Information and Communications Technology Supply Chain Risk Management Task Force

Innovations in ICT Supply Chain Risk Management Conference

Wednesday, June 12, 2024
9:00 a.m. – 5:15 p.m. ET

9:00 a.m. – 9:05 a.m. Opening Remarks

Mona Harrington, Assistant Director, National Risk Management Center, Cybersecurity and Infrastructure Security Agency

9:05 a.m. – 9:10 a.m. Welcome

Jason Providakes, Ph.D., President and Chief Executive Officer, MITRE

9:10 a.m. – 9:40 a.m. Morning Keynote

Jen Easterly, Director, Cybersecurity and Infrastructure Security Agency

9:40 a.m. – 10:10 a.m. Fireside Chat: Impact of Cyber Incidents on Supply Chains - The Monetary Losses are Real

Discussion of Paper: Pirates without Borders: The Propagation of Cyberattacks through Firms' Supply Chains *by Matteo Crosignani, Marco Macchiavelli, and Andre Silva*

Paper Description: The paper, Pirates without Borders: The Propagation of Cyberattacks through Firms' Supply Chains, documents the supply chain effects of the most damaging cyberattack in history. The disruptions propagated from the directly hit firms to their customers, causing a four-fold amplification of the initial drop in profits. These losses were larger for affected customers with fewer alternative suppliers. Internal liquidity buffers and increased borrowing, mainly through bank credit lines, helped firms navigate the shock. The cyberattack also led to persisting adjustments to the supply chain network, with affected customers more likely to create new relationships with alternative suppliers and terminate those with the directly hit firms.

Moderator: ***Robert Mayer***, Senior Vice President, Cybersecurity and Innovation, USTelecom

Speaker: ***Matteo Crosignani***, Financial Research Advisor, Federal Reserve Bank of New York

10:10 a.m. – 11:05 a.m. Panel 1: Supply Chain Transparency - How HBOM, SBOM, and Illumination Tools Increase SCRM Resilience

Supply chain transparency is a key element of any supply chain resilience strategy. SBOMs and HBOMs, which create a comprehensive itemization of the components in both the hardware and software that make up a product, are among some of the tools that can play a pivotal role in product development and supply chain risk management. They serve to help manufacturers and suppliers identify the source of quality issues or defects in their products and enable organizations to track and manage vulnerabilities and dependencies. Illumination tools, such as visualization platforms, and data analytics also play an important role in transparency, allowing organizations to analyze, track, and monitor their suppliers and logistics throughout their multi-tiered supply chain. Panelists will discuss how these tools can provide necessary transparency and where work still needs to be done to enhance their usability and accuracy.

Moderator: ***Kanitra Tyler***, Supply Chain Risk Management Service Element Lead, National Aeronautics and Space Administration

Panelists:

Allan Friedman, Ph.D., Senior Advisor and Strategist, Cybersecurity and Infrastructure Security Agency

Chris Oatway, Managing Associate General Counsel, Verizon

Rebecca McWhite, Cyber Supply Chain Risk Management Technical Lead, National Institute of Standards and Technology

Andrea Little Limbago, PhD, Senior Vice President, Research & Computational Risk Modeling, Interos

11:05 a.m. – 12:00 p.m. Panel 2: The Role of Technology in SCRM - Are Quantum, Artificial Intelligence (AI), and Blockchain Changing the Game?

Technologies such as quantum computing, AI, and blockchain hold tremendous potential to transform supply chain management, offering the possibility for a new era of efficiency and responsiveness. With its powerful processing capabilities, quantum computing can tackle highly complex and variable optimization and simulation models with incredible accuracy. The ability to harmonize countless data sets, simplify the variability of plans and suppliers, and optimize transportation and logistics presents an opportunity to revolutionize supply chain modeling. AI can provide organizations with intelligence insights and decision-making capabilities, while also using machine learning to predict patterns related to demand and inventory levels, enhance predictive maintenance schedules, and improve communication throughout the supply chain. Blockchain, with its distributed ledger, can increase supply chain resilience by providing product traceability and can deliver increased efficiency and speed while reducing disruptions and counterfeiting. The panel will discuss how these technologies can create this optimized end-to-end visibility now and in the future.

Moderator: ***Vaibhav Garg (VG)***, Executive Director, Cybersecurity and Privacy Engineering Research & Public Policy, Comcast Cable

Panelists:

Brett Attaway, Senior Director, Strategic Microelectronics, Siemens

Jason Boswell, Vice President & Head of End-to-End Security, Ericsson North America

Tommy Gardner, Chief Technology Officer, HP Federal

Shon Lyublanovits, Cyber Supply Chain Risk Management Lead, Cybersecurity and Infrastructure Security Agency

12:00 p.m. – 12:45 p.m. Lunch

12:45 p.m. – 1:45 p.m. Afternoon Keynote: Leadership Insights - The Importance of Creating Enduring Security and Collaborative Partnerships

In an age marked by unprecedented connectivity and digital innovation, the cybersecurity landscape has become increasingly complex and the adverse consequences, more pronounced. Hear from Tom Fanning, Retired Chairman, President, and CEO of Southern Company, as he provides unique, real-world insights gained from running a large critical infrastructure company and the risks he contended with to protect and secure both the company's physical and cyber assets while ensuring ongoing supply chain resilience. Additionally, given his experience as the former Chair of CISA's Cybersecurity Advisory Committee, Mr. Fanning will speak to the importance of public-private partnerships, like CISA's ICT SCRM Task Force and the Joint Cyber Defense Collaborative, and how government and industry can best work together on a variety of requirements such as the National Security Memorandum on Critical Infrastructure and Resilience.

