December 2023

Beyond the XBOM:

Holistic Supply Chain Risk Management

ACSAC 2023

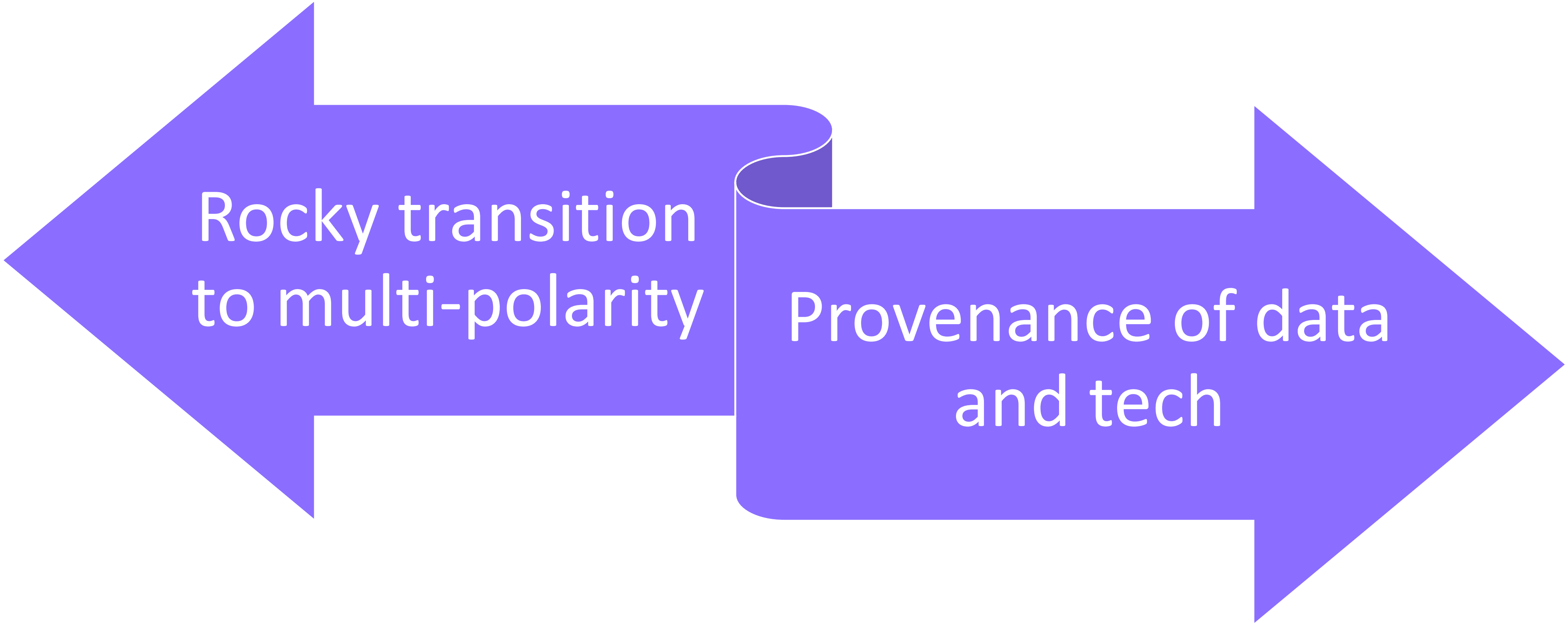
An Existential Introduction

Who am I?

Why am I here?

What have I done?

