Morgan Lewis

TECHNOLOGY MAY-RATHON

Best Practices in Supply Chain Cybersecurity

Morgan Lewis Technology May-rathon

Thank you for joining Morgan Lewis as we present our 9th annual Technology May-rathon.

This year we are offering over 30 in-person and virtual events related to the 21st Century Workplace; Artificial Intelligence and Automation; Fintech, Global Commerce; Medtech, Digital Health, and Life Sciences; Privacy, Cybersecurity, and Big Data; and Regulating Tech.

A full listing and any recordings of our tech May-rathon events can be found via the link on our front page at www.morganlewis.com

Please be sure to Tweet **#TechMayRathon**

Agenda

1. Understanding recent developments in supply chain risks and the resulting risks to national security
2. Managing US and global regulatory requirements
3. Internal cybersecurity practices that mitigate supply chain risk
4. Conducting effective due diligence throughout the supply chain
5. Supply chain security – common gaps in vendor contracts
6. Supply chain security – best practices and market positions

SECTION 01

UNDERSTANDING RECENT DEVELOPMENTS IN SUPPLY CHAIN RISKS AND THE RESULTING RISKS TO NATIONAL SECURITY

Supply Chain Cybersecurity
Why Does it Matter?

- "The U.S. is under systemic assault by foreign intelligence entities (FIEs) who target the equipment, systems, and information used every day by government, business, and individual citizens."
  Supply Chain Risk Management Background Paper (National Counterintelligence and Security Center, Supply Chain Directorate) (2018)

- "A major factor enabling supply chain threats has been the globalization of our supply chains, characterized by a complex web of contracts and subcontracts for component parts, services and manufacturing extending across the country and around the world. The multiple layers and networks of suppliers in this chain are frequently not well understood by either manufacturers or consumers. Our most capable adversaries can access this supply chain at multiple points, establishing advanced, persistent, and multifaceted subversions."
  Supply Chain Risk Management Background Paper (National Counterintelligence and Security Center, Supply Chain Directorate) (2018)

- A supply chain is only as strong as its weakest link. The cyber threat from foreign adversaries, hackers, and criminals presents significant and new risks to government and industry. Constant, targeted, and well-funded attacks by malicious actors threaten government and industry alike by way of their contractors, sub-contractors, and suppliers at all tiers of the supply chain. Sophisticated threat actors exploit vulnerabilities deep in supply chains as a beachhead from which they can gain access to sensitive and proprietary information further along the chain. Supply Chain Risk Management, Cybersecurity and Infrastructure Security Agency, DHS (2019)

- "[F]oreign adversaries are increasingly creating and exploiting vulnerabilities in information and communications technology and services, which store and communicate vast amounts of sensitive information, facilitate the digital economy, and support critical infrastructure and vital emergency services, in order to commit malicious cyber-enabled actions, including economic and industrial espionage against the United States and its people."
  Executive Order on Securing the Information and Communications Technology and Services Supply Chain, May 15, 2019

Supply Chain Cybersecurity
Why Does it Matter?

- "America's manufacturing and defense industrial base consists of the end-to-end set of capabilities, both private and public, that design, produce, and maintain platforms and systems (hardware and software)…. With ***an extensive, multi-tiered global supply chain***, the industrial base encompasses the extraction and refinement of primary materials, the manufacturing of components and parts, and the ***integration and sustainment*** of …. platforms and systems. It relies on a ***geographically and economically diverse network*** of private sector companies, R&D organizations, academic institutions, and government-owned facilities to develop ad produce …technologies…." (Emphasis added)

  (Report to President Donald J. Trump by the Interagency Task Force in Fulfillment of Executive Order 13806: *Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States* (September 2018)

- "Federal agencies *and other entities* need to take urgent actions to implement a comprehensive cybersecurity strategy, perform effective oversight, secure federal systems, and protect cyber critical infrastructure, privacy, and sensitive data." GAO-19-157SP. *High Risk Series: Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas ("Ensuring the Cybersecurity of the Nation")* (March 2019), at p. 178.

