NIST Cybersecurity Risk Management Conference 2018

Renaissance Baltimore Harborplace Hotel, Baltimore, Maryland

November 7-9, 2018

Conference Purpose: The newly expanded conference format builds on the annual Cybersecurity Framework Workshops held for the past five years and adds other cybersecurity risk management topics: Risk Management Framework, Supply Chain Risk Management, and the Privacy Framework.

This conference will provide participants with:

1) An opportunity to learn about the current state of cybersecurity risk management and innovative approaches that are being deployed, and
2) A forum to voice their opinions on and discuss today's most vital cybersecurity risk management issues and solutions.

Sharing will take place through presentations, panels, and working sessions, as well as ample forums for networking.

Agenda Overview

Wednesday, November 7, 2018

7:30am **Registrant Check-In**
8:30am **Welcoming Remarks**
8:40am **Keynote**: Mr. Leo Simonovich on Siemens Charter of Trust
9:10am **Conference Overview**
9:40am **Break**
10:00am **Plenary Panels**

- Cybersecurity in Large and Distributed Organizations
- Key NIST Cybersecurity and Privacy Program Overview

12:00pm **Lunch** – to include Lunch-and-Learn sessions
1:00pm **Afternoon Sessions I**

- Secure Software: Toward A Proposed Benchmark
- Friends Don't Let Friends Tackle Cybersecurity Alone: Taking a Team Approach to Strengthening Cyber Resilience in the Marketplace
- Financial Services Sector Cybersecurity Profile: A NIST-based Approach to Harmonize Cybersecurity Risk Management and Compliance
- Cybersecurity Measurement and Metrics
- Implementing the Cybersecurity Framework
- Federating Cybersecurity Framework Informative References
- Cybersecurity Framework Profiles, Lessons from the Trenches

2:00pm **Break**
2:30pm **Afternoon Sessions II**

- Empirical Measurement of Perceived Privacy Risk
- Cybersecurity Risk Management: Finding and Fixing Your Security Vulnerabilities
- Risk Management for Automotive Cybersecurity

- Israeli Secure Supply Chain Scheme
- Actuarial Approach to Cybersecurity Risk Measurement
- Framework for Improving Critical Infrastructure Cybersecurity: A Practical Implementation
- NIST Cybersecurity Framework and PCI DSS
- How Japanese Industry Uses the NIST Framework to Overcome Manpower Shortage
- Enabling Executive Level Decisions
- Cyber Strategy Optimization for Risk Management – A New Approach
- Supply Chain Attacks and Resiliency Mitigations
- Managing the Hidden Cybersecurity Risks
- Using NIST Guidance to Implement and Information Systems Risk Management Program for a Small National Government
- Reducing the Burden of Cyber Security
- Is Our Critical Infrastructure Cyber Resilient?
- Use of NIST Guidance in Governmental Settings, Including the U.S. Federal Government: Department of Defense (DoD) Components Adopting the Risk Management Framework (RMF) Process. A Practical Implementation
- Simple, Consistent, Secure – Cybersecurity and Privacy in Small and Medium-sized Organizations
- Are We Building "Maginot Lines" in our Networks?

4:45pm **Adjourn**

Thursday, November 8, 2018

7:30am **Registrant Check-In**

8:30am **Plenary Panels**

- U.S. National Critical Infrastructure Risk Management
- Government Use of NIST Cybersecurity Publications

10:30am **Break**

10:45am **Morning Sessions III**

- Connecting the Dots Between Threats & Mitigations in Federal Networks
- Vendor Management & NIST SP 800-171
- Cyber Supply Chain Strategy
- Enhancing Cybersecurity Risk Management Across the Federal Enterprise
- Software Bill of Materials: Best Practices for Machine-Readable Assurance Data in Mission Operations
- Integrated Cyber Playbooks for Identity Threat Prevention (ITP) within the NIST Risk Management Framework
- A Tale of Two Frameworks: Optimizing Federal Agency Use of the RMF and CSF through Framework Profiles

11:45am **Lunch** – to include Lunch-and-Learn sessions

1:15pm **Afternoon Sessions IV**

- Adding Rigor and Depth to RMF Step 2 (Select Security Controls)
- Evaluating "Reasonable" Cyber Risk Using CIS RAM
- Cybersecurity Coalition Distributed Denial of Service Mitigation Profile

- US Federal Government Sector Guidance
- Integrating Privacy into the Risk Management Framework
- Electrical Manufacturers' Role in Cyber Supply Chain Risk Management

2:15pm **Break**

2:45pm **Afternoon Sessions V**

- Cyber Threat Framework
- Connecting to the Business Mission: Why Context Matters for Security Teams
- Measuring an Organization's Security Maturity using the NIST Cybersecurity Framework
- The Business and Regulatory Value of Third-Party Certification to the NIST Cybersecurity Framework
- Helping Communities Utilize the NIST Cybersecurity Framework ISAOs as a Catalyst for Developing Community Cybersecurity Programs
- A Framework for Cyber Security Performance
- Implementing Secure Systems using the PMBOK and NIST Cybersecurity Framework and Baldrige Excellence Tool
- Enterprise Risk Mitigation Using the NIST CSF and Cyber Analytics
- The ISF Standard of Good Practice and the NIST Cybersecurity Framework
- Automated Cyber Hardening
- Role-Based Risk Management Framework – RMF and NICE Framework Convergence
- Risk Data Sharing for Situational Awareness
- Using the NIST Framework to Design and Implement Risk-based Cybersecurity Management in a Global Conglomerate
- Measuring the Cybersecurity Risk of Software-Intensive Systems
- NIST Cybersecurity Guidance as Systems Engineering Construct and not DIACAP by Another Name
- Achieve Cybersecurity Excellence
- How Tradeoffs Increase Cyber Supply Chain Risk
- Using a Controls Framework to Address NIST, HIPAA, and GDPR Security Requirements, and to Ensure Management of Cyber Threats
- How To: Develop a Cybersecurity Framework Profile
- A Structured Approach for Privacy Risk Assessments for Federal Organizations
- The Transformation of Global Value Chains: Hardening the Weakest Link

5:00pm **Adjourn**

Friday, November 9, 2018

7:30am **Registrant Check-In**

8:30am **Keynote**: Mr. Bruce Potter on Making Risk Management Real

9:30am **Break**

10:00am **Morning Sessions VI**

- Reducing Cybersecurity Risk Exposure in Medical Devices
- Building Security In: How the RMF Impacts Legacy Practices and System Modernizations
- Lock Down Your Login

- MEP / Manufacturing Cybersecurity
- Tips & Tricks for Small Business Cybersecurity Framework Implementation
- Towards Autonomic Security Management
- Proactive Cybersecurity Through Cross-domain Intelligence
- Deriving Business Insight from CSF Findings
- The Digital Fast Lane – Helping NonProfits Keep Up
- State Supporting in Cybersecurity for SMB Organizations
- Best Practices Learned from Mitigating Risks of Data Breaches to Build a Data Privacy Program
- Cyber-Enterprise Risk – Through the Shareholder Lens
- Cybersecurity in Small and Medium-sized Businesses
- Cybervets: Leveraging Veterans to Build the Cybersecurity Workforce
- Demystifying ICS Cyber Risk
- Implementing Cybersecurity Framework
- Understanding and Managing Cyber-Risk with a Dwell Time Base
- Risk is Money

12:30pm **Lunch** – to include Lunch-and-Learn sessions

1:45pm **Afternoon Sessions VII**

- IoT Security – Past, Present and Future
- A Practical Approach to IT Security for Small and Medium-sized Businesses Based on the NIST Cybersecurity Framework
- Using the Framework as an Umbrella for Your Cloud
- Data Driven Breach Response Planning
- Spanning the Org Chart from Metrics to Risk
- Data-Driven Risk-based Decision Making

2:45pm **Adjourn**

Plenary Speakers

Keynote: Siemens and the Charter of Trust

Leo Simonovich, Siemens

Mr. Leo Simonovich, Siemens Vice President and Global Head of Industrial and Digital Cyber, discusses the ten principles of the Charter of Trust, how Siemens approaches cybersecurity, and practical steps attendees can take to build a more secure digital world.

Leo Simonovich is responsible for setting the strategic direction for Siemens' industrial cyber security business worldwide. He identifies emerging market trends, works with customers and Siemens businesses to provide best-in-class cyber offers, and contributes to the company's thought leadership on the topic. He is particularly focused on solving the cyber security challenge in the O&G and power sectors by bringing unique solutions to customers looking to address a growing and costly operational security risk. He frequently speaks on such topics as cyber governance, risk management, and organizational transformation in operational environments.

Cybersecurity in Distributed Organizations

Panelist: Mihoko Matsubara, Nippon Telegraph and Telephone Corporation
Panelist: Donald Heckman, U.S. Department of Defense
Panelist: Michael P. Darling, Venable L.L.P.
Panelist: To Be Announced
Moderator: Matthew Eggers, U.S. Chamber of Commerce

Risk executives discuss approaches to cybersecurity risk management in a large distributed organization. How are cybersecurity risk management decisions made, how are those done within the context of larger risk discussions, and what governance methods are the most effective in institutionalizing consideration of cybersecurity (e.g., alongside of other considerations like safety and quality).

Mihoko Matsubara

Mihoko Matsubara is Chief Cybersecurity Strategist, NTT Corporation. She is responsible for public advocacy to strengthen or expand networks with global thought leaders in academia, government, and industry by sharing NTT's and Japan's cybersecurity efforts via publications and speakership.

Matsubara worked at the Japanese Ministry of Defense for nine years before receiving a Fulbright Scholarship to pursue an MA at the Johns Hopkins School of Advanced International Studies in Washington DC. Afterward, she accepted a fellowship at Pacific Forum CSIS (now Pacific Forum) in Honolulu to research Japan-US cybersecurity cooperation.

Matsubara then joined Hitachi Systems as cybersecurity analyst, and next took a position at Intel K.K., Tokyo, as Cybersecurity Policy Director. Her most recent experience includes Vice President and Public Sector Chief Security Officer (CSO) for Asia-Pacific at Palo Alto Networks in Singapore. Directly prior, Matsubara was CSO for Palo Alto Networks in Japan. During that time, she was on a cybersecurity strategy committee for the Japanese National Center of Incident Readiness and Strategy for Cybersecurity (NISC) to advise the Japanese government on how to enhance cybersecurity toward the 2020 Tokyo Summer Olympic and Paralympic Games.

She is a prolific writer and has spoken at various engagements internationally. She has a weekly cybersecurity column for the Mainichi Shimbun newspaper in the digital version. She has contributed articles and papers to the Council on Foreign Relations, Lawfare, and Royal United Services Institute. She was the first Japanese speaker at the NATO International Conference on Cyber Conflict in Estonia (2015).

She is an Adjunct Fellow at Pacific Forum, Honolulu, and Associate Fellow at the Henry Jackson Society, London.

Donald Heckman

Mr. Donald Heckman is the Principal Director, Deputy Chief Information for Cybersecurity Department of Defense, Office of the Chief Information Officer. Mr. Heckman is responsible for ensuring the department has a well-defined and well-executed cybersecurity program. He is responsible for coordinating cybersecurity standards, policies and procedures with other federal agencies, coalition partners and industry.

Mr. Heckman began his career at NSA in 1983. He has served in a variety of technical and management positions over his career, including project engineer, program manager and manager up to Deputy Directorate level. He has also led several DoD-wide IA programs and initiatives. He is a key leader who has a deep technical knowledge of all aspects of the Information Assurance (IA) mission and has attained the Master level in the NSA Engineering and Physical Science Technical Track program and he is a Certified Information Systems Security Professional (CISSP) by the International Information Systems Security Certification Consortium (ISC)2. He has received numerous awards from the Defense, and Intelligence communities in recognition of his vision, leadership, and

accomplishments including the Meritorious Presidential Rank Award in 2017. He was appointed to the Senior Executive Service in October 2005.

Prior to Mr. Heckman's current assignment he served as the Deputy Chief to the Cybersecuirty Solutions (CSS) Group. He led the organization in developing capabilities that span a large variety of technology areas, to include cloud & enterprise services, merged voice and data, mobile, high speed networks, cross domain and authentication to support a spectrum of national security customer environments ranging from key management infrastructures, strategic and tactical high speed network communications, to military weapon systems and architectures. Additionally he was selected to be the Assistant Deputy Director of Trusted Engineering Solutions (TES) within the Information Assurance Directorate (IAD) and Chief of the IAD's Architecture Group. He has held key NSA leadership positions supporting Information Assurance, Systems Security Engineering and Key Management missions. Additionally, he served as the NSA/CSS Representative (NCR) to DISA/Deputy NCR STRATCOM for JTF-GNO. He also led the establishment of the DoD's Cryptographic Modernization and Global Information Grid Information Assurance Portfolio (GIAP) offices.

Mr. Heckman graduated from Johns Hopkins University with a Master of Science degree in Electrical Engineering and he received a Bachelor of Science degree in Electrical/Computer Engineering from Drexel University.

Mr. Heckman resides in Bel Air, MD. He enjoys reading, golfing and is active in the Boy Scouts of America. He and his wife Michelle are proud parents to their three children, Alysha, Emily and Zachary.

Matthew J. Eggers

Matthew J. Eggers is vice president for cybersecurity policy in the Cyber, Intelligence, and Security Division at the U.S. Chamber of Commerce. He leads the Chamber's Cybersecurity Working Group, which focuses on developing and advocating for the Chamber's cyber policies before Congress, the administration, and the business community. Eggers frequently presents to organizations and is quoted regularly in the media on a broad range of issues connected to cyber legislation, regulation, and business strategy.

Key NIST Cybersecurity and Privacy Program Overview

Panelists: Naomi Lefkovitz, NIST Privacy Engineering
Panelist: Vicky Pillitteri, NIST Risk Management Framework
Panelist: Jon Boyens, NIST Supply Chain Risk Management
Panelist: Matt Barrett, NIST Cybersecurity Framework
Moderator: Kevin Stine, National Institute of Standards and Technology

NIST key program managers (e.g., Risk Management Framework, privacy engineering, supply chain risk management, Cybersecurity Framework) to present basal information, describe recent and near-term program milestones, and discuss harmonization across programs.

Matt Barrett

Mr. Barrett and his team are responsible for establishing and maintaining relationships with both private and public sector (Cybersecurity) Framework stakeholders. Mr. Barrett works through those relationships to provide perspective and guidance, as well as gather input on use and evolution of the Framework. To fulfill stakeholder needs, Mr. Barrett also collaborates with a variety of NIST cybersecurity programs.

Matt previously led NIST's Security Content Automation Protocol program and support of the Office and Management and Budget's Federal Desktop Core Configuration initiative. Matt has also served in various executive roles including roles such as president and chief executive officer.

U.S. National Critical Infrastructure Risk Management

Panelist: Bob Kolasky, Director of the U.S. Department of Homeland Security National Risk Management Center
Panelist: Karen Evans, U.S. Department of Energy
Panelist: To Be Announced
Panelist: To Be Announced
Moderator: Matt Barrett, National Institute of Standards and Technology

A panel to discuss the new U.S. Department of Homeland Security National Risk Management Center and its relationship to pre-existing Sector Specific Agencies and, how Framework and C Cubed factor in, systemic critical infrastructure risk measurement/management, and possibly the National Cyber Incident Response Plan.

Government Use of NIST Cybersecurity Publications

Panelist: Eva Ignatuschtschenko, United Kingdom
Panelist: Aviram Atzaba, Israel
Panelist: Stuart Daniels, Bermuda
Panelist: Daniel Caduff, Switzerland
Moderator: Vincent Voci, U.S. Chamber of Commerce

Senior officials from governments of other nations to discuss international approaches to cybersecurity, what guidance, methodologies, and best practice are effective in delivering those approaches, and opportunities for harmonization.

Eva Ignatuschtschenko

Eva Ignatuschtschenko is leading on behavior change policy in the Cyber Security Incentives and Regulation Team at the UK Government Department for Digital, Culture, Media and Sport. Her work focuses on how individuals and organizations can be incentivized to take action to improve their cybersecurity posture. She previously advised on cybersecurity and cyber harm at the University of Oxford's Global Cyber Security Capacity Centre, after working on cybercrime, emerging crimes and organized crime at the United Nations Office on Drugs and Crime (UNODC). In her roles in international

organizations, academia and government, Eva has worked on a variety of issues, with a focus on the links between cyber risk, digital government, crime and emerging technologies.

Aviram Atzaba

Aviram Atzaba is the Director of Methodology & Audit Center in the Israel National Cyber Directorate. In this role, he is responsible for the development of Cyber Defense methodologies for the Israeli market and for the performance of Cyber Resiliency testing of the Israeli critical infrastructures. In his previous positions, he served in the Israeli Air Force. His areas of expertise are Avionics, Connectivity, System of Systems, Network Centric Warfare and Cyber Warfare.

Stuart Daniels

Stuart Daniels, Security Manager, Department of Information and Digital Technologies, Government of Bermuda, and his team are responsible for developing and administering the Information Systems Risk Management program and sub-programs for the Government of Bermuda. Stuart has 20 years of experience in information technology, management and information systems security. Stuart serves on the Government Information Systems Risk Management Committe, and provides advice to department heads, the Civil Service Executive and the Cybersecurity Cabinet Committee on security matters. He also serves on the Cybersecurity Working Group, a public-private partnership that is developing Bermuda's National Cybersecurity Strategy.