Two tech-tonic shifts

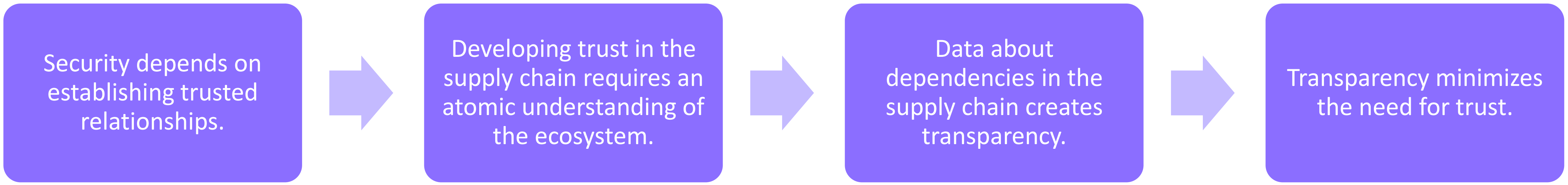


Rocky transition to multi-polarity

Provenance of data and tech

Paradox of Perennial Surprise

Securing technology demands trust in how it works and is created – and by whom



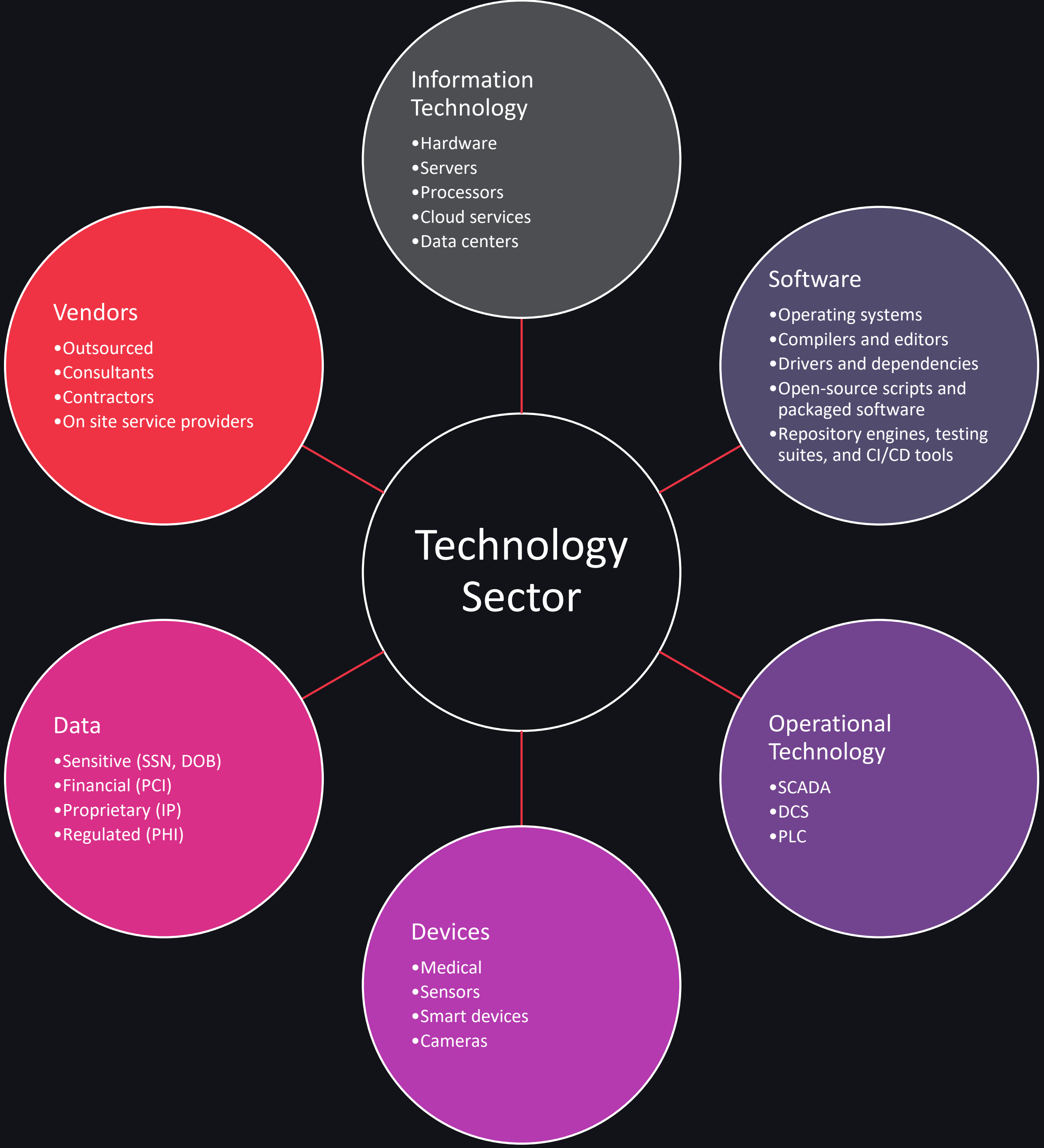
Security depends on establishing trusted relationships.

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

Data about dependencies in the supply chain creates transparency.

Transparency minimizes the need for trust.

