Tuesday, April 2, 2013

7:30 am - 8:30 am	**Registration and Continental Breakfast**

Presented by Quantum Secure, Inc.

8:30 am - 8:45 am	**Opening Remarks** Bob Bragdon, Publisher, CSO magazine
8:45 am - 9:30 am	**Opening Keynote: CyberSecurity - The Executive Order and Defining the Future of Information Security** Phil Agcaoili, Chief Information Security Officer, Cox Communications, Inc.

With the Cybersecurity Act still in congressional limbo, President Obama enacted an executive order for improving critical infrastructure cybersecurity in February 2013, and it is a directive that companies simply can't ignore. The order calls for partnership between government and owners and operators of critical infrastructure to improve cybersecurity information sharing and collaboratively develop and implement risk-based standards. The Department of Homeland Security has identified 18 critical sectors for cybersecurity -- including the power grid, communications, and water systems -- critical for the safe and secure operation of government and industry, and outlines protections to address their vulnerabilities. In this keynote, Phil Agcaoili, Chief Information Security Officer with Cox Communications, Inc., discusses the implications of the cybersecurity executive order for the critical sectors and share insights on what to pursue in order to prepare for the long-term implications of information security.

9:30 am - 9:45 am	**Connecting Security to the Business** Dwayne Melancon, Chief Technology Officer, Tripwire, Inc.

Now that information security is a boardroom topic, how can CISOs show value to their organizations in meaningful ways? In this session, Dwayne Melancon, Tripwire's Chief Technology Officer, shares techniques to elevate security strategies and tactics in a way that demonstrates

greater business value, makes it easier to defend and acquire resources, and contributes to the success of your organization.

9:45 am - 10:03 am   **Boxing Outside the Think: Conducting Creative Vulnerability Assessments**
Roger Johnston, Head, Vulnerability Assessment Team, Argonne National Laboratory, a CSO40 Winner Organization for 2013

Argonne National Laboratory is one of the U.S. Department of Energy's largest national labs for scientific and engineering research. The Lab has collected enormous amounts of knowledge from all the cumulative years the Lab's scientist and engineers spend studying and working to solve the nation's most important challenges in energy, the environment and national security. In this session, Dr. Roger Johnston, who heads the lab's vulnerability assessment team, will share very effective -- if not unusual -- right-brained, creative vulnerability assessment techniques to help your organization outsmart the bad guys, while improving security.

10:03 am - 10:21 am   **Modernizing Security Assessments to Meet the Needs of Organizational and Application Growth**
Jerry Walters, Director of Information Security, OhioHealth, a CSO40 Winner Organization for 2013

Expansion, regardless of the cause, requires organizations to rethink existing security initiatives. With multiple hospitals and healthcare centers, OhioHealth's growth through acquisition and the proliferation of new applications tested the traditional security assessments the IT team had been relying on. Through detailed and accurate study and planning, OhioHealth modernized its approach. In this session, hear how the new assessments enable automation, dashboards, and real-time processes and elevate OhioHealth's overall security, disaster recovery and business continuity efforts.

10:21 am - 10:39 am   **Best Practices in Security and Vulnerability Assessment: A Q&A Panel Discussion**
Roger Johnston, Head, Vulnerability Assessment Team, Argonne National Laboratory, a CSO40 Winner Organization for 2013
Jerry Walters, Director of Information Security, OhioHealth, a CSO40 Winner Organization for 2013
Bob Bragdon, Publisher, CSO magazine

10:39 am - 11:09 am   **Networking Break**

Presented by Qualys, Inc

11:09 am - 11:24 am   **The Value of Actionable Threat Intelligence**
Don Gray, Chief Security Strategist, Solutionary, Inc

When security teams understand the threat landscape, they can demonstrate the value of security programs to executive decision-makers. Join us as we share case studies and findings from a recent industry survey that reveal the positive impact actionable threat intelligence can have on an organization.

