

NEW YORK STATE
CYBER SECURITY CONFERENCE

JUNE 3-4, 2014

SOLVING THE SECURITY

PUZZLE

MOBILE APPLICATION
BUSINESS NEED
USER AWARENESS
RISK MANAGEMENT
FUNDING

BYOD

FOCUS

WWW.DHSES.NY.GOV/GO/CONFERENCE2014

TERABYTE SPONSOR



PRESENTED BY



WWW.ITS.NY.GOV



WWW.NYSFORUM.ORG



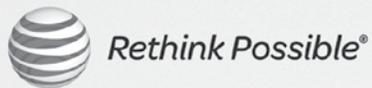
UNIVERSITY
AT ALBANY
State University of New York

WWW.ALBANY.EDU/IASYMPOSIUM

The only thing growing faster than citizen data is the need to secure it.

Understanding why government agencies need to secure big data is the easy part; cyber security attacks are escalating every year – putting citizen data at an increased risk. What's not always clear is whom city and county governments can trust to help make securing and monitoring big data simple and efficient. At AT&T, we have over 1,500 security experts dedicated to helping local governments increase big data security without exhausting resources. The experience we've gained while protecting over 52 PetaBytes of our own network data every business day is what makes us uniquely qualified to help governments of all sizes secure more – with less.

Learn how AT&T is securing the future of communications at att.com/securebigdata



Welcome



June 3, 2014

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 17th Annual New York State Cyber Security Conference.

The Conference provides a forum to learn about emerging information security trends and solutions. This year's conference theme is *Solving the Security Puzzle*. Risk management, technology, user awareness and training, policies and standards, effective budget strategies, and internal controls are just a few of the key interlocking "pieces" involved in providing a secure environment to meet today's business demands. The knowledge sharing and networking that takes place during the Conference's 48 sessions will provide you with the tools to assemble the pieces of the puzzle and enable you to proactively mitigate cyber risk. The 9th Annual Symposium on Information Assurance (ASIA), which runs concurrent to the main Conference, will present papers on information security topics by experts within academia.

This year, we are pleased to welcome Michael Daniel, Special Assistant to the President and the White House Cybersecurity Coordinator, who will provide the keynote on Wednesday, June 4. Members of the Governor's Cyber Security Advisory Board will present the keynote on Tuesday, June 3. Thomas P. Abt, Richard Clarke, Shawn Henry, Benjamin M. Lawskey, Will Pelgrin, Philip Reitingner, and Howard Schmidt will engage in an interactive discussion of current challenges facing the information security community and provide their insight into how those challenges are being met.

New to the Conference this year is a cyber competition called Panoply, two training classes, and a mobile event guide. We hope these additions enhance your Conference experience. An Exhibit Hall featuring the latest information and technological solutions from our sponsors and exhibitors will be on site Tuesday and Wednesday.

Thank you for your continued commitment to cyber security awareness and preparedness. 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



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. In November 2012, approximately 3,500 professionals from over 37 agencies were consolidated into the new ITS. ITS provides 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.

Joan M. Sullivan

**Executive Director
The NYS Forum, Inc.**

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

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

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

Robert J. Jones

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

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.

Lifesaving information, delivered with time-saving mobility.

In emergency response, speed is everything. AT&T can deliver solutions to improve response time by increasing your team's mobility. We've been working side by side with emergency-response teams since the development of 9-1-1. Our own experience with disaster recovery makes us uniquely qualified to help others. We understand the need to keep responders informed and to engage citizens in the midst of emergencies. Information plays a critical role in your preparedness and response. We can help it work even harder for you.

To learn how, visit att.com/publicsafetyguide



Rethink Possible



June 3, 2014

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

Hart Theatre at The Egg

Governor's Cyber Security Advisory Board

Governor Andrew Cuomo created the New York State Cyber Security Advisory Board in May 2013 to advise the administration on developments in cyber security and make recommendations for protecting the state's critical infrastructure and information systems. The members of this board are among the world's leading experts in cyber security and bring vast experience in both the public and private sectors.

William F. Pelgrin serves as co-chair of the Board, along with New York Superintendent of Financial Services **Benjamin M. Lawsky** and NYS Deputy Secretary for Public Safety **Thomas P. Abt**.

Mr. Pelgrin is currently the President and CEO of the Center for Internet Security (CIS) located in East Greenbush. Prior to his current position, he served for 29 years in state government, as director and Chief Cyber Security Officer of the New York State Office of Cyber Security and Critical Infrastructure Coordination ("CSCIC"), where he founded the Multi-State Information Sharing and Analysis Center.

As New York's first Superintendent of Financial Services, Mr. Lawsky led Governor Andrew Cuomo's initiative to make the Department of Financial Services into a modern unified financial regulator. He is the former chief of staff to Governor Cuomo and was Deputy Counsel to then-Attorney General Cuomo. Prior to that, Mr. Lawsky was an Assistant U.S. Attorney and Chief Counsel to New York Senator Chuck Schumer.

As the Cuomo Administration's Deputy Secretary for Public Safety, Mr. Abt leads the State's efforts to enhance public safety and ensure the wellbeing of New York's families and neighborhoods. Prior to joining New York State, Mr. Abt served as Chief of Staff to the Office of Justice Programs at the U.S. Department of Justice where he coordinated the National Forum on Youth Violence Prevention. Mr. Abt was also an Assistant District Attorney in Manhattan.

The other members of the board have all held significant cyber security positions with the U.S. government, and include:

Richard E. Clarke, Chairman and CEO of Good Harbor Consulting, LLC and former senior White House advisor for the last three administrations. Prior to serving in the White House, Mr. Clarke served for 19 years in the Pentagon, the State Department, and various intelligence agencies. Mr. Clarke is the author of, among other titles, *Cyber War: The Next Threat to National Security And What To Do About It*.

Shawn Henry, President and Chief Security Officer of CrowdStrike Services and former Executive Assistant Director of the Criminal, Cyber, Response, and Services Branch of the Federal Bureau of Investigation where he oversaw all of the FBI's criminal and cyber programs and investigations worldwide. Mr. Henry also led the establishment of the National Cyber Investigative Joint Task Force ("NCIJTF"), a multi-agency cyber security center.

Philip R. Reiting, Senior Vice President and Chief Information Security Officer of the Sony Corporation and former Director of the National Cyber Security Sector at the U.S. Department of Homeland Security. Previously, Mr. Reiting had positions at the U.S. Department of Homeland Security, where he assisted in securing critical infrastructure systems. Mr. Reiting worked previously for the Department of Defense, the Department of Justice, and Microsoft.

Hon. Howard A. Schmidt, a Partner at Ridge-Schmidt Cyber, LLC, who brings 31 years of public service in the cyber security field, including a position as President Obama's White House Cyber Security Coordinator and Special Adviser for Cyberspace Security for President George W. Bush. Mr. Schmidt also served as Vice President and Chief Information Security Officer for eBay Inc., and formerly served as the Chief Security Officer for Microsoft.

Fireside Chat: A Candid Conversation with the Governor's Cyber Security Advisory Board, moderated by board co-chair William F. Pelgrin

Members of the New York State Cyber Security Advisory Board will engage in an interactive discussion of current challenges facing the information security community and provide their insight into how those challenges are being met. The session will also be an opportunity for the members of the Board to discuss other items of interest, such as the input they have provided to the State on its cyber security planning, and other efforts in the federal government and the private sector to enhance cyber security capabilities across the State and the nation.



Tweet the Conference at [#nyscyber](https://twitter.com/nyscyber)



The Administration's Perspective on Cybersecurity

Michael Daniel
Special Assistant to the President and Cybersecurity Coordinator

June 4, 2014
8:30 a.m. -10:00 a.m.
Hart Theatre at The Egg

Michael Daniel is a Special Assistant to the President and the Cybersecurity Coordinator. In this position, Michael leads the interagency development of national cybersecurity strategy and policy, and he oversees agencies' implementation of those policies. Michael also ensures that the federal government is effectively partnering with the private sector, non-governmental organizations, other branches and levels of government, and other nations.

Prior to coming to the National Security Staff, Michael served for 17 years with the Office of Management and Budget (OMB). Michael played a key role in shaping intelligence budgets, improving the management of the IC, and resolving major IC policy issues including cybersecurity, counterterrorism spending, and information sharing and safeguarding.

Michael received a Bachelor's in Public Policy from the Woodrow Wilson School at Princeton University, and a Master's in Public Policy from the Kennedy School of Government at Harvard.

Congratulations

2014 New York State Cyber Security Award Winners
Christopher Stanley
and
Michael McManus



Special thanks to Tina Post
for Career Contributions to New York State Cyber Security



Legal / Mobile Security

Tuesday June 3, 2014 – Day One

Legal Track

Recent Attacks on the Third Party Rule Creates Greater Risk of Allegations of Eavesdropping and Illegal Searches and Seizures

Steve Treglia
Absolute Software Corporation

11:00 a.m. – 11:50 a.m.

Meeting Room 5

Beginning in January, 2012, with U.S. Supreme Court Justice Sonia Sotomayor's concurring opinion in *United States v. Smith*, a generation-long practice of not requiring law enforcement to utilize a warrant when communicated information is shared with a third party has been brought increasingly into question. Growing public awareness of the kinds of information that can be collected as a result of online activity has generated a demand for a legal response to shield this information from law enforcement acquisition by less than probable cause and court supervision. Moreover, the awareness Edward Snowden has brought to the public of the actions of the National Security Agency in monitoring communications has significantly heightened the rhetoric on both sides of the battle. As a result of this growing pressure, courts decisions have started weighing on both sides of this issue turning what had once been a very bright-line standard into a muddy slope that becomes slipperier and slipperier. This lecture will analyze a series of court cases decided since *Smith*, along with unrelated legislative attempts to similarly alter the legal landscape, to demonstrate how truly tenuous this once clear-cut and definitive rule has become.