- The Government Accountability Office first designated cybersecurity as a risk in 1997

  - Identified the protection of critical infrastructure assets in 2003
  - Identified the protection of personal identifier information in 2015

- These issues affect a range of parties and benefit from a coordinated approach (Report to President Donald J. Trump by the Interagency Task Force in Fulfillment of Executive Order 13806: *Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States* (September 2018), p. 9

Cybersecurity and Supply Chain
Why Does it Matter?

- EO 13806 outlined areas of concern such as:
  - The erosion of the US industrial base
  - The threat (both long and short term) to the US lead in existing and emerging technologies
  - The persistent press by multiple adversaries of cyber intrusions; and
  - The critical loss of intellectual property
- These concerns inform how we define the cybersecurity threats to the supply chain
- The US has developed an overarching approach to cybersecurity and supply chain requirements through laws, regulations, policies and directives, designed to identify the threats, determine the vulnerabilities, assess the consequences, and ultimately, manage risk

Defining Cybersecurity and Supply Chain

- Cybersecurity and supply chain – as concepts – are generally understood to include:
  - Cybersecurity: "Definition: The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation.

    Extended Definition: Strategy, policy, and standards regarding the security of and operations in cyberspace, and encompass[ing] the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure."

    CNSSI 4009, NIST SP 800-53 Rev 4, NIPP, DHS National Preparedness Goal; White House Cyberspace Policy Review, May 2009
  - Supply chain: "Definition: A system of organizations, people, activities, information and resources, for creating and moving products including product components and/or services from suppliers through to their customers.

    Related Term(s): supply chain risk management. CNSSI 4009, NIST SP 800-53 Rev 4"
  - Supply Chain Risk Management: "Definition: The process of identifying, analyzing, and assessing supply chain risk and accepting, avoiding, transferring or controlling it to an acceptable level considering associated costs and benefits of any actions taken.

    DHS Risk Lexicon, CNSSD 505"

Defining Cybersecurity and Supply Chain

- Unique aspects of cybersecurity and supply chain:
  - The interrelationship (or symbiotic relationship) between governments and organizations
  - The difficulty in identifying and/or remediating issues
- Threats include, but are not limited to:
  - External actors
  - Internal actors
  - Compromised systems
  - Compromised services
  - Unidentified risks (lack of knowledge of the threat)
- Vulnerabilities include, but are not limited to:
  - Weak security protocols
  - Poorly trained work force
  - Lack of 'cyber hygiene'
  - Unenforced company policies
  - Improperly implemented regulatory requirements – *i.e.*, failure to obtain export authorizations for transfers
- Consequences include, but are not limited to:
  - Loss of data (destruction)
  - Data corruption (segments of data are unreliable)
  - Data manipulation (reorienting or restructuring data, such as reconfiguring a bill of material)
  - Data exfiltration (theft)
  - System disruption (denial of service or denial of access)
  - System compromise or manipulation (known or unknown)