11:24 am - 11:42 am   **Managing Trade Controls and Compliance with Access Security**
Tom Rohling, Manager, Enterprise Security & Collaboration, GE Aviation, a CSO40 Winner Organization for 2013

Like many global enterprises, GE Aviation must navigate numerous trade controls and regulations, and the task is further complicated due to a strong military market presence. To ensure only authorized employees, contractors, and others have access to regulated and controlled technical data -- and thus keep GE Aviation in compliance with global trade restrictions without impacting collaboration and productivity -- the IT teams developed a robust Trade Control Access Solution. Today, the system sustains more than 200,000 queries daily to ensure worldwide export and import compliance. In this session, hear about the key components of the solution, including data classification management systems and real-time evaluation interfaces and infrastructure.

11:42 am - 12:00 pm	**Harnessing Security to Drive Business**

Mark Coderre, Head of Security Architecture, Aetna Inc., a CSO40 Winner Organization for 2013
Jonathan Swanson, Lead Business Consultant, ITSO Business Optimization, Aetna Inc., a CSO40 Winner Organization for 2013

Aetna's global presence is growing, but with growth comes complexity. Each country has its own set of regulations and risks, and Aetna must continually assess its security governance to ensure regulations are met and risks are mitigated. In this session, hear how a team of analysts and security architects renewed Aetna's assessment processes, centralized the information, and created a collaborative ecosystem of legal, compliance, IT and business stakeholders – all working to ensure Aetna's international business and IT operations are secure, and to expedite future growth by better understanding costs and risks as the company expands its global footprint.

12:00 pm - 12:18 pm	**Compliance in the Global Economy: A Q&A Panel Discussion**

Mark Coderre, Head of Security Architecture, Aetna Inc., a CSO40 Winner Organization for 2013
Tom Rohling, Manager, Enterprise Security & Collaboration, GE Aviation, a CSO40 Winner Organization for 2013
Jonathan Swanson, Lead Business Consultant, ITSO Business Optimization, Aetna Inc., a CSO40 Winner Organization for 2013
Bob Bragdon, Publisher, CSO magazine

12:18 pm - 12:48 pm	**Enabling Secure Mobile and Cloud Collaboration**

Hormazd Romer, Senior Director of Product Marketing, Accellion

Today's enterprises need to make content available to all employees to access anytime, anywhere, and on any device -- yet the challenges go far beyond just BYOD and employees using unsecure apps on their own devices. Today's model of the collaborative and mobile enterprise, coupled with cloud computing at the core of its infrastructure, can leave organizations at risk. The BYOD model, coupled with easily accessible and free consumer-grade cloud services, has just made it more difficult than ever to control and secure enterprise content. Join us for this session to learn how your organization can realize the gains of the new enterprise mobility model while maintaining data security, control, and compliance. This presentation will focus on the importance Enterprise Mobility Management (EMM), including secure collaboration and mobile access to content on ECM systems, and we'll also discuss the benefits and risks of private vs public cloud deployment solutions.

12:48 pm - 2:00 pm	**Networking Lunch with Table Topic Discussions Hosted by Selected CSO40 Honorees**

Presented by Accellion

<u>Discussion Table Topics and Moderators:</u>

Improving Security Operations with Cyber Intelligence and Insider Threat Reporting (Bob Cheong, Chief Information Security Officer, Office of Information Security, Los Angeles World Airports)

Effective Strategies for Improving Risk Awareness (Andy Ellis, CSO, Akamai)

The Evolution of Information Security Within Organizational Workflows (Stephen Gay, Information Technology Service Associate Director - Information Security, Kennesaw State University)

Creative Approaches to Vulnerability Assessment (Roger Johnston, Head, Vulnerability Assessment Team, Argonne National Laboratory)

Cybersecurity Threat Management to Protect Customer Data (Jack Key, CISO, USAA)

Information Risk Management (Karolyn Maloney, Security Architect, Aetna)

Governance and the Importance of Senior Leadership Engagement (Gene Oliver, Vice President, Global Systems & IT, Online Computer Library Center, Inc (OCLC); William Lisse, Director, Security Intelligence & Architecture, Vantiv (formerly CISO, OCLC when managing the CSO40 project))

Managing Ecosystem Security Risks: Phishing, Malware and the DNS System as a Whole (Andy Steingruebl, Senior Manager, Customer and Ecosystem Security, PayPal)

International Privacy and Security Challenges for U.S.- Based Organizations (Jonathan Swanson, Security Architect, Aetna)

Effectively Managing Regional Security Command Center Operations (Mike Yong, SVP, Regional Security Command Center (Asia Pacific), Citi)

2:00 pm - 2:15 pm	**Security Metrics Aligned with Business Initiatives** Elizabeth Ireland, Vice President Marketing , nCircle

Business initiatives often require investments in IT security, yet those investments are not always well-understood or even fully supported by executives around the boardroom table.   CISOs need to communicate security investments in context of business benefits, helping other organizations and non-security professionals see business alignment between budget support for IT security, and business initiatives.