The Executive Order on Cybersecurity and the Impact on Industry and Government

Robert Mayer
USTelecom

1:00 p.m. - 1:50 p.m.

Meeting Room 5

Exactly one year following the release of the February 2012 Executive Order: Improving Critical Infrastructure Cybersecurity, the

National Institute of Standards and Technology (NIST) released their Cybersecurity Framework which has spurred significant activity across the cybersecurity landscape. In addition, the Department of Homeland Security recently rolled-out their Critical Infrastructure Cyber Community C³ [pronounced C-Cubed] Voluntary Program which it too was required to develop as part of the 2012 Executive Order. The Communications Sector is working to adapt the framework for the broadcast, cable, wireline, wireless, and satellite industries within the current FCC Communications Security Interoperability and Reliability Council (CSRIC). Many enterprises have begun to incorporate this new framework into their risk management processes. This presentation will provide an overview of some of the major activities and accomplishments to date and the opportunities and challenges for all stakeholders going forward. With the Framework becoming the basis for voluntary use by many private and public-sector entities, this presentation will help participants understand the impact of these developments on policy, regulation, markets and business operations.

Cyberbullying and the Police Response: The Bullet Doesn't Fit the Gun

Kathy Macdonald
Global Cyber Security Courses

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

Meeting Room 5

As Internet use increases, so have cybercrimes, cyber-conflict, cyber-risk and the devastating effects of cyber bullying. Law enforcement is facing an uphill battle when responding to the unprecedented global increase in a broad range of technological crime. Should the public lower their expectation of law enforcement's ability to respond to every form of cyber-related crime?

Could cyber bullying instead be dealt with in the schools or handled by family? What role should websites and apps play when their platforms contribute so heavily to the problem? This presentation will discuss the role of law enforcement in battling cyberbullying and how the community could work more cooperatively with law enforcement to combat this growing problem.

Retaliatory Hacking: Legitimate Corporate Defense?

Ronald Raether
Faruki Ireland & Cox P.L.L.

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

Meeting Room 5

The presentation discusses the most common of the various types of affirmative defense and retaliatory hacking activities, the possible legal and practical risk associated therewith, and viable alternatives that financial institutions may consider.

Mobile Security Track

BYOD – A Big Piece to Solving the Security Puzzle

Aaron J. Williams
AT&T

11:00 a.m. -11:50 a.m.

Meeting Room 4

Mobile security has evolved from a traditional Mobile Device Management targeted towards Corporate Owned devices to a model supporting an increasingly BYOD (individually owned devices) adoption. The challenges have increased and the liability of separation between privacy and protecting corporate data has grown for companies. This presentation will outline the criterion to address these challenges and provide a framework for incorporating your business operations for the secure mobile workplace while maintaining the employee's personal privacy and experience.

Mobile for Education: Getting It Right the First Time

Eric Green
Mobile Active Defense

1:00 p.m. - 1:50 p.m.

Meeting Room 4

It's amazing how different education is for managing and securing mobile - but it sure is. Learn the importance of and how to build requirements from experience with the largest school district in the U.S. among others.

Understand device limitations as well as many device characteristics that are helpful for education that many (including the device manufacturers) are unaware of or don't understand the significance of.

Common pitfalls and wrong turns as well as success stories will be outlined. The goal with this session is to walk out knowing enough that you won't fall into the trap of having some mobile (MDM or otherwise) vendor be the one telling you what you can and can't do - you will have knowledge to both build and achieve your requirements.

Kids are smart, very smart. It's amazing how good they are with technology and getting to what they want even if they are not allowed to. The trick is staying ahead of that with proper security, BUT also using security and management that make it disadvantageous to try to circumvent. Want to know more - come to the session.

Business Need Track

Security Services Design in the Next Generation Data Center

Ken Kaminski
Cisco

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

Meeting Room 4

The evolving complexity of the data center is placing increased demand on the network and security teams to come up with inventive methods for enforcing security policies in these ever-changing environments. The goal of this session is to provide participants with an understanding of features and design recommendations for integrating security into the data center environment. This session will focus on recommendations for securing next-generation data center architectures which are built for high availability and with asymmetric flows as a norm. Areas of focus include security services integration, firewall design considerations with both large scale physical firewalls dealing with north-south traffic and virtual firewalls focused on east-west server-to-server traffic, and considerations and recommendations for server virtualization including visibility from a threat defense perspective.

The Future of PCI: Securing Payments in a Changing World

Bob Russo
PCI Security Standards Council

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

Meeting Room 4

The presentation will address the following key elements:

- An overview of the Council and its mission
- What's ahead with the new version of the PCI Standards
- The future of the Council and its impact on the payments landscape
- How to utilize new PCI SSC resources and training programs to address payment security challenges
- Ways you and your organization can be more involved with the Council and its initiatives

The Internet of Everything Track

Emerging Threats in Cyberland: Is the "Internet of Everything" Everything It's Cracked Up to Be?

Matthew Lane
Janus Associates

11:00 a.m. - 11:50 a.m.

Meeting Room 6

A look at the "Internet of Everything" including the bad things coming to your organization and home soon.

This presentation takes a serious look at the future and risks of living in a continuous and over connected environment.

In addition to the normal business of running a secure data center, organizations have adapted, with mixed success, to the need for remote providers to maintain the basic building requirements of electric, air, water and life safety systems. Now the refrigerators, vacuums and everything else found in society are ready to join the network as well.

Security polices, controls and resources have stretched to meet the challenge of BYOD, social networks and APT's.

The security experiences learned in the business environment need to be adapted to the "Internet of Everything" as well.

Emerging Threats in Cyberland will explore the following topics:

- What is the "internet of everything"?
- What forces are driving the "internet of everything"?
- Does the end user really benefit from all of these devices? If not, who does?
- The absence of security and privacy protocol standardization within "the internet of everything" and the resultant risks to government entities and businesses.
- A look at some of the devices and "things", and the data they collect, who sees the data, and how it might be used and misused.
- The blurring and disillusion of boundaries between business and personal as a result of "the internet of everything"
- A study of possible negative scenarios that could result due to data leakage
- How to protect your organization and yourself from "the internet of everything"

Securing Everything

Renault Ross
Symantec

1:00 a.m. - 1:50 p.m.

Meeting Room 3

The Internet of Things is forcing government agencies to rethink their IT security strategy and to include security from the beginning. According to Gartner there will be nearly 26 billion devices on the Internet of Things by 2020. This session would explore a strategy to assist these organizations in ensuring security is an enabler to their business drivers, mission and strategic initiatives. The presentation will cover the blueprints for building a solid Security Program across their endpoints, mobile devices and tablets for administrators and users.

Torturing Open Government Data System for Fun, Profit, and Time Travel

Dr. Thomas P. Keenan
University of Calgary

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

Meeting Room 3

"I'm from the government and I'm here to help you" takes on a sinister new meaning as

jurisdictions around the world stumble over each other to 'set the people's data free'. NYC boasts in subway ads that 'our apps are whiz kid certified' (i.e., third party) which of course translates to 'we didn't pay for them, and don't blame us if somebody got it wrong and the bus don't come.' This session reports on my (and other people's) research aimed at prying out data that you're probably not supposed to have from Open Government Systems around the world. For example, Philadelphia, PA cavalierly posted the past 7 years of political contribution receipts which contained the full names and personal addresses of thousands of people, some of whom probably didn't want that information to be out there in such a convenient form. The entire database was also trivially downloadable as a CSV file and analysis of it yielded some fascinating and unexpected information. Referring back to classic computer science and accounting principles like 'least privilege' and 'segregation of duties' the presentation will suggest some ways to have our Open Data cake without letting snoopy people eat it.

Architecture of Global Surveillance

Raj Goel
Brainlink International, Inc.

3:20 p.m. – 4:15 p.m.

Meeting Room 3

This presentation will discuss the origin of the modern surveillance state and what we can do about it.

Snowden, Anonymous, NSA, FBI, GCHQ, Boeing, China, Cisco, ATT, Verizon, Google, Facebook, GM, Ford, Apple, Amazon, your doctor, spouse, grocer, iPhone, Android, your child's school. What do they have in common? Each and every one is a spy. Individuals, corporations and governments have built the modern surveillance state.

Executive over reach, insufficient planning, systemic flaws, and blind faith in institutions has led to a global panopticon. Our jobs, social interactions and technology have made it extremely easy to become a spy...or a peeping tom. It's much harder not to look, than to look.

App stores, vendors, governments have transmogrified society into the Truman Show. This presentation delves into how we got here, what lessons we have learned, what lessons we have yet to learn, and where we're headed.

Based on 10 years of research, this presentation will delve into history, technology, the Bill Of Rights, EU Privacy Charter, George Orwell and others to discuss the origin and architecture of the modern surveillance state and what we can do about it.

What's the difference between the US & China? US and Russia? Come and find out.

ID a Hack Track

Why You Are pwned And Don't Know It!

Ben Miller
Parameter Security

11:00 a.m. – 11:50 a.m.

