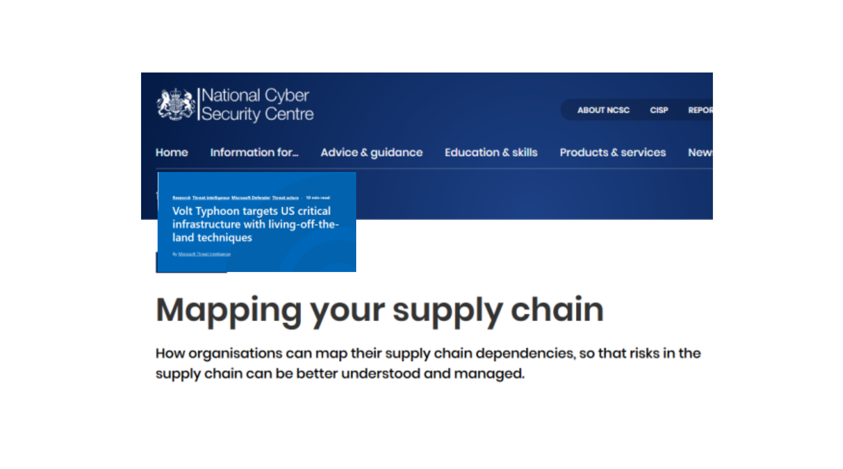
Exiger

Q4 2023

Cyber Risk & C-SCRM Exiger

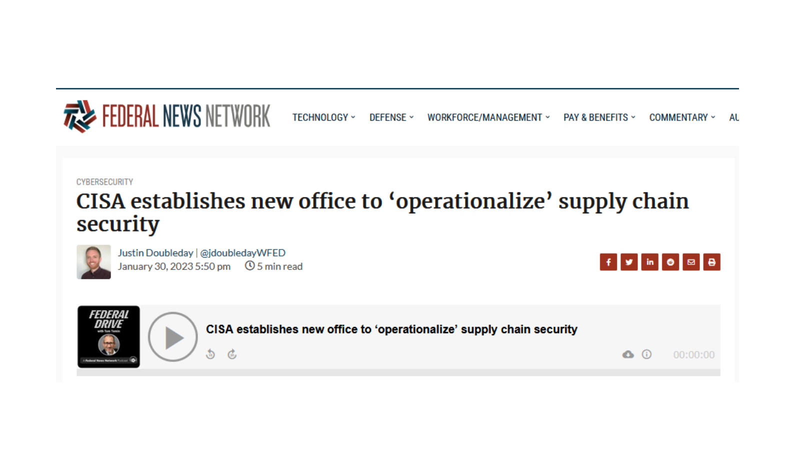
Cyber Supply Chain Risk Spans Borders and Businesses



Volt Typhoon targets US critical infrastructure with living-off-the-land techniques

Mapping your supply chain

How organisations can map their supply chain dependencies, so that risks in the supply chain can be better understood and managed.