Daniel Caduff

Daniel Caduff is the deputy head of the ICT-Division at Switzerland's Federal Office for National Economic Supply FONES. FONES' duty is to secure infrastructure that is vital to the Swiss economy in general, while Daniel and his team are focusing on ICT-risks in particular. As a federated country, Switzerland pursues a cooperative approach between various government agencies and the private sector. Switzerland provides assistance to the private sector. Awareness, training, open-source tools and transparent information form the basis for this and establish trust between the State and private sectors. In August 2018 FONES released its "Minimum standard for improving ICT resilience" to the public. This standard is based on the NIST Framework Core and has been added to NISTs "International Resources". Daniel holds a master degree in political science and international law and is a DIY-Digital Native. Daniel joined FONES as a project leader for Switzerland's national strategy against cyber-risks, and eventually became Deputy Head of the ICT-Division in 2016. Before joining FONES, Daniel worked for a major Swiss ISP and a consulting company in the field of IT-risk-management-consulting.

Vincent Voci

Vincent Voci is senior policy manager in the Cyber, Intelligence, and Security Division at the U.S. Chamber of Commerce.

Voci also leads the Chamber's Project Security, which focuses on developing and advocating the Chamber's international cyber policies before foreign governments, the administration, and the business community.

He handles homeland and national security issues, with a particular focus on cybersecurity, on behalf of the Chamber's 200-plus National Security Task Force members.

Voci provides strategic guidance and support to the senior vice president of the department. He is actively engaged in developing and executing the department's policy agenda and advocates on behalf of the U.S. business community on a wide range of cybersecurity issues before the U.S. Congress and government officials.

Voci leads the Chamber's Cybersecurity Education and Awareness Campaign. Improving Today. Protecting Tomorrow.TM, which focuses on advancing cybersecurity policies and legislation while educating businesses of all sizes about cyber threats and how to protect against them.

Previously, Voci worked for former Sens. Scott Brown (MA) and George Allen (VA) and at the departments of Transportation and Homeland Security.

Voci is a graduate of American University in Washington, D.C. with a B.A. in political science. A native of Cape Cod, Massachusetts, he currently resides in Alexandria, Virginia.

Keynote: Making Risk Management Real
Bruce Potter

An old boss of mine had a great expression regarding threats from cyber attacks: "Risk is Everywhere!" At the time he said it nearly 20 years ago, I thought it was a trite marketing term. But it turns out, he was right. Modern corporate environments, from small business with a few employees to the largest financial institutions, have discovered that indeed, cyber risk is everywhere and to be successful, you have to manage it.

The big question is "how?" Big banks, multinational healthcare companies, and similar organizations generally have sophisticated risk management processes that take into account cyber risk like any other type of risk. But for smaller organizations, managing cyber risk can seem like a dark art. Sure, you have a bunch of security controls and some policies, but does that really constitute managing risk?

In this talk, I'll examine the modern risk management landscape. Every organization is different, but frameworks like the NIST CSF can be useful to companies of all shapes and sizes. I'll show examples of how to utilize the CSF for organizations of differing maturity levels and present ideas of how to operationalize risk management quickly and effectively. Further, this talk will provide a roadmap to help you mature your risk management processes over the coming years.

Bruce Potter is Expel's (expel.io) chief information security officer (CISO). He's responsible for cyber risk management and ensuring the secure operations of Expel's services. He also remains perpetually frustrated that employees pronounce CISO not-the-way-he-wants.

Previously, Bruce co-founded Ponte Technologies, a cybersecurity research and engineering company that worked with organizations ranging from hedge funds to intelligence agencies. Bruce sold Ponte Technologies to the KeyW Corporation where he served as CTO for two years. In another life, Bruce founded the Shmoo Group and helps run the yearly hacker conference, ShmooCon (shmoocon.org), in Washington, DC. Bruce has co-authored several books and written numerous articles on security (or the lack thereof). He is a regular speaker at conferences including DefCon, Blackhat, and O'Reilly Security as well as private events at the United States Military Academy, the Library of Congress and other government agencies.

Afternoon Sessions I

Secure Software: Toward A Proposed Benchmark

Tommy Ross, BSA|The Software Alliance, John Banghart, Venable, David Lenoe, Adobe, Jamie Brown, CA Technologies, et al.

This panel will present and discuss a working concept for a new software security framework developed by BSA | The Software Alliance. Modeled on the NIST Cybersecurity Framework, the first-of-its kind software security framework will offer a benchmark for defining software security and measuring organizational progress toward its specified objectives. It presents a voluntary, flexible, outcome-focused approach that is aligned with internationally recognized standards and best practices. The panel moderator will present the structure and key elements of the proposed framework. The panel discussion will address the gap the framework is intended to fill and the potential applications of the framework for developers, security professionals, and policymakers. The discussion will expose the audience to an exciting new approach to one of the more elusive and vexing challenges in cybersecurity and invite their input and involvement as the project advances.

Friends Don't Let Friends Tackle Cybersecurity Alone: Taking a Team Approach to Strengthening Cyber Resilience in the Marketplace

Panel: To Be Announced – Moderator: Matthew Eggers, U.S. Chamber of Commerce

Department of Homeland Security Secretary Kirstjen Nielsen announced in July that the danger posed by terrorist incidents has been eclipsed by the threat of cyberattacks. Most organizations cannot cope with criminal groups or foreign nations alone. Cybersecurity calls for a buddy system. Leading solution providers—including software, technology, and insurance firms—are banding together to offer their customers a holistic approach to mitigating cyber risks. A joint solution helps businesses bolster their cyber defenses and can make them eligible to score more favorable terms for cyber insurance, along with support services in the event of an attack. Learn how these businesses leverage each other's talents to reinforce cyber resilience in the marketplace and the obstacles they face.

Financial Services Sector Cybersecurity Profile: A NIST-based Approach to Harmonize Cybersecurity Risk Management and Compliance

Josh Magri, Bank Policy Institute, Denyette DePierro, American Bankers Association, Nadya Bartol, BCG Platinion

Starting in 2016, the financial services industry -- through its Financial Services Sector Coordinating Council -- began mapping the many regulatory issuances against the NIST Cybersecurity Framework, CPMI-IOSCO, and ISO 27000 standards. Through the mapping, a pattern emerged: over 80% of the regulatory issuances were topically identical, but semantically different. To reconcile and rationalize these differences, in March 2017, industry began developing the Financial Services Sector Cybersecurity Profile ("Profile"), architected around

the NIST Cybersecurity Framework. This session offers an opportunity to learn about the Profile, its public launch as a Version 1.0, and its potential evolution. At its core, the Profile is a harmonized meta-framework approach to cybersecurity that recognizes the multiple, often overlapping, regulations and supervisory/examining agency approaches, while fostering an efficient, results-oriented approach to cybersecurity for institutions of all sizes and complexity.

Implementing the Cybersecurity Framework: A Success Story

Plamen Martinov, University of Chicago

The University of Chicago (UoC) Biological Science Division (BSD) was an early adopter of the Cybersecurity Framework. UoC has remained at the forefront of Framework implementations; it is the first organization to develop a Framework Success Story for NIST. BSD used the Framework to identify a strategy for improving their cybersecurity capabilities in 2015. Many of BSD's initiatives in the past three years have been focused on achieving the goals defined within the Target State Profile created during their 2015 implementation. In 2018, BSD reassessed their cybersecurity program using the Framework once again. This second assessment helped BSD to understand changes in their organization and risk environment.

Cybersecurity Framework Profiles, Lessons from the Trenches

Dave Weitzel, MITRE

Certain industry sectors have brought together stakeholders to develop coordinated Industry Profiles. One such set of Industry Profiles was developed under the leadership of the United States Coast Guard. Three Profiles were developed Maritime Bulk Liquid Transfer, Offshore Drilling & Production Operations, and a Passenger Vessel Profile. Working with industry, the USCG utilized the NIST NCCoE in its coordination with the oil and natural gas industry and the cruise line industry. Similarly, the Intelligent Transportation Systems Joint Program Office (ITS JPO) of the Department of Transportation along with the Volpe Center have worked with the intelligent transportation community to develop Cybersecurity Framework Profiles that are being used as baselines for the cybersecurity of connected vehicle pilot deployments. This session will discuss the process for the developing the profiles, industry outreach strategies, lessons learned, and early adoption.

Afternoon Sessions II

Empirical Measurement of Perceived Privacy Risk

Jaspreet Bhatia, Carnegie Mellon University

The speaker will present an empirical framework to measure privacy risk based on how a person's information is collected, used and shared. The framework consists of factorial vignette surveys which are used to measure the effect of contextual factors on how users perceive risks to their privacy. The presentation includes experimental results to evaluate six factors: the type of information processed, the type of computer where the information was stored, the purpose for which the data was processed, the privacy harm, the likelihood of the harm, and several individual demographic factors, such as age range, gender, education level, ethnicity and

household income. To measure likelihood, the framework introduces a new likelihood scale based on Construal Level Theory from psychology. The scale frames individual attitudes about risk likelihood based on social and physical distance to the privacy harm. Findings include predictions about the extent to which the above factors correspond to risk acceptance -- including that perceived risk is lower for induced disclosure harms when compared to surveillance and insecurity harms as defined in Solove's Taxonomy of Privacy. Another finding: participants are more willing to share their information when they perceive the benefits of sharing. The framework and findings will appear in a forthcoming issue of the ACM Transactions on Human Computer Interaction.

Cybersecurity Risk Management: Finding and Fixing Your Security Vulnerabilities

Phil Renaud, Ohio State University

Research from The Risk Institute found 28% of financial, non-financial, public and private firms have been victims of a cyber attack. The risk is enormous: cyber-attacks can shut down industrial facilities, utilities and infrastructure systems, interfere with military operations and compromise national security, yet firms are continually decreasing their risk management units. The growing dependence on cyber networks means a cyber-attack is one of few threats that can have truly national implications. It's crucial that leaders in all industries understand the implications of security breaches and how to prepare beforehand. In this presentation, Phil will discuss how predictive analytics have been proven to mitigate cyber risk by determining future outcomes and allowing a firm to create a plan ahead of time. Through better understanding of the economic consequence of cyber-attacks and how risk management tactics can reduce these, both private and public sectors can improve their cyber risk management.

Risk Management for Automotive Cybersecurity

Bill Mazzara, Fiat Chrysler Automotive Group

The auto industry continues to add connectivity to vehicles to satisfy the customer's insatiable appetite for technology, but cars are not just insecure endpoints on some computer network as some have portrayed. Vehicle cybersecurity is forging a new field of product cybersecurity. Working collaboratively with ISO, best processes are being established for industry-wide cybersecurity preparedness. Risk policies must be established for processes of a risk-based methodology based on risk assessment. Enterprise cybersecurity risk assessment methods must be reworked and used in a consistent manner across the Industry. ISO 21434 proposes common interpretations of methods leveraging the existing wealth of knowledge in asset categorization and assessment of impact and attack potential in order to estimate risk to products.

Israeli Secure Supply Chain Scheme

Aviram Atzaba, Israel

In recent years supply chain has been a challenging cyber-attack vector for many organizations. The main challenge is that supply chain cyber security is not in control of the organization. To date, the ability of an organization to manage the cyber risk of its supply chain has been extremely limited - contractual basic requirements for cyber protection, audits for a limited number of suppliers, etc. Not to mention the risk of the supply chain of the supply chain... The Israeli National Cyber Directorate (INCD) decided to offer an end-to-end service to the Israeli market to help organizations manage their supply chain cyber risk. That includes:

1. Methodology for a secure supplier - which includes terminology, supplier's categorization according to risk source, definition of required threshold controls. The methodology explains in simple terms each control and defines how to test the control (including what is required as evidence of compliance).

2. A web application for Cyber security Self-Assessment of the above methodology by suppliers, issuing a cyber-security status and report (in addition, the Application will enable sectorial view of the suppliers).

3. Cooperation with the Israeli Standards Institute for training and certification of cyber security auditors for the supply chain according to the above methodology.

Current status: Pilot to the above process with a number of significant companies in the Israeli economy, from a variety of sectors (finance, transportation, energy, government…). On January 1, 19, the critical infrastructure and government offices shall be regulated to use the method and tools developed on their suppliers. Since supply chain is global, expanding the model and harmonizing it globally is of outmost importance.

Actuarial, Statistical and Other Analytical Approaches to Cyber Risk Measurement

Alex Krutov, Navigation Advisors

This session will focus on practical considerations and options available to an enterprise assessing its cybersecurity risk with the Framework, as outlined in the new section of the Framework introduced in Version 1.1 this year.

The general goal of the Cybersecurity Framework is to reduce risk. But how do you measure, assess or characterize risk? How do you know whether, and by how much, the risk has been reduced? How can you tell whether the reduction in risk is sufficient to justify the required cybersecurity investments? How can this be best communicated to senior management and be incorporated in the overall enterprise risk governance?
These and other questions will be discussed in practical terms.

The session will also address how this topic relates to the Framework implementation tiers and target profiles. In addition, it will discuss important limitations of assessments in the face of limited information and overall uncertainty.

Using a Controls Framework to Address NIST, HIPAA, and GDPR Security Provisions -- to Ensure Management of Cyber Threats

Bryan Cline and Anne Kimbol, HITRUST; Iliana Peters, Polsinelli

Ensuring appropriate cybersecurity risk management, including complying with the variety of regulatory and voluntary industry cybersecurity standards, continues to be a resource- intensive and complicated process for organizations. Organizations need an effective and efficient way to address identified cyber risk and ensure appropriate protections are in place to protect against cyber threats. The panel will discuss security management provisions under HIPAA, the NIST Cybersecurity Framework, and the European Union's General Data Protection Regulation. Presenters will highlight how such laws and guidance address cybersecurity issues and educate attendees on how tools like the HITRUST Cybersecurity Framework can help manage cybersecurity risk. Panelists will present proposals for incentivizing use of controls frameworks across industry sectors and discuss related proposed policy and regulatory initiatives.

Framework for Improving Critical Infrastructure Cybersecurity: A Practical Implementation

William Westwater, Boeing

This presentation will provide a practical example of how to implement the NIST Cybersecurity Framework in a scalable manner for a large enterprise. This approach focuses on the management of technical controls and "security hygiene" activities that should address vulnerabilities that are frequently leveraged as an avenue for penetration and attacks on critical infrastructure systems. This is an under-emphasized aspect of security that is often overshadowed by "sexy" technical controls that, while critically important, are undermined if the full suite of controls is not present and functioning. This presentation and discussion will enable an organization to manage computing security actions, relate them to risk, and prioritize those actions and the spending associated with securing an enterprise.

NIST Cybersecurity Framework and PCI DSS

Troy Leach and Lauren Holloway, PCI Security Standards Council

This session will cover PCI *Security Standards Council's (SSC)* current efforts to map controls between the Cybersecurity Framework and PCI Data Security Standard (DSS). The similarities and relationship between the Framework and PCI DSS will also be described. Additionally, the presentation will help organizations understand how achievement of Cybersecurity Framework outcomes may also address controls in other standards and guidelines

How Japanese Industry Uses the NIST and NICE Frameworks to Overcome Manpower Shortages

Masato Kimura, Nippon Telephone and Telegraph Corporation

This session aims to share how Japanese industry uses the NIST Framework to tackle the challenge of cybersecurity talent shortage. The Japanese government expects Japan will be short of 193,010 cybersecurity professionals in 2020, when the Tokyo Summer Olympic and Paralympic Games will be held. Because cybersecurity will be crucial for the success of Tokyo

2020, Japan has been prompted to cultivate cybersecurity professionals. In 2015, NTT, NEC, and Hitachi took the initiative to launch the Cross-Sector Forum to collaborate with academia and government and create an ecosystem to educate, recruit, retain, and train cybersecurity professionals. Today, the Forum has 48 major Japanese critical infrastructure companies from the chemical, energy, finance, media, telecommunication, and transportation sectors. The Forum uses both the NIST Cybersecurity Framework and NICE Cybersecurity Workforce Framework to unify the language used among members to map cybersecurity skillsets by sector, department, and function.

Enabling Executive Level Decisions

Jack Jones, FAIR Institute

The bread and butter of executive life involves making difficult trade-offs regarding where to apply their limited resources. These trade-offs invariably require value/liability-based comparisons that need to be as "apples-to-apples" in nature as possible. In this session, the presenter will describe how to help executives make well-informed decisions about their investments in cybersecurity by combining the NIST Cybersecurity Framework with quantitative analytics based on the Factor Analysis of Information Risk (FAIR) model. By expressing risk and risk reduction in economic terms, this approach enables cost-benefit measurements that executives innately understand, and which supports rational and defensible choices that otherwise aren't possible.