Meeting Room 3

2013 was the year of the hacker. Network breaches made media headlines everywhere you turned. Was your company one of them? If not, did you check all of your systems, metrics, users, and logs to ensure unauthorized access did not occur? Did you find evidence of a breach? Of course not, you are GLBA/HIPAA/PCI compliant! That means you are secure, right? WRONG! In this eye-opening presentation, Ethical Hacker, Ben Miller reviews network baselines, how Trojan activity (which could be on your network RIGHT NOW) is extremely hard to detect if you aren't properly looking for it. Using tools that are readily available to any wannabe malicious attacker, Miller demonstrates how hiding traffic in home and corporate networks can evade detection. The FUD will be kept to a minimum but the "secret" to protecting your networks will be unveiled.

The FBI Session

Michael Keller
FBI

1:00 p.m. - 1:50 p.m.

Meeting Room 6

Malware Root Cause Analysis: Don't Be a Bone Head

Corey Harrell
New York State Office of the State Comptroller

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

Meeting Room 6

Computer users are confronted with a reoccurring issue every day. This happens

regardless if the user is an employee doing work for their company or a person doing online shopping trying to catch the summer sales. The user is using their computer and the next thing you know it is infected with malware. Even Hollywood is not immune to this issue as illustrated in the TV show Bones. The most common action to address a malware infection is to reimaging, rebuild, and redeploy the system back into production. Analysis of the system to understand where the malware came from is not a priority or goal.

Root case analysis needs to be performed on systems impacted by malware to improve decision making. The most crucial question to answer is how did this happen since it will determine if we were targeted and more importantly what can be done to mitigate this from re-occurring.

In this technical presentation Corey will discuss the root cause analysis process to determine how malware infected a computer running the Windows operating system. The topics will include: why perform root cause analysis, how not to perform root cause analysis, compromise root cause analysis model, attack vector artifacts, and multiple malware infection scenarios.

Your Security Efforts Are Futile: Why an Advanced Attacker Will Always Find a Way in Regardless of the Defenses You Have in Place

Tyler Wrightson
Leet Systems

3:20 p.m. – 4:15 p.m.

Meeting Room 6

In this talk Tyler confronts a fact that is staring us all in the face; no matter what defenses are in place any target can be hacked. Tyler will explain how we got to this point, what it means for most organizations as well as what the future will look like. He will discuss the big picture elements as well as some tactical points which lead to this undeniable conclusion. Tyler will review a set of enlightening empirical evidence that points to this fact, as well as cover some of his firsthand experience and relevant stories from his career as a penetration tester. Finishing with thoughts on what the future holds and what will be needed to defend your organization.

Threats and Reports Track

2014 Data Breach Investigative Reports: Ideas and Directions

Chris Novak
Verizon

11:00 a.m. – 11:50 a.m.

Meeting Room 2

The Data Breach Report is an internationally recognized report that brings together statistics and findings from worldwide investigative response organizations around the globe, as of 2013 there were 19 and more are being added yearly. The contributors include: The Dutch National High Tech Crime Unit, US Secret Service, Australian Federal Police, Irish Reporting and Information Security Service and Police Centrale-crime unit. Chris Novak is Managing principal on the Verizon Investigative Response team and a contributing author to the Data Breach report. He is knowledgeable regarding data breaches, cybercrime and investigations worldwide. In this session Chris will discuss the current DBIR as well as the new approaches and methodologies used to improve it. The 2014 report is expected to look at patterns across industries which should enable a more relevant focus, have additional root cause analysis and have improved information on breach impact and cost.

Rise of the Avengers: Evil, Innovation, and the Battle for the Future of the Internet

Greg Metzler

1:00 a.m. - 1:50 p.m.

Meeting Room 2

As a security professional, a scan of recent news headlines can be quite depressing. It seems like the bad guy is running all over the good guys. Retailers, banks, even government agencies are suffering major breaches in security. Money is being stolen. Secrets (both national and corporate) are being revealed. Personal information is exposed.

Boy do we need some heroes...

While the capabilities of individual threat actors has become increasingly sophisticated, and we will certainly dive into emerging threats and their potential (or demonstrated ability) to cause significant damage; the good guys have not been idle. Great threats often spark even greater innovation.

Take heed evil-doers. The good guys are smart people, too- and there are more of us...

2014 Global Security Report

Richard Schenck
Trustwave

2:10 p.m. – 3:00 p.m.

Meeting Room 2

Cybersecurity threats are increasing as quickly as businesses can implement measures against them. At the same time, businesses must embrace virtualization and cloud, user mobility and heterogeneous platforms and devices.

They also have to find ways to handle and protect exploding volumes of sensitive data. The combination of business and IT transformation, compliance and governance demands and the onslaught of security threats continues to make the job of safeguarding data assets a serious challenge for organizations of all types—from multinational corporations to independent merchants to government entities.

Today, organizations need not only to understand current trends in security threats but also be able to identify inherent vulnerabilities within existing systems. In the 2014 Global Security Report, Trustwave tested, analyzed and discovered the top vulnerabilities and threats that have the most potential to negatively impact organizations.

Resident Security System for Government/Industry Owned Computers

Dr. Victor Skormin, Binghamton University
Slawomir J. Marcinkowski, NYS Technology Enterprise Corporation (NYSTEC)

3:20 p.m. – 4:15 p.m.

Meeting Room 2

Misuse of modern computer systems presents a formidable threat not only to integrity and confidentiality of stored data, but to computer-controlled processes. Nowadays, most industrial, military and government processes are run through dedicated computer systems. Operation of such processes implies that the end user accesses such a process not directly but through a special computer interface by defining required operational regimes, or data to be retrieved, or information to be recorded, or data to be transmitted, etc. Then it is up to the computer to provide the necessary set point values to process controllers, to sample sensors, to perform search, retrieval of the requested data, to operate printers or computer graphics, to locate available communication channels, code and transmit data, etc. Examples go far beyond power plants and rocket launchers. Banking industry, insurance, libraries, data depositories, hospitals utilize their own dedicated computer facilities operating in this fashion. "Dedicated" is the key word - it emphasizes that these computer facilities run only a few preapproved applications and are closed to general public. (In contrast, a university campus computer is open to general public and runs virtually any application.) Attacking dedicated computers offers a highly efficient way to render useless the processes they service and compromise stored information.

We developed a novel cyber security technology intended for computers that run "only a few preapproved applications". It is based on behavioral normalcy profiling and operates on the level of functionalities that provides unambiguous representation of the goals of the particular applications. The approach reliably detects malware and non-malicious applications that are not approved for a particular computer system. Fully operational system prototype enhanced by advanced visualization will be demonstrated.

Tuesday, June 3, 2014

Meeting Room 1

SYMPOSIUM SESSION 1: Cyber Attacks and Hacking

Chair: Merrill Warkentin, Mississippi State University, MS

11:00 a.m. - 11:50 a.m.

Paper: AVOIDIT: A Cyber Attack Taxonomy?

Chris Simmons, Sajjan Shiva, Harkeerat Singh Bedi and Dipankar Dasgupta,
University of Memphis, TN

Paper: Even Hackers Deserve Usability: An Expert Evaluation of Penetration Testing Tools

Michael Bingham, Adam Skillen, and Anil Somayaji, Carleton University,
Canada

SYMPOSIUM SESSION 2: Risk Assessment

Chair: Bill Stackpole, Rochester Institute of Technology, NY

1:00 p.m. - 1:50 p.m.

Paper: A Comprehensive Risk-based Auditing Framework for Small and Medium Sized Financial Institutions

Petter Lovaas, Niagara University, NY

Paper: An Exploratory Survey of the Affects of Perceived Control and Perceived Risk on Information Privacy

Clare Doherty and Michael Lang, National University of Ireland, Galway

SYMPOSIUM SESSION 3: Covert Channels

Chair: Anil Somayaji, Carleton University, Canada

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

Paper: Google Maps KML Covert Channel

Allen Sabernick and Daryl Johnson, Rochester Institute of Technology, NY

Paper: A Channel for Exchanging Information Covertly Using Game Save File in Prison Architect

Hashem Assayari and Daryl Johnson, Rochester Institute of Technology, NY

SYMPOSIUM SESSION 4: Emerging Topics

Chair: Daryl Johnson, Rochester Institute of Technology, NY

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

Paper: An Adaptive Approach for Active Multi-Factor Authentication

Abhijit Kumar Nag and Dipankar Dasgupta, University of Memphis, TN,
Kalyanmoy Deb, Michigan State University, MI



Afternoon Cookie Breaks

June 3 at 3:00 p.m.-3:20 p.m. and
June 4 at 2:30 p.m.-2:50 p.m.

Re-energize with a beverage and a snack!

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

Wednesday June 4, 2014 – Day Two

Business Need Track

Credit Card Security and PCI 3.0 – What Do You Need to Know?

Jeremiah Sahlberg
Tekmark Global Solutions

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

Meeting Room 2

PCI 3.0 is here. It took effect on January 1, 2014 and organizations have until January 1, 2015 to get on the new standard.

- What you need to know about Credit Card Security and PCI 3.0
- Details of 3.0 and what has changed
- How do you get ready for the new standard?

Cloud Services and Business Process Outsourcing

Kevin Wilkins
iSecure LLC

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

Meeting Room 6

Businesses have been outsourcing various processes and services for many years. Recently, IT services and applications have been moved to "The Cloud". What are the benefits and risks in utilizing outside parties vs. direct hires and internal infrastructure? What are some considerations in making a move to The Cloud safely?

This security-oriented presentation will cover both technical and business oriented considerations when utilizing cloud-based and managed services.