SECTION 02

MANAGING US AND GLOBAL REGULATORY REQUIREMENTS

Cybersecurity and Supply Chain Legal, Regulatory and Policy Requirements

- Defining the threats, vulnerabilities, and consequences allow for development of a risk mitigation strategy that allows for the buy-in needed by organizations to ensure that effective protections are developed
- Laws, regulations, policies and directives that affect the development of a mitigation strategy for addressing cybersecurity and supply chain risks include, but are not limited to:
  - Federal Information System Management Act of 2014 (FISMA), 44 USC 3551, et seq. (PL 113-283)
  - National Defense Authorization Act of FY 2011, Supply Chain, 10 USC 2339a
  - National Defense Authorization Act of FY 2019, PL 115-91 (§ 881 updates supply chain requirements)
  - National Defense Authorization Act of FY 2019, PL 115-91 (include §§ 845, 871, 885, 1613, 1639, 1645, 1648, 1650, and 1654)
  - Export Control Reform Act of 2018, PL 115-91 (incorporated into the NDAA of FY 2019)
  - US Homeland Security, Defense and General Acquisition Regulations and Directives
    - "Requirements related to Supply Chain Risk," 80 FR 67244-67252 (October 30, 2015), updated 84 FR 4368-4370 (February 15, 2019); DFARS 252.239-7018 and DFARS 252.239-7017
    - "Restrictions on Acquisition from Foreign Sources," 83 FR 65560-65562 (December 21, 2018)
    - PDD 21: Critical Infrastructure Security and Resilience Directive (identifies 16 key sectors)
    - PDD 21: Critical Infrastructure Security and Resilience Program (C-SCRM) (DHS and NIST)
    - DHS Binding Operational Directives (e.g., 'do not buy' lists or 'remove from systems' lists)
    - Entity List or Denied Party designations by the Departments of Commerce and State
- Resources (Government and Private) include:
  - National Institute of Standards and Technology/Supply Chain Risk Management SCRM Program
  - National Counterintelligence and Security Center Foreign Economic Espionage in Cyberspace (2018)
  - North American Transmission Forum: Cyber Security Supply Chain Risk Management Guidance (2018)
  - Software Supply Chain Attacks Summary (DHS-CERT)
  - Summaries on Supply Chain and Cyber Risks by FireEye, RSA, Mandiant, and The MITRE Corporation

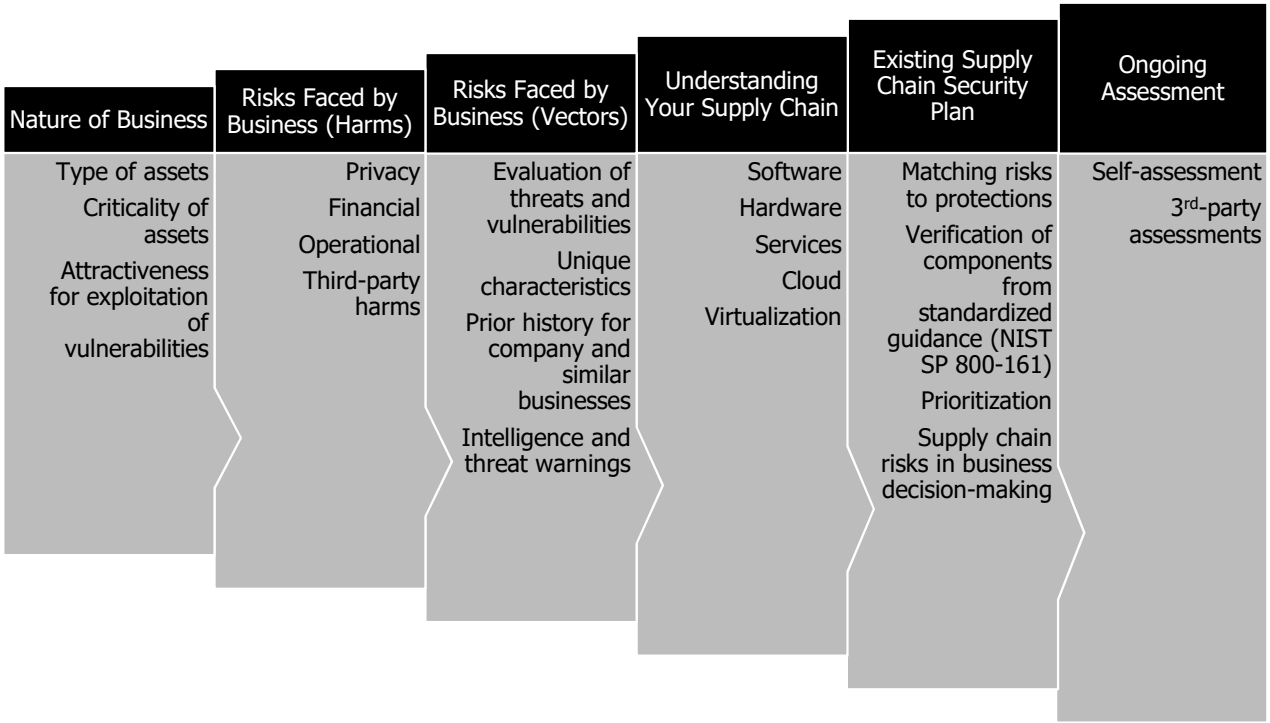
What's Next?