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



Technology Sector

Information Technology

- Hardware
- Servers
- Processors
- Cloud services
- Data centers

Software

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

Operational Technology

- SCADA
- DCS
- PLC

Devices

- Medical
- Sensors
- Smart devices
- Cameras

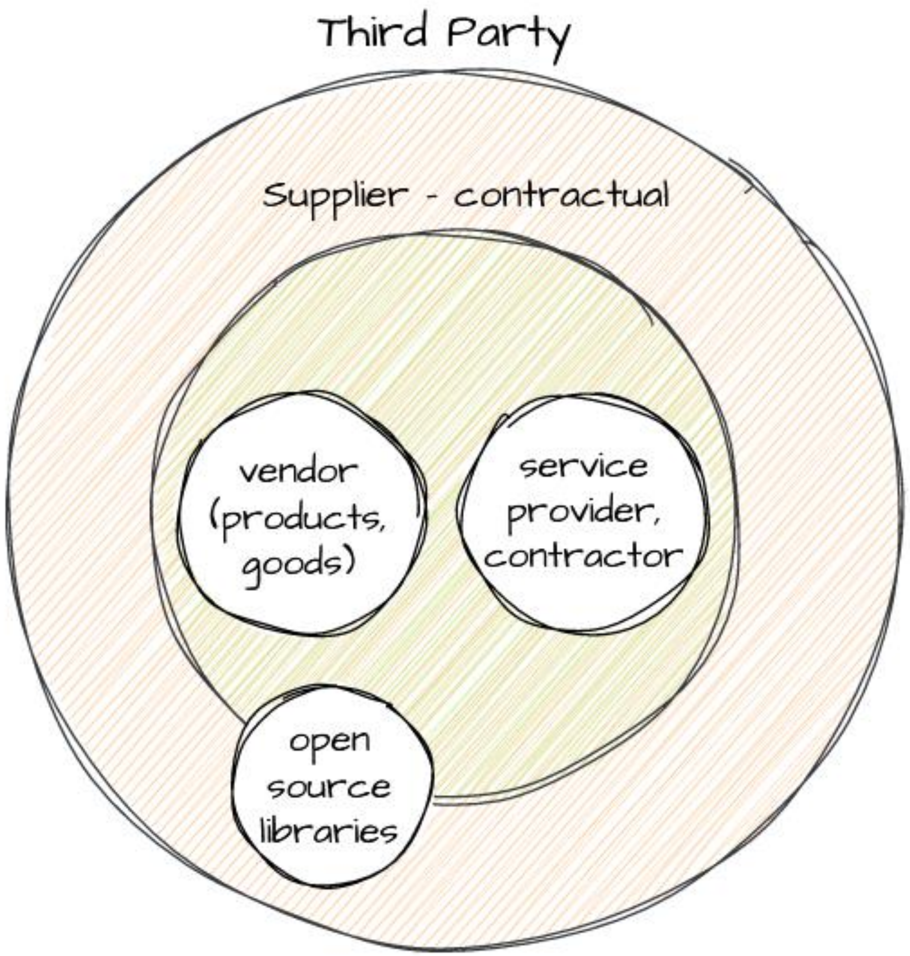
Data

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