Cyber Strategy Optimization for Risk Management: A New Approach

Michael Coden, Boston Consulting Group

This presentation lays out a novel methodology for calculating the ROI on cybersecurity initiatives in an organization. The methodology blends operational risk management, theory, and cybersecurity disciplines. It applies the NIST Cybersecurity Framework to organize project portfolios and evaluate current and target states of cybersecurity within the enterprise. Using the Loss Distribution Approach from operational risk management the methodology shows that it is possible to calculate a relative risk reduction by implementing cybersecurity projects that either protect the organizations assets or reduce the impact of potential incidents to those assets. Use of portfolio theory in this methodology helps account for synergies and overlaps in projects that are potentially impacting the same controls, or protecting the same assets. This bended model helps guide cybersecurity project selection to optimize project spending, while maximizing the results in both dollar risk reduction and cyber maturity increase. Ultimately, the model produces a relative ROI for each of the alternative portfolios to help decision makers select an optimal project portfolio for their organization.

Supply Chain Attacks and Resiliency Mitigations – Guidance for System Security Engineers

Ellen Laderman and William Heinbockel, MITRE

This presentation extends the NIST Supply Chain Risk Management Guidance from NIST SP 800-161 to further enhance the cyber resilience of the supply chain and its supporting systems and missions. We apply the cyber-attack lifecycle framework to the Department of Defense (DoD) Acquisition lifecycle to discuss an adversary's goals for attacking a supply chain. Resiliency techniques are recommended based on these goals and their potential impact to the system. Our analysis found that the most effective point to apply cyber resiliency mitigations is the Production and Deployment phase, while the later stages present the best opportunity to gain information about potential adversary targets and activities. An example of how to apply these resiliency techniques is provided based on the NSA Commercial Solutions for Classified capability package for a Wireless Local Area Network (WLAN).

Managing the Hidden Cybersecurity Risks

Tony Giles, Rhia Dancel, NSF International

The presentation will explore best practices which organizations take in managing and understanding their risk environment. These best practices have been captured through global feedback and have allowed organizations to continually monitor risk probability, impact and treatment. The presentation will focus on top identified risks and feedback on best practices for risk treatment. Attendees will hear how organizations can utilize their risk assessment to focus on the development and prioritization of their POAM's (Plan of Action and Milestones). The presenters will also cover hidden risks organizations face and provide training on how to look into and treat those risks. The presenters will use real-world examples and demonstrations to support organizations' continual risk improvement practices.

How Tradeoffs Increase Cyber Supply Chain Risk

Marjorie Windelberg, Cyber Pack Ventures

Tradeoffs made by acquirers and suppliers in cyber supply chains increase risks that can impact the trustworthiness of systems. Tradeoffs are often (but not always) conscious choices among factors such as cost, schedule, and requirements. Also, tradeoffs between competing requirements arise. Requirements may be partially or wholly omitted, or new requirements may be substituted for previously agreed upon requirements. Within an acquirer, different groups make different tradeoff decisions, and these occur from initial acquisition through operations and maintenance. Different acquirers also have distinct risk profiles, depending on their assessed threats. Each supplier in the chain also makes tradeoffs, with or without downstream acquirers' knowledge. Furthermore, tradeoffs are influenced by explicit or implicit trust assumptions. These trust assumptions are based on the perception that risk from a tradeoff is low. Thus, risk tolerance and even understanding of risk are major cyber supply chain variables.

Using NIST Guidance to Implement and Information Systems Risk Management Program for a Small National Government

Stuart Daniels, Dr. Marisa Stones, Government of Bermuda

Although Bermuda is a small island, the Government has 83 Departments and Ministries that process sensitive information and provide critical services. A comprehensive Information Systems Risk Management Program was needed to ensure an adequate level of cybersecurity across the organization. Several NIST standards, including the Cybersecurity Framework and the Risk Management Framework, have provided invaluable guidance that helped the Government of Bermuda to craft a program that meets its varied needs. The NIST Cybersecurity Framework has underpinned the Government's efforts to secure its information systems by providing a means to assess and communicate information security issues to members of the Cabinet and the Civil Service Executive. The Security and Privacy Controls in NIST 800-53 provided valuable guidance for creating a policy framework and the Risk Management Framework informed the process of integrating security within the Systems Development Lifecycle. This presentation will provide an overview of the Government of Bermuda's use of NIST standards to develop its Information Systems Risk Management Program, including a discussion of the challenges and critical success factors.

Reducing the Burden of Cybersecurity

Eva Ignatuschtschenko, United Kingdom

This presentation focuses on how the UK is working with industry, civil society, and academia to correct market failures that have led to an insufficient uptake of desired cybersecurity behavior across the economy and society. To an extent, the system is set up to prompt undesired behaviors and the UK is working to reduce the burden of cybersecurity downstream, where possible, by advocating for secure-by-design and correcting market failure. This presentation will highlight two areas of our work that align with the NIST Cybersecurity Framework: 1) the UK has been working with U.S. counterparts on improving the security of the Internet of Things, shifting the burden away from the consumer towards industry and 2) the UK is developing better cybersecurity metrics that can be used to communicate the cybersecurity risk postures of organizations to boards.

Is Our Critical Infrastructure Cyber Resistant?

Matthew Gardner and Megan Brown, Wiley Rein

The WannaCry malware attack from North Korea, whipped up a flurry of federal cybersecurity activity in December of 2017, increasing government concern about networks, supply chain security, software, IoT, patching, and technical integrity across the economy. With the recent updates to NIST's "Framework for Improving Critical Infrastructure Cybersecurity," as well as the U.S. Department of Homeland Security planning an aggressive approach to public-private collaboration, expectations for private sector collaboration will raise the stakes for private companies. Executive boards will be expected to ratchet up their review of internal risk management, and companies will face demands to share information and expertise with the

government. This panel will discuss the threats to critical infrastructure, and the impact relevant legislative, regulatory and government initiatives will have on organizations.

Use of NIST guidance in Governmental Settings, including the U.S. Federal Government: Department of Defense (DoD) Components Adopting the Risk Management Framework (RMF) Process. A practical implementation

Gina Nairn and Bob Altiero, Business and Technical Support Group

This presentation details the RMF process throughout the system development life cycle, from configuration management to continuous monitoring to system decommission. Within DoD, RMF combines Information Security (IS) and risk management activities into the authorization process for IT systems. Discussion includes RMF implementation requirements unique to DoD, including the DISA TAG Body of Evidence, DoD common control inheritance, how eMASS integrates into the process (or not), best practices for policies and procedures, and tips for compliance, accreditation and continuous monitoring success. Participants will engage in an interactive work session to concepts, learning how RMF provides capabilities to more effectively manage security risks in diverse environments of complex and sophisticated cyber threats and ever-increasing system vulnerabilities. Speakers will present real-world examples of successes and failures, examples of actual tools and working papers used. This session is for professionals who plan and/or provide resources, manage, administer, support or accredit DoD systems.

Morning Sessions III

Supply Chain Initiatives: Global Strategy to Enterprise Risk Management

Robert Mayer, United States Telecommunications Association, John Miller, Information Technology Industry Council, Chris Boyer, AT&T

As NIST and others have observed, supply chains are complex, globally distributed, and involve interconnected sets of resources and processes. At the strategic level, supply chain issues implicate global commerce, geopolitical risk, nation-state norms, and the integrity of the digital ecosystem writ large. At the enterprise level, supply chain impacts relationships with external parties including vendors, customers and other stakeholders, as well as technologies and processes deployed throughout the organization. NIST, through its Cybersecurity Framework 1.1 update and a series of publications over the years, continues to evolve resources and capabilities to support organizational risk management. DHS recently initiated the ICT Supply Chain Task Force to develop consensus recommendations for actions to address key strategic challenges to identify and mange global supply chain risks. The panel will explore how these initiatives work together to create a holistic and robust partnership across government, the private sector, academia and civil society.

Enhancing Cybersecurity Risk Management Across the U.S. Federal Enterprise

Doug Scoville, Associate Chief Information Security Officer, U.S. Department of Treasury
Gabriela Smith-Sherman, Assistant Director within the Office of Chief Information Officer, U.S. Department of Justice
Tim McCrosson, Cyber Analytics Analyst, U.S. Department of Homeland Security
Peter Gouldmann: Enterprise Risk Officer for Cyber, U.S. Department of State
Taylor Roberts, Cybersecurity Advisor, U.S. Office of Management and Budget

There are a variety of efforts underway to leverage new technologies, processes, and programs to enhancing cybersecurity risk management both within agencies and across the Federal enterprise. This panel will provide some examples of these efforts and solicit their input on how we can move from a more compliance driven approach to cybersecurity towards one that truly uses risk as a means of informed decision making. Such approaches should include: cybersecurity architecture review, ongoing authorization through centralized visibility, quantifying risk, and risk challenges for small-mid agencies.

Software Bill of Materials: Best Practices for Machine-Readable Assurance Data in Mission Operations

JC Herz, Ion Channel

This panel will cover how machine-readable Software Bill of Materials (SBOM) are being consumed and operationalized to raise the security posture and accelerate approval of mission capabilities. Discussions will include case studies about how open formats are being used in defense and industry. Panelists will review the evolving consensus on standards and formats (e.g. SPDX, SWID), similarities and differences between software, firmware, hardware and data provenance, and how machine-readable SBOMs factor into high-assurance and continuous-integration/continuous-delivery workflows. More controversially, this will also include discussion about the software supply chain assurance landscape of both proprietary products and open source ecosystems, which vary widely in their exposure to supply-chain risk and vulnerability to supply-chain injection, capture and attack.

Integrated Cyber Playbooks for Identity Threat Protection (ITP) within the NIST Risk Management Framework

Dr. John Callahan, Veridium US LLC

Identity has become the new attack surface because of the movement of enterprises from perimeter-based systems to global SaaS services.

Called & “ZeroTrust” or “BeyondCorp” (Google) systems, these SaaS-centric approaches to enterprise IT services present new challenges to cybersecurity risk management: What authentication factor(s) should be used for different levels of access and authorization? How long should sessions remain authenticated before implicit or explicit re-authentication? How should cyber threat conditions affect the level of authentication required? What conditions should step-up authentication be required by policy and dynamically based on the threat conditions?

This panel will examine such questions relative to automated orchestration "playbooks" that possess a central role in the Integrated Adaptive Cyber Defense (IACD) program, a joint effort sponsored by DHS & NSA. We will explore the use of playbooks within the NIST Risk Management Framework as a method for reducing and eliminating authentication and authorization vulnerabilities for distributed enterprises.

A Tale of Two Frameworks: Optimizing Federal Agency Use of the Risk Management Framework and Cybersecurity Framework through Framework Profiles

Christina Sames and Julie Snyder, MITRE

The Risk Management Framework (RMF) has been guiding federal agency cybersecurity risk management activities since 2002. In 2017, Executive Order 13800 required heads of federal agencies to also use the Cybersecurity Framework (Cybersecurity Framework) to manage their agency's cybersecurity risk. While these two frameworks share a common goal of addressing cybersecurity risks as part of an organization's enterprise risk management program, the scope and approach of each differ. Despite their differences, the two frameworks complement each other in ways that allow organizations to realize the best of both in their implementation. This session will: introduce the basic concepts of each framework, provide an overview of Cybersecurity Framework Profiles, and explore opportunities for using those Profiles to bring greater efficiencies to each step in the RMF using a worked example for an information system.

Afternoon Sessions IV

Cybersecurity Coalition Distributed Denial of Service Mitigation Profile

Ari Schwartz, Coalition for Cybersecurity Policy and Law

The Cybersecurity Coalition has been developing Distributed Denial of Service (DDoS) mitigation profile of the Cybersecurity Framework. This is a critical deliverable identified in the DOC/DHS botnet report submitted to the President in May 2018. It is also a little different than past Cybersecurity Framework profiles, which were focused on sectors rather than a specific threat (DDoS.)

Adding Rigor and Depth to RMF Step 2 (Select Security Controls)

Thomas Llanso, Johns Hopkins University Applied Physics Laboratory

With the ultimate goal of resilient, survivable missions and related cyber systems, this presentation focuses on on-going work at Johns Hopkins University Applied Physics Laboratory in the area of risk analytics. The talk discusses a small set of complementary analytics that together inform recommendations for a security architecture and related mitigations (security controls). The analytics include threat exposure, asset mission criticality, derived risk, mitigation recommendations, and multi-objective tradespace analysis. The analytics make use of the recently released NSA/CSS Technical Cyber Threat Framework (version 1.0) as well as additional datasets that map threats to cyber-related asset types and mitigations to the threats. The presentation illustrates the analytics with a common example.

Evaluating "Reasonable" Cyber Risk Using the Center for Internet Security Risk Assessment Method

Phyllis Lee, Center for Internet Security, Paul Otto, Hogan Lovells US LLP, Chris Cronin, HALOCK Security Labs

Center for Internet Security published a new risk assessment method in April 2018 that enables organizations to conduct risk assessments so they are meaningful to both internal and external audiences: regulators, litigators, cyber security specialists, and non-technical managers. The Center for Internet Security Risk Assessment Method (CIS RAM) provides detailed and practical guidance that builds on NIST 800-30, and is consistent with regulatory and legal expectations for establishing "reasonable" and "appropriate" risk. The proposed panel discussion will feature the authors of CIS RAM who will present the method, its basis in security frameworks and law, and case studies that illustrate its use in legal and non-legal contexts.

Integrating Privacy into the Risk Management Framework

Celeste Dade-Vinson, U.S. National Institutes of Health, Elizabeth Koran, U.S. Department of Health and Human Services

The Health and Human Services (HHS) Office of Privacy and Information Management (PIM) and National Institutes of Health (NIH) Senior Official for Privacy/Privacy Act Officer will lead a panel discussion on critical considerations when integrating privacy into an organization's assessment and authorization process -- particularly the establishment of a privacy continuous monitoring program. The conversation will focus on a range of concerns, including whether and to what extent the privacy control assessments can be integrated with security, whether and to what extent the assessments can or should be automated, and challenges in implementing such a program in a federated department with multiple potential loci of control. The panel will include perspectives from both a policymaker and implementer. They will provide practical lessons learned that can be leveraged in establishing a privacy control assessment and authorization process in unique contexts.

Electrical Manufacturers' Role in Cyber Supply Chain Risk Management

Steve Griffith, National Eletrical Manufactures Association, Pranesh Rao, Nidec Motor Corporation, Harsha Banavara, Signify, James McLean, Siemens Healthineers, Max Wandera, Global Products Cybersecurity Center of Excellence

This panel session will discuss how the manufacturers of a wide range of connected electrical and medical imaging products are using industry best practices to secure their supply chains, secure their operations, and secure their products, minimizing cybersecurity threats along the way. The panel will include specific case studies from NEMA member companies.

How to Develop a Cybersecurity Framework Profile

Julie Snyder and Dave Weitzel, MITRE

Since 2015, the NIST NCCoE has worked with the oil and natural gas industry, the cruise line industry, and the intelligent transportation community to develop Cybersecurity Framework Profiles. that are being used as baselines for organizations to refine for enterprise use. Based on lessons learned, the NCCoE has developed a Cybersecurity Framework Profile How-To Guide. nccoe.nist.gov in collaboration with NIST colleagues and industry members. The How-To Guide to describes the approach we use, provides guidance regarding identifying candidate team members, stakeholders, development steps, workshop materials, and tools for the development of a Cybersecurity Framework Profile, and shares the tools that have enabled our process. Through participation in the workshop, profile developers will gain tools and knowledge to implement profiles in their environment.

Afternoon Sessions V

Cyber Threat Framework

Robert Mate, U.S. Office of the Director of National Intelligence

The Cyber Threat Framework was developed by the US Government to enable consistent characterization and categorization of cyber threat events, and to identify trends or changes in the activities of cyber adversaries. The Cyber Threat Framework is applicable to anyone who works cyber-related activities, its principle benefit being that it provides a common language for describing and communicating information about cyber threat activity. The framework and its associated lexicon provide a means for consistently describing cyber threat activity in a manner that enables efficient information sharing and cyber threat analysis, that is useful to both senior policy/decision makers and detail oriented cyber technicians alike.

Connecting to the Business Mission: Why Context Matters for Security Teams

Efe Orhun, Derivative Technology

Security teams today deal with everything from nation state attacks to new digital product launches; and while a security team's prime directive is to mitigate the risk of desired business outcomes, making the connection between these and IT security operational activities is often shaky as best. Companies of every size and industry can benefit from a structured approach that connects business impact with security governance and IT operations, to not only connect security team to the business mission, but also to build shared roadmaps that focus on what matters most via an effective use of limited resources.

This session will talk through such an approach, how technology can support it, and discuss case studies where it has been successfully applied to reduce risk and augment over-stretched security teams.

Measuring an Organization's Security Maturity Using the NIST Cybersecurity Framework

Scott Davis, Clorox

Many organizations often are very good at measuring security metrics from traditional controls and monitoring solutions. However, the challenge has been providing an overall view of the security organization to management and business customers and tracking progress over time. This session will explain how using the NIST Cybersecurity Framework along with a maturity model (Initial – Optimize), organizations can provide a view into how effective the security program is performing year after year using a well-defined set of metrics.