Social Media Considerations for Cyber Security and Crisis Response

Joseph Treglia
Syracuse University

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

Meeting Room 6

Social media allows for greater information sharing and engagement with citizens and stakeholders by government entities. Still,

there is no such thing as a free lunch, pitfalls, conflicts of interest, and of course security issues must be addressed so that optimal value can be achieved, and unintended consequences avoided or mitigated. Current problems and approaches to social media are presented for various scenarios.

Running an Effective Information Security Program

Dan Srebnick
Technical Merits LLC

2:50 p.m. – 3:45 p.m.

Meeting Room 2

We've heard about cyber risk, defense in depth, data breaches and their inevitability. Is the situation that grim or is there an effective way to manage information security and achieve positive results? Dan Srebnick, retired CISO of New York City shares his thoughts, successes, and challenges after 14 years of running information security in NYC.

User Awareness Track

Badges, Bombers and Barbarians: 7 New Tactics for Arming Corporate Citizens

Reg Harnish
GreyCastle Security

10:30 a.m. – 11:20 a.m.

Meeting Room 3

While some security pundits evangelize the failures of security awareness training and corporate budgets wasted on human security, the rest of us persevere, knowing that awareness is but one part of the security equation. And while glorious triumph may be unrealistic, success is achievable to those that are calculated, rhythmic and committed. But you're not going to get there with your grandfather's awareness kit. Join us for a frank conversation on what's working, what's not, and 7 new tactics to make your awareness program more effective.

Cyber Security Strategy: Managing your Controls in the Context of Risk

Ben Densham
Nettitude

11:40 a.m. – 12:30 p.m.

Meeting Room 3

Organizations often implement multiple controls to address internal cyber security concerns. Many are implemented due to compliance pressures or driven by IT developments and changes. However, cyber breach reports frequently show that many implemented controls are not effective in preventing and detecting malicious activity when it occurs. Is this because they are not up to the job? Is it because they are incorrectly configured? OR is it because the wrong controls have been applied?

We will take a high level look at what is happening within both the threat landscape and the industry at large and ask the question: who is deciding what is to be protected and why within your organization? This question will form the basis for an understanding of the risks that need to be mitigated, the threats to be defended against and the vulnerabilities that should be addressed.

Understanding the right controls to implement and the overall objective is key for all organizations. What should your cyber strategy look like? How should this be governed and implemented? How do you measure the effectiveness of your controls? Ultimately, are you realizing and addressing the real risk to your business?

Incident Response Track

Death, Taxes and a Computer Incident: Designing Your Incident Response Plan

Tom Sammel
Dell SecureWorks

1:40 p.m. – 2:30 p.m.

Meeting Room 3

The average cost of a U.S. data breach is greater than \$4.4 million¹. Aside from death and taxes, organizations have one more inevitable situation to worry about: a security incident on their computer or network. And when it strikes, you had better be prepared.

If you've ever wondered what you would do if your computer network were attacked or your entire website went down, and don't know, you probably don't have an effective tried-and-true Computer Incident Response Plan (CIRP).

Having a CIRP in place to help organizations stop the incident and repair the damages as quickly as possible could mean the difference between losing hundreds of dollars and tens of thousands of dollars. And conducting forensics after the incident could let you know who the hacker was and how to prevent future attacks.

In this session, attendees will learn

- What constitutes an "incident"?
- How to prepare an Incident Response Plan tailored to their organization
- Which people in the organization need to be involved in the planning and become a member of the Community Emergency Response Team
- How to decide what systems are most critical to get back online first
- What the best ways are to stop an incident before it spreads
- How to conduct a tabletop exercise to test the organization's ability to respond to an incident.

1 Ponemon Institute, LLC, "Cost of Data Breach Study: Global Analysis"

The Evolution of Endpoint Security: Detecting and Responding to Malware Across the Entire Kill Chain

Jessica Couto
Bit9

2:50 p.m. – 3:45 p.m.

Meeting Room 3

Over the past decade, the volume of malware produced and potentially infecting organizations, has multiplied by orders of magnitude. The scope of the threat, in conjunction with little to no innovation by traditional security vendors has left organizations like yours vulnerable. The time is NOW to expand security infrastructures to include detection and response capabilities that allow you to fully scope, contain and remediate

each threat in real-time on your endpoints and servers. Join Bit9 to discuss the emergence of endpoint malware and the new class of security solutions that can detect threats early and across more points in the kill chain.

Solutions Track

Encryption, Hashing, and Complexity, Oh My!

James L. Antonakos
WhiteHat Forensics

10:30 a.m. – 11:20 a.m.

Meeting Room 4

In this session James describes the techniques of encryption and hashing and the complexity of the algorithms that are used for both techniques. Insight into the techniques and complexity provides better understanding of the need for strong encryption keys, why brute force attacks can be successful, and why there is a need for both encryption and hashing.

Business Continuity in the Cyber Security Context

NYS Forum Business Continuity Workgroup

11:40 a.m. – 12:30 p.m.

Meeting Room 4

You hear the phrase, "Cyber Security". Cyber Security is protecting connected systems against vulnerabilities. Timely involvement of all business area leadership is crucial. That said, there might be opportunities to better integrate the IT response with the organization's business continuity program and structure, so that if an event does occur, the organization can provide a timely and coordinated response. How do we obtain clear proof of data recoverability and security? How do we utilize business continuity for logging and backing up data to avoid destruction of evidence while shutting down access? How can we achieve this at a lower cost with more visibility on pricing? After all, cyber security incidents can have business continuity implications and impacts that extend far beyond IT.

This panel session discusses answers to these questions with an overview of the current security landscape, while providing a walkthrough of lessons learned covering additional topics such as contracts, security

reviews, and plan development. We will discuss highlights of different actions an organization can take now to better align business continuity and cyber security efforts and increase organizational resilience.

Battling the Snowden Effect: Securing the Management Plane

Brian Ford
Cisco Systems

1:40 p.m. – 2:30 p.m.

Meeting Room 4

In the wake of a torrent of sensitive information disclosures by individuals who may have exploited their administrative rights and duties many IT organizations are re-examining how they secure the management plane of their IT infrastructure. This presentation looks at what type of access network administrators have to data that transits their networks and presents a number of solutions that can be used to put controls in place that safeguard data and the integrity of the administrators.

Adaptive Vigilance: Building the Capability to Detect Today's Threats

Joe Magee
Vigilant by Deloitte

2:50 p.m. – 3:45 p.m.

Meeting Room 4

Over the past decade, defending against cyber attacks has become geometrically more complex. As more of society's core infrastructure has become networked and digitized, electronic data, itself, has become a precious commodity, leading to the development of an increasingly sophisticated underground market in stolen data that has the ability to change rapidly to evade detection. Hackers are aggressively zeroing in on state organizations in an effort to extract the vast amount of citizen data stored in systems. And as more and more critical infrastructure – transportation systems, power distribution, and central communications – are operated through network-connected control systems, we introduce new potential for attacks that can seriously and rapidly impact public health and safety.

Despite the layers of best practices and security controls organizations have installed over the years, perfect security is impossible. Malicious actors shift tactics and procedures very rapidly

to circumvent controls, and exploit gaps in our complex environments. While it is essential to be proactive in protecting what we can, it is essential to also invest in monitoring systems that can more effectively detect emerging threats and unusual patterns of activity that may indicate unauthorized activity.

In this presentation, Mr. Magee will outline a risk-intelligent, threat-aware method for building detection capabilities that are tightly aligned with an organization's top risk priorities, and help organizations better adapt to the constant flux of both the threat landscape and the IT environment. He will also address practical considerations for how to build improved capabilities within tight budget constraints.

Info Sec Program Track

Implementing Security While Under Attack

Michael Corby
CGI Technology and Solutions Inc.

10:30 a.m. – 11:20 a.m.

Meeting Room 5

Implementing a reliable security program is a complex undertaking under ideal circumstances. Successful security is exponentially more difficult when faced with the high potential for attack. This can come in the form of attention by criminals, terrorists, political opponents and sometimes unknowingly by unanticipated volume. Partners need to be more carefully selected and timely operational statistics are more crucial. This session will present some proven practices and creative ideas for implementing security with conditions that are less than optimum.

Organizational and Business Issues

Manny Morales
New York State Office of the State Comptroller

11:40 a.m. – 12:30 p.m.

Meeting Room 5

With the ever growing threats in Internet breaches and intrusions, the reality of economic struggles within countries, and the skill talent shortage, how can an organization cope in providing a Cyber Security program that can

work? If you look on how a business is run, it's about profit and lost, marketing and creating new ideas, and managing a budget and acquiring talent. A Cyber Security program now needs to take these business issues more into consideration and not just view the issues from an IT perspective. The new economy struggles have changed the global economy, with the Internet being the engine that fuels this economy. The lone hacker will soon be no more. With countries, and organizations looking to either make a profit or a political statement, running your Cyber Security program as an IT entity will no longer meet these challenges. In this session, the speaker will provide a new way of running a Cyber Security program. By looking at this from more of a business prospective, the attendee will learn to run their Cyber Security Program more like a business model, than an IT entity.

Access Control Track

Access Granted. But to the Right Person?

Vik Bansal
Deloitte

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

Meeting Room 5

States have an obligation to protect citizen data and securely exchange information with others when necessary. In addition, they need to ensure the protection of infrastructure to maintain the required level of citizen services for their health and safety. A fundamental necessity is to identify and authorize access to information and services based on trusted credentials from citizens, employees, and third-party providers. Agencies can better combat potential cyber risks with effective Identity and Access Management framework that supports the agency's business model. This includes understanding where organizations' digital identities live—in the enterprise, cloud, or siloed services, what they can access, and to which job functions and processes they correspond. Learn how organizations have redefined the path to information to enhance their cybersecurity effectiveness.