2:15 pm - 2:33 pm	**Yes to IS – Gaining Consensus on a Comprehensive Budget for Information Security, Risk Management and Compliance** Stoddard Manikin, Director, Information Systems Security, Children's Healthcare of Atlanta

Hired to shape a next-generation, five-year information security program for Children's Healthcare of Atlanta, Stoddard Manikin has a lot on his plate. He and his team have to consider all the new technologies that expand access, such as mobile devices, while locking down privacy, mitigating risks and maintaining compliance with numerous regulations. Of course, it takes funding. In this session, Stoddard will share best practices and tips for preparing a comprehensive budget that management understands and funds.

2:33 pm - 2:51 pm	**Yes, Better Risk Management is Like Herding Lizards -- But It Can Be Done** Andy Ellis, CSO, Akamai Technologies, a CSO40 Winner Organization for 2013

Ever watch lizards scatter haphazardly when they are threatened, or when they simply recognize something they suspect is dangerous? It's the same arbitrary action organizations often take when they're told of the potential dangers to their information and supporting technology. Rather than understand and own the risks -- and then develop focused risk management models to effectively mitigate them -- organizations instinctively scramble for any (and as much) cover as they can. In this session, hear how organizations generate real security value when they are aware of -- and believe in -- the risks, seize the opportunity to understand their risk appetites, and change their instincts to be proactive rather than reactive.

2:51 pm - 3:09 pm	**How Do We Create and Enable Better Risk Management?: A Q&A Panel Discussion** Andy Ellis, CSO, Akamai Technologies, a CSO40 Winner Organization for 2013 Stoddard Manikin, Director, Information Systems Security, Children's Healthcare of Atlanta Bob Bragdon, Publisher, CSO magazine
3:09 pm - 3:39 pm	**Networking Break**
3:39 pm - 3:54 pm	**Protecting Data in the Post-PC World** Jennifer Cheng, Product Marketing Manager, WatchDox, Inc.

As the use of tablets and mobile devices has proliferated in enterprises, the issue of protecting sensitive data has jumped to the forefront of many CIOs' minds. Whether sanctioned by IT or not, employees have begun to access and share their data on post-PC devices, often via file-syncing applications like Dropbox and as email attachments. There are a variety of approaches to protecting this data, including mobile device management (MDM), mobile application management (MAM), application containerization, virtual desktops, backhauling traffic, and building security into the data itself. Join us as we facilitate a discussion of the pros and cons of the various approaches, including case studies featuring organizations that have met challenges around file sharing, collaboration and data protection.

3:54 pm - 4:09 pm	**Focusing Company Management on Appropriate Risk Mitigation Strategies** Greg Bell, Principal—Global & Americas Service Leader for Information Protection, KPMG

A key focus today for our boards of directors and senior leadership is " Cyber Risk." As security and risk practitioners, we need to focus the conversation on developing a manageable and maintainable enterprise program for the long haul. To add value, we need to link security and risk solutions to innovation in the business, as opposed to the traditional IT spend. In this discussion, Greg Bell will highlight some of the key challenges and suggested strategies that work today.

4:09 pm - 4:24 pm	**Identity and Access Management for the Real World**

Marc Potter, North American Sales, Dell

It seems like security, governance and compliance are the hot topics these days, but have we looked closely at what it takes to achieve real success with them? The real world has limited budgets, tight deadlines, ever increasing environmental complexity, and a constantly changing security landscape. In this session, Marc Potter will discuss how to develop an identity and access management approach that works with these realities. The discussion will focus on access governance, privileged account management and identity administration that doesn't require heavy investments, rigid infrastructure and inflexible technologies — and that can be built on a company's existing foundation.