The Business and Regulatory Value of Third Party Certification to the NIST Cybersecurity Framework

John DiMaria, British Standard Institute, Ronald Tse, Ribose

BSI's "NIST Cybersecurity Framework (NCFS)" assessment tool provides a harmonized approach to cybersecurity, and now has joined the ranks of ISO (ISO 27103). Third party certification has been embraced globally by many countries as a way to increase global consistency to cybersecurity approaches and to support an industry-based self-regulatory system rather than a government-based mandated regulatory system. This session will feature one of the first global organizations certified by BSI to the NIST Cybersecurity Framework. Attendees will hear how: company leadership has picked up the vocabulary of the Framework and having informed conversations about cybersecurity risk; the Framework's tiers are used to determine optimal levels of risk management; and the process of creating profiles promotes understanding of current cybersecurity practices and helps in integrating these findings with their information security management system. The organization implementing the NIST Framework also will explain how the Framework's holistic nature integrates with ISO/IEC 27001, how that helps in prioritizing and budgeting for cybersecurity improvement activities, and how the certification process validated their approach and proved the effectiveness of their process.

Helping Communities Utilize the NIST Cybersecurity Framework -- ISAOs as a Catalyst for Developing Community Cybersecurity Programs

Greg White, University of Texas San Antonio, Information Sharing and Analysis Organization Standards Organization

With the expansion of the information sharing community beyond the original Information Sharing and Analysis Centers (ISACs), new organizations are being formed, including Information Sharing and Analysis Organizations (ISAOs) focused on states and communities. These geographic-based ISAOs are not limited to critical infrastructures; they are public-private partnerships including all entities within their geographic boundaries. ISAOs can become a catalyst for establishing viable and sustainable security programs. In particular, they can help with the adoption of the NIST Cybersecurity Framework by all sectors in varied geographic areas. Often small and medium-size organizations do not have the expertise to implement the Framework and may struggle with establishing their own security program. Using a local ISAO

and following the Community Cyber Security Maturity Model (CCSMM), these entities can be provided with a roadmap and mentors to help them establish their programs and incorporate the Framework.

Simple, Consistent, and Secure Cybersecurity and Privacy in Small and Medium-Sized Organizations

Koushik Subramanian, UI Labs

Many small and medium-sized organizations face similar challenges with regards to cybersecurity and privacy. The biggest hurdle is the lack of resources. This can be a lack of budget, talent, time, etc. The sheer thought of cybersecurity can cause a lot of organizations to simply accept the risk under the guise of "no one would attack us." This type of thinking must evolve. Maturing an organization's cybersecurity posture even by a little bit can ensure that they are not the low-hanging fruit that most commonly gets attacked. This presentation offers simple, actionable items to help organizations to prioritize and tackle cybersecurity and privacy concerns and mature their overall cybersecurity posture.

A Framework for Cyber Security Performance

Russell Thomas, George Mason University

This talk has three goals. First, we will define performance, as distinct from practices, and make the case for a distinct framework focused on performance and incentive-based cyber security management. Second, a ten-dimensional framework will be presented. Rather than focusing on details of each dimension, we will focus on "double loop" organization learning, capability building, and how the framework maps to the NIST-CSF and NIST-RMF. Finally, a method for measuring aggregate performance will be introduced. This talk will close with a call to action regarding how to advance the development and adoption of this framework and approach.

Implementing Secure Systems using the PMBOK and NIST Cybersecurity Framework and Baldrige Excellence Tool

Lawrence Capuder, ConsultantC Services

Federal agencies and other entities with critical IT infrastructure need to ensure that secure IT infrastructure standards are integrated into new and upgrade IT design, development and implementation projects. These organizations need to provide special attention to disruptive technologies, such as cloud computing, that the FISMA and FedRAMP projects encourage. This session will answer key questions related to ensuring that appropriate security and controls are followed in carrying out these projects. These include: How well do the NIST Cybersecurity Framework and Baldrige Cybersecurity Excellence Builder self-assessment tools address not only existing systems, but also new IT initiative projects? Why is using a well-defined project management methodology, such the Project Management Institute's (PMI) Project Management Book of Knowledge (PMBOK), crucial to implementing secure systems? How can the PMBOK be integrated with the NIST Framework and Baldrige tool to specifically address secure Federal and critical infrastructure systems?

Enterprise Risk Mitigation Using the NIST Cybersecurity Framework and Cyber Analytics

Dave Simprini, Grant Thornton

Participants will learn about a case study of a large State government client in which cyber risk data from across state agencies was collected, assessed, and aggregated into a cyber analytics tool. This solution allowed the State to look across the enterprise and determine where its most significant vulnerabilities existed, where to prioritize and spend limited funds to maximize the "bang for buck", and to identify areas where agencies were strengthening their cyber posture.

Are We Building "Maginot Lines" in our Networks?

Joseph Drissel, CyberESI

This presentation will walk thru an actual network based attack. As we go through the actual key strokes of the attacker and other aspects of the incident, we will correlate the actions taken by the actor to aspects of NIST Publication 800-171. From this perspective we will work together to identify which security measures will work and which ones will be "Maginot Line" security controls. "Maginot Line" security controls within our networks give the network owners a false sense of security and actually increase the risk of a serious intrusion.

The ISF Standard of Good Practice and the NIST Cybersecurity Framework

Mark Chaplin, Information Security Forum

The Information Security Forum (ISF) Standards of Good Practice and the NIST Cybersecurity Framework are two of the world's most used frameworks for cybersecurity programs. While each provides users with value, leveraging both approaches together can provide added benefits in terms of cybersecurity guidance and communication mechanisms for all levels of the organization. This talk will explore the intersection of the two documents through an exercise in implementing NIST Interagency Report 8204, *Cybersecurity Framework Online Informative References (OLIR) Submissions* (DRAFT).

Automated Cyber Hardening

Michael Worden and Austin Garret, Raytheon

DevOps is a software development and delivery process that emphasizes communication and collaboration between product management, software development, and operations professionals. Cybersecurity is a particularly thorny challenge for DevOps as applied to Satellite Mission Management Systems, especially when complicated by governmental security requirements defined in the Risk Management Framework (RMF). This talk will outline the evolution of a cybersecurity automation approach to automate the application of STIGs (Secure Technical Implementation Guides) and detail important lessons learned, including: application of security rules via infrastructure as code, leveraging automation platforms like Chef or Puppet, and integrating security testing using Nessus and ACAS. In addition, attendees will learn about STIGLER, a tool which ingests DISA STIGs and automates the application of the hundreds of hardening rules needed to make Windows and Linux platforms compliant with RMF.

Risk is Money

Paul Neslusan, Leidos

All cybersecurity -- from the strategic to the tactical -- depends on proper business risk assessment. One of the most important aspects is tying risks to dollar values. The presenter will explain how risk tied to monetary value drives decisions for everyone from shareholders to the security practitioners themselves, and how this will drive cyber security spending for years to come. The security industry is rapidly moving away from selling and buying based on fear; it is aggressively moving toward analytics driven purchasing. During time spent advising security practitioners from the analyst level to the C-Suite, the presenter saw considerable frustration: people feeling unheard, critical projects unfunded, and glaring concerns left unattended. This presentation presents a clear picture of why financially-tied risk assessment is important to both vendors and security practitioners, and how they can use this knowledge to accomplish their goals while ignoring distractors.

Role-Based Risk Management Framework -- RMF and NICE Framework Convergence

Jeffrey Monroe, U.S. Department of Interior

Frameworks help to organize and unpack complicated matters. NIST has developed two helpful frameworks for information security programs. Learn one method to overlay these frameworks, build cohesion between the frameworks, and improve your security program.

Risk Data Sharing for Situational Awareness

Dr. David Ferlemann and Dr. Pearl Rayms-Keller, U.S. Naval Surface Warfare Center

Maintaining cyber situational awareness requires effective and timely exchange of risk information among analysts, managers, and experts across internet networks. This exchange of critical information has not been effective due to several factors. First, the current state of cyber risk assessment involves assessing many risk frameworks and technologies -- yet finding common denominators has been challenging. Organizations and their branches often choose different policies, risk assessment tools and communication methods. A second factor working against efficient sharing of common risks is organizations' reluctance to point to internal vulnerabilities to external partners, which then might expose themselves to potential threats. In terms of technical challenges, modeling and capturing a diversity of risk data is difficult, and processing and presenting the risk data at this scale in a timely manner is also a great obstacle. The presenters will discuss possible architectures to exploit advances in learning algorithms (artificial intelligence) and better information systems. They will also discuss the role that organizational psychology plays in this cyber vulnerable age and provide a strategy on how "building trust" across organizations could be the first step to achieve multi-domain cyber risk situational awareness.

Using the NIST Framework to Design and Implement Risk-based Cybersecurity Management in a Global Conglomerate

John Petrie, Nippon Telegraph and Telephone Corporation

The speaker will share NTT's ongoing efforts to use the NIST Cybersecurity Framework to unify cybersecurity practices among its global operating companies. NTT has grown globally through merger and acquisition. Each operating company has a different country franchise, size, culture, and business focus. Currently, its global business size is $20 billion (USD) with more than 20 significant operating companies. NTT aims to develop a "One NTT with diversity" strategy for its cybersecurity management, and to use the NIST Framework to develop and implement this strategy. The presentation will describe: NTT's international businesses, its aspiration to develop harmonized cybersecurity practices, the role of the NIST Cybersecurity Framework in developing a common goal across NTT's diversified operating companies, and key challenges in the on-going efforts. This will be a unique case, where the NIST Framework is being used with a global scope and significant size. By sharing a success story, the speaker aims to stimulate active discussions and welcomes the opportunity to learn from participants about how to apply the NIST Framework to a different business culture, focus, and size.

Measuring the Cybersecurity Risk of Software-Intensive Systems

Bill Curtis and Marc Jones, Consortium for IT Software Quality

The Consortium for IT Software Quality (CISQ) has developed standards for measuring structural quality in the areas of Reliability, Security, Performance Efficiency, and maintainability. These measures are calculated from statically detecting and measuring severe structural defects in source code. These standards are currently being revised for application to embedded software. When calibrated against operational performance, these measures can assess several areas of cybersecurity risk to which a software system exposes the enterprise. These measures comply with software product quality definitions in ISO/IEC 25010 and supplement the behavioral measures in ISO/IEC 25023 by measuring software quality attributes at the source code level. The talk will describe how these measures can be applied in software acquisition, in agile/DevOps environments, and in implementing the NIST Cybersecurity Framework. It will end by discussing the possibilities and challenges of certifying the structural quality of software.

NIST Cybersecurity Guidance as Systems Engineering Construct -- and not DIACAP By Another Name

Gary Stoneburner, Johns Hopkins University Applied Physical Laboratory

This presentation will provide perspective on the current, common state-of-affairs with regard to organizations' use of the NIST cybersecurity guidance more as prescriptive policy requirements than as descriptive guidance for use in engineering adequate responses to risks from the use and dependence on information technology. Attendees will hear a rationale for why the recent NIST guidance on System Security Engineering (Special Publication 800-160) is a key element of effective risk management. The presenter also will suggest specific steps for understanding the

underlying engineering focus already included in the NIST guidance – something that is essential to achieving the needed assurance of mission/business success without causing undue harm elsewhere.

Achieve Cybersecurity Excellence: Learn and Apply the NIST Cybersecurity Framework, Baldrige Cybersecurity Excellence Builder and the NIST NICE Cybersecurity Workforce Framework

Peter Romness and Steve Caimi, Cisco

"Cybersecurity Excellence" means finding a way to both efficiently and effectively manage cyber risks. It means asking the right questions and focusing investments in security controls that that matter most. It means successfully defending critical systems and sensitive information despite persistent threats, ongoing talent shortages, and ever-present budget constraints.

Do you have what it takes to achieve Cybersecurity Excellence in your organization?

This engaging session provides the specific knowledge and tools that enable Cybersecurity Excellence. First, we'll examine the NIST Cybersecurity Framework (CSF) to show you how to identify the essential security controls that your organization needs immediately -- and what might be able to wait. Next, we'll explore the Baldrige Cybersecurity Excellence Builder which complements the NIST CSF by helping you ask the right questions -- ones that guide you toward critical risk-based investment decisions. Third, we'll explain the NIST NICE Cybersecurity Workforce Framework to help you understand how to attract, develop, and retain the right people with the right cyber skills. Then we'll summarize by showing you how each of these tools work together in your organization to help you achieve Cybersecurity Excellence.

Morning Sessions VI

Building Security In: How the RMF Impacts Legacy Practices and System Modernizations

Ronda Henning, Harris Corporation

For the last 15 years, the Systems Engineering disciplines have embraced the Capability Maturity Models (CMMIs) as the gold standard of risk mitigating development practices. Various specialty engineering disciplines have developed comfortable tools and methodologies to address their contributions to the system development life cycle. The Risk Management Framework, with tailored security controls, overlays, and hybrid controls, is a different way of doing business within the SDLC. This discussion addresses the new way of doing business the RMF represents; and how to mitigate the potential impacts of the RMF to legacy practices and system modernization initiatives. Included in this topic will be a discussion of "building security in" to the agile development methodologies and microservices architecture models.

Lock Down Your Login

Maryam Cope, Goldstein & Cope

Critical infrastructure are those assets the loss of which would result in great harm to the nation's security, economy, health and safety, and morale. Without a doubt, cybersecurity and resiliency is of increasing importance to legislative bodies worldwide as they face cyber and hacking threats from highly competent and organized actors. In addition, the attack surface of legislative bodies is varied and complex. This session will discuss the implementation of Lock Down Your Login, a public-private partnership that uses the NIST Cybersecurity Framework to improve the cybersecurity posture of the US Capitol, the official offices of Members of Congress, and their staff. This panel will discuss the challenges and benefits of using the NIST Cybersecurity Framework to help secure a young, dynamic, and connected workforce, as well as the unique cybersecurity risk-management issues facing legislative bodies in democracies worldwide.

Towards Autonomic Security Management

Stefano Iannucci and Craig Shorter, Mississippi State University

The continuous increase in quantity and sophistication of cyber attacks is making it more difficult for system administrators to handle the alerts generated by Intrusion Detection Systems. To deal with this problem, several Intrusion Response Systems have been proposed to automatically respond to detected attacks. However, to the best of our knowledge, most existing approaches are not adequate because a response is usually selected either with a static attack-response mapping or by quantitatively evaluating all the available responses, which introduces serious scalability issues in managing countermeasures. In this talk, the presenters will propose a methodology based on reinforcement learning – a technique that automatically learns the behavior of the system and of the attacker, and autonomously drives the protected system towards a safe state. The approach will be framed into the Monitor, Analyze, Plan, Execute autonomic loop, showing how it can be connected to existing state-of-the-art technology.

Proactive Cybersecurity Through Cross-Domain Intelligence

Greg Jaeger, Advanced Technology International

Cross-domain collaboration merges the unique skills, perspectives, and contributions of Operations and Development roles that yields unparalleled cyber resilience. This presentation explores how a cyber-event led to the development and implementation of processes leading to a proactive cybersecurity posture on a fixed-price contract without additional tools, data or personnel. The transformation applied incremental changes in Team roles, relationships, and activities based on the tenets: 1) cybersecurity is a core requirement; 2) system awareness is the high ground; 3) cyber subject matter expertise is resident in development and operations; and 4) combined perspectives magnify intelligence. The institutionalized cybersecurity awareness enabled the detection and intervention within hours of the same exploit that Equifax failed to notice for more than two months. The methodology matured the existing workforce with requisite system knowledge into a high-performance cybersecurity team that produced measurable cyber risks and strengthened management confidence in making smarter, risk-based decisions.

Deriving Business Insight from Cybersecurity Framework Findings

Brett Young, Leidos

This presentation outlines five uses for results from a NIST Cybersecurity Framework assessment. Based on well-established criteria, the CMMI (Capability Maturity Model Integration) allows assessment teams to quantify an organization's maturity for each of the sub-categories listed in the Cybersecurity Framework. The resulting scorecard can be used as an input into a variety of governance and business intelligence metrics. For most companies this type of insight can reduce their security spend by comparing the company's stated security objectives with best practices. The results can be useful for determining cybersecurity strategy. Example studies will be highlighted:

- Using quality inputs – How to ensure that the scores used are consistent.
- Tools and Controls – How do the organization's tools and controls address the provisions of the NIST Cybersecurity Framework sub-categories? This facilitates decisions on budgets and policy development.
- Team responsibilities – Which teams/roles are responsible for policy based on the Cybersecurity Framework?
- Cybersecurity Initiatives – How do the organization's cybersecurity initiatives compare with the vulnerability profiles from Cybersecurity Framework results?
- Managed Service Provider (MSP) - outsourced services – Which responsibilities should an MSP bear, and how to map those to the Cybersecurity Framework.
- Quantifying Risk – Assessments, along with technical scans represent the best source for assessing risk using methods such Factor Analysis of Information Risk (FAIR).

Participants will receive a spreadsheet with examples of each study discussed.

The Digital Fast Lane – Helping Nonprofits Keep Up

Kelley Misata, PhD, SightLine Security

The last time you gave money or time to your favorite charity did you think about their information security? Did you wonder what measures they were taking to protect your data? Nonprofits are being targeted for the same types of intrusions as large commercial organizations, but have far fewer resources to defend themselves and they are often overlooked by the security field. This presentation will spotlight the challenges facing nonprofits and will present a new and holistic approach to help them create confidence through assessments, plans, and measurements to improve information security. Based on research utilizing the NIST Cybersecurity Framework and from the unique view of a survivor of cyberstalking turned Ph.D., the presenter will spotlight her study and strategies for how the security community can make a difference.