Privileged Access Control and Security Strategy

Adam Gray
Novacoast, Inc.

2:50 p.m. – 3:45 p.m.

Meeting Room 5

Participants will get an understanding of the current trends that security engineering, security operations and auditors face as it relates to security strategy, automation, and privileged access control (PAC). Topics will include private cloud automation, workload automation, reduced root/admin privilege techniques, and future trends. This session will also cover some of the regulations and reasons for why this move is happening within regulated organizations.

Risk Management Track

Understanding the Risk Management Framework

Kelley Dempsey
National Institute of Standards and Technology

10:30 a.m. – 11:20 a.m.

Meeting Room 6

Risk cannot be eliminated, so we must learn to manage it! This session begins with a short discussion about the National Institute of Standards and Technology (NIST) and the Federal Information Security Management Act (FISMA) before turning to the NIST Risk Management Framework (RMF) itself. The NIST RMF is a comprehensive information security risk management process that is easily adapted to any size or type of organization. The six steps of the RMF and multiple associated guidance-based publications that facilitate RMF implementation will be detailed.

Security Frameworks, Strategies and Mitigation Efforts: Will They Work for You in Lowering Your Risk?

Peter Allor
IBM

11:40 a.m. – 12:30 p.m.

Meeting Room 2

Of late, governments around the globe are looking to secure not only their environments and citizens, but also critical infrastructures and the private sector supply chains that keep government domains and services provided to the private sector organizations operating on an ongoing, uninterrupted basis. With their priorities fixated on risk, organizations need to focus more on how they are securing their networks by reviewing risk management processes for business operations.

Organizations also need to bring in their IT department into this approach as opposed to the best-of-breed point product traditionally used to offset new attacks and vulnerabilities. With this new outlook on strategy, this non-regulatory approach differs from the compliance checklist that many security professionals have used and brings back the focus and strategy of the business, transforming security from a 'Doctor No' to an enabler of business. In this standalone talk, Peter Allor will discuss this view and how security professionals can embrace and lead their businesses to a more secure process in the continued evolution of advanced federal threat protection.

Microgrids, Energy, and Cyber Security: What You Need to Know for the Days Ahead

Samuel Chun
HP

1:40 p.m. – 2:30 p.m.

Meeting Room 2

The United States is becoming one of the global leaders in the ultra-fast growing microgrids market. Microgrids are expected to grow to over \$25B and over 5 GW in the near future. What are microgrids? How are they different from traditional power generation, transmission, and distribution? What should IT leaders and security professionals know about this emerging technology? What threats loom ahead? This session will explore microgrids and where security practitioners will likely run into them and the opportunities and threats that they are likely to present to everyone in the near future.

Data Breach Protections: First Step, Risk Assessment

Robert Zeglen and Vince Hannon
NYS Technology Enterprise Corporation (NYSTEC)

2:50 p.m. – 3:45 p.m.

Meeting Room 6

When it comes to data breaches, the risks for organizations and individuals have never been higher and prevention remains an elusive goal. From an organization perspective,

responsibilities for sensitive customer data continue to grow while at the same time the lines between corporate computing and personal are becoming blurred. Sharing sensitive data with one's business associates is becoming a requirement for organizational success and client service. Traditional solutions that rely on containment within the corporate network and systems are being challenged thanks to mobile device computing and outsourced systems. Before an organization can be certain they have implemented sufficient controls they must first understand the problem and this starts with a risk assessment. Risk assessments, when done properly, result in an organization understanding the touch points between their business and underlying information systems where breaches can occur.

The first step in protecting against data breaches begins with understanding just how your organization is doing business and what the risks are.

In this talk, NYSTEC will present an overview of how organizations should conduct risk assessments as a first step towards reducing the likelihood of a data breach. NYSTEC will also discuss some recent public breaches, examine the underlying causes and look for patterns that should be influencing organizational risk assessments.



Afternoon Cookie Breaks

June 3 at 3:00 p.m.-3:20 p.m. and June 4 at 2:30 p.m.-2:50 p.m.

Re-energize with a beverage and a snack!

Wednesday, June 4, 2014

Meeting Room 1

SYMPOSIUM SESSION 5: Security Policies

Chair: Yuan Hong, University at Albany, SUNY, NY

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

Invited Paper: Exploring the Role of the Temporary Workforce on Information Security Policy Compliance

Shwadhin Sharma and Merrill Wartenkin, Mississippi State University, MS

SYMPOSIUM SESSION 6: Game Theory in Security

Chair: Daryl Johnson, Rochester Institute of Technology, NY

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

Paper: Application of Stackelberg Security Games in Information Security

Abrahamyan, Ashot, Armenia

SYMPOSIUM SESSION 7: Digital Forensics

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

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

Paper: Quantifying the Danger of Mobile Banking Applications on the Android Platform

Brett Ferris, Jay Stahle and Ibrahim Baggili, University of New Haven, CT

Paper: Automated Input Generator for Android Applications

Tae Oh, Rochester Institute of Technology, NY

SYMPOSIUM SESSION 8: Software Security

Chair: Sanjay Goel, University at Albany, SUNY, NY

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

Invited Talk: Enhancing Security in the Software Development Life Cycle (SDLC)

Eweoya Ibukun and Sanjay Misra, Covenant University, Ova, Nigeria

Invited Talk: Identification of Suspected Files Using Timeline Construction Approach

Gaurav Balaiwar and Upasna Singh, Defence Institute of Advanced Technology (DU), India

View the Conference agenda and your schedule with the Conference Mobile Event Guide:

<https://www.regonline.com/register/m/?eventid=1375817>



Training Track

Attendees must be pre-registered to attend

Cyber Incident Analysis – Tuesday, June 3

Martin Manjak, Jonathan McKinney, Marquis Montgomery, and Sanjay Goel

11:00 a.m. – 4:00 p.m.

Meeting Room 7

Cyber Incident Analysis is becoming a key function for organizations' security analysts. They analyze the source of attack, the damage that has been caused, and the underlying vulnerabilities that made the attack possible. A recent spate of attacks on several large corporations such as Target, Neiman Marcus, and Michaels, and Sally Beauty has highlighted the rising sophistication of attacks necessitating advanced analytic skills for incident response. The goal of this tutorial is to provide students with a method for performing cyber incident analysis. We will use real incident data sets to illustrate different incident analysis techniques. Students will learn to identify the data sources, e.g. log files, and how to process the data into a meaningful analysis format. The tutorial will cover analysis of individual files as well as techniques to correlate information across multiple log sources to build a chain of evidence across those log files. We expect the students to work hands-on during the tutorial using data sets that we will provide for download. By the end of class, students will understand the process of cyber incident analysis and will be able to perform the first level of analysis.

Digital Forensic Incident Response and Advanced Persistent Threats – Wednesday, June 4

Peter Stephenson, Ph.D.

Norwich University

10:30 a.m. – 3:30 p.m.

Meeting Room 7

DFIR – Digital Forensic Incident Response – is a buzzword and, curiously, about the only place one can get any serious training in it is SANS. This half day session will describe DFIR, look at some tools and techniques and talk specifically about APTs – Advanced Persistent Threats. It is a good introduction for the more in-depth training that SANS provides.

The session begins with a definition of DFIR, what it includes, what it is, who does it, etc. and then looks at some of the tools used to analyze a digital incident. Many DFIR tools are open source, but this session also will use AccessData's new platform, InSight as a teaching tool since it ties all of the DFIR pieces together nicely.

The session then takes a deeper dive into some live malware samples and, after a discussion of APTs examines a recent malware both statically and dynamically to understand what makes it both persistent and advanced.

Finally, the session will provide a representative list of open source tools that should be in every DFIR tool kit as well as reference books that should be in every DFIR library. The topics to be covered are:

- What is DFIR?
- How does one conduct DFIR including both technical and administrative details?
- What tools are useful for DFIR? Brief looks open source and commercial tools.
- Dynamic and static malware analysis fundamentals – live demos
- What do we mean by APTs? What makes them advanced? How do they achieve persistence?
- Demo of analysis of a recent APT – The Eviction Notice Scam

Please remember to complete the Conference survey at
<https://www.surveymonkey.com/s/NYSCSCEval14>



PANOPLY



New for this year! Panoply is a network assessment and network defense competition combined into a single event. Participants compete for control of common resources and the critical services on those resources. Once an individual takes possession of a resource, they must secure that resource against attacks from other players while maintaining the critical services running on the resource. Participants accumulate points for controlling and operating critical services. The player with the highest point total at the end of the competition wins.

Game play will take place in the Convention Hall on **Tuesday, June 3 from 8:30 a.m. to 4:15 p.m. and on Wednesday, June 4 from 8:30 a.m. to 3:45 p.m.** Each day will be held as a separate competition with different target sets. Awards will be given to the top three scorers at the conclusion of each day of competition.

On-site registration is available in the Convention Hall. **Note players must provide their own laptop and assessment tools.**

Congratulations

Congratulations to the winners of the 2014 Cyber Aces New York State Championship and to the winners of the 2013-2014 New York State “Kids Safe Online” Poster Contest!



The 2014 NYS Cyber Security Conference would like to thank all of our sponsors, exhibitors, speakers, and volunteers for making this another successful year!