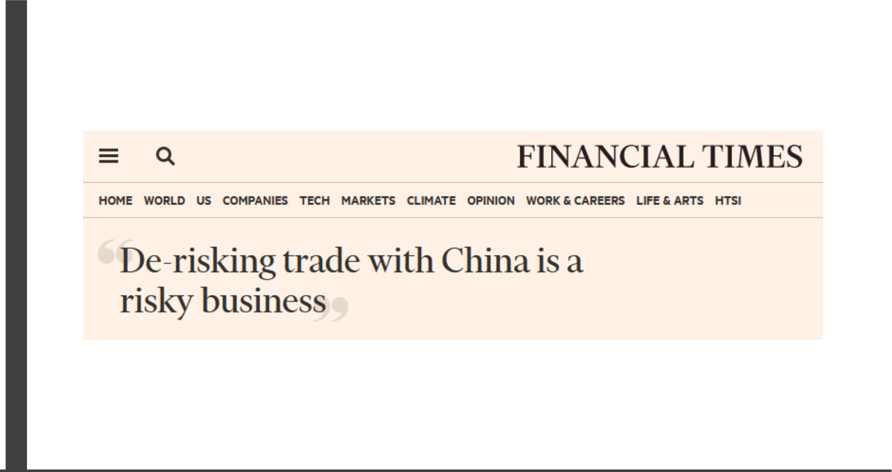


CYBERSECURITY

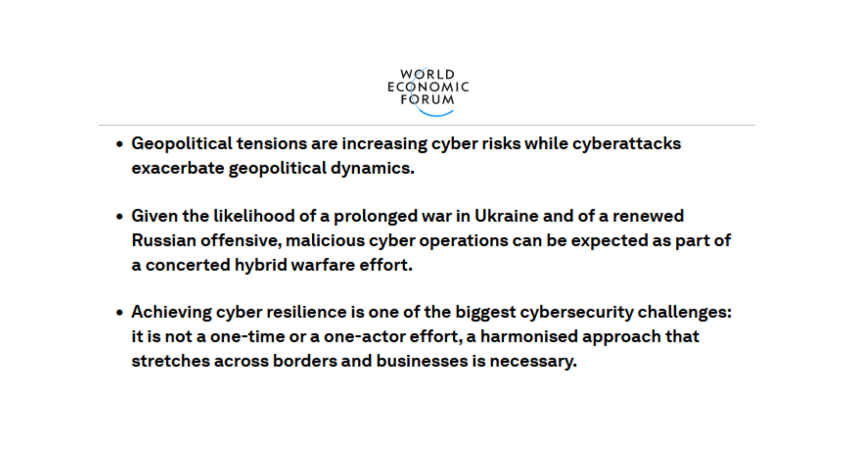
CISA establishes new office to ‘operationalize’ supply chain security

Justin Doubleday | @jdoubledayWFED
January 30, 2023 5:50 pm 5 min read

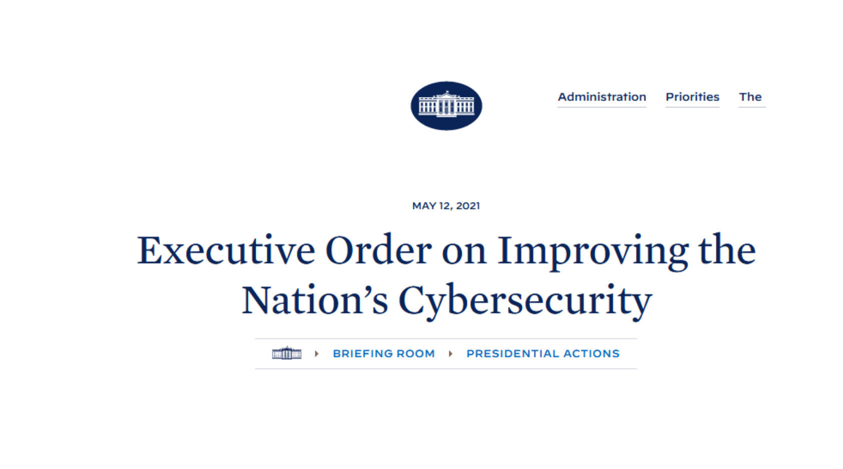
CISA establishes new office to ‘operationalize’ supply chain security



“De-risking trade with China is a risky business”



- Geopolitical tensions are increasing cyber risks while cyberattacks exacerbate geopolitical dynamics.
- Given the likelihood of a prolonged war in Ukraine and of a renewed Russian offensive, malicious cyber operations can be expected as part of a concerted hybrid warfare effort.
- Achieving cyber resilience is one of the biggest cybersecurity challenges: it is not a one-time or a one-actor effort, a harmonised approach that stretches across borders and businesses is necessary.



MAY 12, 2021

Executive Order on Improving the Nation’s Cybersecurity

RECENT POLICIES SUPPORTING C-SCRM EFFORTS

Executive Order 14017 – (February 24, 2021) *Securing America’s Supply Chains*. Directs each department in the administration to assess potential supply-chain risks within their jurisdiction and develop strategies to mitigate or overcome these.

Executive Order 14028 – (May 12, 2021) *Improving The Nation's Cybersecurity*. Lays out several key points that all organizations and government agencies must adhere to protect themselves from cyber threats. It defines critical software and sets up a system for information sharing to help organizations protect themselves from cyber threats.