State Supporting in Cybersecurity for SMB Organizations – Best Practices in Korea

Yeseul Lee, South Korea

To prevent the spread of cyber incidents of Korean private sector, KISA(KrCERT) is operating 24/7 cyber incident responding systems and services. Cyber curing service on zombie PCs and infected smartphones is one of these services.

When a PC or smartphone is identified to be infected, notification and guidance are provided to treat the victimized devices. DDoS sheltering service is to block DDoS attacks and support SMEs to provide normal web services since most of SMEs have less interest in cyber security and low ability to overcome cyber attacks.

When there is a DDoS attack, this shelter will block all attack packets and only normal packets can flow into to websites. There is also a Bug Bounty Program through which people can report software vulnerabilities. So over 2000 cases in Korea have been reported and over 1000 cases have been rewarded.

Best Practices Learned from Mitigating Risks of Data Breaches to Build a Data Privacy Program

Anne Connell, Carnegie Mellon University

It is not a matter of 'if', but rather, 'when' a data breach will transpire. The presenter will discuss the most common vectors of data breaches to provide insight into the lifecycle of an incident, especially incidents involving Personally Identifiable Information (PII). Due to the sensitivity associated with breach investigations and intrusions, many security practitioners and investigators are unwilling to report or disclose this information, but they have been willing participants to share this knowledge with the rest of the cybersecurity community. Attendees will learn about the most common attack vectors against organizations of any size -- and those that seek to take advantage of end users, which is the most common entry point for a PII attack. While the human element is the most common vector for an attacker, there are many areas outside of the control of a typical end-user that may contribute to the problem. To achieve a baseline, researchers conducted many interviews with security practitioners and investigators to learn the most common attack vectors involved in incidents impacting a variety of organizations in multiple industries as well as the response to a successful data breach. Using the information collected, researchers used the NIST Cybersecurity Framework to build an effective data privacy program to mitigate risk. They also used the NIST Guide to Threat Information Sharing to coordinate incident handling, including producing and consuming PII, participating in information sharing communities, and protecting incident related data. The goal of this talk is to inform and educate security practitioners on best practices to protect data privacy and to mitigate the risk of data breach using these frameworks.

Cyber Risk – Through the Shareholder Lens

Bob Gardner, New World Technology Partners

If Executives, Public Officials and their Boards could measure the impact of cyber risk on the net income (net revenue, earnings per share, retained earnings), capital (risk weighted assets) and free cash flow, as well as the consequences to share value and volatility, they could determine more appropriate risk appetites and tolerances. When they feel the impact on their shareholders', donors' or constituents' vital interests, they can allocate resources, make prudent disclosures and demonstrate duty of care commensurate with exposure.

Close analogies exist for federal agencies' financial, reputation and geopolitical risk exposure affecting National Security (America's Enterprise) Risk.

There are several approaches available to quantify enterprise risk consequences by evidence-based, mathematical analyses, elements of which may be found in the NIST CSF and other Enterprise Risk Management (ERM) paradigms & tools.

Cybersecurity in Small and Medium-sized Businesses

Johnathan Hard, H2L Solutions

Small and Medium businesses are an important part of our nation's economic and cyber infrastructure. Small businesses alone produce approximately 46% of our nation's private-sector output and create 63% of all new jobs in the country. However, with the ever growing and constantly evolving cyber threat landscape; small and medium businesses (SMBs) are at a much higher inherent risk of being involved in today's cyber-attacks as compared to larger organizations.

There are a variety of reasons for the increase in today's cyber criminals targeting small and medium businesses (SMBs). The most prevalent being that such businesses do not have the resources or budgets to invest in basic information security systems.

Our goal is to address best practices in small and medium organizations, as well as explore the cybersecurity framework posed to (SMBs) by the National Institute of Standards and Technology (NIST).

Cybervets: Leveraging Veterans to Build the Cybersecurity Workforce

P. Shane Gallagher, SG Systems Consulting, and Frank Domizio, Centers for Medicare and Medicaid Services

This presentation describes the Center for Medicare & Medicaid Services (CMS) innovative "Cybervets" program designed to address the severe shortage of skilled cybersecurity workers using highly capable veterans. Current estimates indicate that nearly half of all veterans are unprepared to transition into the civilian workforce. Beginning in June 2018, this joint program between CMS, the Veterans Administration, and the Office of Personnel Management began providing a year-long immersive advanced cybersecurity training program through cognitive

apprenticeship and mentoring. The training uses a hands-on, problem-based approach combined with the opportunity to shadow experienced analysts in the CMS security operations center (SOC) to help the Cybervets acquire the relevant experience, knowledge, skills, and abilities (KSAs) associated with the NICE Framework Cyber Defense Analyst (PR-DCA-001) position. Program evaluation activities to date indicate a high level of participant satisfaction and knowledge growth.

Demystifying ICS Cyber Risk

Mike Radigan, Leidos

For plant operations management to support and fund new cybersecurity initiatives, they must understand the relative positive impact on reliability and safety compared to applying these same resources to mitigate more familiar operational risk issues. This presentation will demonstrate by case study how 1) cyber risk was analyzed, quantified and compared to the top operational risk issues for a power plant and 2) risk mitigation options were evaluated and chosen based on a common financial metric of risk reduced per unit cost. Attendees will learn how to compliment the SP 800-30 Guide for Conducting Risk Assessments with The Open Group's Risk Taxonomy v2.0 (O-RT, Ref C13K) quantitative risk model and analytics within an operational environment. Using these resources can demystify cyber risk and answer the most challenging questions facing plant operations today: How much cyber risk is there and how does it compare with operational risk issues?

Implementing the Cybersecurity Framework

Ernest Begin, KAMAN

How can you measure your cybersecurity posture? What is your IT risk tolerance? Are our cybersecurity practices mature enough? Hear how Kaman, a mid-sized provider of aerospace and industrial solutions, identified and implemented the Cybersecurity Framework from an IT policy perspective, how they measure their cybersecurity maturity, and how they plan to communicate that to their suppliers and customers.

Understanding and Managing Cyber Risk with a Dwell Time-Based Approach

Arun Sood, George Mason University

Preventing all intrusions is nearly impossible. The presenter suggests adding a different layer of defense by using the Moving Target Defense paradigm that seeks to minimize damage after an intrusion has occurred by limiting the time available to the attacker. Intruder DWELL TIME can be an important defense mechanism, and has the added advantage of being easily understood and measured. A typical attack takes place in 3 phases – Get In (Phishing), Stay In (Lateral Move) and Act (Ex-filtration). Attendees will learn about an approach that reduces available time during the Stay In and the Act steps which can mitigate IT and OT attacks. The presentation will address: 1. Defining resilience and recovery and compare recovery systems with alert systems. 2. Mitigating direct and indirect attacks (Building Automation Systems and Security

Camera Networks). 3. Benefits and limitations of a dwell time-based approach. 4. Use cases.

A Structured Approach for Privacy Risk Assessments of Federal Organizations
Sarbari Gupta, Electrosoft

The presenter will propose a two-level Privacy Risk Assessment (PRA) methodology: 1) an organizational-level PRA that focuses on NIST SP 800-53 Rev4 Appendix J privacy controls; and (2) a system-level PRA for each information system that focuses on system-level privacy controls and analyzes the Privacy Impact Assessment (PIA) for that system. At each PRA level, the goal is apply an SP 800-30 Rev1-style risk assessment approach by identifying applicable threats, gaps/weaknesses (vulnerabilities) in privacy control implementations, a likelihood of occurrence, and the resulting impact. The impact of an attack (a privacy threat exploiting a privacy vulnerability) can be derived by considering the magnitude of harm to individuals if their PII suffers from low quality, unintended aggregation, unauthorized disclosure, or unauthorized modification/ destruction as a result of the attack. The risk is low, moderate or high if the individual suffers limited, serious, or catastrophic harm, respectively.

The Transformation of Global Value Chains: Hardening the Weakest Link
Jorge Portugal, Portugal

This presentation will cover the increasing complexity on business space networks dictated by digitalisation impacting value and supply chains, the changing nature of the threat landscape (from espionage to disruption), evidence of the weakest links (both human and organisational) and discussion on possible solutions to mitigate and countermeasure risks on this new brave, interconnected world. We will share our own case as an innovation business network, as an exporter country, open to the world economy.

Afternoon Sessions VII

A Practical Approach to IT Security for Small and Medium-Sized Businesses Based on the NIST Cybersecurity Framework
Jim Wentworth, JAC Associates

As the Internet of Things (IOT) and cloud computing extend the IT security perimeter well beyond the traditional data center, organizations must embrace an IT strategy that addresses today's security needs while evolving to meet new, more sophisticated threats in the future. Small- and medium-sized businesses (SMBs) face an even more daunting challenge. While they have the same IT security needs as larger organizations, they typically do not have enough resources dedicated to planning and maintaining their IT security. This session targets the IT security skill needs of these SMBs by identifying five key components of an effective IT security strategy and outlining a series of clear, practical steps which SMBs can execute to enhance their IT security. Session attendees will receive free access to the Grok IT Academy online security course, A Practical Approach to IT Security for Small- and Medium-sized Businesses based on the NIST Cybersecurity Framework.

Data-Driven Breach Response Planning

Jay Brudz, Anand Raj Shah, Drinker Biddle and Reath LLP; Serge Jorgensen, Sylint Group; Kenneth Darrell, Tritura Information Governance; and Jeff Hunt, PulsePoint Group

The expanding scope, sophistication and frequency of data collection provides strategic opportunities for organizations responding to a cyber incident by leveraging timely intelligence and data analytics. Industry experts in information security, crisis communications, law and data science will examine steps that incident response teams can take to implement a data-driven approach to data breach response.

Data-Driven Risk-based Decision Making

Ellen Ambrosini, Teresa Proctor, and Michael Pagels, Centers for Medicare & Medicaid Services, *and Kevin Eiben, MITRE*

The federal Centers for Medicare & Medicaid Services (CMS) has made significant strides in implementing security and privacy capabilities to support risk-based decision making. A CMS panel will discuss its recent experiences and accomplishments including: integrating the use/practicality of the Cybersecurity Framework within the context of the Risk Management Framework; improvements in Automation (eGRC) and Risk Reporting that inform risk-based decision-making; introducing and utilizing a customer service model with the inclusion of a new role, the Cyber Risk Advisor; mentoring and fostering the role of ISSO using a proactive engagement model; developing and utilizing tools that support risk management; the Cyber Risk Advisor Framework, the ISSO Framework, establishing an assessment methodology using prioritized Core Controls; identifying methods and processes that automate the assessments of controls with reliance on repeatable processes and data that informs risk decision making; integrating security and privacy requirements in to agile systems development models; and the role of Privacy Advisors on IT project intake review teams to help build a culture of "privacy by design."

Panels in Progress

- Cybersecurity Measurement and Metrics
  - Panelists: TBD
- Federating Framework Informative References
  - Panelists: TBD
- Connecting the Dots Between Threats & Mitigations in Federal Networks
  - Panelists: TBD
- Vendor Management & NIST SP 800-171
  - Panelists: Renate Neely, Gaurav Pal, John Kupcinski, Theresa Campobasso, Amit Garg
- US Federal Government Sector Guidance
  - Panelists: Julie Chua, (more to be named)
- Reducing Cybersecurity Risk Exposure in Medical Devices
  - Panelists: Armin Torres, (more to be named)
- Manufacturing Extension Partnership and Manufacturing Cybersecurity
  - Pat Toth, (more to be named)
- Tips and Tricks for Small Business Cybersecurity
  - Panelists: Rob Arnold, (more to be named)
- Internet of Things Security – Past, Present and Future
  - Panelists: George Wrenn, Karen Scarfone, Ken Durbin, (more to be named)
- Using the Framework as an Umbrella for Your Cloud
  - Panelists: Michael South, Bill Richmond, Shirley Zhao, Dan Prieto
- Spanning the Org Chart from Metrics to Risk
  - Panelists: David Sliom, Dan Carayiannis, (more to be named)

Facilitated Sessions

- Cybersecurity Framework Implementation
- Cybersecurity Metrics and Measurement
- Governance and Enterprise Risk Management
- Threats and the Cybersecurity Framework
- Small and Medium-sized Business Resources
- International Next Steps

Birds-of-a-Feather Sessions

- Small Business Cybersecurity and Privacy
- Botnet Cybersecurity Framework Profile
- Why Don't We Comply with Our Own Regulations?

Lunch-and-Learn Sessions

- Risk Management Framework
- Privacy Engineering
- Supply Chain Risk Management
- Cybersecurity Framework
- NICE Cybersecurity Workforce Framework
- National Cybersecurity Center of Excellence (NCCoE)
- Baldrige Cybersecurity Excellence Builder

Speaker Biographies

Rob Arnold

Rob Arnold is the CEO of Threat Sketch, a strategic cyber risk management firm helping small organizations manage cybersecurity at the executive level. Mr. Arnold completed his graduate studies in information security at East Carolina University and is ISACA certified in risk and information systems control. He is the author of **Cybersecurity: A Business Solution** and has testified before Congress on the subject of cybersecurity. Nationally, he is a member of the IT Sector Coordinating Council, BENS, Infragard, and two National Small Business Association councils. Active in his local community, Mr. Arnold is a founding member of the Piedmont Triad Cyber Round Table and serves on the board of the Forsyth Technology Community College's cybersecurity program, which is a certified NSA Center of Academic Excellence.

Aviram Atzaba

Aviram Atzaba is the Director of Methodology & Audit Center in the Israel National Cyber Directorate. In this role, he is responsible for the development of Cyber Defense methodologies for the Israeli market and for the performance of Cyber Resiliency testing of the Israeli critical infrastructures. In his previous positions, he served in the Israeli Air Force. His areas of expertise are Avionics, Connectivity, System of Systems, Network Centric Warfare and Cyber Warfare.

Harsha Banavara

Harsha Banavara, CSSLP is a Cybersecurity Technical Policy Manager at Signify (previously Philips Lighting). He has a Master Degree from Auburn University, AL and over 10 years of experience in Information Security. He is one of the primary authors of the Industrial Internet Security Framework and NEMA Supply Chain Best Practices document.

Matt Barrett

Mr. Barrett and his team are responsible for establishing and maintaining relationships with both private and public sector (Cybersecurity) Framework stakeholders. Mr. Barrett works through those relationships to provide perspective and guidance, as well as gather input on use and evolution of the Framework. To fulfill stakeholder needs, Mr. Barrett also collaborates with a variety of NIST cybersecurity programs.

Matt previously led NIST's Security Content Automation Protocol program and support of the Office and Management and Budget's Federal Desktop Core Configuration initiative. Matt has also served in various executive roles including roles such as president and chief executive officer.

Ernest Begin

Ernest Begin is the Executive Director of Information Security & Governance at Kaman Corporation. In that role he is responsible for the information security stature of the company including development of and compliance with IT Policy; detection, reaction and prevention of cyber threats; and the education of the workforce in regards to information security. Prior to this role Ernie spent 13 years in progressive roles at United Technologies Corporation spanning IT security, compliance, audit and governance. He is CISA and CISSP certified and holds a bachelor's degree in management of information systems from WPI.

Benjamin Brooks

Benjamin D. Brooks is the Vice President of Beryllium Information Security Collaborative and Director of Curriculum Development at Cyber Warrior Foundation. A 20-year information security veteran, Benjamin cut his teeth on information security and cyber security for the Department of Defense. Working primarily with the National Institute of Standards and Technology frameworks as guidance, his work focuses on behavioral and administrative controls for organizations to prevent information security breaches and optimize security practice within the organization. He is also a Cybersecurity architect and Red Team member specializing in social engineering, and physical penetration testing.

Some of Benjamin's previous client engagements include Proctor and Gamble, AXA insurance, State of New Jersey Judiciary, Massachusetts Department of Transportation, Pennsylvania Department of Transportation, and The Ohio State University, amongst others where he has performed PCI, HITRUST, and NIST Information Security Engagements.

Benjamin is an 18-year Chief Cryptologic Technician (Technical) veteran of Naval Special Warfare, Special Intelligence and Electronic Warfare teams and a drilling Navy Reservist. During his time in the service, Benjamin quickly distinguished himself in as an expert in electronic signals

exploitation and was assigned to special units for duty with the Navy SEALs and other government organizations. He currently serves as the Navy Information Operations Command TX – Minneapolis Branch Training Officer.

Benjamin recently finished his Executive Master of Business Administration degree at Case-Western Reserve Weatherhead School of Management, where he serves as adjunct professor for executive education in Cybersecurity and Information security. He is a fellow at Ponemon Institute, and also provides subject matter and exam writing expertise for (ISC)².

Jamie Brown

Jamie Brown serves as Policy Advisor for SAFECode (Software Assurance Forum for Excellence in Code), a nonprofit organization exclusively dedicated to increasing trust in information and communications technology products and services through the advancement of effective software assurance methods. Brown has served as Director of Global Cybersecurity Policy and Strategy for CA Technologies, managing global cybersecurity, cloud computing, and Internet of Things policy issues. Brown also serves on the Executive Committee for the IT Sector Coordinating Council, the principal IT industry entity for coordinating with the U.S. Government on critical infrastructure protection and cybersecurity. Brown previously served as a Professional Staff Member on the US House of Representatives Committee on Science, Space and Technology. He has been featured on Government Matters, a multi-platform news program dedicated to providing information and analysis to federal managers and contractors and has written articles for Washington Technology and NextGov.