Terabyte Sponsor

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

In here, government on the go is better connected. Now more than ever, mobile solutions from AT&T enable you to be more effective and efficient from almost anywhere. *In here, cloud aligns costs with consumption.* Transform how you work with secure, on-demand scalable Cloud solutions that help save IT costs while enabling you to accelerate the delivery of citizen services. *In here, we know your world and we know how to secure it.* Analyzing over 23.7 petabytes of data a day, the power of the AT&T proactive and intelligent network helps you safeguard your data to protect citizen information and the public trust. *In here, real time collaboration is a reality.* Unified communications empowers better collaboration by offering one solution for voice, email, messaging and conferencing, which integrates with core applications. *In here, public safety comes first.* From call to car to crisis, AT&T solutions for public safety can help you meet your challenges head on. *In here, our expertise allows you to focus on yours.* AT&T can help manage, monitor and maintain enterprise-wide application solutions so you can concentrate on the longterm strategy while improving performance.



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



Megabyte Sponsor

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



Kilobyte Sponsor

HP is a leading provider of security intelligence and compliance solutions for enterprises that want to mitigate risk and defend against today's most advanced threats. Based on market-leading products from ArcSight, Atalla, Fortify and TippingPoint, HP Enterprise Security Products enables organizations to take a proactive approach to security, integrating information correlation, application analysis and network-level defense. HP Security Research strengthens this portfolio of solutions through innovative research, delivering actionable security intelligence while providing insight into the future of security and the most critical threats facing organizations today. More information about HP Enterprise Security Products is available at <http://www.hpenterprisesecurity.com>.



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.

Sponsors/Exhibitors

23



Kilobyte Sponsor

Twinstate Technologies® specializes in cybersecurity, proactive IT, hosted and on-premise voice solutions, with security being top of mind in every area of service. Its Information Security Services (ISS) detects and defends against cyberattacks via its Preemptive Attack Strategies™ (PAS) platform and Multi-Threat Protection™ (MTP) methodology. As an added layer of ISS, the company offers the guidance of its Information Security Advisory Team (ISAT). A go-to partner for organizations, Twinstate Technologies helps to alleviate internal IT demands while maximizing security posture.

Twinstate Technologies is headquartered in Morrisonville, New York, with offices in Latham, New York; Colchester, Vermont; and Concord, New Hampshire. Service provider for more than 45 years. WBE, C|EH.

518 563 7100 / twinstate.com



The Graduate College at Bay Path College

Bay Path College, located in western Massachusetts, has over 12,000 alumni worldwide, is a member of eight-college consortium with over 24,000 students, offers NCAA Division III Athletics, and is accredited by the New England Association of Schools and Colleges. The Graduate School offers over 20 career-oriented graduate degrees and certificates designed for working adults – including an online MS in Cybersecurity Management that is ideal for those in the field as well as for those who work in related areas. The curriculum cuts across organizational lines, taking a holistic approach to protecting digital assets, data, software, and networks.



Bit9 + Carbon Black offers the industry's most complete solution for advanced threat protection and incident response on endpoints and servers. The company helps organizations protect themselves from advanced threats in two critical ways: by reducing their attack surface through new signature-less forms of prevention, and rapidly detecting and responding to threats. 1,000 organizations—from Fortune 100 companies to small businesses—use Bit9 + Carbon Black to increase security, reduce operational costs and improve compliance.

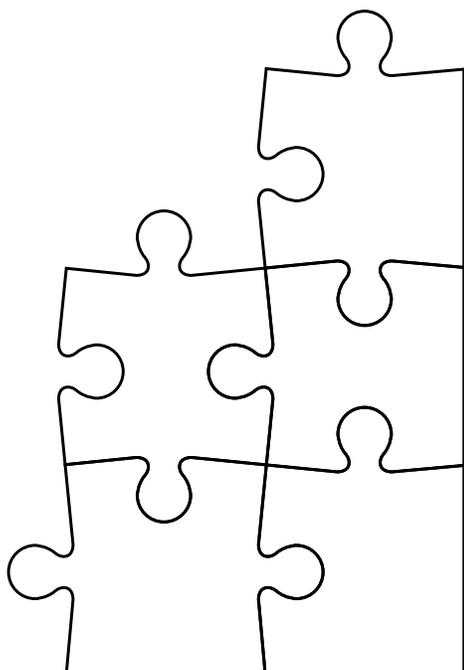
CHAMPLAIN COLLEGE



Champlain College Established in 1878, Champlain College offers degree and certificate programs at the undergraduate and graduate level in Computer Forensics & Digital Investigation, Cyber Security, and over 30 additional areas. Each program integrates projects from your workplace, enabling you to immediately apply what you learn to what you do. cps.champlain.edu



CSC offers a broad portfolio of cybersecurity services. We employ more than 1,700 IT security practitioners armed with subject matter expertise, best practices and advanced security technologies. As a result, CSC has helped more than 250 clients overcome advanced threats. Our Offerings address the six areas all organizations should be addressing. Learn more about how CSC enterprise security services can boost your Cyber Confidence™ today.





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/>



Fact and Measures, LLC is a locally owned MBE and Veteran Owned company. We are a certified Splunk partner with certified Splunk Architects on staff that have deep expertise in the Splunk App for Enterprise Security. We also specialize in Big Data projects, helping you combine your unstructured data with your structured data to find patterns and actionable insight. We have subject matter experts in Government data sources as well as MS and PhD level Statisticians and Mathematicians that slice, dice, and display your data using tools like Splunk, Hunk (Hadoop/Splunk), Tableau, R, SPSS, SAS, Excel, SQL Server SSAS, and SharePoint.



FireEye helps organizations defend themselves against the newest generation of cyber attacks. These highly sophisticated attacks easily circumvent traditional signature-based defenses, such as next-generation firewalls, IPS, anti-virus, and gateways. The FireEye platform provides real-time, dynamic threat protection without the use of signatures to protect an organization across the primary threat vectors, including Web, email, and files. The combination of FireEye's threat prevention platform, people and intelligence helps eliminate the consequences of security breaches by telling their customers when they are being attacked, communicating the risk, and equipping them to rapidly resolve the incident. FireEye has over 1,000 customers including Government, Education, Fortune 100 and more.



GreyCastle Security is a cybersecurity consulting firm focused on risk management, awareness and operational security. Our company was established to counter rapidly evolving cybersecurity threats and manage risks in people, process and technology.

GreyCastle Security is comprised exclusively of highly certified professionals with prior security experience in banking, healthcare, education, retail and gaming. Our team members are all former CISOs, ISOs, security specialists and operators. We bring a client perspective to everything we do.

All we do is cybersecurity. All day, every day. We provide assessments, training, testing and response capabilities to organizations of all sizes, types and industries. We bring passionate practicality to cybersecurity.

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



The Hacker Academy (www.hackeracademy.com) is trusted by some of the world's largest and most notable organizations to educate and secure their staff; both technical and non-technical alike. THA provides members with an engaging, cloud based, security training environment so that they can learn the latest information security techniques and push their technical limits at their own pace. Our Role Based, User Awareness training program is specifically designed for each and every employee within an organization. These Hacker Academy programs can also be purchased through iSECURE, LLC (www.isecurenet.net), a NYS certified, woman-owned security company.



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.

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>

Interface Masters



*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/>



MAC Source offers business communications solutions that include consulting, design, implementation and management services. With a portfolio of voice, data, video, and network security products, MAC Source customers can depend on us for safe and reliable technology solutions. From small business applications to global enterprises to fully-integrated call centers, our experienced professionals ensure your business is optimally connected. Our solution experts take the time to understand your organization and deliver solutions tailored to your individual needs. As part of Meridian Group International, MAC Source can leverage the expertise of a global provider of IT solutions, services, and equipment leasing.



Nettitude is an IT Cyber Security and Risk Management Company with bases in North America and the United Kingdom.

Nettitude specializes in Security Testing, Security Solutions, Incident Response, and Security Consultancy in all areas including compliance for PCI DSS, HIPAA and Sarbanes-Oxley. Our Security Testing Consultants provide industry leading Infrastructure, Application, Mobile and Advanced Persistent Threat Testing for clients ranging from SMB to Enterprise and Government.

As one of less than ten organizations worldwide to be recognized by the PCI Security Council as a QSA, ASV, P2PE-QSA, and PA-QSA, Nettitude is your resource for all areas of PCI DSS Compliance.



Novacoast is an international IT Professional Services and Product Development Company built on a foundation of engineering expertise and a culture of creative problem solving. Empowered on every level by our flexible and fearless perspective, Novacoast combines its advanced technical knowledge with our customers' expertise so together we can make informed decisions and avoid costly IT mistakes.

We've designed and implemented Security Solutions for organizations of all sizes and setups. Our certifications and recognitions with partners, including Symantec, lead the industry. We specialize in security assessments that test every level of an organization's vulnerability.

<http://www.novacoast.com/services/security-compliance/>



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



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.quoterion.com



Since 1995, Regional Computer Recycling & Recovery provides cost effective secure environmental solutions for idle, obsolete, and non-working high technology products; while emphasizing environmentally sound processing methods for maximizing value and recovery while minimizing and/or eliminating disposal of electronics in landfills.



Splunk Inc. provides the leading software platform for real-time Operational Intelligence. Splunk® software and cloud services enable organizations to search, monitor, analyze and visualize machine-generated big data coming from websites, applications, servers, networks, sensors and mobile devices. More than 7,000 enterprises, government agencies, universities and service providers in over 90 countries use Splunk software to deepen business and customer understanding, mitigate cybersecurity risk, prevent fraud, improve service performance and reduce cost. Splunk products include Splunk® Enterprise, Splunk Cloud™, Splunk Storm®, Hunk™: Splunk Analytics for Hadoop and premium Splunk Apps. To learn more, please visit <http://www.splunk.com/company>.



