeting Room 5

Opportunities to monetize data are everywhere. CIO's have become the "Chief Information Optimizer", wrestling with the risks and opportunities presented by Big Data in their enterprises. They face exponential growth in data volumes, velocity, variety and complexity and organizational demands to get more done with less budget, time, and fewer people. Regulatory compliance, governance and security pressures

grow. And they face a mandate to improve the quality and timing of the business insights they help deliver to their lines of business.

This session will discuss some of the proven security solutions that relieve some of the pressure and help ensure that they have the capability to house, protect and gain business insight and value from their data.

### End-to-End Visibility: State Government Virtualization's Secret Sauce

*Renault Ross  
Symantec Corporation*

2:50pm - 3:45pm

Meeting Room 5

As virtualization advances, so must our information security and management solutions for virtualized environments. Specifically, state governments are asking for innovations for greater visibility and control of virtual applications, improved storage input/output performance, reduced impact from backup and recovery operations, and high-performance security and compliance.

But there's a problem: Not all state systems are virtualized. Rather, the typical state government is a complex mix of physical, virtual, cloud, and mobile environments, with several dimensions of workload interactions, numerous administrative and user access points, multiple locations of data assets, and rapid, dynamic movement of virtual machines.

To make sense of it all, what states really need is centralized visibility – a comprehensive risk and compliance view of their entire ecosystem, so that all environments can be more effectively secured, control silos can be consolidated, and redundancies in software deployments, administration, and staffing can be minimized.

In this session, we'll explore solutions for achieving end-to-end visibility across both virtualized and non-virtualized systems (with techniques like cross-console visibility, content integration, automation of manual best practices and shared content, and process integration for automated interactions and remediation).

# 18 Incident Response

## Incident Response Track

### "Corporate Incident Response: Wait! I should have wrote that down!"

*Jeffrey Isherwood*  
*Exelis Inc.*

10:30am - 11:20am

Meeting Room 3

Cyber incident responders operate within nearly every industry and often work in highly diverse and dynamic environments. These personnel are typically, non-law enforcement information technology based incident response practitioners. Primarily tasked with closing security breaches quickly, IT Incident Response Personnel minimize potential loss or damage of data and accountability. Due to the urgent nature of closing security breaches, forensic admissibility and possible prosecution is not typically a priority, and as such, some investigative actions and steps are not properly documented or captured in a forensically sound manner. This scarcity of documentation can impede further investigative and litigation actions taken by our justice system against these intruders.

Lack of reporting and prosecution for cybercrimes and network intrusions emboldens criminals and intruders to believe that they may trespass upon an organization's digital enterprise with impunity. When a cybercriminal violates a network's integrity and is simply denied access once discovered, rather than face the fear of discovery or repercussion, it encourages them to continue or escalate their activity.

This talk will examine the gap between Information Technology and Law Enforcement incident response and will propose some potential solutions at multiple levels as to how this gap may be narrowed.

### What's Been Happening in the Capital Region

*Dan Alfin*  
*FBI*

11:40am - 12:30pm

Meeting Room 6

Special Agent Alfin will present an in-depth look at some of the cases the Albany division's Cyber squad has handled in the past 4 years.

### Seven Must do's: How Great Companies Survive (thrive?), with APT

*John Petrequin*  
*Red Sky Alliance*

1:40pm - 2:30pm

Meeting Room 3

Mr. Petrequin will discuss two case studies of companies who've been compromised and how they dealt with it. The presentation ends with an overview of seven traits that those who've survived (thrived) APT attacks have in common.

### Finding Malware Like Iron Man

*Corey Harrell*  
*New York Office of the State Comptroller*

2:50pm - 3:45pm

Meeting Room 6

There are several common misconceptions about malware. One being that malware is just a nuisance, and is usually the product of bored teenagers sitting in their bedrooms. As a result, the typical response to a malware incident is to reimage, rebuild, and redeploy. The primary focus of this response is getting the system back into production as quickly as possible. Analysis of the malware and further research on the system is not a priority or goal.

Malware is not a nuisance or a minor disruption; it can pose significant risks to an organization. Malware is a tool that is leveraged by numerous threat groups to accomplish specific goals. When malware impacts a system the system does not become sick, it becomes compromised, and our incident response processes need to reflect this accordingly.

Root case analysis needs to be performed on systems impacted by malware to improve decision making. Questions need to be answered including: how did this happen, when did it happen, what (if anything) was taken, were we targeted, or what can be done to mitigate this from re-occurring. By re-imaging and re-deploying malware infected systems we no longer answer these questions, and we lose critical intelligence to better protect our organizations. The first step in root cause analysis is locating the malware.

In this technical presentation Corey will discuss three steps to locate malware on a computer running the Windows operating system. The topics will include the following: what is malware, why perform root cause analysis, program execution artifacts, persistence mechanism artifacts, NTFS artifacts, and freely available tools to parse those artifacts.

At the conclusion of the presentation, attendees will know how to perform three specific examination steps to help identify common artifacts that point to where malware is located on an infected system.



### Afternoon Cookie Breaks

June 4 at 3:00pm-3:20pm and June 5 at 2:30pm-2:50pm

Re-energize with a beverage and a snack!