Daniel Caduff

Daniel Caduff is the deputy head of the ICT-Division at Switzerland's Federal Office for National Economic Supply FONES. FONES' duty is to secure infrastructure that is vital to the Swiss economy in general, while Daniel and his team are focusing on ICT-risks in particular. As a federated country, Switzerland pursues a cooperative approach between various government agencies and the private sector. Switzerland provides assistance to the private sector. Awareness, training, open-source tools and transparent information form the basis for this and establish trust between the State and private sectors. In August 2018 FONES released its "Minimum standard for improving ICT resilience" to the public. This standard is based on the NIST Framework Core and has been added to NISTs "International Resources". Daniel holds a master degree in political science and international law and is a DIY-Digital Native. Daniel joined FONES as a project leader for Switzerland's national strategy against cyber-risks, and eventually became Deputy Head of the ICT-Division in 2016. Before joining FONES, Daniel worked for a major Swiss ISP and a consulting company in the field of IT-risk-management-consulting.

Dr. John Callahan

Dr. John Callahan is Chief Technology Officer (CTO) at Veridium, a leading biometric authentication company. Dr. Callahan recently served as Vice-Chair of the committee for the IEEE 2410-2017 Biometric Open Protocol Standard (BOPS) that specifies secure, end-to-end mobile and server-side biometric processing, encryption in-transit and at-rest, and FIDO compatibility. He also served as the Associate Director for Information Dominance at the US Navy's Office of Naval Research Global (ONRG) London UK office from 2010-2014 via an Intergovernmental Personnel Act (IPA) assignment from the Johns Hopkins University Applied Physics Laboratory (JHUAPL) in Laurel, Maryland USA. Prior to JHU, he was a tenured Associate Professor in the Department of Computer Science and Electrical Engineering at West Virginia University (WVU) in Morgantown, WV USA and research director at the NASA Independent verification and Validation (IV&V) Facility in Fairmont, WV USA. He completed his PhD in Computer Science at the University of Maryland, College Park USA.

Dan Carayiannis

Dan Carayiannis currently serves as RSA's Public Sector Director for the Archer governance portfolio. With a career spanning over 30 years, Mr. Carayiannis has held several executive leadership positions within information technology, IT security, geospatial and services companies servicing government and commercial enterprise customers. Mr. Carayiannis has been with RSA for 12 years and is responsible for Archer's Go-To-Market initiatives in the federal, state, local and international public sector. Mr. Carayiannis' responsibilities also includes defining future solution requirements to serve the public sector as well as support Archer's commercial market initiatives involving federal regulations and directives. Mr. Carayiannis was instrumental in securing the DHS Continuous Diagnostic and Mitigation Dashboard award for RSA through which RSA Archer will be deployed and used to manage cybersecurity risk by senior executives across all Federal civilian government departments and agencies.

Prior to RSA's acquisition of Archer, Mr. Carayiannis served as the President and COO of Susquehanna Technologies a leading software services and development company supporting Federal, state and commercial clients with software solutions and managed services. Mr. Carayiannis holds a BBA from James Madison, an MBA from Marymount University and was awarded a Duke University Executive Development Program certificate. Mr. Carayiannis is an active member of several associations and has served on university and business advisory boards.

Julie Chua

Julie joined the Governance, Risk Management and Compliance (GRC) Division within the Department of Health and Human Services (HHS) Office of Information Security (OIS) in October 2015. As the Branch Chief for Risk Management, Julie is responsible for establishing a Department-wide enterprise risk management program. Julie also leads and oversees high visibility initiatives including the identification and protection of HHS' most critical high value assets and the HHS FedRAMP and Cloud Security Program, which is a standardized approach to security assessments, authorizations, and continuous monitoring of cloud service providers. Julie is a regular speaker at conferences and at HHS CISO leadership council meetings where she briefs executive leadership across all HHS Operating Divisions on upcoming risk management initiatives.

Julie is also the Federal Lead for the implementation of the Cybersecurity Act (CSA) of 2015, Section 405(d): Aligning Health Care Industry Security Approaches. This public-private partnership effort is one of many HHS cybersecurity initiatives to help push forward the cybersecurity and resiliency of the Healthcare and Public Health (HPH) sector.

Prior to joining the GRC Division within HHS OIS, Julie served as the Cybersecurity Team Lead within the Office of the National Coordinator for Health IT (ONC) at HHS. In her previous role, Julie was the lead on White House Critical Infrastructure Cybersecurity efforts and spearheaded these cybersecurity initiatives across HHS and its federal partners and the private sector. She led the effort to establish an information sharing and analysis organization (ISAO) specific for the HPH Sector to enable widespread dissemination of cyber threat information as well as general cybersecurity best practices and lessons learned across the sector. Information sharing within the HPH Sector enhances the ability of the federal government to protect the sensitive personal and health data of millions of Americans. She also initiated the creation of a crosswalk between the HIPAA Security Rule and the NIST Cybersecurity Framework. This crosswalk is now available to HPH sector stakeholders such as hospitals and public healthcare facilities, small and medium-sized providers, providing additional guidance and capabilities towards implementing robust risk management programs.

Before joining the federal government, Julie was a small business owner with projects that focused on federal information security policies and regulations, risk assessments, enterprise-level software application development, and innovative mobile applications development. Majority of clients were from the HPH Sector.

Michael Coden

Michael Coden is Head of the Cyber Security Practice at BCG Platinion, a subsidiary of The Boston Consulting Group that provides cybersecurity, technology architecture, digital, risk, and implementation services. Michael has over 30 years of experience in cybersecurity strategy, organization, processes, technologies, research, and product design for both users and producers of cybersecurity products in all sectors. He has advised organizations in the Americas, Europe, the Middle East, and Asia, and is the North America lead for Cybersecurity at BCG.

Michael is also co-founder and Associate Director, of Cybersecurity at MIT Sloan, the MIT Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity, or MIT- $(IC)^3$. In addition, Michael served as Editor of the ISA99/IEC-62443 Cybersecurity Technical Report and Standard.

Michael was involved in the USA NIST Cybersecurity Framework process and received a letter of appreciation from the White House for his leadership. He has published numerous scholarly articles and a book, appeared on radio and television, and holds 16 patents on cybersecurity hardware and software technologies.

Michael helps clients improve their cyber resilience by working with them on their people, process, and technology strategies. He believes in the importance of educating clients on how to use cybersecurity to improve business and increase profits. Michael's casework at BCG Platinion has ranged from developing and implementing cybersecurity strategies at major clients to developing and researching cybersecurity product and market development, and cyber insurance to providing cyber strategy advisory services and training to corporate boards of directors and C-suite management.

Anne Connell

Anne Connell is a Cybersecurity Engineer with the Cybersecurity Risk & Resilience Directorate of the CERT Division at Carnegie Mellon University's (CMU) Software Engineering Institute (SEI). Anne contributes to research and development focused on improving the security and resilience of the Nation's critical infrastructure and assets. Anne has 19 years of experience in cybersecurity, privacy, instructional design, software development, engineering, and project management. Prior to joining the SEI, Anne was a Network Manager with the CMU School of Design, and a Product Lead with Maya. Anne holds a BS degree in Information Systems and a MS degree in Human and Computer Interaction from Carnegie Mellon University. Anne has made a significant impact in certifying the already remarkable reputation CMU, SEI, and CERT enjoys among the federal law enforcement community. In addition to creating cybersecurity training, her contributions to CERT have been in creating data privacy programs, framework development for implementing privacy standards, information sharing to coordinate incident handling through communities, including producing and consuming PII, and protecting incident related data. She also creates

custom cybersecurity training solutions for sponsors, systems and user requirements gathering, and application development. Anne's research focus is to address privacy and cybersecurity concerns in a manner that protects our customers and complies with regulations. This area consists of compliance management, transactional issues, and data breach response. Anne holds certifications in CIPP and CIPT. Anne was the project lead of the FBI Cyber Investigator Certificate Program (CICP), developed for the 750,000 LEO members on cybersecurity investigations. Anne is an instructor of Privacy in the Digital Age at the CMU Heinz College of Information Systems and Public Policy, and is an active member of the Pittsburgh Public Schools to educate students on the internet and social media.

Maryam Cope

Maryam Cope, who runs the Lock Down Your Login outreach program for the National Cyber Security Alliance, will present. NCSA is the nation's leading nonprofit, public-private partnership promoting cybersecurity and privacy education and awareness. NCSA works with a broad array of stakeholders in government, industry and civil society. NCSA's primary partners are DHS and NCSA's Board of Directors, which includes representatives from ADP; Aetna; AT&T Services Inc.; Bank of America; Barclays; CDK Global, LLC; Cisco; Comcast Corporation; ESET North America; Facebook; Google; Intel Corporation; Logical Operations; Marriott International; Mastercard; Microsoft Corporation; NXP Semiconductors; Raytheon; RSA, the Security Division of EMC; Salesforce; SANS Security Awareness; Symantec Corporation; TeleSign; Visa and Wells Fargo. NCSA's core efforts include National Cyber Security Awareness Month (October); Data Privacy Day (Jan. 28); STOP. THINK. CONNECT.™, the global online safety awareness and education campaign co-founded by NCSA and the Anti-Phishing Working Group with federal government leadership from DHS; and CyberSecure My Business™, which offers webinars, web resources and workshops to help businesses be resistant to and resilient from cyberattacks. For more information on NCSA, please visit staysafeonline.org/about-us/overview/.

Rhia Dancel

Rhia is an ISO 27001 and 9001 Lead Auditor and PenTester for NSF and has previously held several auditing and technical positions in the information security and Pharma quality sectors. Rhia has completed technical writing work and audits for NSF throughout North America, working directly with customers on-site and remotely developing security control matrices. Rhia conducts risk-based security assessments using impact and probability calculations to develop and establish risk matrices to drive an organizations security plan-of-action and milestones. Rhia has developed and built a risk-based platform that supports industry best practices for treating and mitigating risk. Rhia has worked with multiple academic leaders on information security and awareness.

Stuart Daniels

Stuart Daniels, Security Manager, Department of Information and Digital Technologies, Government of Bermuda, and his team are responsible for developing and administering the Information Systems Risk Management program and sub-programs for the Government of Bermuda. Stuart has 20 years of experience in information technology, management and information systems security. Stuart serves on the Government Information Systems Risk Management Committe, and provides advice to department heads, the Civil Service Executive and the Cybersecurity Cabinet Committee on security matters. He also serves on the Cybersecurity Working Group, a public-private partnership that is developing Bermuda's National Cybersecurity Strategy.

John DiMaria

John DiMaria; CSSBB, HISP, MHISP, AMBCI, CERP, is the Global Product Champion for Information Security and Business Continuity for British Standards Institution and a Cloud Security Alliance (CSA) Research Fellow. He has 30 years of successful experience in Standards and Management System Development, including Information Systems, ISMS, Business Continuity and Quality Assurance. John was one of the key innovators of CSA STAR Certification for cloud providers, a contributing author of the American Bar Association's Cybersecurity Handbook, one of working group members and contributor to the NIST Cybersecurity Framework. He currently serves as the CSA OCF, Cloud Trust Protocol working group Co-Chair.

John has been a keynote speaker internationally, and featured in many publications concerning various topics regarding cybersecurity, quality and business continuity. He is a Business Continuity Institute award winner and BSI Innovation award winner.

Joseph Drissel

Before founding CyberESI, Joseph was the Acting Section Chief of the Intrusions Section at the Defense Computer Forensics Laboratory (DCFL), the world's largest accredited computer crime laboratory. In this capacity, Joseph and his team provided intrusion and malware analysis support to DoD entities, Federal Law Enforcement, the National Cyber Investigative Joint Task Force (NCIJTF) and the DoD-Defense Collaborative Information Sharing Environment (DCISE). As not only the Section Chief but a certified DoD Forensic Examiner, Joseph engaged on 1000+ intrusions cases.

Joseph was also employed as a technical trainer within the Defense Computer Investigations Academy. In this capacity, Joseph helped to design the incident response and network-based intrusions curriculum then deliver it to 1000+ federal law enforcement/Intel related personnel.

In November of 2010, Joseph founded Cyber Engineering Services. CyberESI provides patented incident response, intrusion/malware analysis, software and systems, training and cyber related

intelligence to its clients and the community at large. CyberESI personnel have backgrounds that include professionals from Federal Law Enforcement, the Intelligence Community and the Department of Defense. Employees have expertise in the fields of Network Security, Computer Forensics, Incident Response, Intrusions Analysis, and Reverse Engineering Malware, all have extensive knowledge specific to Advanced Persistent Threat related issues.

Joseph has served on the faculty of the Computer Science Department at the University of Maryland, Baltimore County. He regularly speaks on the topics of cyber security, intrusions, forensics analysis and the value of proactive data protection, including at the Department of Defense Cyber Crime Conference, to the U.S. Commerce Department, the National Institute of Standards and Technology (NIST), and a variety of commercial industry leaders.

Matthew J. Eggers

Matthew J. Eggers is vice president for cybersecurity policy in the Cyber, Intelligence, and Security Division at the U.S. Chamber of Commerce. He leads the Chamber's Cybersecurity Working Group, which focuses on developing and advocating for the Chamber's cyber policies before Congress, the administration, and the business community. Eggers frequently presents to organizations and is quoted regularly in the media on a broad range of issues connected to cyber legislation, regulation, and business strategy.

Daniel Eliot

Daniel Eliot is director of small business programs at the National Cyber Security Alliance (NCSA). NCSA is a leading neutral nonprofit public-private partnership devoted to strengthening America's cybersecurity through awareness and education. At NCSA, Daniel runs CyberSecure My BusinessTM, which is a comprehensive national program designed to help businesses of all sizes learn to be safer and more secure online. Daniel brings together the federal government, state and local governments, academia, and the private sector to discuss cutting-edge issues and create and implement high-quality, large-scale education and awareness efforts for the business community.

David Ferlemann

Dr. David Ferlemann, Cybersecurity Engineer, Naval Surface Warfare Center Dahlgren Division, United States Navy, and his team are responsible for design and operations of a DoD-wide Cyber Situational Awareness system and conduct research in technologies that support mission assurance and risk assessment. David has a Ph.D. in Computer Engineering from the University of Tulsa, and a MBA in Finance from Oklahoma City University. David has served in various engineering roles on projects such as Mission Planning systems for the U.S. Air Force, cybersecurity risk assessments and penetration testing for the renewable energy industry.

Mark Ferrari

Mark Ferrari is Executive Vice President of BluePrint Health Information Security, an Intraprise Health business. Prior to his role with Intraprise Health, Mark was Vice President and Chief Information Security Officer for BluePrint Healthcare IT. Mark's experience also includes the Siemens Health Services Corporation's Protected Information Management Council, management of compliance audit preparation, and information security accreditation initiatives for Siemens. Mark also held a project leadership role at a Main Line Health, a multi-hospital health system, where he led enterprise-wide clinical and financial systems implementations. Mark currently sits on the New Jersey Health Information Management Systems Society (NJHIMSS) Security and Privacy Task Force and the HITRUST Alliance Assessor Council. Prior to his involvement in healthcare IT, Mark served as an officer in the United States Air Force.

Mark holds a Bachelor of Science in Business Administration from Villanova University and a Master of Science in Emergency Management from the Millersville University of Pennsylvania. He is certified as a Project Management Professional (PMP), Certified Information Systems Security Professional (CISSP), HealthCare Information Security and Privacy Practitioner (HCISPP), and a HITRUST Certified CSF Practitioner (CCSFP). Mark is also a certified Emergency Medical Technician with over 20 years' experience in pre-hospital care within the City of Philadelphia and its surrounding region, and is an Adjunct Instructor in the Healthcare IT program at Rowan College in Burlington County, NJ.

Tony Giles

Tony is an ISO 27001, ISO 20000 and ISO 9001 Lead Auditor and PenTester for NSF. Currently, Tony is the Director of Custom Audit Programs, also having served as Director of Operations, Director of Business Development and Service Delivery Manager. Tony has conducted audits globally for over 10 years and worked on large-scale security implementation projects, including NIST 800-171, NIST 800-88, ISO 27001, ISO 28000, PenTesting Assessments and other custom security standards. Tony has conducted audits for DoD Suppliers and Private Sector organizations implementing security assessment programs focused on multiple security controls, cryptographic erasure and other custom security programs. Tony has worked throughout the US advancing and building information security awareness.

Steve Griffith

Steve Griffith is an Industry Director for NEMA's Transportation Systems Division. He manages sections within this division in such areas as Intelligent Transportation Systems (ITS), Electric Vehicle Supply Equipment, and Industrial Imaging & Communications. He is also the principle NEMA staff liaison for NEMA's Internet of Things (IoT) and Cybersecurity activities, leading and defining common approaches to standardization, guidelines, and architecture development while enabling connectivity, defining

and simplifying interoperability, and safeguarding privacy and cybersecurity in electrotechnical and medical imaging products.