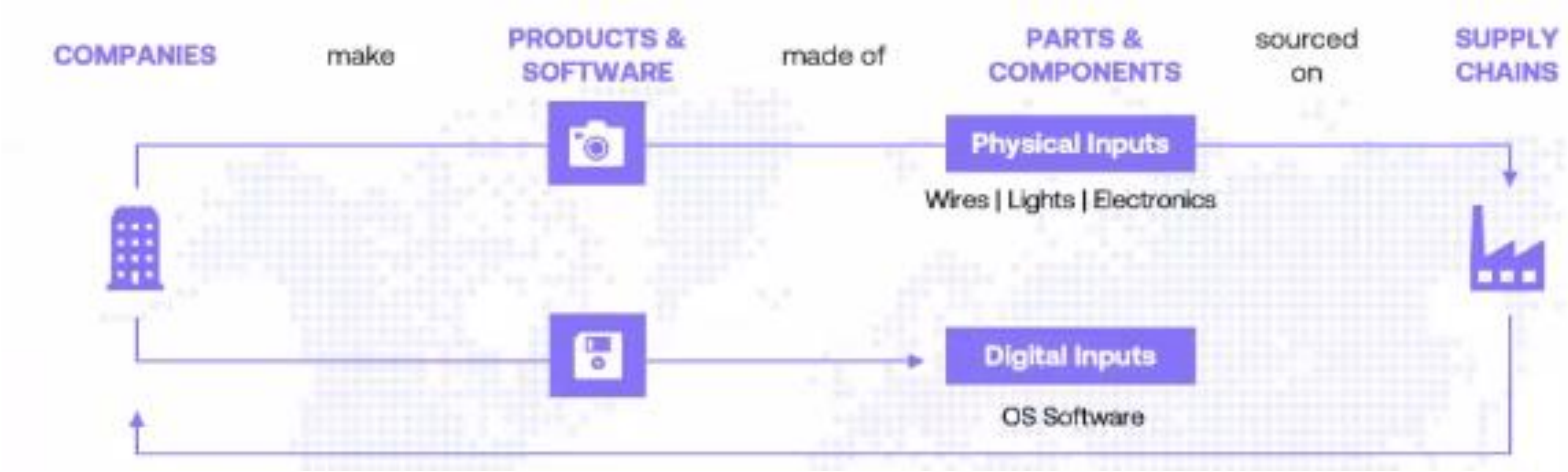
Vendors

- Outsourced
- Consultants
- Contractors
- On site service providers

Supplier, Vendors, Third Parties, Oh My



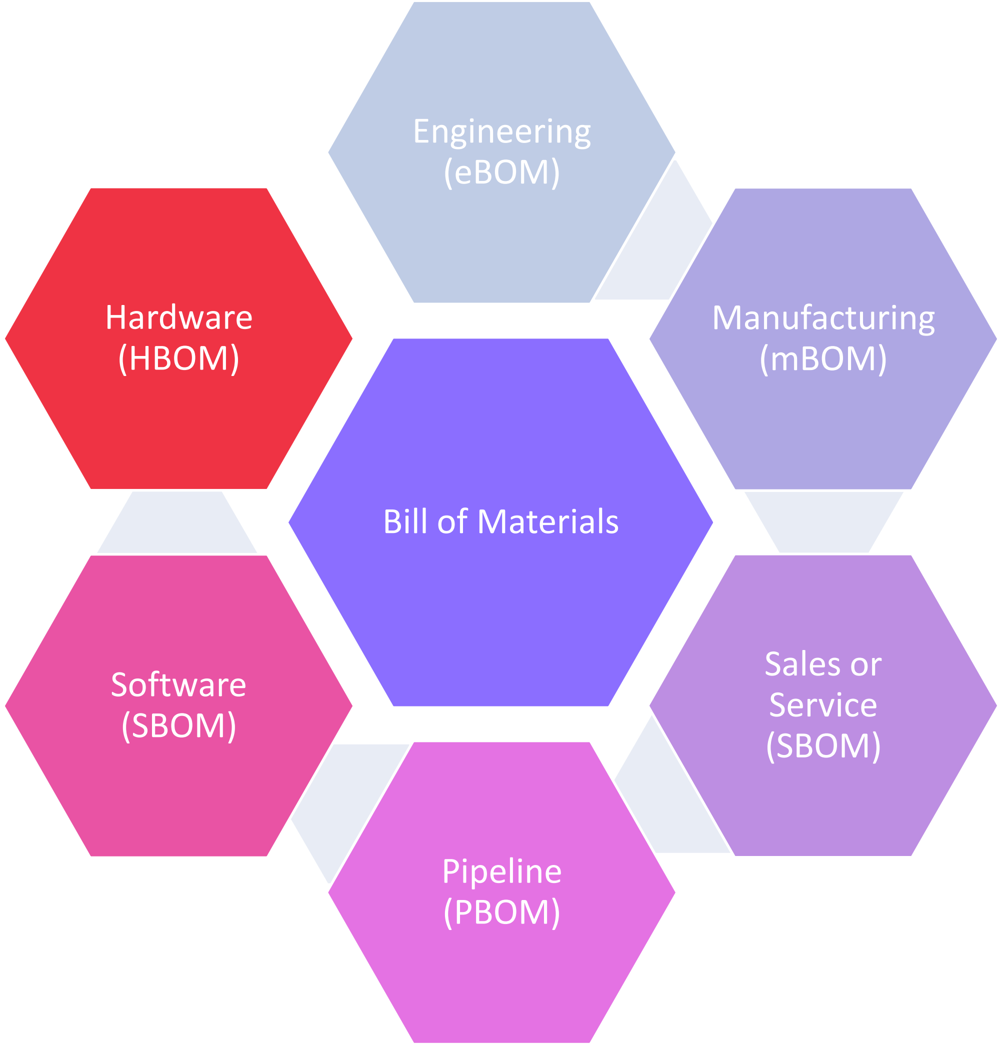
Know the Flow



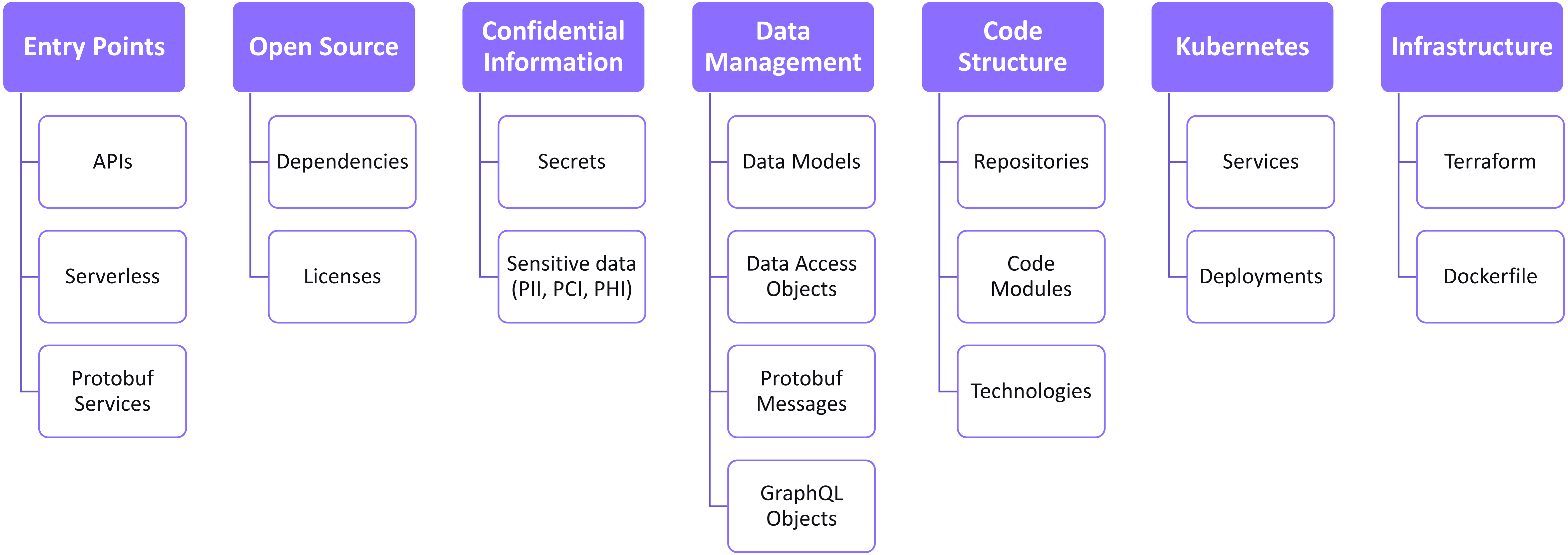
Which XBOM are we talking about?

- Online radio station about post-apocalyptic Las Vegas
- eXtensible Blockchain Object Model
- Market identified code (stock ticker) for an Indian-listed company