# Annual Symposium / 19

## Meeting Room 7

### **SYMPOSIUM SESSION 5:**

#### **Network Security**

*Chair: Tae Oh*  
Rochester Institute of Technology, NY

10:30am - 11:20am

*Paper: **Detecting Infection Source and Building Predictive Blacklists with an Attack-Source Scoring System***

Liyun Li and Nasir Memon, Polytechnic Institute of New York University, NY

*Paper: **A Private Packet Filtering Language for Cyber Defense***

Michael Oehler and Dhananjay Phatak, University of Maryland Baltimore County, MD

### **SYMPOSIUM SESSION 6:**

#### **Data Storage**

*Chair: Sylvia Perez-Hard,*  
Rochester Institute of Technology, NY

11:40am - 12:30pm

*Paper: **Cloud Security: Attacks and Current Defenses***

Gehana Booth, Andrew Soknacki and Anil Somayaji, Carleton University, Canada

*Paper: **Data Breach Reporting Preparation: An Analysis of Practice***

Ernst Bekkering, Northeastern State University, OK

### **SYMPOSIUM SESSION 7:**

#### **Education**

*Chair: George Berg,*  
University at Albany, SUNY, NY

1:40pm - 2:30pm

*Paper: **Mobile Device Vulnerability Exploitation as a Security Curriculum using the Flipped Classroom Model Approach***

Richard Mislán and Tae Oh, Rochester Institute of Technology, NY

*Paper: **Teaching Android Malware Behaviors for Android Platform using Interactive Labs***

Colin Szost, Kriti Sharma, Tae Oh, Bill Stackpole and Rick Mislán, Rochester Institute of Technology, NY

### **SYMPOSIUM SESSION 8:**

#### **Data Storage, Forensics, and Security**

*Chair: Fabio Auffant*  
University at Albany, SUNY, NY

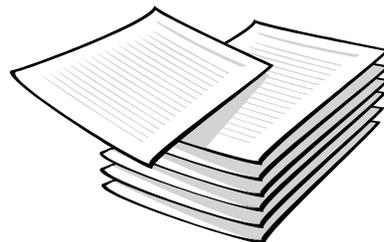
2:50pm - 3:45pm

*Paper: **Discovering Predictive Event Sequences in Criminal Careers***

Carl Janzen, University of the Fraser Valley, Canada and Amit V. Deokar and Omar F. El-Gayar, Dakota State University, SD.

*Paper: **A Conceptual Investigation Towards an Integrative Perspective of Risks in Information Systems Development & Usage***

Jim Samuel, City University of New York, NY



# DAY ONE

## Agenda at a Glance

June 4, 2013

Conference Hours		<b>State Government</b> <b>IT Solutions I</b> <b>Mobile Issues</b> <b>Threat Landscape</b> <b>ASIA</b>										
<b>Legal Issues</b> <b>Research</b>		<b>State Government</b>		<b>IT Solutions I</b>		<b>Mobile Issues</b>		<b>Threat Landscape</b>		<b>ASIA</b>		
8:00am – 4:15pm	Opening of the Exhibit Hall											
8:00am – 9:00am	<b>Welcome Address: Fran Reiter, Executive Deputy Director of State Operations</b> <b>Keynote: "Recommended Cyber Actions for Large Enterprises: An Industry Perspective" Dr. Michael Papay, Vice President and Chief Information Security Officer, Northrop Grumman Information Systems</b>											
10:30am – 11:00am	<b>Visit the Exhibitors (Terabyte Sponsor Demo - AT&amp;T 10:35am-10:55am)</b>											
11:00am – 11:50am	2012: The Year High Courts Get Involved in Tech Privacy Law and Make a Mess of IT Steve Treglia Absolute Software Corporation	You've Been Hacked, Now What? Reg Hamish GreyCastle Security	State Governments at Risk: A Call for Collaboration and Compliance Moderator: Srinji Subramanian, Deloitte & Touche LLP Panelist: Thomas Smith NYS Office of Information Technology Services	Protection from DDoS Attacks: Observations and Protections Brian Rexroad AT&T	Mobile SECURITY (not just MDM): Understanding the Real Risk Eric Green Mobile Active Defense	Is End Point Control Going the Way of the Dodo? Matthew R. Schwartz General Electric	<b>Behavioral Security I</b> Chair: Raj Sharma, University at Buffalo, SUNY <b>Paper: What Drives Perceptions of Threats to Your Facebook Friends?</b> Stephanie Johnson, and Tobiha James, Virginia Tech Merrill Warkentin, Mississippi State University; and Byung Cho Kim, Korea University <b>Paper: Impact of Security and Privacy Concerns among Medicare Patients on Sharing Health Information Online</b> Wencui Han, Rohit Valecha, and Raj Sharma, University at Buffalo, SUNY					
11:50am – 1:00pm	<b>Lunch on your own and Visit the Exhibitors</b>											
1:00pm – 1:50pm	From ".gov" to the Private Sector: Federal Efforts in Securing Cyber Space: 2.0 Bradley Schreiber Applied Science Foundation for Homeland Security	The Intersection of Cyber Security and Public Opinion: from Small Business Owners to Investors John Zogby Zogby Analytics	Securing the Mission of Government: Prevention Rather than Reaction to the Cyber Threat Slawomir Marcinkowski, NYSTEC Deborah A. Snyder, Kishor Bagul NYS Office of Information Technology Services; Dr. Kamal T. Jabbar, Rome Air Force Research Laboratory	Information-Driven Cyber Security: "Why COTS Solutions are not Enough" Bill Russell Northrop Grumman	The BYOD (Bring Your Own Device) Wave: Policy, Security, and Wireless Network Infrastructure Ken Kaminski Cisco Systems	Cyber Warfare: The Reality Is That We Are All Under Attack Matthew Lane JANUS Associates	<b>Behavioral Security II</b> Chair: Bill Stackpole, Rochester Institute of Technology <b>Paper: Customized Behavioral Normality Profiles for Critical Infrastructure Protection</b> Andrey Dolgikh, Zachary Birnbaum and Victor Skormin, Binghamton University <b>Paper: Consumer Acceptance of Smart Metering Technology</b> Merrill Warkentin, Philip Menard, Mississippi State University; and Sanjay Goel, University at Albany, SUNY					
1:50pm – 2:10pm	<b>Visit the Exhibitors (Megabyte Sponsor Demo - Symantec 1:55pm-2:05pm)</b>											
2:10pm – 3:00pm	Data Tagging, Redaction, and the Future of Automated E-Discovery Elton Juter Symantec	2013 Global Security Report Abstract Jonathan Sprull Trustwave SpiderLabs	A Moment in Time: An Outside-In Perspective of the Health and Welfare of State Government Cyber Infrastructure Chris Coleman Lookingglass Cyber Solutions	Finding the Needle in a Stack of Needles David Santeramo Logic Technology Inc.	Future Shock: How Mobility Is Forcing Enterprises to Completely Rethink Security Michael Sutton Zscaler	The Ever-Evolving Threat Landscape Jeff Multz Dell SecureWorks	<b>Risk Assessment</b> Chair: Sanjay Goel, University at Albany, SUNY <b>Paper: Quantifying e-risk for Cyber-insurance Using Logit and Probit Models</b> Arunabha Mukhopadhyay, Indian Institute of Management <b>Paper: Performance Evaluation of Data Classification Techniques used for Data Theft Detection</b> Pratik C. Patel and Upasna Singh, Defence Institute of Advanced Technology					
3:00pm – 3:20pm	<b>Visit the Exhibitors (Megabyte Sponsor Demo - Cisco 3:05pm-3:15pm)</b>											
3:20pm – 4:15pm	Social Media and Cloud Computing: Threats to Privacy, Security and Liberty Raj Goel Brainlink International, Inc.	Investigative Response and the 2013 Data Breach Report Chris Novak Verizon Enterprise Solutions	Scalable Protocol-Based Packet Inspection for Advanced Network Threat Detection Richard Lethin Reservoir Labs, Inc.	Enterprise Security on a Budget: Deciding What Gets Done First and What Doesn't Get Done At All Kristine Briggs Andy Hubbard Neohapsis, Inc.	Breaking the Mobile Mold Mark Vondenkamp FS Networks	Ensuring Software Security Even in Imperfectly Protected or Hostile Environments Dan Stichel Metaforic	<b>Handheld and Wireless Device Security</b> Chair: Anil Somayaji, Carleton University <b>Paper: Malware Analysis for Android Operating Systems</b> Sri Sharma, Trushank Dand, Tae Oh and Bill Stichel, Carleton University <b>Paper: Security Analysis of Certified Wireless Universal Serial Bus Protocol</b> Rishabh Duhhera and Wade Trappe, Rutgers University <b>Paper: Android Malware Research Environment</b> Ben Andrews, Bill Stackpole and Tae Oh, Rochester Institute of Technology					