Steve has over 18 years' experience in program/project management including a Project Management Professional (PMP) Certification. Before joining NEMA he managed projects for various Department of Defense facilities, and the Transportation Security Administration

Sarbari Gupta

Dr. Sarbari Gupta has been active in the information security industry for over twenty years. She has broad base of knowledge and experience in the areas of cybersecurity, privacy and cryptographic solutions. She holds a PhD degree in Electrical Engineering and CISSP and CISA certifications. Dr. Gupta has authored over twenty technical papers/presentations in refereed conferences/journals and several chapters in two cybersecurity books. She holds four patents in areas of cryptography. She has co-authored several NIST Special Publications in the areas of Electronic Authentication, Security Configuration Management, and Mobile Credentials. Dr. Gupta is the Founder and President of Electrosoft, a provider of technology-based services and solutions with a special focus on cybersecurity and serving Federal Government customers since 2001. See https://www.linkedin.com/in/sarbari-gupta-295b252/.

Donald Heckman

Mr. Donald Heckman is the Principal Director, Deputy Chief Information for Cybersecurity Department of Defense, Office of the Chief Information Officer. Mr. Heckman is responsible for ensuring the department has a well-defined and well-executed cybersecurity program. He is responsible for coordinating cybersecurity standards, policies and procedures with other federal agencies, coalition partners and industry.

Mr. Heckman began his career at NSA in 1983. He has served in a variety of technical and management positions over his career, including project engineer, program manager and manager up to Deputy Directorate level. He has also led several DoD-wide IA programs and initiatives. He is a key leader who has a deep technical knowledge of all aspects of the Information Assurance (IA) mission and has attained the Master level in the NSA Engineering and Physical Science Technical Track program and he is a Certified Information Systems Security Professional (CISSP) by the International Information Systems Security Certification Consortium (ISC)2. He has received numerous awards from the Defense, and Intelligence communities in recognition of his vision, leadership, and accomplishments including the Meritorious Presidential Rank Award in 2017. He was appointed to the Senior Executive Service in October 2005.

Prior to Mr. Heckman's current assignment he served as the Deputy Chief to the Cybersecuirty Solutions (CSS) Group. He led the organization in developing capabilities that span a large variety of technology areas, to include cloud & enterprise services, merged voice and data, mobile, high speed networks, cross domain and authentication to support a spectrum of national security

customer environments ranging from key management infrastructures, strategic and tactical high speed network communications, to military weapon systems and architectures. Additionally he was selected to be the Assistant Deputy Director of Trusted Engineering Solutions (TES) within the Information Assurance Directorate (IAD) and Chief of the IAD's Architecture Group. He has held key NSA leadership positions supporting Information Assurance, Systems Security Engineering and Key Management missions. Additionally, he served as the NSA/CSS Representative (NCR) to DISA/Deputy NCR STRATCOM for JTF-GNO. He also led the establishment of the DoD's Cryptographic Modernization and Global Information Grid Information Assurance Portfolio (GIAP) offices.

Mr. Heckman graduated from Johns Hopkins University with a Master of Science degree in Electrical Engineering and he received a Bachelor of Science degree in Electrical/Computer Engineering from Drexel University.

Mr. Heckman resides in Bel Air, MD. He enjoys reading, golfing and is active in the Boy Scouts of America. He and his wife Michelle are proud parents to their three children, Alysha, Emily and Zachary.

Lauren Holloway

Ms. Holloway's role includes coordinating PCI SSC's efforts for the Small Merchant Business Task Force, working with external organizations on various standards and payment initiatives, and working closely within PCI SSC to drive consistency and alignment across the standards and supporting programs. She joined PCI SSC in 2010 as the Director of Data Security Standards. Prior to joining the Council, Ms. Holloway led and coordinated Visa's efforts for PCI DSS and PA-DSS and related programs for several years. Ms. Holloway's extensive information security and audit background includes managing information security at an internet payment gateway, consulting with a Big 4 audit firm, and conducting and managing internal audits for computer systems at a Fortune 500 company. Ms. Holloway holds the CISSP, CISM, and CISA designations.

Eva Ignatuschtschenko

Eva Ignatuschtschenko is leading on behavior change policy in the Cyber Security Incentives and Regulation Team at the UK Government Department for Digital, Culture, Media and Sport. Her work focuses on how individuals and organizations can be incentivized to take action to improve their cybersecurity posture. She previously advised on cybersecurity and cyber harm at the University of Oxford's Global Cyber Security Capacity Centre, after working on cybercrime, emerging crimes and organized crime at the United Nations Office on Drugs and Crime (UNODC). In her roles in international organizations, academia and government, Eva has worked on a variety of issues, with a focus on the links between cyber risk, digital government, crime and emerging technologies.

Stefano Iannucci

Stefano Iannucci is an Assistant Professor of Computer Science and Engineering at Mississippi State University and an affiliated member of the Center for Cyber Innovation (CCI) at Mississippi State University. He received his Ph.D. in 2015 from the University of Rome "Tor Vergata", and his research focuses on cyber-security automation, autonomic computing, Internet of Things and performance modeling and benchmarking. He published over 20 papers on top journals and conferences. Dr. Iannucci serves as NSF panelist, has chaired several international workshops and has been the workshops chair for IEEE ICCAC, one of the leading conferences in autonomic computing.

Jack Jones

Jack Jones has worked in technology, information security, and risk management for over thirty years. He has ten years of experience as a CISO with three different companies, including five years at a Fortune 100 financial services company. His work there was recognized in 2006 when he received the ISSA Excellence in the Field of Security Practices award at that year's RSA conference. In 2012 Jack was honored with the CSO Compass award for leadership in risk management. Jack is an active member in ISACA, serving on the task force that created the RiskIT framework and leading the CRISC certification development. He is also an adjunct professor at Carnegie Mellon University, where he teaches risk measurement and management in the CRO and CISO programs. He is also the creator of the "Factor Analysis of Information Risk" (FAIR) framework adopted by the Open Group as an international standard. Currently, Jack is the EVP Research and Development of RiskLens, Inc., and Chairman of the FAIR Institute, a non-profit organization dedicated to evolving risk management practices. He has also co-authored a book on FAIR entitled "Measuring and Managing Information Risk, a FAIR Approach" which was inducted into the Cyber Security Canon in 2016.

Serge Jorgensen

Serge Jorgensen is founding partner and CTO of the Sylint Group. He provides strategic guidance and active oversight in the areas of computer security, incident response, counter cyber-warfare, eDiscovery, and security architecture. Before co-founding the Sylint Group, Mr. Jorgensen was Vice President of LoCast Corporation, where he directed the development and subsequent patent of HIPM-compliant patient location and status-tracking technologies. Mr. Jorgensen is a nationally recognized speaker on cyber security, actively participating in the Sedona Conference, American Bar Association, and RSA Conference. He has directed the development of several leading-edge security applications, provided response and remediation guidance to multi-billion dollar international espionage and cyber-security attacks, and directed, tasked and managed multi-million dollar litigation, forensic and electronic discovery efforts.

Mike Kijewski

Mike Kijewski (MMP'10/WG'12) is the CEO and co-founder of MedCrypt, a technology startup focused on helping medical device manufacturers secure their devices against malicious hacking. Mike was previously the founder of Gamma Basics, a software company focused on building web-based technologies for use in radiation oncology. Gamma Basics was acquired by Varian Medical Systems in 2013. Mike holds a bachelors in physics from the West Chester University of Pennsylvania, a Master of Medical Physics from the University of Pennsylvania, and an MBA from the Wharton School.

Alex Krutov

Alex Krutov specializes in advanced analytics for risk assessment and management. His primary focus is on the analysis of cybersecurity risk and its probabilistic quantification, assessment of financial consequences of potential and actual data breaches, cyber risk measurement and management at the enterprise level, and risk-based pricing of cyber insurance. He is recognized for expertise in using multi-disciplinary approaches in combining actuarial and statistical methods with qualitative approaches to assess risk in the face of limited information and significant uncertainty.

While focused on practical approaches and tools for quantitatively assessing cyber risk, he has also done research and published on the broader aspects of risk analysis. Over his career, Alex has served in executive roles such as President and Chief Executive Officer. He has spoken at and chaired industry events and conferences.

Troy Leach

Troy Leach is the Chief Technology Officer for the PCI Security Standards Council. In his role, Mr. Leach partners with Council representatives, Participating Organizations and industry leaders to develop comprehensive standards and strategies to secure payment card data and the supporting infrastructure.

He is a congressional subject matter expert on payment security and the current chairman of the Council's Standards Committee. Prior to joining the PCI Council, Mr. Leach has held various positions in IT management, software development, systems administration, network engineering, security assessment, forensic analytics and incident response for data compromise. Mr. Leach holds a Master of Science in Telecommunications & Network Management as well as a graduate degree in Information Security Management from Syracuse University.

Yeseul Lee

Yeseul Lee serves at responding the cyber incidents of private sector at KISA(Korea Internet & Security Agency, KrCERT/CC). Especially Yeseul concentrates on providing and studing the services that enable companies to operate the web safely such as inspecting Web Vulnerabilities, detecting malware/web attacks.

David Lenoe

David Lenoe is Director, Secure Software Engineering at Adobe. In his role, Lenoe manages the Adobe Secure Software Engineering Team (ASSET) responsible for ensuring Adobe's products are designed, engineered and validated using security best practices, as well as the Product Security Incident Response Team (PSIRT) dedicated to responding to and communicating about security issues. In addition, Lenoe manages the teams responsible for developing and maintaining the internal security training program, and reviewing the security posture of Adobe vendors. Lenoe is also responsible for Adobe's vulnerability information sharing via the Microsoft Active Protections Program (MAPP). Lenoe represents Adobe on SAFECode's Board of Directors and acts as SAFECode's Treasurer.

Lenoe joined Adobe as part of the Macromedia acquisition in 2004. At Macromedia, Lenoe held several management and engineering positions in the areas of product security, product management and quality assurance.

Lenoe earned a BA in Japanese language and literature from Connecticut College.

Thomas Llanso

Thomas Llansó conducts applied research in systems security engineering at the Johns Hopkins University Applied Physics Laboratory. His interests include security engineering automation and security risk analytics. He holds a B.S. in Computer Science from the College of William and Mary, an M.S. in Computer Science from Johns Hopkins University, and a D.Sc. in Information Systems from Dakota State University.

Josh Magri

Josh Magri currently serves as Senior Vice President, Counsel for Regulation and Developing Technologies for BITS at the Bank Policy Institute. Previously, he served as Vice President and Counsel for Regulation and Developing Technologies at the Financial Services Roundtable/BITS. In this role, Mr. Magri oversaw regulatory, advocacy, and policy efforts on issues related to cybersecurity, data security and privacy, financial technology ("FinTech"), and developing technologies.

Prior to joining FSR, Mr. Magri was the Associate Vice President at the Internet Security Alliance, a multi-sector cybersecurity trade association, where he co-authored the National Association of Corporate Directors' (NACD) "Cyber-Risk Oversight Handbook." He also helped develop cybersecurity policy that was largely incorporated into Presidential Executive Order 13636 – Improving Critical Infrastructure Cybersecurity.

Before moving to the Washington area, Mr. Magri was a prosecutor in the Bronx County District Attorney's Office. Tenured in both the Appeals and Rackets Bureaus, he handled felony and misdemeanor investigations, prosecutions, and appeals.

Mr. Magri graduated Boston College with a B.A. in Economics and earned a J.D. from Boston College Law School. Following law school, he clerked for the Honorable Fernande Duffly at the Massachusetts Appeals Court.

Mihoko Matsubara

Mihoko Matsubara is Chief Cybersecurity Strategist, NTT Corporation. She is responsible for public advocacy to strengthen or expand networks with global thought leaders in academia, government, and industry by sharing NTT's and Japan's cybersecurity efforts via publications and speakership.

Matsubara worked at the Japanese Ministry of Defense for nine years before receiving a Fulbright Scholarship to pursue an MA at the Johns Hopkins School of Advanced International Studies in Washington DC. Afterward, she accepted a fellowship at Pacific Forum CSIS (now Pacific Forum) in Honolulu to research Japan-US cybersecurity cooperation.

Matsubara then joined Hitachi Systems as cybersecurity analyst, and next took a position at Intel K.K., Tokyo, as Cybersecurity Policy Director. Her most recent experience includes Vice President and Public Sector Chief Security Officer (CSO) for Asia-Pacific at Palo Alto Networks in Singapore. Directly prior, Matsubara was CSO for Palo Alto Networks in Japan. During that time, she was on a cybersecurity strategy committee for the Japanese National Center of Incident Readiness and Strategy for Cybersecurity (NISC) to advise the Japanese government on how to enhance cybersecurity toward the 2020 Tokyo Summer Olympic and Paralympic Games.

She is a prolific writer and has spoken at various engagements internationally. She has a weekly cybersecurity column for the Mainichi Shimbun newspaper in the digital version. She has

contributed articles and papers to the Council on Foreign Relations, Lawfare, and Royal United Services Institute. She was the first Japanese speaker at the NATO International Conference on Cyber Conflict in Estonia (2015).

She is an Adjunct Fellow at Pacific Forum, Honolulu, and Associate Fellow at the Henry Jackson Society, London.

Robert Mayer

Robert Mayer is Senior Vice President of Cybersecurity with the USTelecom Association (USTelecom) with responsibility for leading cyber and national security policy, state relations and coordinating various regulatory initiatives for the wireline broadband industry. He is the current chairman of the Communications Sector Coordinating Council (CSCC) which represents the broadcast, cable, satellite, wireless and wireline industries in connection with the DHS public-private partnership. Mayer was recently appointed as co-chair of the Department of Homeland Security's ICT Supply Chain Task Force, which will develop near- and long-term strategic solutions to supply chain risk. In June 2015, He also serves as co-Chair of the recently announced Counsel to Secure the Digital Economy, (CSDE) which consists of 13 global ICT infrastructure providers who have joined forces to drive solutions that enhance the cyber resiliency of the digital ecosystem. Mayer was appointed to the FCC Communications Security Reliability and Interoperability Council (CSRIC V) after having led a 100 person team of cybersecurity professionals that produced a landmark report to adapt the NIST Cybersecurity Framework to the broadcast, cable, satellite, wireless and wireline industries.

Prior to USTelecom, Mayer served as the top telecommunications official for New York State as Telecom Director of the New York Public Service Commission. In that capacity, he led several major initiatives including regulatory reform efforts and he created a new agency department that focused exclusively on network reliability and public safety matters. Prior to this appointment, Mayer was the lead regulatory practitioner in the Telecommunications and Cable Group at KPMG Consulting and was a consultant with Deloitte Consulting. Before that Mayer worked as an analyst in the international telecommunications divisions of Chase Manhattan Bank and JP Morgan. Mayer served in the US Air Force supervising intelligence and communications operations at NATO Headquarters, Southern Europe in Italy. He received his B.A from Albany State University, his MA in Information Management from Central Michigan University, his MBA from Boston University, and his J.D from New York Law School.

James McLean

James McLean is the Chief Product and Solution Security Officer for Siemens Healthineers Diagnostics. Since 2014, he has been responsible for the security program for the medical devices and associated IT systems, solutions and services that Siemens Healthineers Laboratory Diagnostics develops, sells, maintains and supports.

James also sits on the Siemens Product and Solution Security Board responsible for governance and guidance for the security of the company's products, solutions and services in all sectors including industrial, power, energy, renewables and mobility, in addition to healthcare. He leads the board's work team responsible for supplier management in this area for Siemens employees worldwide. Prior to these roles, James has led medical device-related software development teams and process improvement teams in Laboratory Diagnostics since 2005. James has degrees in business administration (MBA) and electrical engineering (MS and BS). James is a Certified Secure Software Lifecycle Professional (CSSLP) and a Project Management Professional (PMP).

Efe Orhun

Derivative Technology, LLC – San Mateo, CA
Working in the field since 2000, CISSP since 2004, Efe is a founding partner of Derivative Technology and has done significant work in the areas of penetration testing, security architecture & solution design, forensic investigations, risk assessment, management & reporting, IP protection, ISO27K & SOX implementation, IS risk assessment for M&A targets, IS awareness training and disaster recovery planning. Managed global teams of software and hardware developers to develop information security-related software and devices.

Prior to Derivative Technology Efe worked at Palm Inc. and Applied Materials Inc. in Information Security and Intellectual Property Protection. In addition to client engagements, Efe instructed at the 2017, 2018 Cybershield training for the National Guard, where he covered GSM, ICS protocols & threat scenarios, incident planning/response, and GPS vulnerabilities.

Efe co-holds two patents in mobile computing in Australia, is a member of the SF-ECTF and is also ITIL certified.

John Petrie

John Petrie is the CEO of the Americas Region for NTT Security. He is responsible for Canada, United States, Central and South American business. Prior to appointment to CEO, he was the Global Chief Information Security Officer for NTT Security, responsible for the overall global information strategy and the management of the information security management system. He is an accomplished senior executive with more than 26 years of success in the manufacturing, financial services, defence, technology, security, telecommunications, education and healthcare industries. John is a valuable asset for companies seeking guidance on decisions leading to opportunities, minimizing security breaches and identifying the needs of the vertical market place. His areas of expertise include information security strategy, information security policy development, risk management, analysis and mitigation, security compliance and enterprise information security operations.