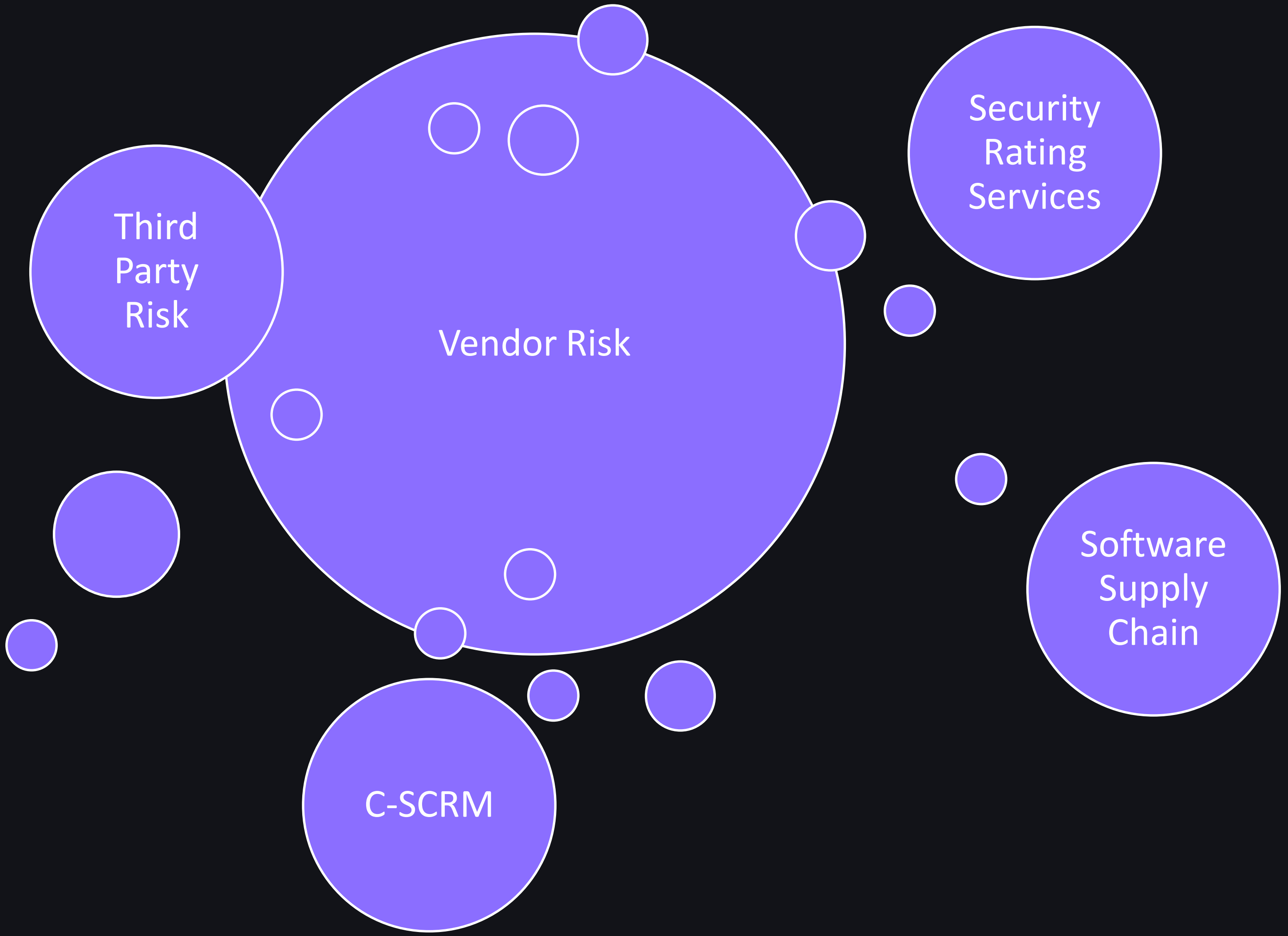
The Genealogy of Development & Production Planning



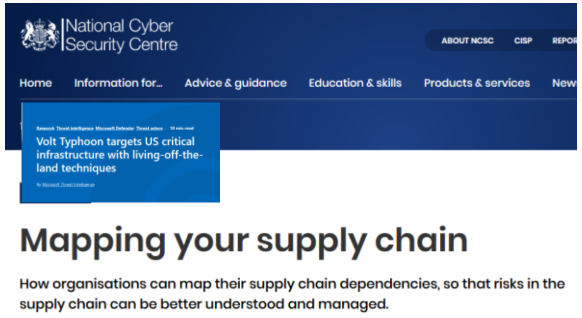
Elements of an XBOM



- Entry Points
  - APIs
  - Serverless
  - Protobuf Services
- Open Source
  - Dependencies
  - Licenses
- Confidential Information
  - Secrets
  - Sensitive data (PII, PCI, PHI)
- Data Management
  - Data Models
  - Data Access Objects
  - Protobuf Messages
  - GraphQL Objects
- Code Structure
  - Repositories
  - Code Modules
  - Technologies
- Kubernetes
  - Services
  - Deployments
- Infrastructure
  - Terraform
  - Dockerfile


Third Party Risk
Vendor Risk
Security Rating Services
Software Supply Chain
C-SCRM

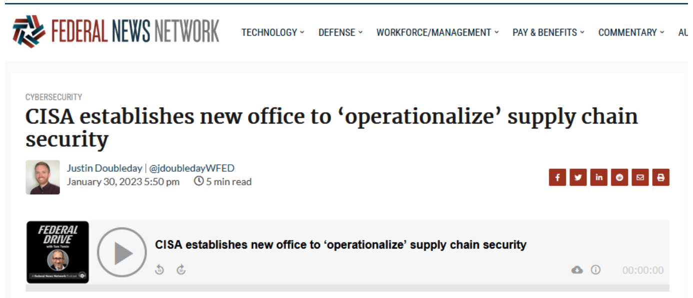
Cyber Supply Chain Risk Spans Borders and Businesses



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.