4:24 pm - 4:39 pm	**Vulnerability Management for the Cloud** Andrew Wild, Chief Security Officer, Qualys, Inc

Vulnerability management is a critical security control, and while it's generally well understood, cloud computing — and particularly infrastructure-as-a-service -- brings about sweeping changes that impact and organization's vulnerability management. Specifically, cloud environments can be extremely dynamic with machines powered up and down frequently, added and removed quickly, and some remaining down for weeks or months — all of which can result in an outdated, stale configuration, and inaccurate vulnerability management information. As well, traditional vulnerability assessment relies upon the IP address of an asset, or a network block of addresses, while IP addresses in IaaS cloud are dynamic, often from shared network blocks. Finally, cloud environments offer the ability to discover important information about an asset through the cloud management system, without accessing the asset directly. Join us as we explore these challenges and opportunities for vulnerability management.

4:57 pm - 5:15 pm	**The Critical Role of Security Maturity to Your Organization's Future** Gary Warzala, CISO, Visa

The concept of security maturity holds the promise to measure security performance to meet critical objectives. In practice, it becomes a meaningful way to communicate and measure progress toward strategic goals — and one that resonates with executive management, makes strategies tangible, and helps motivate the security workforce. Join us for this session to understand how you can apply this concept to your organization.

5:15 pm - 5:33 pm	**Security Intelligence as the Next Frontier -- Why It Matters: A Q&A Panel Discussion** Charles King, Managing Director, The King Group William Lisse, Director, Security Intelligence & Architecture, Vantiv Gary Warzala, CISO, Visa Bob Bragdon, Publisher, CSO magazine
6:00 pm - 7:00 pm	**CSO40 Awards Cocktail Networking Reception** *(open to all qualified attendees)*
7:00 pm - 9:00 pm	**CSO40 Awards Dinner and Ceremony** *(open to all qualified attendees)*

Wednesday, April 3, 2013

7:30 am - 8:30 am	**Registration and Breakfast**

Presented by Zscaler, Inc

8:30 am - 8:45 am	**Opening Remarks and a Brief Announcement About the Cyber Security School Challenge**

Bob Bragdon, Publisher, CSO magazine
Joyce Brocaglia, President & CEO, Alta Associates

The Cyber Security School Challenge is a collaborative outreach program to teach kids how to be safe online, and we are counting on security professionals to volunteer to teach cyber safety and ethics to kids in your neighborhood schools. In these brief remarks, learn about our Cyber Security School Challenge and how to download age appropriate lesson plans, videos and games to teach kids how to be safe online.

8:45 am - 9:30 am	**The Rising Risks of Advanced Persistent Threats and Mobile Computing**

Aaron Turner, Co-Founder & Enterprise Security Partner, N4Struct, Inc.

Whether employees are commuting locally to the workplace -- or traveling to other regions of the world -- many hold company data and network access endpoints in their hands via laptops, smartphones, tablets and other mobile computing devices. All of this opens the door to advanced persistent threats and other security hazards. But just how prepared are organizations to handle these threats and the potential they have to infiltrate mobile devices? In this session, security expert Aaron Turner outlines the security risks of mobility, and discusses the complex ecosystem of technology, processes and practices required to mitigate them.

9:30 am - 9:45 am	**Your Data Center is Vulnerable: How Do you Achieve Physical Access Audit and Compliance?**

Andy Kuchel, Vice President, Business Development, Quantum Secure

Data center vulnerabilities come in many forms, including manual, error-prone processes and inadequate authentication. In this session, Quantum Secure will share insights on automation and best practices for physical access and compliance. We'll describe the Quantum Secure SAFE Software Suite designed to ensure identities have the right authenticated access, to the right areas, for the right duration of time. And we'll reveal how SAFE delivers attestation reports, fosters physical identify management, and provides compliance to regulations like SOX, PCI and HIPAA, among others.