It's a dangerous world out there. tw telecom's security solutions keep your data and network secure. tw telecom helps you stay one step ahead of "mischief" by proactively monitoring network attacks and anomalies. We help you gain deeper visibility into DNS, HTTP and SIP traffic—and remain alert. tw telecom professionals are dedicated to your security issues. End-to-end—network or CPE based—tw telecom has you covered so you have no worries. When you purchase tw telecom's converged services, security is always included. In addition to voice and VPN, converged services includes Secure Internet Access with built-in Managed Firewall. Equip each of your sites with direct access, or central Internet traffic through a single site, either way you'll be protected. tw telecom's Distributed Denial of Service (DDoS) mitigation and managed security solutions make sure "evil-doers" can't bring your network down. www.twtelecom.com



Utica College offers regionally accredited **Online Bachelor's and Master's** degrees in **Cybersecurity** with concentrations in Intelligence, Investigations, Computer Forensics, Cyber Operations, and Information Assurance taught by highly experienced, credentialed faculty. Utica College courseware meets the Committee on National Security Systems (CNSS) rigorous standards for Information Systems Security Professionals (4011) and Risk Analyst (4016). With the renowned Economic Crime & Cybersecurity Institute, and the Center for Identity Management and Information Protection, the College collaborates with industry and government to develop innovative curriculum and provide students with unique door-opening credentials and career opportunities. Call 315-732-2640 or visit <http://programs.online.utica.edu/programs/> for more information.

CSC.COM • BUSINESS SOLUTIONS • TECHNOLOGY • OUTSOURCING

TOGETHER WE DO AMAZING THINGS

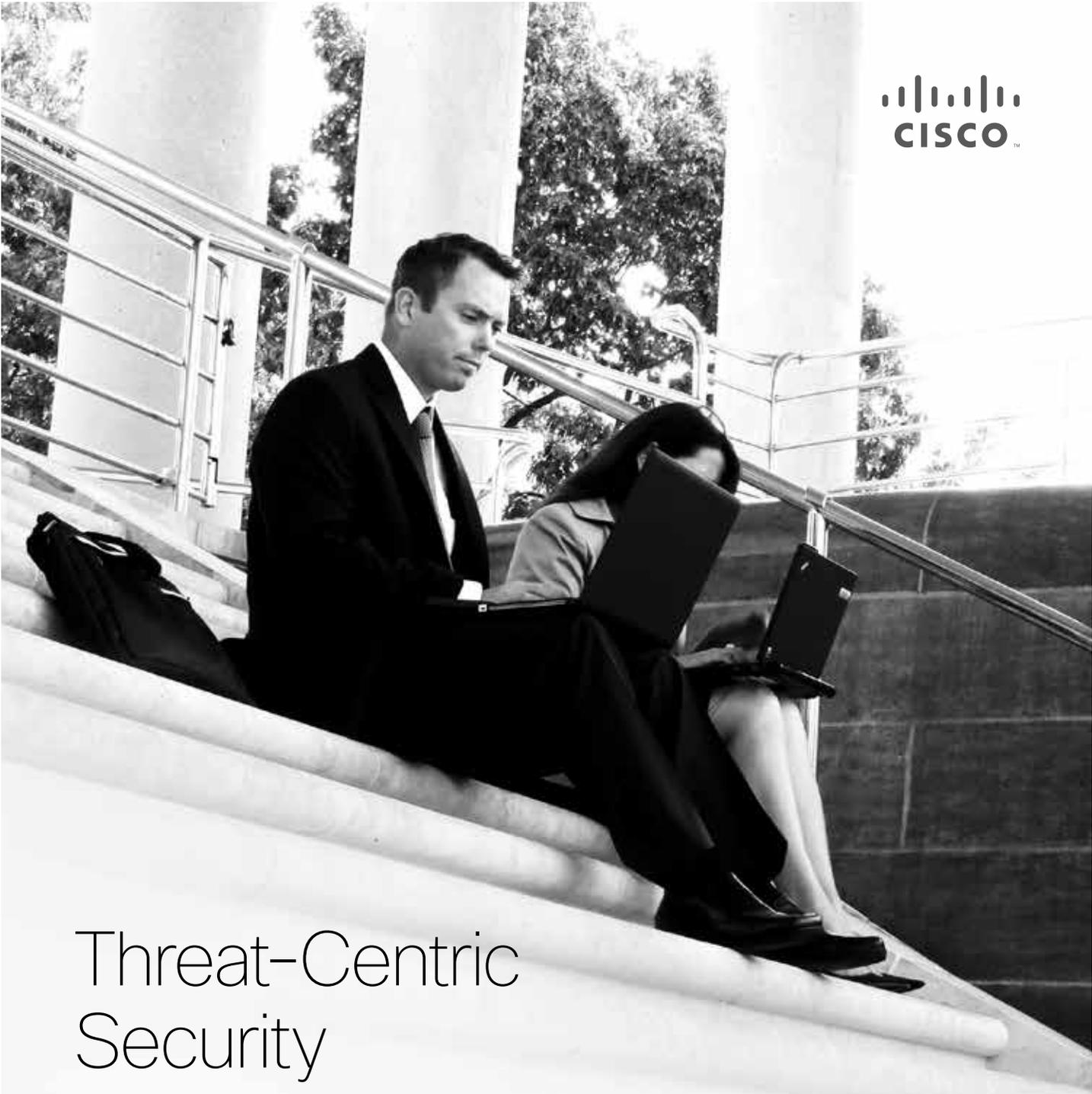


Mobility without vulnerability.

Devices. Apps. Data.



Copyright © 2014 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, the Checkmark Logo, and Norton are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries.

A black and white photograph of two business professionals sitting on a wide set of stone stairs. A man in a dark suit and tie is sitting on the left, looking down at a laptop on his lap. A woman in a light-colored blazer is sitting on the right, also looking at a laptop on her lap. A black bag is on the stairs to the left of the man. The background shows a building with large columns and trees.

Threat-Centric Security

Cisco provides a broad portfolio of integrated solutions that deliver unmatched visibility and continuous advanced threat protection across the entire attack continuum, allowing customers to act smarter and more quickly – before, during, and after an attack.

cisco.com/go/uspscybersecurity



MASTER of SCIENCE in CYBERSECURITY MANAGEMENT

COMPLETELY ONLINE

For more information on the program or to register
for an online webinar, visit: graduate.baypath.edu

graduate@baypath.edu

*588 Longmeadow Street
Longmeadow, MA*

800.782.7284

Bay Path
College

Thin ice is for polar bears.

You ain't no polar bear.



Security Assessment
Security Remediation
Security Management
Incident Response



Greater insight

Change the game on cyber risk

The traditional approach of implementing preventative security measures only — while necessary — may no longer be adequate. The State of New York should consider developing strategies with advanced techniques that provide greater insight into potential threats and options for faster response and recovery. Through an ongoing program to become secure, vigilant and resilient, you can change New York's cyber risk environment and be more confident in your ability to maintain citizen trust.

Attend the following sessions during the 17th Annual New York State Cyber Security Conference to learn more about becoming *Secure.Vigilant.Resilient*.

Wednesday, June 4

1:40 – 2:30 p.m. **“Access Granted. But to the right person?”**
Vikas Bansal, Director, Cyber Risk Services,
Deloitte & Touche LLP

2:50 – 3:45 p.m. **“Adaptive Vigilance.
Building the capabilities to detect today's threats”**
Joe Magee, Director, Vigilant by Deloitte,
Deloitte & Touche LLP



About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Deloitte.

If you want better security, think like a bad guy.

Get to threats before they get to you

We are pleased to be a Kilobyte sponsor
Visit us at booth #31

hp.com/go/esp



© 2014 Northrop Grumman Corporation

UNMANNED SYSTEMS •

CYBER •

C4ISR •

LOGISTICS •

THE VALUE OF ADVANCING THE FRONT LINE IN THE CYBER BATTLE.

From infrastructure to military, our cyber expertise knows no limits. For more than 30 years, Northrop Grumman has been trusted to protect our customers' full range of missions. Our solutions provide the adaptability to face evolving threats and the expertise to eliminate them.

That's why we're a leader in cyber.

THE VALUE OF PERFORMANCE.

NORTHROP GRUMMAN

www.northropgrumman.com/cyber



IF YOU THINK YOUR ORGANIZATION IS SAFE, THINK AGAIN.

Many experts believe it's not a matter of *if* you'll be breached, it's a matter of *when*.

If you are a business owner, CEO, CIO or IT stakeholder in charge of your organization's technology environment, now is the time – more than ever – to be prepared.

Cyberattacks aren't going away – they're escalating.

Twinstate Technologies® is helping to halt the bad guys through its Information Security Services (ISS), designed to detect and defend against malicious cyberattacks. As an added layer of ISS, the company offers the guidance of its Information Security Advisory Team (ISAT), a group of cybersecurity experts, including Certified Ethical Hackers (CEH), dedicated to providing comprehensive best practices on cybersecurity protection.

Shaping Secure, Intuitive and Unified Technology Environments

CYBERSECURITY IT VOICE

Twinstate Technologies is headquartered in Morrisonville, New York, with offices in Latham, New York; Colchester, Vermont; and Concord, New Hampshire.

518.563.7100 / twinstate.com
learn_more@twinstate.com

Twinstate Technologies® is a certified Woman-Owned Business Enterprise (WBE) on the Federal level and in New York, Vermont and New Hampshire.