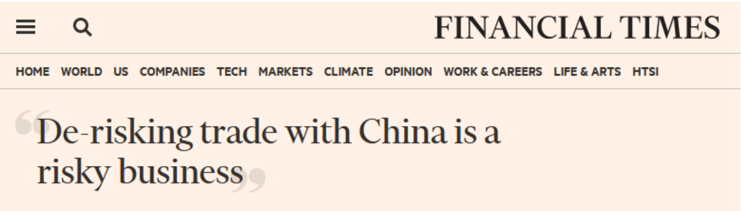


CYBERSECURITY

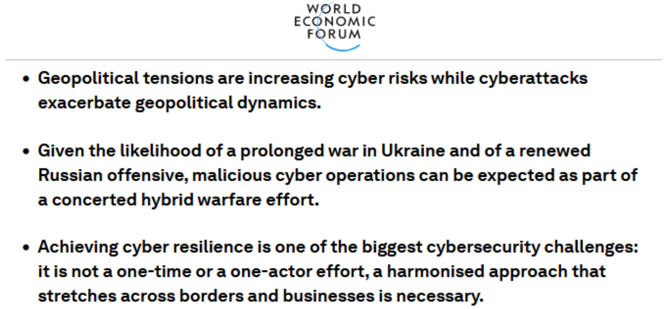
CISA establishes new office to ‘operationalize’ supply chain security

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

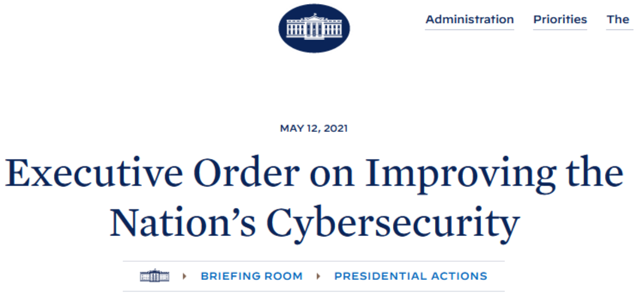
CISA establishes new office to ‘operationalize’ supply chain security



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



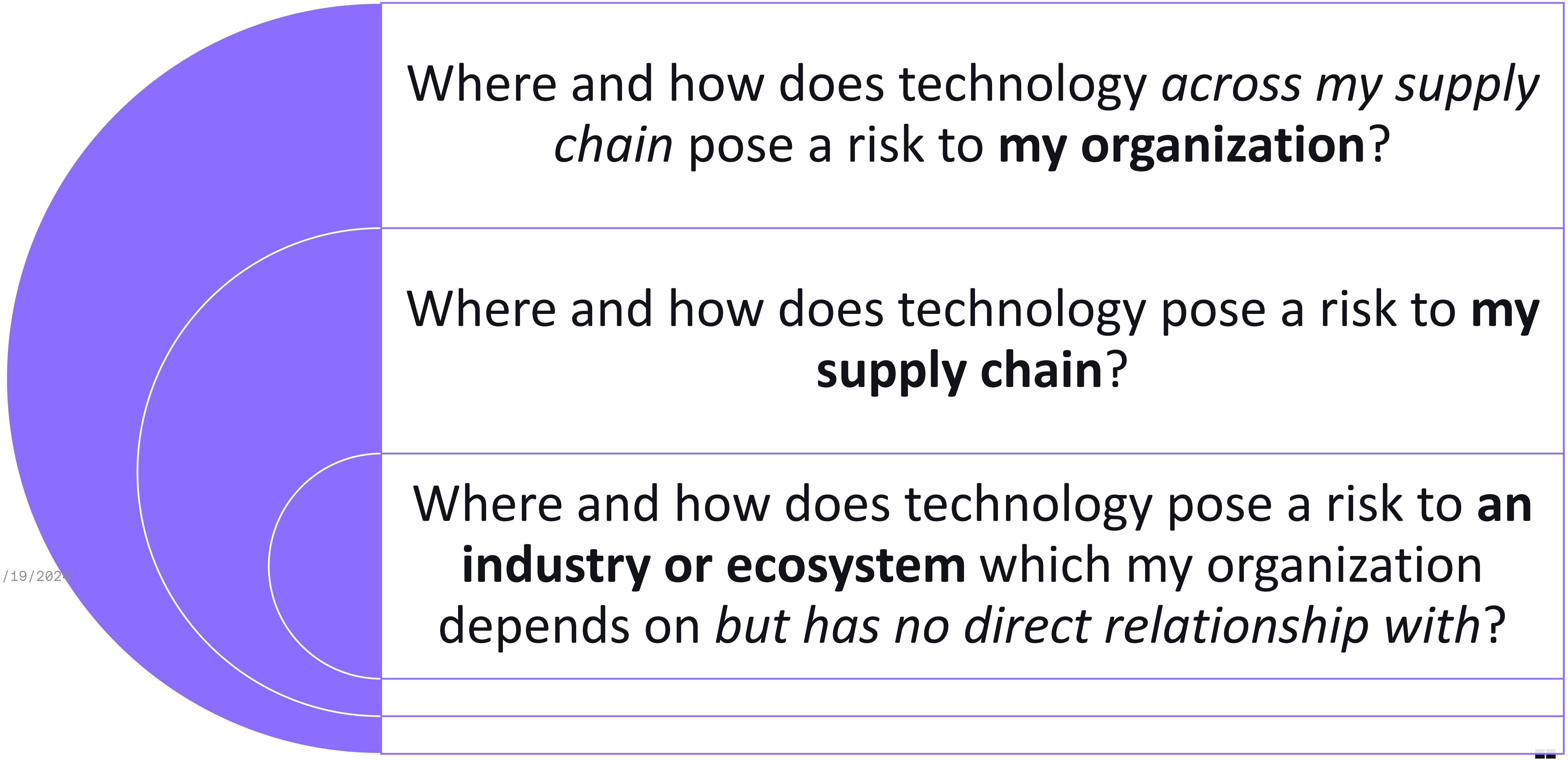
- Geopolitical tensions are increasing cyber risks while cyberattacks exacerbate geopolitical dynamics.
- Given the likelihood of a prolonged war in Ukraine and of a renewed Russian offensive, malicious cyber operations can be expected as part of a concerted hybrid warfare effort.
- Achieving cyber resilience 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