# 22 Exhibitors



## Terabyte Sponsor

Innovation is the drive of the future. 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 identify and implement innovative solutions to transform the business of government.

**Network Transformation:** In here, cloud aligns costs with consumption. The explosive growth in government data requires the ability to capture, store and transform data into meaningful information.

**Voice Transformation:** In the network, even your desk phone gets to be a smart phone. The convergence of voice and data onto a single network promises a range of new applications that can fundamentally change how you communicate.

**Cyber Security:** In here, we know your world and we know how to secure it. AT&T monitors over 19 Petabytes of IP traffic each business day for suspicious activity and employs more than 1,500 security experts and support professionals.

**Mobilizing Government:** Data – If you can collect it, you can unlock it. With the explosion of mobile communications, data growth is unlimited, and government is seeking new ways to unlock its potential.

**Secure Workforce:** Work anywhere, security everywhere. Whether the data is in your pocket, on your desktop or in the network, state and local governments can count on AT&T to provide both security and BYOD solutions to support and protect your agency.

**Public Safety:** In here, the public's safety always comes first. AT&T solutions for public safety enable first responders to access and share mission critical information when they need it, where they need it—from call to car to crisis.

Visit [www.att.com/stateandlocal](http://www.att.com/stateandlocal) to learn more.



## Megabyte Sponsor

Cisco is the global leader in the development and sale of networking, collaboration and communication technology. The security of our products and the security of networks are at the core of our business. Cisco's has a strong focus on network security, and occupies a unique position as a global leader and trusted advisor to customers in both the private and public sectors. Cisco Cybersecurity Solutions harness the capabilities built into every Cisco product and provide a secure network to develop and execute a successful cyber security strategy. They allow organizations to strategically leverage their existing Cisco secure network fabric to provide a multi-layer defense against cyber threats. [www.cisco.com/go/uspscybersecurity](http://www.cisco.com/go/uspscybersecurity)



## Megabyte Sponsor

Symantec protects the world's information, and is a global leader in security, backup and availability solutions. Our innovative products and services protect people and information in any environment – from the smallest mobile device, to the enterprise data center, to cloud-based systems. Our world-renowned expertise in protecting data, identities and interactions gives our customers confidence in a connected world. More information is available at [www.symantec.com/publicsector\\_us](http://www.symantec.com/publicsector_us) or by connecting with Symantec at: [go.symantec.com/socialmedia](http://go.symantec.com/socialmedia).



## Kilobyte Sponsor

Northrop Grumman provides the most advanced and integrated cybersecurity solutions across all domains to the intelligence community, Department of Defense, and civilian agencies. As the largest provider of full-spectrum cybersecurity solutions to the federal government, the company safeguards highly sensitive, mission critical networks and information systems, offering customers innovative solutions to help secure the nation's cyber future. Northrop Grumman also offers cybersecurity tools and capabilities for state and local agencies that can be leveraged to protect critical infrastructure and support public safety solutions. For more information about Northrop Grumman in cybersecurity, go to [www.northropgrumman.com/cybersecurity](http://www.northropgrumman.com/cybersecurity)



BTB Security provides an extensive range of services encompassing all aspects information security and digital forensics - vulnerability assessments to digital forensic investigations. BTB Security was built from the ground up to provide superior solutions with flexibility and lower costs in mind, and operates out of PA, IL and CA. Operating as if each customer is our only customer, our customers' success is our own success. If you are looking to achieve your goals and objectives by leveraging honest and trustworthy partners, BTB Security is the team you can trust. [www.btbsecurity.com](http://www.btbsecurity.com)



**Check Point**  
SOFTWARE TECHNOLOGIES LTD.

Check Point Software Technologies Ltd. ([www.checkpoint.com](http://www.checkpoint.com)), the worldwide leader in securing the Internet, provides customers with uncompromised protection against all types of threats, reduces security complexity and lowers total cost of ownership. Check Point continues to develop new innovations based on the Software Blade Architecture, providing customers with flexible and simple solutions that can be fully customized to meet the exact security needs of any organization. Check Point is the only vendor to go beyond technology and define security as a business process. Check Point 3D Security uniquely combines policy, people and enforcement for greater protection of information assets and helps organizations implement a blueprint for security that aligns with business needs. Customers include tens of thousands of organizations of all sizes, including all Fortune and Global 100 companies.