Executive Order 13873 – (June 09, 2021) *Securing the Information and Communications Technology and Services Supply Chain*. Directs the federal government to strengthen efforts to prevent foreign adversaries from exploiting vulnerabilities in the ICT supply chain and protect the vast amount of sensitive information being stored in and communicated through ICT products and services.

NIST SP 800-161r1 – (May 2022) *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*. Provides guidance to organizations on how to identify, assess, and mitigate cybersecurity supply chain risks at all levels.

Cybersecurity Supply Chain Risk Management Guide – GSA – (May 2022) This guide is intended to provide agencies with a high-level description of Cybersecurity Supply Chain Risk Management (C-SCRM) and resources for acquiring products and services that align with CSCRM best practices.

NIST IR 8276 – (February 2021) *Key Practices in Cyber Supply Chain Risk Management: Observations from Industry*. Provides a set of Key Practices that any organization can use to manage cybersecurity risks associated with their supply chains.

PUBLIC LAW 115–390—(DEC. 21, 2018) Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act'' or the ``SECURE Technology Act. Requires the Secretary of Homeland Security to establish a security vulnerability disclosure policy, to establish a bug bounty program for the Department of Homeland Security, to amend title 41, United States Code, to provide for Federal acquisition supply chain security, and for other purposes.

Federal Acquisition Security Council (FASC) Final Rule – (September 27, 2021) Implement the requirements of the laws that govern the operation of the FASC, the sharing of supply chain risk information, and the exercise of the FASC's authorities to recommend issuance of removal and exclusion orders to address supply chain security risks.

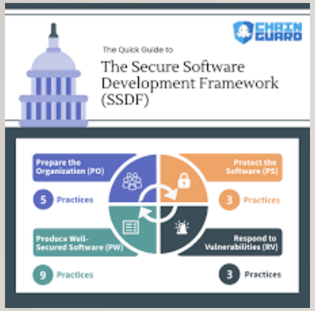
NEW US GOVERNMENT GUIDANCE REQUIRES ENHANCED SOFTWARE VETTING CAPABILITIES

BRIEFING ROOM

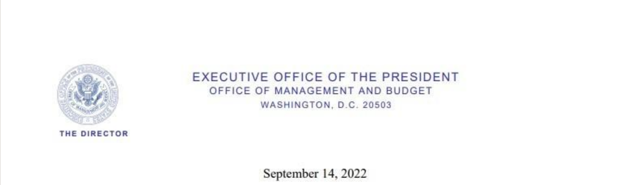
Executive Order on Improving the Nation's Cybersecurity

MAY 12, 2021 • PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:



CHAIN GUARD
The Quick Guide to
The Secure Software Development Framework (SSDF)
Prepare the Organization (PO)
5 Practices
Protect the Software (PS)
3 Practices
Produce Well-Secured Software (PW)
9 Practices
Respond to Vulnerabilities (RV)
3 Practices



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

September 14, 2022

- EO 14028 directs NIST to develop guidelines for creating and publishing Software Bills of Materials (SBOMs) in Federal procurement processes
- NIST SP 800-218 provides guidelines for using SBOMs as part of a secure software development
- The US National Telecommunications and Information Administration defines a set of minimum elements to be included in an SBOM
- The Office of Management and Budget memorandum M-22-18 issued on Sept 14, 2022, requires agency CIOs and CAOs to obtain self requires self-attestation from software producers before using software products

- **US agencies are required to obtain a self-attestation from the software producer.**
- **U.S. agencies will be required to obtain from their software producers SBOMs and documented processes to validate code integrity**

VARIOUS CONNECTIONS BETWEEN CYBER RISK AND SUPPLY CHAIN RISK

Right now, these are generally separate risks, with very specific overlaps. The shared concern, however, is risk exposure from the supply ecosystem