Key Pain Points + Driving Questions

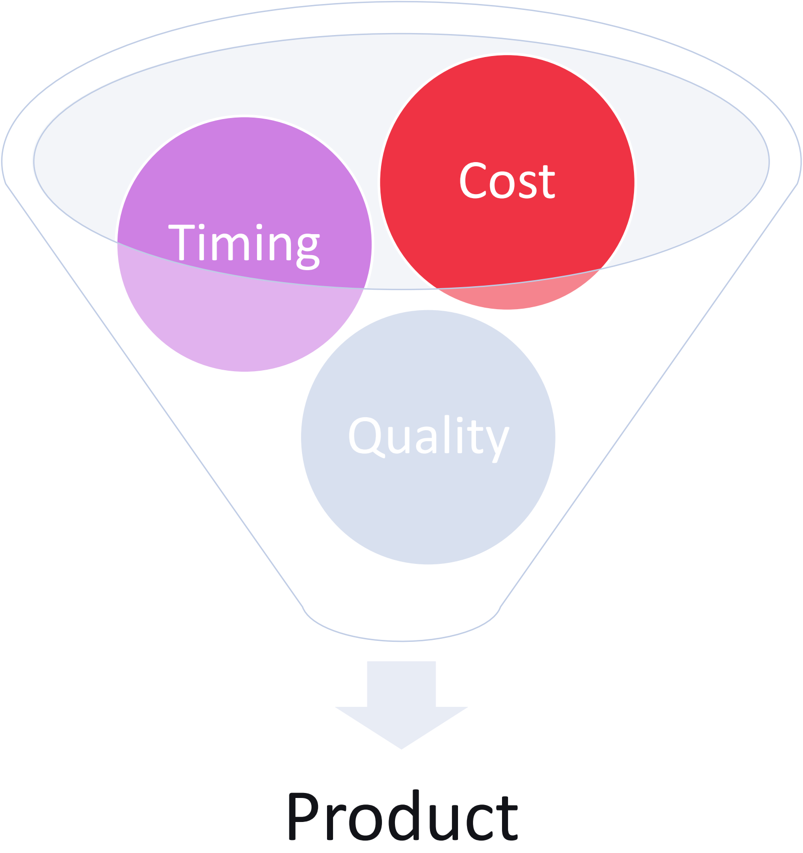


Where and how does technology *across my supply chain* pose a risk to **my organization**?

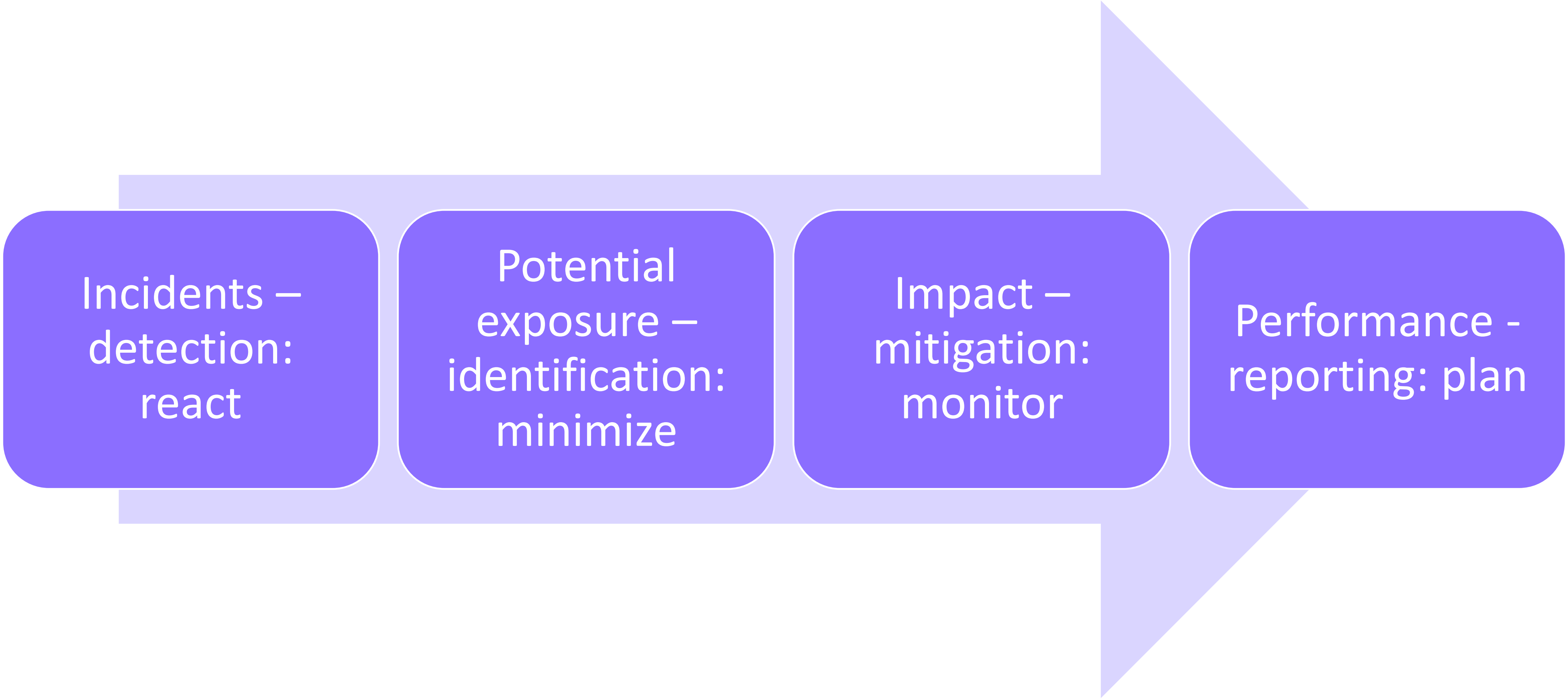
Where and how does technology pose a risk to **my supply chain**?