Speaker: ***Tom Fanning***, Retired Chairman, President, and Chief Executive Officer, Southern Company

1:45 p.m. – 2:30 p.m. Panel 3: Small and Medium-Sized Businesses - Understanding their Unique SCRM Challenges

SMB information technology and communications providers represent more than 160,000 companies in the United States; connect millions of households and businesses to the internet every day; and acquire, build, and integrate technology solutions for themselves and their customers. Implementing supply chain security practices is therefore critical for these ICT entities. For many, knowing where to start—and how an SMB can take on the financial, personnel, or other resources necessary to implement certain ICT supply chain practices—can seem overwhelming. The panel will discuss how to practically identify ICT-related supply chain risks, how those risks might be different than in larger companies, and how to best mitigate risks.

Moderator: ***Jeffery Goldthorp***, Associate Bureau Chief, Federal Communications Commission

Panelists:

Jerry Horton, Director of Technology and Cybersecurity, Blue Valley Technologies, Inc.

Ola Sage, Chief Executive Officer, CyberRx

Mike Regan, Vice President of Business Performance, Telecommunications Industry Association

2:30 p.m. – 3:15 p.m. Panel 4: Increasing the Trustworthiness of AI/LLM - Treating Data as a Supply Chain Asset

Ensuring only empirical data, thoroughly vetted for accuracy and integrity is mined and analyzed by Artificial Intelligence (AI) and large language models (LLMs) is critical to upholding the reliability and trustworthiness of outputs, especially for supply chain and security risk prediction capabilities. Panelists will discuss the areas in which guiding principles will need to be developed to ensure the accuracy and transparency of data used by these technologies, the techniques and validation methods that can be adopted to increase the fidelity of AI/LLM analysis output, and the essential "accuracy guardrails" that need to be embedded in the AI/LLM algorithms to ensure trustworthiness.

Moderator: ***John Miller***, Senior Vice President of Trust, Data, and Technology and General Counsel, Information Technology Industry Council

Panelists:

Cheri Caddy, Senior Advisor, Cybersecurity Policy and Strategy, U.S. Department of Energy

Edna Conway, Chief Executive Officer, EMC Advisors, LLC (Former Chief Security and Risk Officer, Microsoft Cloud Infrastructure; Chief Security Officer, Cisco Global Value Chain)

Joyce Corell, Senior Technology Advisor, Office of the Director of National Intelligence

3:15 p.m. – 3:45 p.m. Presentation

Eric Goldstein, Executive Assistant Director, Cybersecurity Division, Cybersecurity and Infrastructure Security Agency

3:45 p.m. – 4:30 p.m. Panel 5: Critical Components of the Data Landscape - Cybersecurity in SCRM

The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten public and private sector supply chains as well as America's economic and national security. Vulnerabilities that have previously been used to exploit public and private organizations are a frequent attack vector for malicious cyber actors of all types and pose significant risk. Panelists will discuss how tools such as the ICT SCRM Task Force's *Software Acquisition Guide for Government Enterprise Consumers: Software Assurance in the SCRM Lifecycle*, as well as CISA initiatives such as Secure by Design and Open Source Software Security, can assist organizations to anticipate and remediate known vulnerabilities. These tools help to ensure the security of information technology assets that are such a critical component of supply chains across federal and private sector enterprises.

Moderator: ***Emily Frye***, Director, Cyber Integration, MITRE

Panelists:

Dick Brooks, Co-Founder and Lead Software Engineer, Reliable Energy Analytics LLC

Joe Jarzombek, Software Assurance Subject Matter Expert (Retired), Department of Homeland Security and Synopsys

Jack Cable, Senior Technical Advisor, Cybersecurity and Infrastructure Security Agency

Tim Mackey, Head of Software Supply Chain Risk Strategy, Synopsys

4:30 p.m. – 5:10 p.m. Panel 6: Achieving ICT Supply Chain Nirvana - A Field Guide

Over the past few years, ICT organizations around the world have weathered the perfect storm of challenges and uncertainties in the field of supply chain risk management. The COVID-19 pandemic disrupted the traditional just-in-time inventory model and exposed deep vulnerabilities in the global value chain. As a result, many businesses are focusing on building resilience and agility by reevaluating their sourcing strategies, diversifying suppliers, ordering more inventory, and considering nearshoring or reshoring to reduce dependency on distant and often, single, sources. Hear from supply chain practitioners about the shifts they have undertaken and the trends they see as they navigate today's complex supply chain environment.

Moderator: ***Kathryn Condello***, Senior Director, National Security/Emergency Preparedness, Lumen Technologies, Vice-Chair, Communications Sector Coordinating Council

	Panelists: ***Steve Baum***, Associate Director, Verizon Global Supply Chain ***Jon Amis***, Supply Chain Solutions Principal, LMI ***Ryan Elliott***, Partner and Co-Founder, PRISM, A.T. Kearney
5:10 – 5:15 p.m.	Closing Remarks
	Mona Harrington, Assistant Director, National Risk Management Center, Cybersecurity and Infrastructure Security Agency