More attention on the supply chain of technology products and providers

Cyber is a type of supply chain risk

The supply chain is a vector of cyber attacks

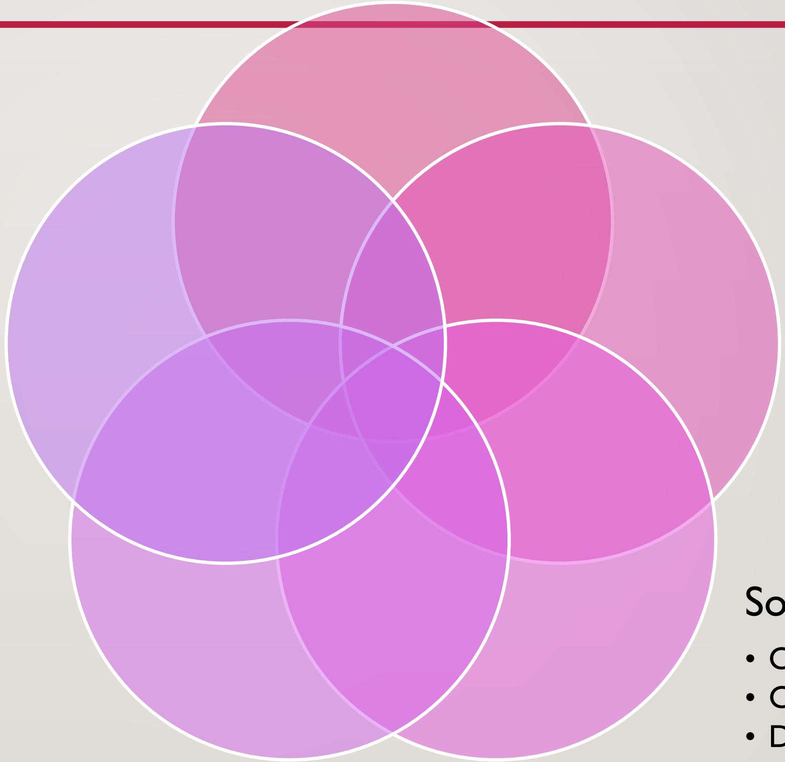
CYBER RISK AT DIFFERENT PARTS OF THE SUPPLY CHAIN

Enterprise/Agency	Network compromise Leaked / stolen credentials Business email compromise
Supplier/Vendor	Data breach Ransomware / wiper virus DDoS attack
Product/Parts	Open source quality Malware Firmware backdoor
Sector/Portfolio	Concentration of suppliers Patterns of shared products Interdependencies

TECHNOLOGY SUPPLY BASE

Information Technology

- Hardware
- Processors
- Cloud services
- Data centers



Vendors

- Outsourced
- Consultants
- Contractors
- On site service providers

Operational Technology

- SCADA
- DCS
- PLC

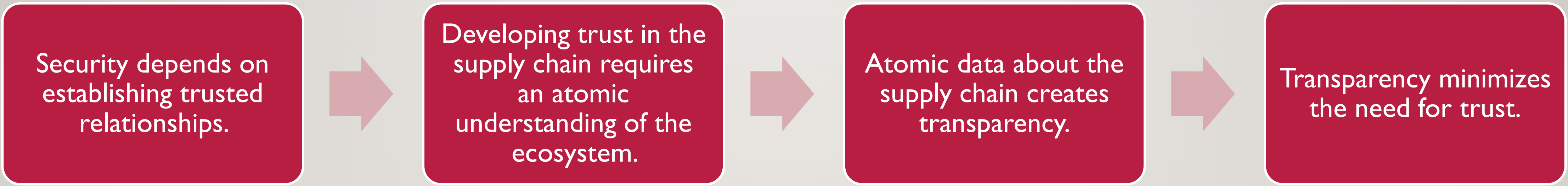
Third Party Data

- Sensitive (SSN, DOB)
- Financial (PCI)
- Proprietary (IP)
- Regulated (PHI)

Software

- Operating systems
- Compilers and editors
- Drivers and dependencies
- Open-source scripts and packaged software
- Repository engines, testing suites, and CI/CD tools

SECURING TECHNOLOGY DEMANDS TRUST IN HOW IT WORKS AND IS CREATED – AND BY WHOM



Security depends on establishing trusted relationships.

Developing trust in the supply chain requires an atomic understanding of the ecosystem.