John holds an MBA in Information Systems from City University; a Bachelor of Science in Liberal Artsfrom the University of the State of New York, and is a graduate of the Defense Intelligence College in Washington D.C

Jorge Portugal

Since 2016, Jorge Portugal acts as general manager of COTEC Portugal, a leading business network for promoting technology and innovation collaborative networks. Jorge served for 10 years as advisor on innovation, entrepreneurship and competitiveness for the President of Portugal. Previously, he served as consultant for the Portuguese Government on innovation in public services. Jorge accumulated extensive corporate management experience in innovation projects in retail, banking and information technology sectors. He usually lectures in several universities and post graduation courses on management subjects as entrepreneurship, business strategy, international business, marketing and innovation. He acts in several advisory bodies for public and private organisations.

Jorge earned his graduation, MSc and PhD studies in mechanical engineering from Instituto Superior Técnico, University of Lisbon. He earned a MBA from NOVA School of Business and Economics and he attended an Advanced Leadership Program on Cybersecurity from US Department of State.

Bruce Potter

Bruce Potter is Expel's (expel.io) chief information security officer (CISO). He's responsible for cyber risk management and ensuring the secure operations of Expel's services. He also remains perpetually frustrated that employees pronounce CISO not-the-way-he-wants.

Previously, Bruce co-founded Ponte Technologies, a cybersecurity research and engineering company that worked with organizations ranging from

hedge funds to intelligence agencies. Bruce sold Ponte Technologies to the KeyW Corporation where he served as CTO for two years. In another life, Bruce founded the Shmoo Group and helps run the yearly hacker conference, ShmooCon (shmoocon.org), in Washington, DC. Bruce has co-authored several books and written numerous articles on security (or the lack thereof). He is a regular speaker at conferences including DefCon, Blackhat, and O'Reilly Security as well as private events at the United States Military Academy, the Library of Congress and other government agencies.

Mike Radigan

Mike Radigan has a 17 year career in the cyber risk management and network security industries. His subject matter expertise in expressing cyber risk in financial or "business terms" provides a unique and highly valued perspective to decision makers.

Mike joined Leidos Cyber, Inc. in December of 2017 and is responsible for the Operational Technology (OT) cyber security strategy and managing the OT partner relationships. Mike came to Leidos from ABB Power Generation where he held the role of Sr. Advisor of Cyber Risk Management providing customers guidance on managing the cyber and compliance risk posed to their operations.

Pranesh Rao

Pranesh joined Nidec in February 2017. In this position, Pranesh is responsible for driving forward the development of Nidec Motor Corporation's IoT platform and application specific solutions, including continued hardware and software development, solutions and technology roadmap definition, and project management.

Prior to joining Nidec, Pranesh co-founded a startup that focused on an IIoT platform for the energy industry. He also has extensive experience leading product development in several areas of power systems and controls including generation and distribution, renewable energy development and integration, grid battery storage and IoT, serving a global customer base.

Pranesh earned his Master of Science in Electrical Engineering degree from the University of Missouri-Rolla and his Bachelor's degree in Electrical Engineering from Bangalore University in India. Pranesh resides with his wife and daughters in the St. Louis area.

Tommy Ross

Tommy Ross serves as Senior Director, Policy with BSA | The Software Alliance. In this role, he works with BSA members to develop and advance global policy positions on a range of key issues, with a focus on cybersecurity, privacy, and market access barriers.

Prior to joining BSA, Ross served as the Deputy Assistant Secretary of Defense for Security Cooperation. He was the Senior Advisor for Intelligence and Defense to Senate Majority Leader Harry Reid, the Legislative Director for U.S. Representative David Price, and a research assistant for Senate Majority Leader Tom Daschle.

Ross is a graduate of Davidson College in North Carolina and Union Theological Seminary in New York. He is based in BSA's Washington, DC, office.

Karen Scarfone

Karen Scarfone is the principal consultant for Scarfone Cybersecurity in Clifton, Virginia. She develops cybersecurity guidelines and technical standards for Federal agencies and other organizations. Karen has over 25 years of professional experience in information technology, with nearly 20 years of that dedicated to security. Karen was formerly a senior computer scientist for the National Institute of Standards and Technology (NIST), where she oversaw the development of system and network security publications for federal civilian agencies and the public. She has coauthored more than 60 NIST Special Publications and Internal Reports, including the new draft NIST IR 8228, Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks. In recognition of her work for NIST, Karen received a Federal 100 award and a Department of Commerce Bronze Medal Award. She also received a Gold Medal Award for her contributions to security automation standards development. Karen holds a bachelor's degree in computer science from UW-Parkside, a master's degree in computer science from the University of Idaho, and a master's degree in technical writing from Utah State University.

Ari Schwartz

Ari Schwartz is Venable's Managing Director of Cybersecurity Services. He directs the firm's cybersecurity consulting services, assisting organizations with understanding and developing risk management strategies, including implementation of the Cybersecurity Framework and other planning tools to help minimize risk. Previously, Mr. Schwartz served at the White House National Security Council, as Special Assistant to the President and Senior Director for Cybersecurity where he led legislative and policy outreach to businesses, trade groups and others. Before his work at the White House, Schwartz led the Department of Commerce's Internet Policy Task Force, worked at the National Institute of Standards and Technology, and served for twelve years at the Center for Democracy and Technology.

Craig A Shorter

Craig A Shorter is a former CISO at Wells Fargo Card Services, Nationwide Insurance, First Tennessee Bank, and Erie Insurance, also Security and Compliance Program manager at Mellon Bank/Bank of New York and Fulton Bank. Programmer, Project manager, Cybersecurity and Compliance program implementer, formerly Cisco Certified Network Associate, over 15 years and currently ISACA Certified Information Security Manager (CISM) - and currently Security and Compliance Manager at NSPARC at Mississippi State University. Craig has a broad range of information security experiences and has built programs and managed security teams for over 20 years.

Leo Simonovich

Leo Simonovich is responsible for setting the strategic direction for Siemens' industrial cyber security business worldwide. He identifies emerging market trends, works with customers and Siemens businesses to provide best-in-class cyber offers, and contributes to the company's thought leadership on the topic. He is particularly focused on solving the cyber security challenge in the O&G and power sectors by bringing unique solutions to customers looking to address a growing and costly operational security risk. He frequently speaks on such topics as cyber governance, risk management, and organizational transformation in operational environments.

Previously, Leo led the cyber risk analytics practice area at the management consulting firm, Booz Allen Hamilton. He refined his expertise through his work with large government and commercial customers to improve their cyber risk posture. While at Booz Allen, Leo created an industry recognized methodology to evaluate the financial benefits of investment in cyber security. Leo holds both a Masters in Global Finance and an MBA from the University of Denver.

Dave Simprini

Dave Simprini is a Principal overseeing Grant Thornton's Public Sector Information Assurance and Cybersecurity Practice. He has extensive experience assessing IT controls governed by the National Institute of Standards and Technology (NIST), Federal Information Security Modernization Act (FISMA), and FedRAMP. He has led engagements with specific focus on cyber risk, IT assurance/audit support, service organization controls attestations (SSAE 18/AT-C 320), cyber analytics, vulnerability management, penetration testing, disaster recovery, NIST/FISMA controls assessments, and social engineering campaigns for clients from a broad spectrum of federal, state & local as well as commercial entities. Prior to his cybersecurity career, Dave served as a Surface Warfare Officer in the US Naval Nuclear Propulsion Program.

David Sliom

David Sliom has more than 20 years' experience working in the federal space in IT Security. As the Certification Agent for the 2010 Decennial Census, Mr. Sliom was one of the earliest adopters of the NIST Risk Management Framework. As Director of Cybersecurity for TELESIS, he is responsible for the management of all Civilian Federal Cybersecurity contracts, as well as managing the internal Cybersecurity Practice at TELESIS. Mr. Sliom is also currently managing the implementation program for the Cybersecurity Framework (CSF) at the Department of Housing and Urban Development. This program includes the establishment of extensive metrics to determine the Tier Level for the CSF integration through an executive dashboard.

Julie Snyder

Julie Snyder is a Lead Privacy & Security Engineer at MITRE, a private, not-for-profit corporation that operates federally funded research and development centers (FFRDCs). She supports multiple defense and civilian agencies with cybersecurity and privacy risk management. In her role with National Institute of Standards and Technology (NIST) in the National Cybersecurity Center of Excellence (NCCoE), she works with the U.S. Coast Guard and Department of Transportation to develop Cybersecurity Framework Profiles for subsectors of the oil & natural gas, passenger vessel, and connected vehicle industries. She also supports the Department of Defense (DoD CIO) with privacy and security matters and recently supported the Government of Japan Cabinet Secretariat's National Center of Incident Readiness and Strategy for Cybersecurity (NISC) with the cybersecurity strategic risk assessment program for the Tokyo 2020 Olympics.

Ms. Snyder is a co-author of NIST guidance on cyber threat information sharing (NIST SP 800-150), a Committee on National Security Standards (CNSS) instruction for protecting personally identifiable information (PII) in information systems (CNSSI No. 1253 Privacy Overlays), MITRE's Privacy Engineering Framework., and the Data Privacy and Data Security chapters of Modern Data Strategy. Prior to joining MITRE in 2009, she was a Manager at PwC where she supported various industries with improving their cybersecurity programs and later led the Federal Privacy Practice. Ms. Snyder earned her BBA in Information and Operations Management (MIS) from Texas A&M University and holds the CIPM, CIPP/G, CIPP/US, and CIPT certifications.

Gary Stoneburner

Gary Stoneburner is a member of the senior professional staff of the Johns Hopkins Applied Physics Laboratory (JHU/APL) where is supports APL and government sponsors as a system security engineer. His prior experience includes civil service at NIST where he was one of two US technical representatives to the international Common Criteria project, the lead for NIST's first publication on managing cyber-related risks, and a major contributor to many of the NIST cybersecurity publications. Previously he was with The Boeing Company where he served as lead hardware engineer for a very high assurance router (TCSEC, Orange Book Class A1) and as the company's security architect. He is an Army Signal Officer with 8 years of active duty and retired

from the reserves where his assignments included Deputy Chief IA Branch, J6, USSOUTHCOM; technical advisor to the INSCOM (US Army Intelligence and Security Command) accreditor; Deputy Team Chief Army Information Operations Red Team; and Watch Officer Army Global Network Operations and Security Center. In addition he is retired from the state defense force of Maryland with a commission from the governor as a Colonel and having served as the defense force CIO and Assistant Chief of Staff, Signal.

Russell Thomas

Mr. Thomas is a Senior Data Scientist at Zions Bancorporation and a PhD Candidate in Computational Social Science at George Mason University. Mr. Thomas as a Bachelor of Science in Electrical Engineering and Management (double major) from Worcester Polytechnic Institute. He has decades of Computer Industry experience, starting at Hewlett-Packard in R&D, manufacturing, marketing, and engineering productivity. For ten years, Mr. Thomas was a Senior Manager at KPMG Consulting, specializing on CRM, business process reengineering, enterprise architecture, and business transformation. Consulting clients include Pacific Bell, Apple/Claris, Microsoft, Cisco Systems, and Extreme Networks. Since 2007, Mr. Thomas has been involved in research on information security, primarily in metrics, risk, economics, and cyber security performance.

Blog: https://exploringpossibilityspace.blogspot.com

Ronald Tse

Ronald Tse is the founder and CEO of Ribose. Under his leadership, Ribose has been awarded the industry's highest cloud security ratings: the world's first organization to achieve certification to the NIST Cybersecurity Framework (Tier 4), Singapore's Multi-Tier Cloud Security (Level 3), the only organization to be triple-assured by CSA's STAR program, as well as the first in the cloud industry to receive BSI's Kitemark for Secure Digital Transactions.

He serves CalConnect as Vice President and Director of External Relationships, founding co-chair of CalConnect's TC VCARD, TC DATETIME and TC PUBLISH committees, CSA's SaaS Governance and DevSecOps groups, and Convener-Elect of ISO/TC 154/WG 5, where he helped shaped date and time standards such as ISO 8601-1 and ISO 8601-2. He is an expert contributor to ISO/TC 154, ISO/TC 211, ISO/TC 46, ISO/TC 37, and ISO/IEC JTC1/SC27; and received the Ron Knode award for his contributions to CSA.

Ronald is a member of Sigma Xi, a IAPP Fellow of Information Privacy, a CISSP-ISSAP, ISSMP, CSSLP, CAP, SSCP, CISA, CISM, CRISC, CGEIT, CIPP/US, CIPM, CIPT, PSM I-II-III, PSPO I-II, PSD and CCIE #9650.

Vincent Voci

Vincent Voci is senior policy manager in the Cyber, Intelligence, and Security Division at the U.S. Chamber of Commerce.

Voci also leads the Chamber's Project Security, which focuses on developing and advocating the Chamber's international cyber policies before foreign governments, the administration, and the business community.

He handles homeland and national security issues, with a particular focus on cybersecurity, on behalf of the Chamber's 200-plus National Security Task Force members.

Voci provides strategic guidance and support to the senior vice president of the department. He is actively engaged in developing and executing the department's policy agenda and advocates on behalf of the U.S. business community on a wide range of cybersecurity issues before the U.S. Congress and government officials.

Voci leads the Chamber's Cybersecurity Education and Awareness Campaign. Improving Today. Protecting Tomorrow.TM, which focuses on advancing cybersecurity policies and legislation while educating businesses of all sizes about cyber threats and how to protect against them.

Previously, Voci worked for former Sens. Scott Brown (MA) and George Allen (VA) and at the departments of Transportation and Homeland Security.

Voci is a graduate of American University in Washington, D.C. with a B.A. in political science. A native of Cape Cod, Massachusetts, he currently resides in Alexandria, Virginia.

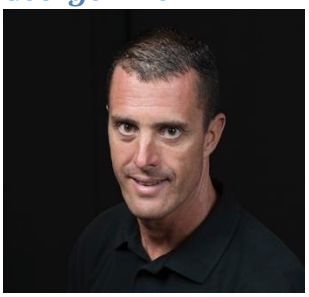
Steffani Webb

Steffani has worked in academic medicine throughout her career, first at Duke University Medical Center for 22 years, and at the University of Kansas Medical Center for the past 14 years. With a passion for excellence, she took on the role of Vice Chancellor for Administration at KUMC seven years ago, providing leadership, planning and support to KUMC's infrastructure and administrative functions, including information resources, information security, compliance, enterprise analytics, human resources, facilities management, public safety, and organizational improvement. In this role, Steffani has been leading an organization-wide performance improvement initiative and cultural transformation using the principles of the Baldrige Performance Excellence Framework and most recently has engaged members of her team in using the Baldrige Cybersecurity Excellence Builder as a framework for self-assessment and program development.

Greg White

Dr. Gregory White has been involved in computer and network security since 1986. He spent 30 years with the Air Force and Air Force Reserves. He obtained his Ph.D. in Computer Science from Texas A&M University in 1995 conducting research in the area of Computer Network Intrusion Detection and he continues to conduct research in this area today. He currently serves as the Director of the Center for Infrastructure Assurance and Security (CIAS) and is a Professor of Computer Science at The University of Texas at San Antonio (UTSA). In addition, Dr White also serves as the Executive Director of the Information Sharing and Analysis Organization (ISAO) Standards Organization (SO) and is the Chairman of the National Cybersecurity Preparedness Consortium (NCPC).

George Wrenn

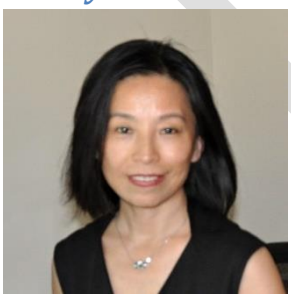


George Wrenn is a Research Affiliate in Management Science at the MIT Sloan School of Management. He is the founder & CEO of CyberSaint Security, formerly the vice president of Cybersecurity for Schneider Electric. He has more than 20 years of experience in the field of cyber security. Prior to the present role, George was as a senior managing consultant with IBM helping cross-industry Fortune 1000 customers reach compliance to NIST, FISMA, ISO/IEC, HIPAA, PCI, NERC/CIP, and other key regulatory frameworks, developing cyber security strategy, roadmaps, and global cyber security programs. He is expert in cloud security and has been awarded US patents in this area.

Brett Young

Brett Young is a consultant at Leidos Cyber, specializing in security architecture assessments, design and transformation projects for process control environments including oil & gas, electric, and manufacturing environments.

Shirley Zhao



Shirley Zhao has practiced in a broad spectrum of IT domains, including software engineering, system integration, infrastructure architecture and cybersecurity program development. In the most recent years, she has consulted at various government agencies and commercial organizations, providing enterprise wide cloud computing and cyber security advisory service. Her clients included DoD, USDA, HHS, etc. She develops strategies, policies, processes, and roadmaps that have organization-wide impact as well as works directly with technical and functional stakeholders to carry out mission critical initiatives. Through governance models and frameworks, Shirley advocates for holistic, business driven and collaborative approach in addressing enterprise IT and cyber security challenges.