DynTek is a leading provider of professional technology services to mid-market companies, such as state and local governments, educational institutions and commercial entities in the largest IT markets nationwide. From virtualization and cloud computing to unified communications and collaboration, DynTek provides professional technology solutions across the three core areas of our customers' technical environment: Infrastructure/Data Center, Microsoft Platform, End Point Computing. DynTek's multidisciplinary approach allows our clients to turn to a single source for their most critical technology requirements. For more information, visit <http://www.dyntek.com>.



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. <http://www.excelsior.edu/>



GreyCastle Security is an information security consulting firm, focusing on risk management, awareness and operational security. Our company was established because a need existed for an information security consulting firm truly focused on managing risks in people, process and technology, not pushing the latest hardware and software.

GreyCastle Security is comprised exclusively of former CISOs, ISOs, security specialists and operators - we have all answered to audit committees, CEOs and boards. We bring a client perspective to everything we do.

All we do is information security. All day, every day. [www.greycastlesecurity.com](http://www.greycastlesecurity.com)



HP creates new possibilities for technology to have a meaningful impact on people, businesses, governments and society. The world's largest technology company, HP brings together a portfolio that spans printing, personal computing, software, services and IT infrastructure to solve customer problems.

[www.hp.com/go/publicsector](http://www.hp.com/go/publicsector)



We're in a perfect IT security storm. Hackers are more sophisticated, your data is increasingly accessed anytime and anywhere and often resides in the cloud. Fewer access points are corporately-controlled, and there is a growing digital data explosion while the compliance demands on staff and systems escalate.

These trends mean corporate IT security can no longer be an afterthought where a secure perimeter is good enough. Instead, security intelligence preventing, detecting and addressing system breaches anywhere must start in the boardroom and become part of your organization's IT fabric. It is now imperative to be woven into your everyday business operations.

# 24 Exhibitors

IBM Security solutions help you do this by providing a comprehensive security framework that spans hardware and software along with the service expertise to provide integrated security solutions customized for your unique needs and designed to lower your total cost of ownership.

<http://www-03.ibm.com/software/products/us/en/category/SWI00>



Infoblox (NYSE:BLOX) helps customers control their networks. Our innovative solutions help businesses automate complex network control functions to reduce costs, increase security and maximize uptime.

Our technology enables automatic discovery, real-time configuration and change management and compliance for network infrastructure, as well as critical network control functions such as DNS, DHCP and IP Address Management (IPAM) for applications and endpoint devices. Leveraging our patented Grid™ technology, Infoblox delivers higher availability, and an authoritative network database for real-time and historical reporting.

Infoblox solutions help over 6,100 enterprises and service providers in 25 countries make their networks more available, secure and automated. [www.infoblox.com](http://www.infoblox.com)

## 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/>



At IPLogic we are a team of technology experts focused on delivering advanced business communications solutions such as Unified Communications and Collaboration, Data Center and Virtualization and Cloud Computing Solutions. But we are also much more than that.

Sometimes our solutions are about solving technical challenges and sometimes they're focused on business and organizational complexity. Whatever the key drivers are, our team is fully prepared to help your team overcome the challenges you face as you strive to achieve greater outcomes for your organization. [www.iplogic.com](http://www.iplogic.com)

At IPLogic we are a team of technology experts focused on delivering advanced business communications solutions such as Unified Communications and Collaboration, Data Center and Virtualization and Cloud Computing Solutions. But we are also much more than that.

Sometimes our solutions are about solving technical challenges and sometimes they're focused on business and organizational complexity. Whatever the key drivers are, our team is fully prepared to help your team overcome the challenges you face as you strive to achieve greater outcomes for your organization. [www.iplogic.com](http://www.iplogic.com)



At Juniper Networks, we are leading the charge to architecting the new network. At the heart of the new network is our promise to transform the economics and experience of networking for our customers. We offer a high-performance network infrastructure built on simplicity, security, openness, and scale. We are innovating in ways that empower our customers, our partners, and ultimately everyone in a connected world



THE POWER OF INGENUITY

ITT Exelis ([www.exelisinc.com](http://www.exelisinc.com)) is a global aerospace, defense and information solutions company. The Information & Cyber Solutions (ICS) Department of Exelis, located in Rome NY, is an industry leader in information protection and sharing capabilities and provides research, development, testing and evaluation of information technology solutions. ICS' scope of technical expertise includes: Information Assurance; Certification & Accreditation; Cyber Security; Data Loss Prevention; Cyber Education and Training; and Power Engineering for the Reliability, Maintainability, Supportability and Quality of Facility Operations. Exelis' commercial offerings include a data loss prevention suite called PuriFile® (<http://purifile.com/>) and our cyber education and training center called Secure-U (<http://secure-u.is.exelisinc.com/>).



