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
   • Federating Cybersecurity Framework Informative References
   • Secure Software: Toward A Proposed Benchmark
   • Implementing the Cybersecurity Framework
   • Cybervets: Leveraging Veterans to Build the Cybersecurity Workforce
2:00pm Break
2:30pm Afternoon Sessions II
   • Evaluating “Reasonable” Cyber Risk Using the Center for Internet Security Risk Assessment Method
   • A Practical Approach to IT Security for Small and Medium-Sized Businesses Based on the NIST Cybersecurity Framework
   • Using NIST Guidance to Implement and Information Systems Risk Management Program for a Small National Government
   • Risk Management for Automotive Cybersecurity

This draft agenda is subject to change and will be updated as schedules and session titles are confirmed.
• Cybersecurity Risk Management: Finding and Fixing Your Security Vulnerabilities
• A Tale of Two Frameworks: Optimizing Federal Agency Use of the Risk Management Framework and Cybersecurity Framework through Framework Profiles
• Proactive Cybersecurity Through Cross-Domain Intelligence
• Reducing the Burden of Cybersecurity
• Framework for Improving Critical Infrastructure Cybersecurity: A Practical Implementation
• Implementing the Cybersecurity Framework
• NIST Cybersecurity Framework and PCI Data Security Standard
• Adding Rigor and Depth to Risk Management Framework Step 2 (Select Security Controls)
• Deriving Business Insight from Cybersecurity Framework Findings
• Using a Controls Framework to Address NIST, HIPAA, and GDPR Security Provisions -- to Ensure Management of Cyber Threats
• Is Our Critical Infrastructure Cyber Resistant?
• The ISF Standard of Good Practice and the NIST Cybersecurity Framework
• Understanding and Managing Cyber Risk with a Dwell Time-Based Approach

4:45pm Adjourn

Thursday, November 8, 2018

7:30am Registrant Check-In
8:30am Plenary Panels
• U.S. National Critical Infrastructure Risk Management
• National Cybersecurity Risk Management Approaches
10:15am Break
10:45am Morning Sessions III
• Botnets and the Cybersecurity Framework
• Integrated Cyber Playbooks for Identity Threat Prevention within the NIST Risk Management Framework
• Measuring the Cybersecurity Risk of Software-Intensive Systems
• Best Practices Learned from Mitigating Risks of Data Breaches to Build a Data Privacy Program
• Supply Chain Initiatives: Global Strategy to Enterprise Risk Management
• Electrical Manufacturers’ Role in Cyber Supply Chain Risk Management

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

This draft agenda is subject to change and will be updated as schedules and session titles are confirmed.
1:15pm  Afternoon Sessions IV
• Friends Don't Let Friends Tackle Cybersecurity Alone: Taking a Team Approach to Strengthening Cyber Resilience in the Marketplace
• Integrating Privacy into the Risk Management Framework
• US Federal Government Sector Guidance
• Implementing Secure Systems using the PMBOK and NIST Cybersecurity Framework and Baldridge Excellence Tool
• Draft Botnet Cybersecurity Framework Profile
• Towards Autonomic Security Management
• How Tradeoffs Increase Cyber Supply Chain Risk
• Supply Chain Attacks and Resiliency Mitigations – Guidance for System Security Engineers

2:15pm  Break
2:45pm  Afternoon Sessions V
• Actuarial Approach to Cybersecurity Risk Measurement
• 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
• Data-Driven Risk-based Decision Making
• Simple, Consistent, Secure - Cybersecurity and Privacy in Small and Medium-Sized Organizations
• NIST Cybersecurity Guidance as Systems Engineering construct and not DIACAP by another name
• Enterprise Risk Mitigation Using the NIST CSF and Cyber Analytics
• Measuring an Organization’s Security Maturity using the NIST Cybersecurity Framework
• How Japanese industry uses the NIST Cybersecurity Framework to overcome manpower shortage
• Automated Cyber Hardening
• Risk Data Sharing for Situational Awareness
• Risk is Money
• A Structured Approach for Privacy Risk Assessments for Federal Organizations
• Role-Based Risk Management Framework - Risk Management Framework and National Initiative for Cybersecurity Education Framework Convergence
• Financial Services Sector Cybersecurity Profile: A NIST-based approach to harmonize cybersecurity risk management and compliance
• Using the NIST Framework to design and implement risk-based cybersecurity management in global conglomerate
• How Tradeoffs Increase Cyber Supply Chain Risk
• International Next Steps
• Empirical Measurement of Perceived Privacy Risk

5:00pm  Adjourn

This draft agenda is subject to change and will be updated as schedules and session titles are confirmed.


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
• Tips & Tricks for Small Business Cybersecurity Framework Implementation
• Data-Driven Breach Response Planning
• Why Don’t We Comply with Our Own Regulations?
• Enabling Executive Level Decisions
• The Digital Fast Lane – Helping Non-Profits Keep Up
• Cyber Defense for SMBs
• State Supporting in Cybersecurity for SMB Organizations - Best Practices in Korea
• Practical Application of Risk Management and Associated Risk Culture
• Threats & the Framework
• SMB Resources
• Framework Implementation
• Cyber Strategy Optimization for Risk Management
• Demystifying ICS Cyber Risk
• Enterprise Architecture and the NIST Cybersecurity Framework: Two Complementary Scopes of Interest

12:30pm  Lunch – to include Lunch-and-Learn sessions
1:45pm  Afternoon Sessions VII
• Manufacturing Extension Partnership and Manufacturing Cybersecurity
• Small Business Cybersecurity and Privacy
• Governance and Enterprise Risk Management

2:45pm  Adjourn