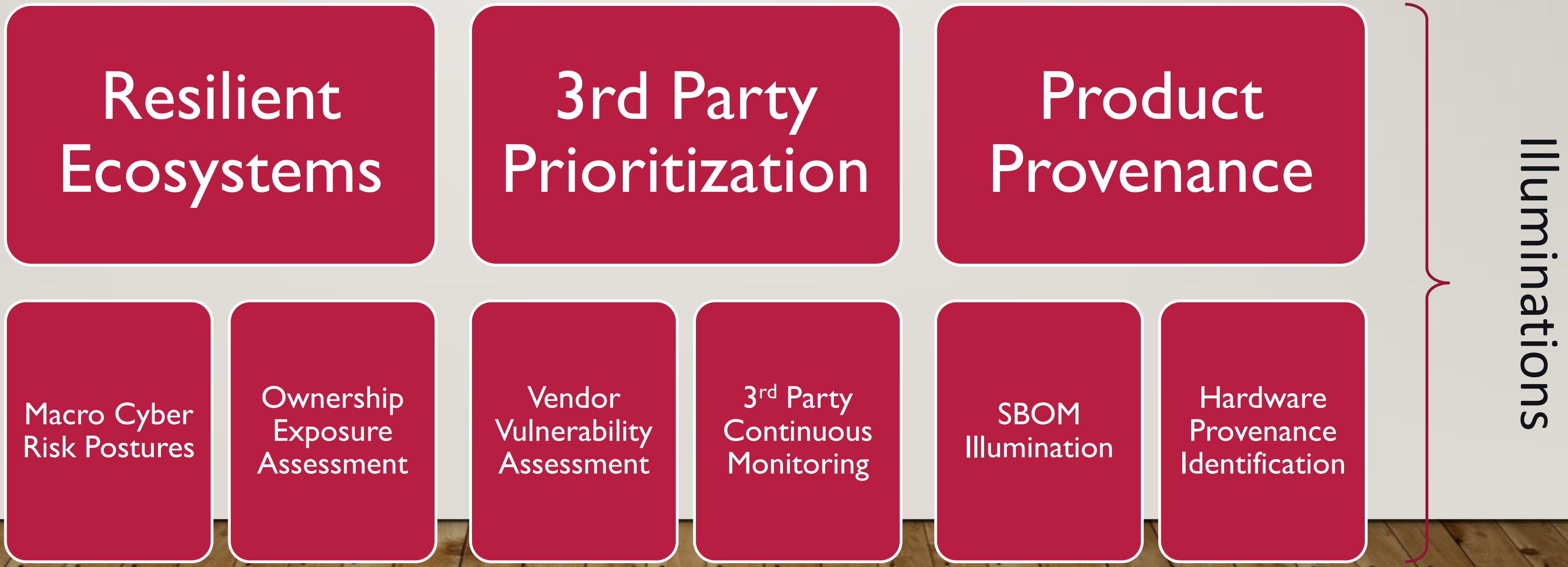
Atomic data about the supply chain creates transparency.

Transparency minimizes the need for trust.

Managing cyber supply chain risk expects an understanding the suppliers, products, and ecosystem.

EXIGER'S PLATFORM USES DATA TO UNCOVER RISK IN BUSINESS RELATIONSHIPS

Exiger's risk management platform is specifically designed to assess supply chain risk management of third parties by systematically investigating cyber risks to and through the supply chain, prioritizing by potential impact, and continuously monitoring of risk exposure.