MAC Source Communications offers experience in business communications consulting along with telecommunications system design, implementation and management services. With a responsive team of solution experts, MAC Source invests time understanding an organization in order to deliver solutions that meet immediate needs and optimize infrastructures for the future. By being part of

Meridian Group International (MGI), MAC Source is supported by over three decades of financial stability and a deep understanding of IT, leasing, and finance. With offices in the United States, United Kingdom, Germany, and Australia, MGI has international influence and the collective power to deliver results. [www.macsourceinc.com](http://www.macsourceinc.com)

## **METAFORIC™**

Metaforic is a leading provider of security software for protection against attack, specializing in providing high performance solutions for embedded, enterprise and mobile security. The core offering is a real time anti-tamper and integrity checking solution for firmware, OS and applications that protects against subversion, theft, malware, tampering or other corruption. Our technology is proven in millions of deployed instances, from consumer deployments through to business devices.

Metaforic solutions directly prevent any change to code or data by automatically adding real time security to code that is to be protected. This defeats custom malware and malicious hacking such as Man-in-the-Middle attacks, Man-in-the-Mobile attacks, attacks on rules, configuration and heuristics, firmware modification and application layer hacks. [www.metaforic.com](http://www.metaforic.com)



NYSTEC serves as a trusted technology advisor to state agencies, local governments, and private institutions. A not-for-profit corporation, NYSTEC applies proven processes for information security, project management and system integration to assist clients with security, technology acquisition, IT strategy, converged networks, health IT and education IT. Since the company's founding, NYSTEC's highly skilled staff has been augmented by the technical knowledge base of the Air Force Research Laboratory (AFRL) Information Directorate in Rome, NY. At this year's Cyber Security Conference, NYSTEC is also partnering with the Griffiss Institute, a non-profit Rome-based corporation that facilitates inter-organizational cooperation in developing cyber security solutions. [www.nystec.com](http://www.nystec.com)



**the network security company™**

Palo Alto Networks is the network security company. Its innovative platform enables enterprises, service providers, and government entities to secure their networks and safely enable the increasingly complex and rapidly growing number of applications running on their networks. The core of the Palo Alto Networks platform is its next-generation firewall, which delivers application, user, and content visibility and control integrated within the firewall

through its proprietary hardware and software architecture. Palo Alto Networks products and services can address a broad range of network security requirements, from the data center to the network perimeter, as well as the distributed enterprise. More than 11,000 customers in over 100 countries use Palo Alto Networks products. [www.paloalto.com](http://www.paloalto.com)

## **QUANTERION** SOLUTIONS INCORPORATED

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](http://www.quanterion.com)



RCR&R offers data security and electronics recycling services for idle, obsolete and non-working technology products throughout New York State and the Northeast. Since 1995 over 7000 corporations, state agencies, education institutions and municipalities have participated in our programs. Data security programs include physical destruction of data enabled devices and media, hard drive shredding, and NAID certified data wiping services. Recently, RCR&R became the 1st and only electronics recycler in New York State to be AAA certified by NAID, the National Association of Information Destruction. RCR&R offers Ewaste recycling solutions in conjunction with the NYS Electronics Recycling and Reuse Act. [www.ewaste.com](http://www.ewaste.com)

## **Reservoir Labs**

Privately owned, in business since 1990, and with laboratories in Manhattan (NOHO) and Portland Oregon, Reservoir specializes in optimizing compilers, network processing, and software verification, embodied in a suite of technology products for research and end-user deployments. Reservoir delivers cutting-edge technology products, customized solutions, and advanced R&D services to commercial and government clients. Reservoir will be exhibiting our R-Scope® product family, which provides cyber security for high-speed, high-fidelity network analysis. R-Scope includes protocol-based analysis and load-balancing technologies to provide scalable, semantic behavior detection. [www.reservoir.com](http://www.reservoir.com)

# 26 Exhibitors



Tailwind Associates

TECHNOLOGY SOLUTIONS AND SERVICES

Since 1992, Tailwind Associates has been the leading Information Technology (IT) Professional staffing, recruiting, and consulting services partner to our clients in the Albany, New York Capital Region and New York City area. In 2008 we expanded our service in IT delivery territories to include North Carolina, South Carolina, Mississippi and Texas, with offices in Charlotte and Austin.

We are a Microsoft Certified Partner and specialize in SharePoint and .NET Application Development; and we include IBM, Oracle, and HP TippingPoint among numerous other technology partners and platforms.

With 20 years of experience in IT services, covering both the public and private sectors, Tailwind Associates offers customers direct job placement services, outsourced or managed technology solutions, or project-based information technology applications as well as infrastructure services. [www.tailwindassoc.com](http://www.tailwindassoc.com)



Unique Comp, Inc.

UCI is an award winning, ISO 9001-2008 certified, minority and woman owned certified business with a 15 year successful track record of providing high quality information technology services to our clients and our business partners. We offer a complete range of information technology services by leveraging our vertical domain knowledge, expertise and strategic alliances with CA Technologies and the award winning Security Solutions they provide. <http://uciny.com/>



Utica College offers regionally accredited Online Bachelor's and Master's degrees in Cybersecurity with concentrations in Intelligence, Investigations, Computer Forensics and Information Assurance taught by highly experienced, credentialed faculty. Utica College courseware meets all of the elements of the Committee on National Security Systems (CNSS) rigorous standards for Information Systems Security Professionals (4011) and Risk Analyst (4016). With the renowned Economic Crime Institute, and the Center for Identity Management and Information Protection, the College attracts collaborations with top institutions in government, public and private sectors, to develop innovative curriculum and provide students with unique door-opening credentials and opportunities.

For more information, visit us at <http://programs.online.utica.edu/>

## Work anywhere, security everywhere.

AT&T has solutions to protect constituent data, no matter where it is – in a pocket, on a desk or dwelling in a data center.

State and local governments can count on AT&T's legendary reliability to provide both security and solutions to support and protect your agency.

Rethink how government does business inside the network of possibilities from AT&T.

To find out how, visit [att.com/secureworkforce](http://att.com/secureworkforce)



VULNERABLE

PROTECTED



Download the free scanner app at <http://scan.mobi> and scan this code to learn more.