9:45 am - 10:03 am	**Building the Trusted Platform Security Infrastructure (TPSI) Program**

Denise Hucke, VP, Technical Security Services, Global Security, Automatic Data Processing, Inc., a CSO40 Winner Organization for 2013
VJay LaRosa, Senior Director, Converged Security Architecture, Global Security, Automatic Data Processing, Inc., a CSO40 Winner Organization for 2013

Three years ago, ADP took a hard look at its security risk and management roadmap, developed an analysis of its existing security platform, and realized that -- in order to remain ahead of risks -- it had to migrate away from standardized protection models. So ADP built a net new, worldwide monitoring and security intelligence and threat prevention ecosystem, incorporating more than 10 different enterprise technologies including a security intelligence data warehouse, designed to manage risks and support controlled assurance. Of critical importance, the platform provides unstructured data protection – looking at where data is, who has access to it, and where it goes. Ultimately, this technology integration creates ADPs centralized management and monitoring infrastructure into a single operational platform for its cyber, fraud and corporate security interests -- and allows rapid decision-making based on the ability to easily look at global internal and external intelligence.

10:03 am - 10:21 am	**Leveraging the Client Security Management Office Portal (CSMO)**

Devon Bryan, Senior Director, Client and Vendor Security Management, Automatic Data Processing, Inc., a CSO40 Winner Organization for 2013
Phani Dasari, Program Manager, Client Security Management Services, Global Security , Automatic Data Processing, Inc., a CSO40 Winner Organization for 2013

When managing the world's largest software-as-a-service platform, ADP is no stranger to the high volume of pre-sales and post-sales client inquiries about the ways it keeps its business secure. In fact, while its not often that a company can point to specific security initiatives that impact top-line revenue, ADP can with its Client Security Management Office Portal – a platform that not only catalogues specific answers for reuse, but generates business intelligence on what clients want and need to know. This centralized repository enables ADP to generate critical responses to clients within days and hours, significantly reducing the time between client proposal to closure.

10:21 am - 10:39 am	**How to Build Better Security Intelligence: A Q&A Panel Discussion**

Devon Bryan, Senior Director, Client and Vendor Security Management, Automatic Data Processing, Inc., a CSO40 Winner Organization for 2013
Roland Cloutier, CSO, Automatic Data Processing, Inc., a CSO40 Winner Organization for 2013
Phani Dasari, Program Manager, Client Security Management Services, Global Security , Automatic Data Processing, Inc., a CSO40 Winner Organization for 2013
Denise Hucke, VP, Technical Security Services, Global Security, Automatic Data Processing, Inc., a CSO40 Winner Organization for 2013
VJay LaRosa, Senior Director, Converged Security Architecture, Global Security, Automatic Data Processing, Inc., a CSO40 Winner Organization for 2013
Bob Bragdon, Publisher, CSO magazine

10:39 am - 11:09 am	**Networking Break**
11:09 am - 11:24 am	**APT Protection Via Data-Centric Security**

Alan Kessler, President and CEO, Vormetric, Inc

The APT tornado is getting larger, is gathering speed, and we're all in its path of destruction. Perimeter security and simple encryption don't cut it. Perimeter security is irrelevant when the threat is inside, while simple encryption gives a false sense of security since it lacks the policy control

to protect against privileged user exploitation. Moreover, while many believe that compliance equals safety, it doesn't. "Check box" security may give comfort, but like a placebo, it offers limited real protection against today's sophisticated cyber-attacks. As the APT landscape evolves, the risk to valuable data is always present, so enterprises need to take a data-centric protection approach, adding defense layers around the very thing that matters most: sensitive data. Join us as we discuss the best ways to reduce the attack surface of APTs and that yield high-value security intelligence.

11:24 am - 11:54 am	**Transforming to a Next-Generation and Business-Enabling Security Organization**
	Jason Clark, Chief Security and Strategy Officer, Websense
	James Robinson, Security Architecture and Strategy Officer, Websense

Today's CISOs must completely re-think the way they do business by transforming from reactive and focused on infrastructure to proactive data- and risk-centric business leaders. Join Jason Clark, CSSO for Websense and James Robinson, Security Architecture and Strategy Officer as they discuss new concepts for layering data controls alongside infrastructure controls to transform your security defenses. By examining these concepts and the framework and tools essential for enabling people, process and technology to collaborate and re-define a next generation security program, they'll provide actionable insights to recalibrate security defenses and protect company intellectual property. Topics they'll cover include: new data-driven approaches to identifying, mitigating and combating threats; ways to transform your users from the greatest vulnerability to a volunteer security team; and how to evolve your threat model from acceptable to amazing security.