Resilient Ecosystems

- Macro Cyber Risk Postures
- Ownership Exposure Assessment

3rd Party Prioritization

- Vendor Vulnerability Assessment
- 3rd Party Continuous Monitoring

Product Provenance

- SBOM Illumination
- Hardware Provenance Identification

Illuminations

MANAGING PRODUCT RISK: IDENTIFY PRODUCT PROVENANCE AND PEDIGREE

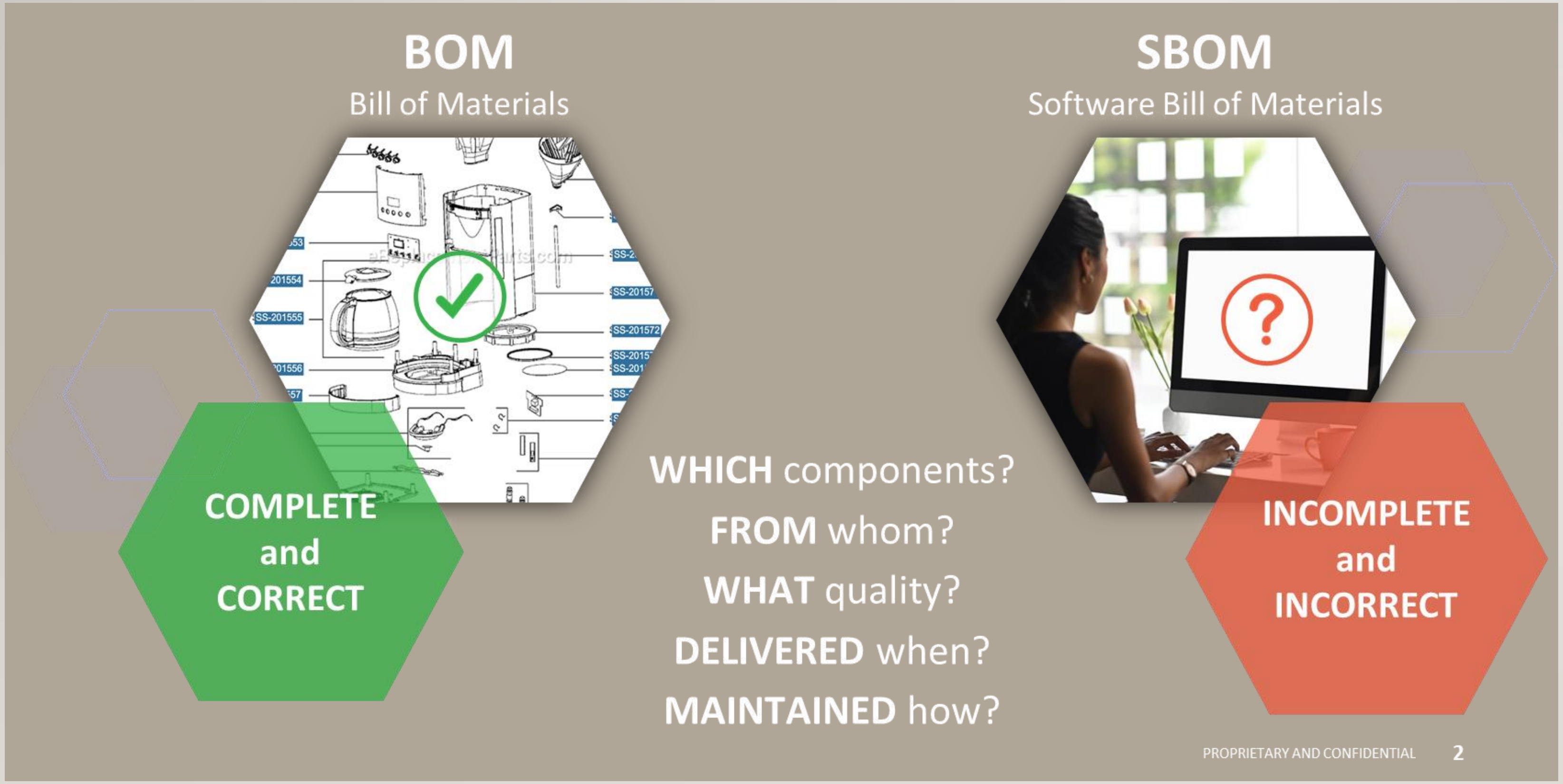
Complex interdependencies make it impossible to ensure the security of *all* components *and* contributors to supply chain.

Software Bill of Materials Illumination. Transparency into software components and libraries. Automated inventory identifies potential compromised software and potential software security vulnerabilities in supplier systems.

Hardware Provenance Identification. Item level identification of hardware parts and provenance. Material and component parts forecasting. Early warning of supply chain disruptions. Identification of counterfeit hardware or hardware with embedded malware.

SOFTWARE RISKS ARE LARGELY UNKNOWN AND UNADDRESSED

Software supply chains are a blind spot for many organizations: weaknesses can come from any component in your software supply chain, and threat actors know this.