SERVICE PROVIDER FOR MORE THAN 45 YEARS

Sponsor Demonstration Schedule

This year the Terabyte and Megabyte sponsors will hold demonstrations at their booths. The demos are scheduled for:

Terabyte Sponsor

AT&T

June 3 at 10:40 a.m. - 11:00 a.m. and June 4 at 10:05 a.m. - 10:25 a.m.

Megabyte Sponsors

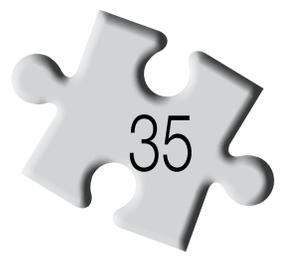
June 3

1:55 p.m. – 2:05 p.m. Cisco Systems
3:05 p.m. - 3:15 p.m. Symantec Corporation

June 4

11:25 a.m. - 11:35 a.m. Symantec Corporation
2:35 p.m.-2:45 p.m. Cisco Systems

Conference Co-Hosts



Deborah Snyder

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

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

From November 2001 to November 2012, she served as the Chief Information Security Officer for the New York State Office of Temporary and Disability Assistance (OTDA), where she established and lead the agency's Information Security Office and comprehensive Information Security Assurance Program. She informed and advised executive management on security governance, risk and compliance, and managed a portfolio of initiatives designed to increase awareness, mitigate risk, optimize protection of information assets and prevent, detect and recover from incidents.

Ms. Snyder has extensive experience in state and local government program administration, information technology and information security services. Prior to serving as the agency's CISO, Ms. Snyder served as the Director of Human Services Modernization, leading program reform, redesign and system modernization initiatives encompassing multiple agencies and systems, managing state program, IT, and vendor resources to deliver innovative program and technology solutions.

Ms. Snyder is an active participant and contributor to the IT and Information Security community. She has championed efforts to strengthen the State's information security posture and advance the profession at large. She has served as Co-Chair of the NYS Forum Information Security Work Group, VP of Education for the local ISACA Chapter, and is a member of the Project Management Institute, InfraGard, Information Systems Security Association (ISSA), Information Systems Audit and Control Association (ISACA), and the Institute of Internal Auditors (IIA). She co-authored the book entitled "SECURE – Insights From The People Who Keep Information Safe," which offers industry leaderships insights and perspective, and has received recognition for excellence in government information services, and outstanding contributions to the field of information security and cyber security. She is a highly regarded speaker and instructor on topics critical to executive-level business and IT professionals.

Ms. Snyder graduated from the State University of New York at Albany, and holds several industry certifications including Certified Information Systems Security Professional (CISSP), Certified in Risk and Information Systems Control (CRISC), SANS Global Information Assurance Certification in Security Leadership (GIAC GSLC) and Project Management Professional (PMP).

Sue R. Faerman

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

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

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

Donald Siegel

*Dean of the School of Business and Professor of Management
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*, *Strategic Management Journal*, *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 36 special issues of leading journals in economics, management, and finance.

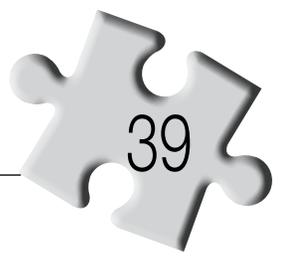
Don was recently ranked #2 in the world for research on university entrepreneurship and #760 in the world among academic economists. He has published 101 articles and 7 books on issues relating to university technology transfer and entrepreneurship, the effects of corporate governance on performance, 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*, the *Oxford Handbook of Corporate Governance*, the *Oxford Handbook of Corporate Social Responsibility*, and the *Oxford Handbook of the Economics of Gambling*, all published by Oxford University Press, and the *Handbook of University Technology Transfer and Academic Entrepreneurship* (forthcoming, University of Chicago Press). His citation count, according to Google Scholar, is 17,416 with an h-index of 58.

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.

Please remember to complete the Conference survey at
<https://www.surveymonkey.com/s/NYSCSCEval14>



Terabyte Sponsor



at&t

Megabyte Sponsors



Kilobyte Sponsors

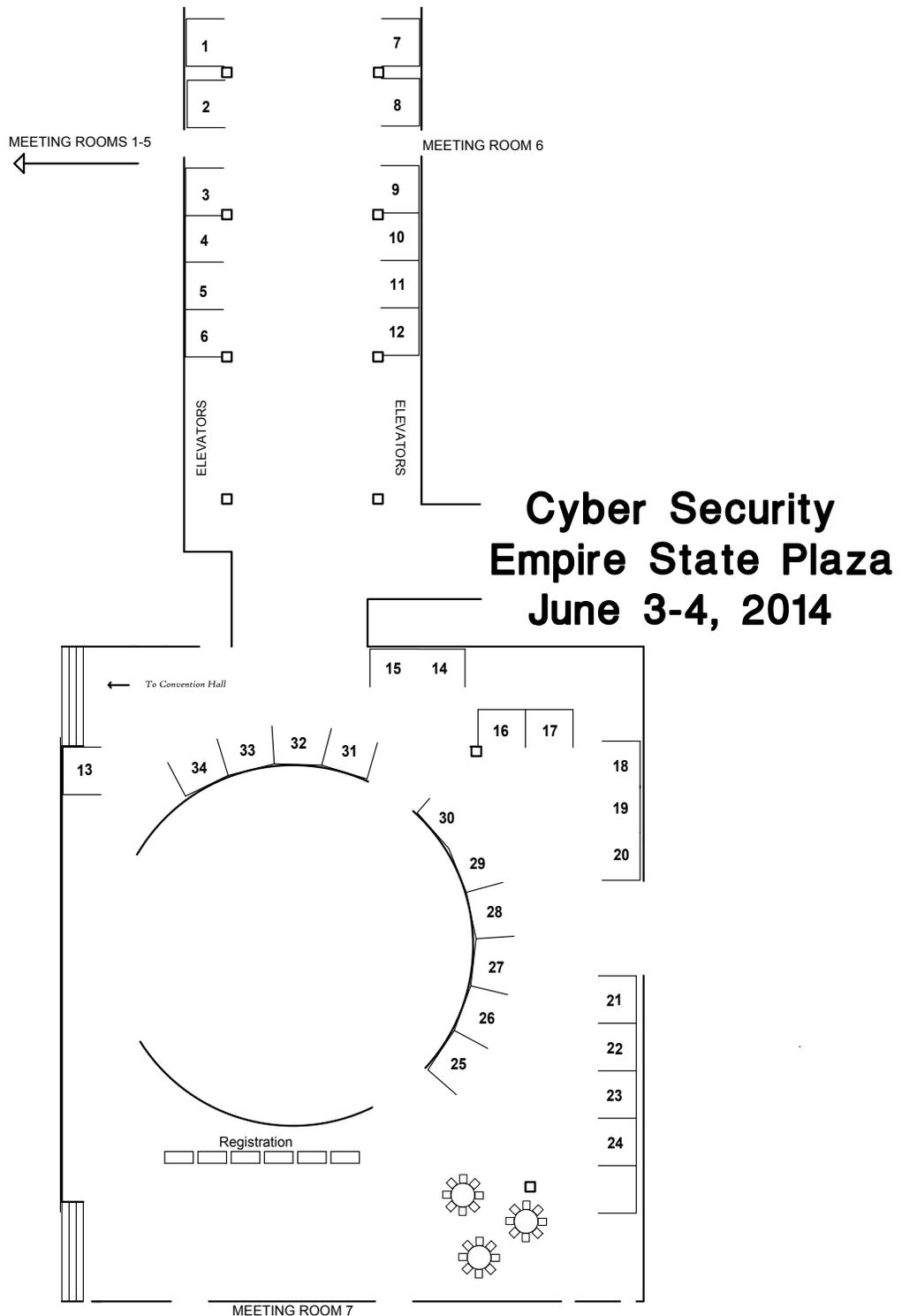


NORTHROP GRUMMAN



Booth Assignments

- 01: NYS Forum
- 02: Excelsior College
- 03: Novacoast Inc.
- 04: NYSTEC
- 05: Quanterion Solutions Incorporated
- 06: FireEye, Inc.
- 07: Facts and Measures, LLC
- 08: Bit9
- 09: MAD Security
- 10: Champlain College
- 11: CSC
- 12: Nettitude Inc.
- 13: NYS Office of Information Technology Services
- 14: Cisco – Megabyte Sponsor
- 15: Cisco – Megabyte Sponsor
- 16: Twinstat Technologies – Kilobyte Sponsor
- 17: GreyCastle Security
- 18: AT&T – Terabyte Sponsor
- 19: AT&T – Terabyte Sponsor
- 20: AT&T – Terabyte Sponsor
- 21: Regional Computer Recycling & Recovery
- 22: University at Albany’s College of Computing and Information and School of Business
- 23: IBM
- 24: Utica College
- 25: The Graduate School at Bay Path College
- 26: MAC Source Communications
- 27: Dyntek Services
- 28: Splunk Inc.
- 29: Symantec – Megabyte Sponsor
- 30: Symantec – Megabyte Sponsor
- 31: HP – Kilobyte Sponsor
- 32: Interface Masters Technologies
- 33: tw telecom
- 34: Northrop Grumman – Kilobyte Sponsor



Passport Drawing



Visit all of the Exhibitors for a chance to participate in the Passport raffle. Bring the Exhibitor passport to each booth and have it stamped. Drawings will be held on Tuesday, June 3 – 3:10 p.m. - 3:20 p.m. and Wednesday, June 4 - 1:30 p.m. - 1:40 pm. Complete the passport early for more opportunities to win. Hand the completed passport in by 2:30 p.m. on June 3 to be entered in the drawings on both days!