| 11:54 am - 12:12 pm | **Driving Security Innovation Through Partnerships** |
| | Dennis Treece, CSO, Massachusetts Port Authority, a CSO40 Winner Organization for 2013 |

The Massachusetts Port Authority (Massport) is testing a cargo scanning system so powerful and accurate that it can find hidden nuclear weapons -- or distinguish regular soft drinks from diet soft drinks. For the first time ever, they may be able to positively identify all the contents of any shipping container -- in under a half a minute -- without ever needing to open it. They also are testing a camera system that's so precise it can identify individual blades of grass from 100 meters away. These prototypes are just some of the innovative technologies in development with the help of the Massport Transportation Security Center of Excellence -- a security technology test-bed and fast-prototype effort to find, prove and quickly bring to market promising new security technologies. In this session, learn more about the center, the technologies it's exploring, and get ideas on how your organization can develop partnerships with government and business to drive security innovation.

| 12:12 pm - 12:30 pm | **Turning Technology Into A Business Traveler's Watchdog** |
| | Richard Gunthner, Vice President & Chief Security Officer, MasterCard Worldwide, a CSO40 Winner Organization for 2013 |

People are a company's greatest asset, so it follows that companies want and need to provide for their safety and security. It's no different for MasterCard, especially since many employees and customers travel to and work in high-risk regions of the world. In this session, hear how the July 2005 terrorist bombings of London's transit system inspired MasterCard's 'I'm OK" program. What started as a simple telephone check-in solution is now fully automated, with built-in logic, to handle hundreds of security messages each month delivered on multiple devices, including

BlackBerrys. The sophisticated system can capture travel reservations as they are booked through MasterCard travel agencies, and gives travelers and MasterCard management peace of mind gained through advanced technologies.

12:30 pm - 12:48 pm	**Optimizing the Intersection of Physical and Information Security: A Q&A Panel Discussion**

Richard Gunthner, Vice President & Chief Security Officer, MasterCard Worldwide, a CSO40 Winner Organization for 2013

Dennis Treece, CSO, Massachusetts Port Authority, a CSO40 Winner Organization for 2013

Bob Bragdon, Publisher, CSO magazine

12:48 pm - 2:00 pm	**Networking Lunch with Table Topic Discussions Hosted by Selected CSO40 Honorees**

Presented by Dell SecureWorks

Discussion Table Topics and Moderators:

An Effective Cloud Security Assessment Methodology (Jack Baker, Executive Director, IT Security, Quintiles Transnational)

Best Practices for Building a Successful Security Operations Center (Tonya Byers, Director, Information Security, Blue Cross Blue Shield of Michigan; Angela Williams, Sr. Manager, Information Security, Blue Cross Blue Shield of Michigan)

International Privacy and Security Challenges for U.S.- Based Organizations (Mark Coderre, Head of Enterprise Security Architecture, Aetna)

The Critical Intersection of Information and Physical Security (Richard Gunthner, VP & CSO, MasterCard)

Reputational Risk Management: Protecting the Brand Through Security and Corporate Communications Team Cooperation (Jim Hutton, Director, Global Security & CSO, Procter & Gamble)

International Governance, Risk and Compliance (James Kidd, Head of International Delivery, Aetna)

Effective Information Risk Management and Security: Enhancing Visibility and Response (Jay Leek, CISO, Blackstone)

Conducting a Global IT General Control Assessment (Audrey Mydosh, Director, IT Risk and Security, MetLife)

2:00 pm - 2:18 pm	**Modernizing Security for a Digital Native Workforce**

James Beeson, CISO and IT Risk Leader, GE Capital Americas

Digital natives – those who were born during or after the introduction of digital technologies – are joining the knowledge workforce. They think, work and solve problems differently, and their computing habits and privacy perceptions require a fresh approach to IT security practices. In this session, CISO and IT risk leader James Beeson will share the new risks digital natives pose to your organization's security, and offer ideas for mitigating them in ways that don't unduly dampen their productivity.