Where and how does technology pose a risk to **an industry or ecosystem** which my organization depends on *but has no direct relationship with*?

Risk Management = Resource Allocation



Lessons for Transparency in Cyber Risk from Other Supply Chain Risks



Incidents – detection: react

Potential exposure – identification: minimize

Impact – mitigation: monitor

Performance - reporting: plan

Forced Labor

Foreign Ownership

Cyber Risk to *and* through the Supply Chain

Attacks can occur at every link in a typical software supply chain, and these kinds of attacks are increasingly public, disruptive, and costly.

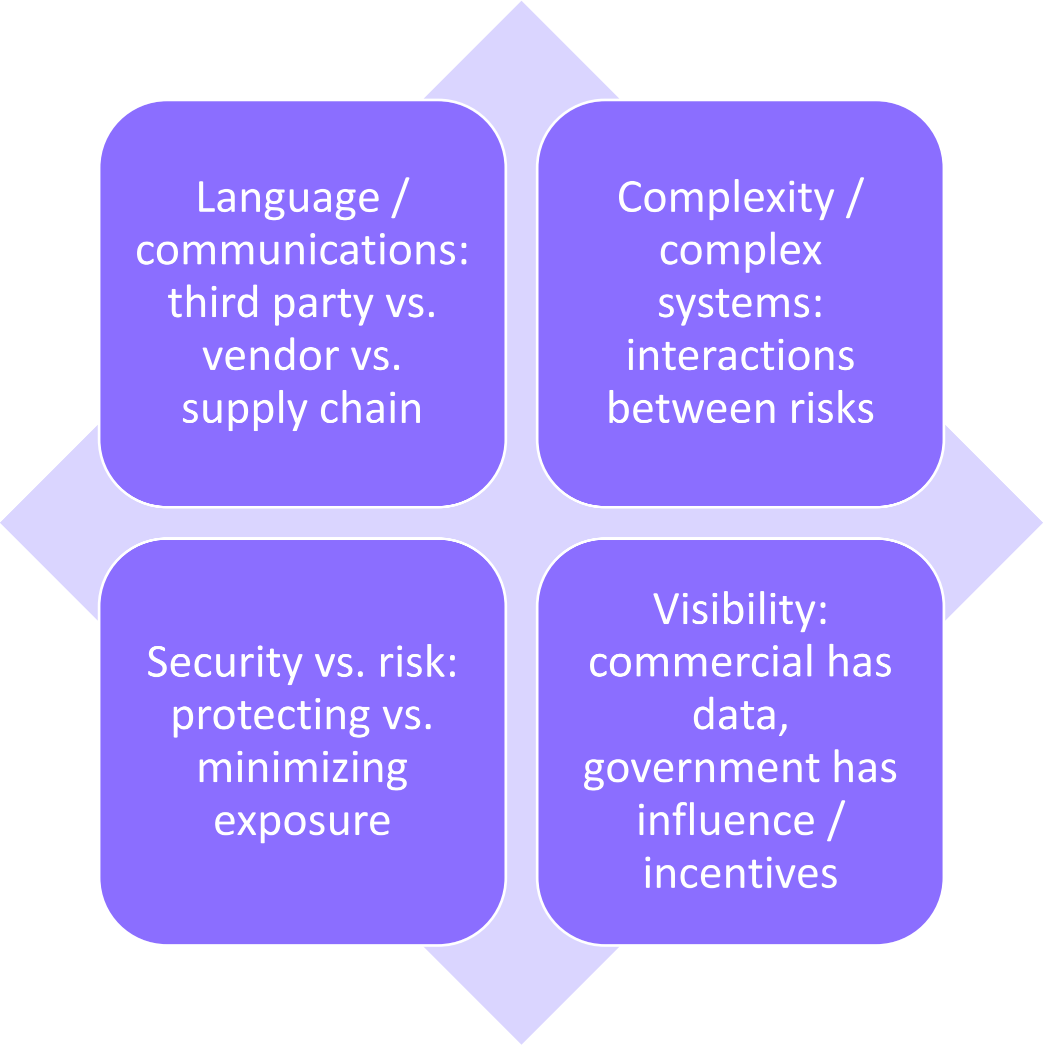
From the recent spate of serious supply chain attacks, the industry learned three painful lessons:

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

Threat actors are economic, efficient, and entrepreneurial – and target weak links.

Third party exposure is not your fault, but it is your problem.

Additional Areas of Research



Language / communications: third party vs. vendor vs. supply chain

Complexity / complex systems: interactions between risks

Security vs. risk: protecting vs. minimizing exposure

Visibility: commercial has data, government has influence / incentives

Thank you!

Best way to find me:
mwaltherpuri@exiger.com