- Congress continues to develop legislative solutions
  - S. 29: Office of Critical Technologies and Security
  - S. 937: Protecting American Technology Act
  - S. 1459: China Technology Transfer Control Act of 2019
- The Executive Branch continues to issue Executive Orders and policy statements concerning the need to address the cyber related security gaps in IT and infrastructure systems as well as in the supply chain – *e.g.*, Addition to the Department of Commerce, Bureau of Industry and Security Entities List of parties that the Government has identified as national security risks (May 16, 2019)

SECTION 03

INTERNAL CYBERSECURITY PRACTICES THAT MITIGATE SUPPLY CHAIN RISK

Understand Your Supply Chain Risks



Control What Is In Your Hands

- Significant portions of supply chain security concerns are best addressed in coordination with vendors and their suppliers, but even in the absence of that coordination, significant steps can be taken to reduce supply chain cybersecurity risk.

1. Track public alerts and databases of incidents related to vendors and vulnerabilities related to vendor-provided products and services
2. Develop an incident response plan for supply chain cyber incidents
3. Track and grant vendor access to networks, physical locations, and sensitive information repositories based on need
    1. Review need decisions regularly and revoke quickly
    2. Limit access to narrow group of non-company personnel
4. Verify software integrity and authenticity
5. Establish strict controls for remote access and system-to-system communications by vendor
6. Coordinate with your ISAC or other governmental points of contact to remain information on known risks
7. Take advantage of governmental information protection programs
8. Review cyber insurance

Establish Good Cybersecurity Hygiene

- Apply NIST Cybersecurity Framework with a goal of achieving the appropriate target profile
  - Established as a result of Executive Order 13636, "Improving Critical Infrastructure Cybersecurity" (Feb. 2013)
- Measure cybersecurity policy against a standardized current cybersecurity guideline to avoid gaps
  - NIST Special Publication 800-53 Rev. 4, "Security and Privacy Controls for Federal Information Systems and Organizations" (Updated Jan. 2015)
  - Consider relevance of certifications (such as ISO/IEC 27001)
- Conduct audits of cybersecurity program compliance, including security tests, interviews of relevant personnel, review of documentation, and technical inspection of systems and networks

SECTION 04

CONDUCTING EFFECTIVE DUE DILIGENCE THROUGHOUT THE SUPPLY CHAIN

Understanding What You Want to Review

Every company or asset in a deal has supply chain cybersecurity risk, but not all such risks quires the same level of diligence/review.

High Dollar Risks (or High Profile/Disruptive Risks)

- Information breaches
  - Significant privacy breaches
  - Loss of proprietary information
  - Information subject governmental information restrictions
- Legal requirements for cybersecurity, where applicable, such as:
  - Critical infrastructure owners/operators
  - Financial institutions
  - Health care providers
- Integrity of key company cyber assets
- Systems that threaten significant third-party harm (worst case scenarios)

Unique Characteristics

- All businesses have risks that form a rough baseline. What makes this business different that may create higher-than-normal risk in certain areas? Possible considerations:
  - Type of equipment (Off-the-shelf equipment vs. bespoke equipment)
  - Type of threat (Financial crimes, general disruption and mischief, state-sponsored)
  - Critical assets (Are there one or two key systems? Or does the company rely on a broad array of typical computer systems that provide significant resiliency?)
  - Location of vendors and sources of vendor-supplied goods and services (Is this a country with a history of supply chain exploitation?)
  - Official notices/warnings issued or provided by government agencies (does the company rely on vendors for which warnings have been issued?)
  - Does the company purchase solely from OEMs or authorized distributors and resellers?
  - Does the company have a supply chain cybersecurity policy and evidence it has been implemented?