© 2012 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies.

Rethink Possible® 



# Security Without Compromise

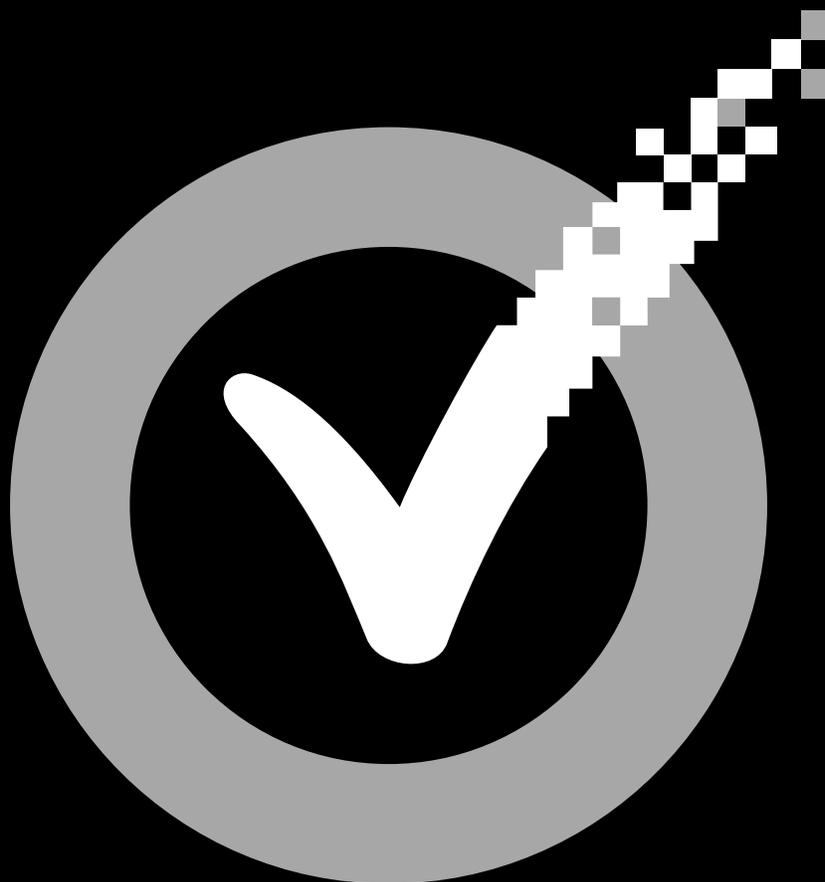
Visibility. Intelligence. Control.

Cisco is the global leader in the development and sales of networking, collaboration, and communication technologies. The security of our products is at the core of our business. Cisco has a strong focus on network security, and occupies a unique position as a global leader and trusted advisor to customers in both, the private and public sector. Our technology and experience combine to make Cisco the most capable partner in cyber and network security.

Contact Tony Suraci at [asuraci@cisco.com](mailto:asuraci@cisco.com) or your Cisco representative for a New York State Cyber Security Assessment.

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

# The security intelligence to keep you safe.



Even as hackers and cybercriminals race to exploit new technologies, Symantec keeps you safe. Our leading security intelligence identifies and stops mutating malware, protects business data and apps from mobile to the cloud, and uses advanced behavioral data to prevent malicious insiders from exploiting sensitive information.

**Visit Booth #8 & #9 to experience how Symantec's security intelligence network stops threats others can't.**

Confidence in a connected world.



Copyright © 2013 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.

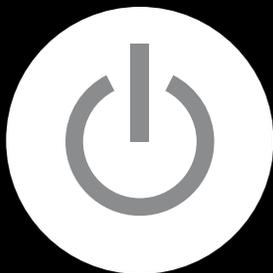
**THE VALUE OF  
STAYING AHEAD OF  
CYBER THREATS  
INSTEAD OF  
JUST KEEPING UP  
WITH THEM.**

**THE VALUE OF PERFORMANCE.**

***NORTHROP GRUMMAN***

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

© 2013 Northrop Grumman Corporation



## Cybersecurity. We're on it

State agencies are balancing new demands for security and privacy with performance and openness. And they're being asked to do it in real time. That's why government turns to Deloitte. We are relentless at getting to the core of an issue to help manage risks, deter threats, and help government help America. Let's start now. Visit [www.deloitte.com/us/stategovernment](http://www.deloitte.com/us/stategovernment).

As used in this document, "Deloitte" means Deloitte LLP and its subsidiaries. Please see [www.deloitte.com/us/about](http://www.deloitte.com/us/about) for a detailed description of the legal structure of Deloitte LLP and its subsidiaries.

Copyright © 2013 Deloitte Development LLC. All rights reserved.  
Member of Deloitte Touche Tohmatsu Limited  
36USC220506

**Deloitte.**

Hey we just met you.  
And this is crazy.  
We saw your headline.  
  
So call us maybe.



Risk Management  
Security Assessment  
Incident Response  
Security Awareness Training  
Penetration Testing  
Security Consulting  
Cloud Security

(518) 274-SAFE (7233)  
[www.greycastlesecurity.com](http://www.greycastlesecurity.com)  
[www.twitter.com/greycastlesec](http://www.twitter.com/greycastlesec)  
[blog.greycastlesecurity.com](http://blog.greycastlesecurity.com)



EXHIBITS & DISPLAYS    SIGNS & GRAPHICS    BRAND INTEGRITY    INTERIOR DECOR  
 PROJECT MANAGEMENT    CORPORATE IDENTITY    INSTALLATION    CONTENT DEVELOPMENT

**FASTSIGNS**<sup>®</sup>  
More than fast. More than signs.<sup>™</sup>

[www.fastsigns.com/518](http://www.fastsigns.com/518)

## Progressive Landscape Design

*Commercial—Residential—Free Estimates*



*Owner, Designer &  
Landscape  
Dan Frederick*

*518-357-4469*

### **TURFCO LAWN & LANDSCAPE**

**lawn care and landscape  
maintenance firm**

*For over 25 years, Turfco has been serving customers and creating beautiful lawns.*

*Specializing in fertilization and weed/grub control programs. With over 2,000 satisfied customers in the area, Turfco is the largest privately-owned lawn care company in the Capital Region.*



*Isn't it  
time you  
called  
Turfco?*

518-399-1442

The 2013 NYS Cyber Security Conference would like to thank all of our sponsors, exhibitors, speakers, and volunteers for making this another successful year!