2:18 pm - 2:33 pm	**The Evolution of Today's Advanced Threat Actor's Capabilities and Its Impact on Future Security and Risk**

Barry Hensley, Executive Director. Counter Threat Unit , Dell SecureWorks

In just 15 minutes, you will learn evolving Threat Actor Tactics, Techniques and Procedures associated with compromising networks, advancing hunting techniques necessary to detect these advanced threats, and security best practices associated with defending against today's threats.

2:33 pm - 2:48pm	**How the Cloud is Transforming Enterprise Security to Enable Mobility, Cloud Apps and Social Media** Jay Chaudhry, CEO, Zscaler, Inc

As tablets and smartphones outpace PCs as the device of choice in the enterprise, CIOs are looking for ways to securely enable mobile devices and users. At the same time, more organizations are using cloud applications, and more and more enterprise employees are using social media to connect with customers. Join us for this session as we discuss why many IT organizations are choosing to adopt a cloud-based approach to securely enable mobility, cloud applications and social media -- while simultaneously ensuring compliance and reducing risk.

2:48 pm - 3:06 pm	**ID and Access Management: How to Cut Costs, Streamline Processes and Achieve Scalability** Wyatt MacManus, Associate Director, Information Security, Sharp Electronics Corporation, a CSO40 Winner Organization for 2013

Managing user IDs and access controls is a necessity of any reliable information security program. But Sharp Electronics has derived greater value from its ID and Access Management initiatives through innovative application and integration of multiple technologies. User ID creation and security controls provisioning – processes that once took days – take just hours now, saving time and money. Moreover, employees now have access to self-service apps, and effective business workflows strengthen compliance. In this session, get the details and learn about the many benefits the company now enjoys.

3:06 pm - 3:24 pm	**A Security Evolution: Leveraging ID and Access Management for Business Value** Stephen Gay, Associate Director of Information Technology Services, Kennesaw State University, a CSO40 Winner Organization for 2013 McCree Lake, Associate Director of Information Technology Services, Kennesaw State University, a CSO40 Winner Organization for 2013

Identity and access management solutions promise to create more effective security by synchronizing passwords, streamlining workloads and eliminating redundancies. But those don't have to be the only benefits. Learn how Kennesaw State University's Information Technology Services team not only decided to confront those initial security challenges but how they have transformed an identity and access management initiative into a business value driver for the enterprise. In this session, the leaders of the initiative, Stephen Gay and McCree Lake, will discuss the origins of Kennesaw State's IAM project along with the strategy it leveraged to transform the implementation into an information ecosystem that is cutting infrastructure costs, providing attractive new services to customers and generating revenue for the organization.

3:24 pm - 3:42 pm	**The Sure-Fire Way to Privileged ID Management** Julia Ford, Program/Portfolio Manager, Security Engineering, TD Bank Group, a CSO40 Winner Organization for 2013

It can take just one privileged ID management misstep to bring down multiple systems, and the chances are greater when an enterprise has to manage tens of thousands of credentials. That was the challenge for TD Bank Group, but an aggressive, infrastructure technology systems corporate-wide initiative to structure a vaulted system for its privileged IDs has proven to be the answer. In this session, hear how TD Bank Group engaged more than 100 Infrastructure technology groups across the enterprise to create new standards, store privileged IDs, provide a secure way to access them, test them and automate password management. The result is an intricate and secure system that elevates TD Bank Group's compliance and helps protect it from security breaches.

3:42 pm - 4:00 pm	**Moving the Identity and Access Management Needle to State-of-the-Art: A Q&A Panel Discussion**

James Beeson, CISO and IT Risk Leader, GE Capital Americas
Julia Ford, Program/Portfolio Manager, Security Engineering, TD Bank Group, a CSO40 Winner Organization for 2013
Stephen Gay, Associate Director of Information Technology Services, Kennesaw State University, a CSO40 Winner Organization for 2013
McCree Lake, Associate Director of Information Technology Services, Kennesaw State University, a CSO40 Winner Organization for 2013
Wyatt MacManus, Associate Director, Information Security, Sharp Electronics Corporation, a CSO40 Winner Organization for 2013
Jack Rosamond, IT Manager, Security Engineering, TD Bank Group, a CSO40 Winner Organization for 2013
Bob Bragdon, Publisher, CSO magazine

4:00 pm   **Closing Remarks and Conference Concludes**