Discoverable

- Given the diffusion of the supply chain, it is often impossible, if not impractical, to examine all supply chain cybersecurity risks fully. In those circumstances, a diligence exercise needs to determine what level of risk is acceptable given the inefficiencies of identifying all risks. Considerations include:
  - Reliance on evidence of implementation for controls (e.g., software verification/authenticity)
  - Steps in supply chain and nature of buyer's relationship with suppliers
  - Practicality of hardware examination
  - Leveraging internal or external audits/reviews to identify vulnerabilities
  - Cross-checking with National Vulnerability Database and similar resources
  - What can be quickly identified and fixed following a transaction

Mechanisms for Addressing Supply Chain Risk in Deals

Pre-Transaction Reviews

- Review of certification documentation
- Audits of supply chain cybersecurity
- Identification of key suppliers and their cybersecurity risks
- Review of vendor agreements
- Traditional diligence questions

Deal Documents and Seller Commitments

- Representations
- Warranties
- Covenants for ongoing assistance and transition

Post-Consummation Reviews and Improvements

- Internal or third-party reviews
- Tightening supply chain requirements and implementing stronger vendor controls

SECTION 05

SUPPLY CHAIN SECURITY – COMMON GAPS IN VENDOR CONTRACTS

Peculiar Nature of Information Security

- Risk v. Reward Disparity
  - Technology is getting cheaper.
  - Data is getting more valuable.
  - Traditional approaches to risk allocation might not work (i.e. 12 month fees).

- Security can be a Shared Responsibility.
  - Consider User Credentials.
  - Configurations.
  - Really good security is expensive and slow.

Shifting Market has Created Gaps

- In the past 5 – 7 years, there has been a shift in the market.

- Sophisticated vendors are unwilling to bear full risk for cybersecurity issues.
  - Breach Security Obligations vs Security Breaches
  - Development of Vendor Information Security Requirements
  - Liability Limits
  - More Tailored Indemnity Provisions

- Role of Cyberliablity Insurance.

SECTION 06

SUPPLY CHAIN SECURITY – BEST PRACTICES AND MARKET POSITIONS

Filling the Gaps (as best as possible)

- **Base Obligation**
  - Vendor should do what it says it will do. Cannot be a moving target.
  - Attach the Information Security Requirements as an Exhibit.
  - If they modify it in a manner that is favorable, Customer gets the benefit. If they modify in a manner that is detrimental, Customer keeps the old version.

- **Think Mitigation, Not Allocation**
  - Training obligations.
  - Clear communication structure.
  - Review the Information Security Requirements to ensure that they are "real"

Filling the Gaps (as best as possible)

- **Indemnity**
  - Unlikely to get full indemnity for a Security Breach. Can try!
  - Require Indemnity for Breaches of Information Security Requirements.

- **Limitations of Liability**
  - Can reasonably push for uncapped to the extent covered by indemnity.
  - Supercaps common. (12 month fees might not cut it.)

- **Require Cyberliablity Insurance**.

Biography

Giovanna M. Cinelli
Washington, D.C.
T +1.202.739.5619
F +1.202.739.3001

Giovanna M. Cinelli is the leader of the international trade and national security practice. As a practitioner for more than 25 years, she counsels clients in the defense and high-technology sectors on a broad range of issues affecting national security and export controls, including complex export compliance matters, audits, cross-border due diligence, and export enforcement, both classified and unclassified.

Biography

Doneld G. Shelkey
Boston, MA
T +1.617.341.7599
F +1.617.341.7701

Doneld G. Shelkey represents clients in global outsourcing, commercial contracts, and licensing matters, with a particular focus on the e-commerce and electronics entertainment industries. Doneld assists in the negotiation of commercial transactions for domestic and international manufacturers, technology innovators, and retailers, and counsels clients in the e-commerce and electronics entertainment industries on consumer licensing and virtual property matters.