## Thomas D. Smith

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

Thomas D. Smith serves as Chief Information Security Officer (CISO) for the State of New York. In his role as CISO, Mr. Smith oversees the NYS Enterprise Information Security Office (EISO) within the Office of Information Technology Services. The EISO develops and evaluates compliance with statewide information security policies; provides cyber incident response assistance, distributes real-time advisories and alerts; provides managed security services, and implements statewide information security training and exercises for state and local government.

From July 2010 through March 2013, Mr. Smith served as the Director of the New York State Office of Cyber Security within the Division of Homeland Security and Emergency Services. In addition to serving as the State's Chief Cyber Security Officer, he also oversaw coordination of the State's Geographic Information Systems (GIS) program.

Prior to being appointed Director, Mr. Smith served as Assistant Deputy Director and Counsel for the NYS Office of Cyber Security and Critical Infrastructure Coordination (CSCIC). In that position, he assisted in the agency's policy direction; managed the agency's large scale procurements; coordinated the agency's legislative program; and served as Co-Chair of the Multi-State Information Sharing and Analysis Center's Procurement Workgroup. He also served as the agency's Ethics Officer and Records Appeals Officer.

Before joining the CSCIC in 2007, Mr. Smith served as a supervising attorney at the State Office for Technology where he oversaw the legal team for the State Data Center and served as legislative liaison. From 1986-2000, he worked in the New York State Office of the State Comptroller, where he served as an associate attorney in the Division of Legal Services/Municipal Law Section and the Division of Legal Services/Investments.

Mr. Smith graduated cum laude from Dartmouth College and earned his Juris Doctor from Albany Law School. He and his wife reside in the City of Albany and have three children.

## Peter A. Bloniarz

*Dean of the College of Computing and Information  
University at Albany*

Prof. Peter Bloniarz is Dean of the College of Computing and Information at the University at Albany/State University of New York. Dean Bloniarz 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. 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 Bloniarz is currently chair of TechConnex, an organization devoted to fostering new IT businesses in Tech Valley, as well as the chair of the Computing Research Association's Deans Group. Prior to becoming dean, he was UAlbany's Interim Vice President for Research. Specializing in government's use of information technologies to improve service to citizens, he was one of the founders and research director of the University's award-winning Center for Technology in Government. An advocate for quality teaching at research universities, he received the SUNY Chancellor's Medallion for Excellence in Teaching, served as interim director of the university's center for teaching and learning, and is a Collins Fellow. He joined the computer science department at UAlbany in 1977 after receiving his doctorate from M.I.T. in electrical engineering and computer science.

## Donald Siegel

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

Dr. Donald Siegel is Dean of the School of Business and Professor of Management at the University at Albany, SUNY. He also serves as President of the Technology Transfer Society, a non-profit organization devoted to interdisciplinary analysis of entrepreneurship and technology transfer from universities and federal laboratories to firms. 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 co-editor of *Academy of Management Perspectives*, editor of 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 Management Studies*, *Journal of Business Venturing*, *Corporate Governance: An International Review*, and *Strategic Entrepreneurship Journal*. He has also co-edited 32 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 97 articles and 7 books on issues relating to university technology transfer and entrepreneurship, the effects of corporate governance on performance, productivity analysis, and corporate and environmental social responsibility in such leading journals in management, economics, and finance as the *American Economic Review*, *Economic Journal*, *The Review of Economics and Statistics*, *Journal of Law and Economics*, *Journal of Financial Economics*, *Brookings Papers on Economic Activity*, *Research Policy*, *Academy of Management Review*, *Academy of Management Journal*, *Academy of Management Perspectives*, *Academy of Management Learning & Education*, *Strategic Management Journal*, *Journal of Business Venturing*, *Journal of International Business Studies*, *Journal of Management Studies*, and *Journal of Management*. His most recent books are *Innovation, Entrepreneurship, and Technological Change* (Oxford University Press) and the *Oxford Handbook of Corporate Social Responsibility* (Oxford University Press). He is currently co-editing the *Handbook of University Technology Transfer* (University of Chicago Press), the *Oxford Handbook of Corporate Governance* (Oxford University Press), and the *Oxford Handbook of the Economics of Gambling* (Oxford University Press). His citation count, according to Google Scholar, is 14,131 with an h-index of 55.

Dr. Siegel 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, 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. Professor Siegel was a member of the Advisory Committee to the Secretary of Commerce on "Measuring Innovation in the 21st Century Economy" and a member of Governor David Patterson's Small Business Task Force. He is co-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. In 2011, Dr. Siegel testified before the House Committee on Science, Space, and Technology regarding re-authorization of the SBIR program. He also serves on the Board of Directors of the Research Foundation of the State University of New York and New York State Industries for the Disabled.