BOM

Bill of Materials

SBOM

Software Bill of Materials

COMPLETE and CORRECT

INCOMPLETE and INCORRECT

WHICH components?

FROM whom?

WHAT quality?

DELIVERED when?

MAINTAINED how?

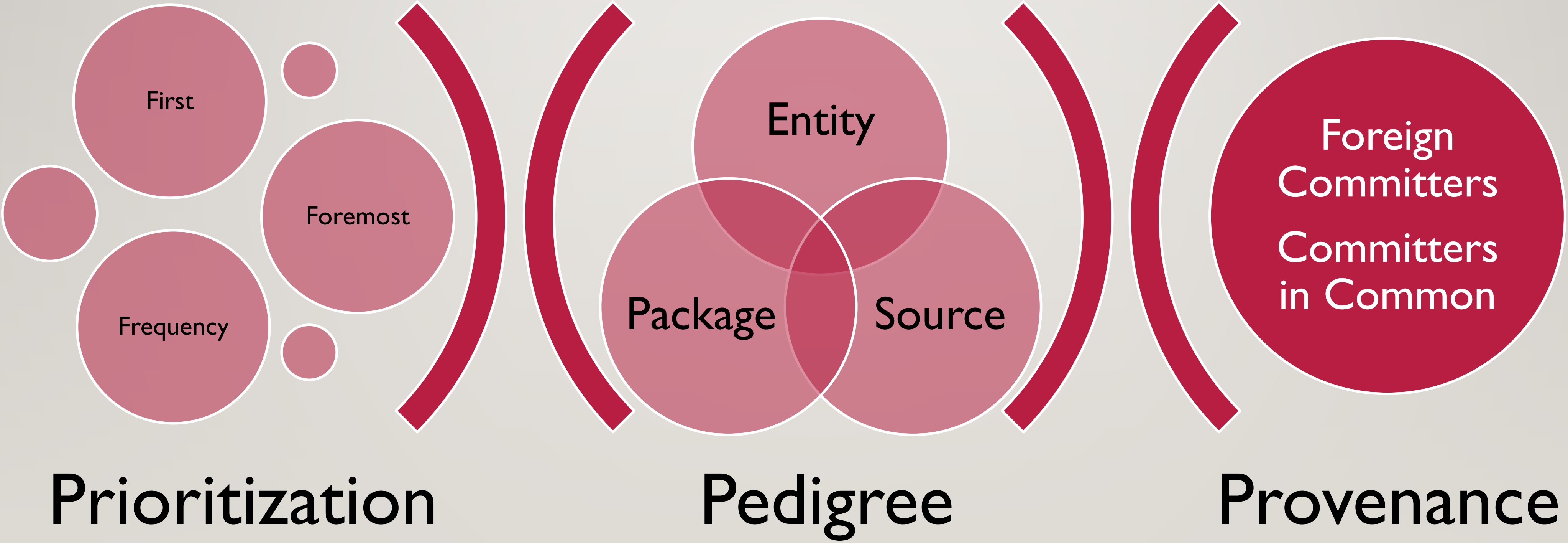
PROPRIETARY AND CONFIDENTIAL 2

- Using tools that only assess “known vulnerabilities” will miss key supply chain risk events; it is not enough to identify the hidden risks that lurk when you inherit, purchase or outsource software capabilities.
- Open source software accounts for 75% of codebases, on average– a major source of unknown risks.

CVES AND VULN IDENTIFICATION ARE LAGGING INDICATORS

Software risk includes managing challenges like insipient malware and adversarial control. Code commits are an early warning indicator and allow upstream detection.

Understanding what is supposed to be in software vs. what is *actually* in software requires more than an SBOM; it requires measurement.



BUILD A CYBER RESILIENT SUPPLY CHAIN

Identify Hidden Risks and Dependencies in Products

Prioritize the Vulnerable Vendors and Third Parties

Uncover Who is Really Building Your Trusted Tech

Understand Exposure for the Entire Supply Ecosystem

Make Data-Driven Procurement Decisions

Safeguard Trust with Transparency Through Data