Biography

J. Daniel Skees
Washington, D.C.
T +1.202.739.5834
F +1.202.739.3001

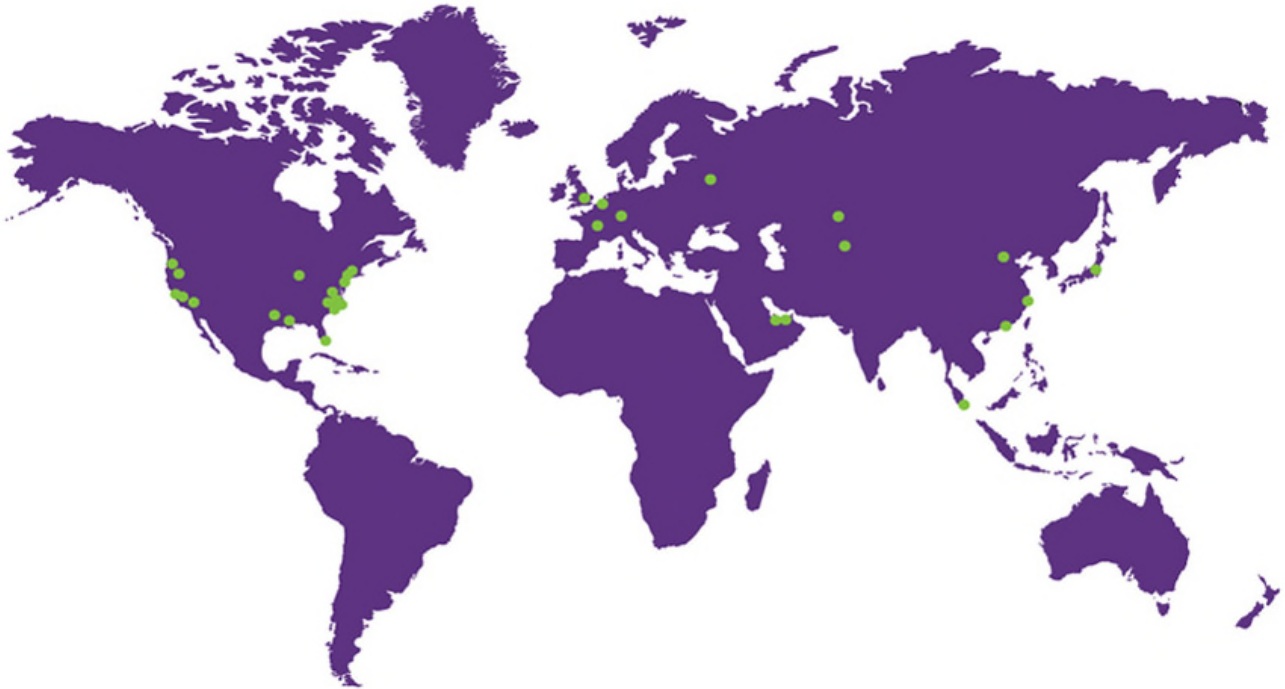
J. Daniel Skees represents electric utilities before the Federal Energy Regulatory Commission (FERC) and other agencies on rate, regulatory, and transaction matters. He handles rate and tariff proceedings, electric utility and holding company transactions, utility financing, electric markets and trading issues, reliability standards development and compliance, and transmission development. In handling appeals of FERC decisions, Dan has successfully represented clients before both the US Court of Appeals for the District of Columbia Circuit and the US Court of Appeals for the Fifth Circuit.

Our Global Reach

Africa
Asia Pacific
Europe
Latin America
Middle East
North America

Our Locations

Abu Dhabi
Almaty
Beijing*
Boston
Brussels
Century City
Chicago
Dallas
Dubai
Frankfurt
Hartford
Hong Kong*
Houston
London
Los Angeles
Miami
Moscow
New York
Nur-Sultan
Orange County
Paris
Philadelphia
Pittsburgh
Princeton
San Francisco
Shanghai*
Silicon Valley
Singapore
Tokyo
Washington, DC
Wilmington



Morgan Lewis

*Our Beijing and Shanghai offices operate as representative offices of Morgan, Lewis & Bockius LLP. In Hong Kong, Morgan Lewis operates through Morgan, Lewis & Bockius, which is a separate Hong Kong general partnership registered with The Law Society of Hong Kong as a registered foreign law firm operating in Association with Luk & Partners. Morgan Lewis Stamford LLC is a Singapore law corporation affiliated with Morgan, Lewis & Bockius LLP.

THANK YOU