## Sponsor

### Demonstration Schedule

This year the Terabyte and Megabyte sponsors will demonstrate a product in the Exhibit Hall near Meeting Room 7. The following Demos are scheduled:

### Terabyte Sponsor

**AT&T**

June 4 at 10:35am – 10:55am  
and June 5 at 10:05am – 10:25am

### Megabyte Sponsors

**June 4 at**

1:55pm – 2:05pm Symantec Corporation  
3:05pm – 3:15pm Cisco Systems

**June 5 at**

11:25am – 11:35am Cisco Systems  
2:35pm – 2:45pm Symantec Corporation

Terabyte Sponsor

---



Megabyte Sponsors

---



Kilobyte Sponsor

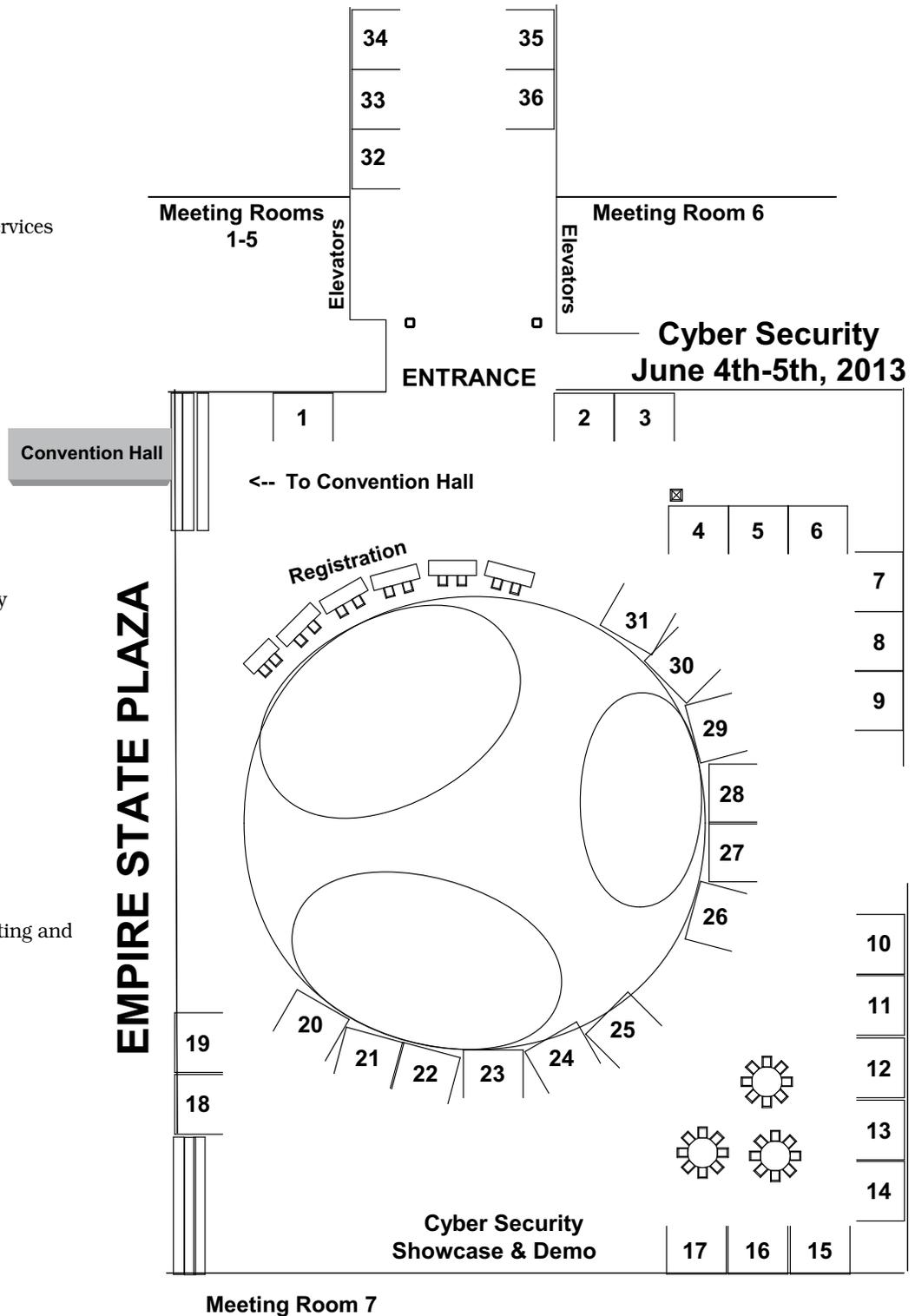
---

***NORTHROP GRUMMAN***

A thick, curved underline line that starts under the "N" and extends to the right, ending under the "N" of "GRUMMAN".

# Booth Assignments

- 01: NYS Office of Information Technology Services
- 02: Cisco Systems – Megabyte Sponsor
- 03: Cisco Systems – Megabyte Sponsor
- 04: AT&T – Terabyte Sponsor
- 05: AT&T – Terabyte Sponsor
- 06: AT&T – Terabyte Sponsor
- 07: GreyCastle Security
- 08: Symantec – Megabyte Sponsor
- 09: Symantec – Megabyte Sponsor
- 10: Regional Computer Recycling & Recovery
- 11: Excelsior College
- 12: HP
- 13: NYSTEC
- 14: IPLogic
- 15: Utica College
- 16: IBM
- 17: UCI
- 18: University at Albany’s College of Computing and Information and School of Business
- 19: The NYS Forum, Inc.
- 20: Check Point Software Technologies, Inc.
- 21: Exelis Inc.
- 22: Palo Alto Networks
- 23: BTB Security
- 24: Interface Masters Technologies
- 25: Metaforic
- 26: Northrop Grumman – Kilobyte Sponsor
- 27: Dyntek Services
- 28: Reservoir Labs
- 29: MAC Source Communications
- 30: Infoblox
- 31: Tailwind Associates
- 32: Quanterion Solutions, Inc.
- 33: Juniper Networks



## Passport Drawing

Bring the Exhibitor passport to each booth and have it stamped. Visit all of the exhibitors for a chance to participate in the Passport raffle. Drawings will be held on Tuesday, June 4 – 3:15-3:20 p.m. and Wednesday, June 5 - 1:30-1:40 pm. Complete the passport early for more opportunities to win. Hand the completed passport in by 2:30 p.m. on June 4 to be entered in the drawings on both days! You must be present to win!