CYBER – SUPPLY CHAIN ATTACKS – RISK IDENTIFICATION, MITIGATION AND RESPONSE

PRESENTERS: KEILY BLAIR, PETER LEFKOWITZ AND HEATHER EGAN SUSSMAN

September 30, 2021





Presenters



Keily Blair
Partner| Head Cyber, Privacy & Data Innovation London
Orrick



Peter Lefkowitz
Vice President, Chief Digital Risk Officer
Citrix



Heather Egan Sussman
Partner | Global Head of Cyber, Privacy & Data Innovation
Orrick

Presentation Agenda

- Introduction and Background
- Regulatory Environment
- Proactive Preparation
- Detection and Response

INTRODUCTION AND BACKGROUND

Definition?

NIST Definition

A supply chain attack when a cyber threat actor infiltrates a software vendor's network and employs malicious code to compromise the software before the vendor sends it to their customers.

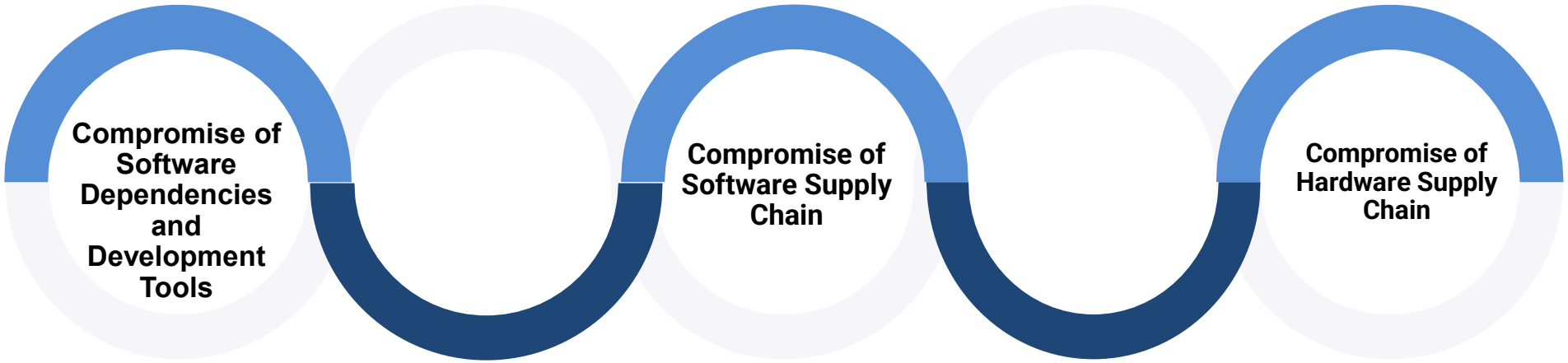
MITRE Definition

Adversaries manipulate products or product delivery mechanisms prior to receipt by a final consumer for the purpose of data or system compromise.

Market Perception

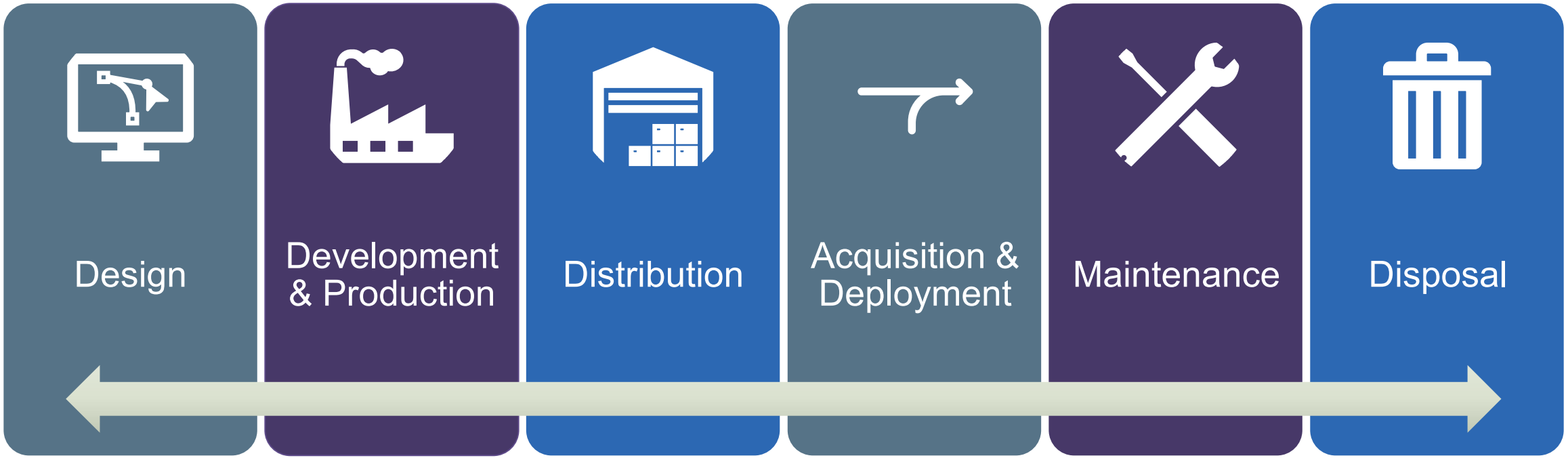
Any compromise within your vendor supply chain potentially impacting your data or systems, even if it never impacts the security of your network.

Types of Supply Chain Attack

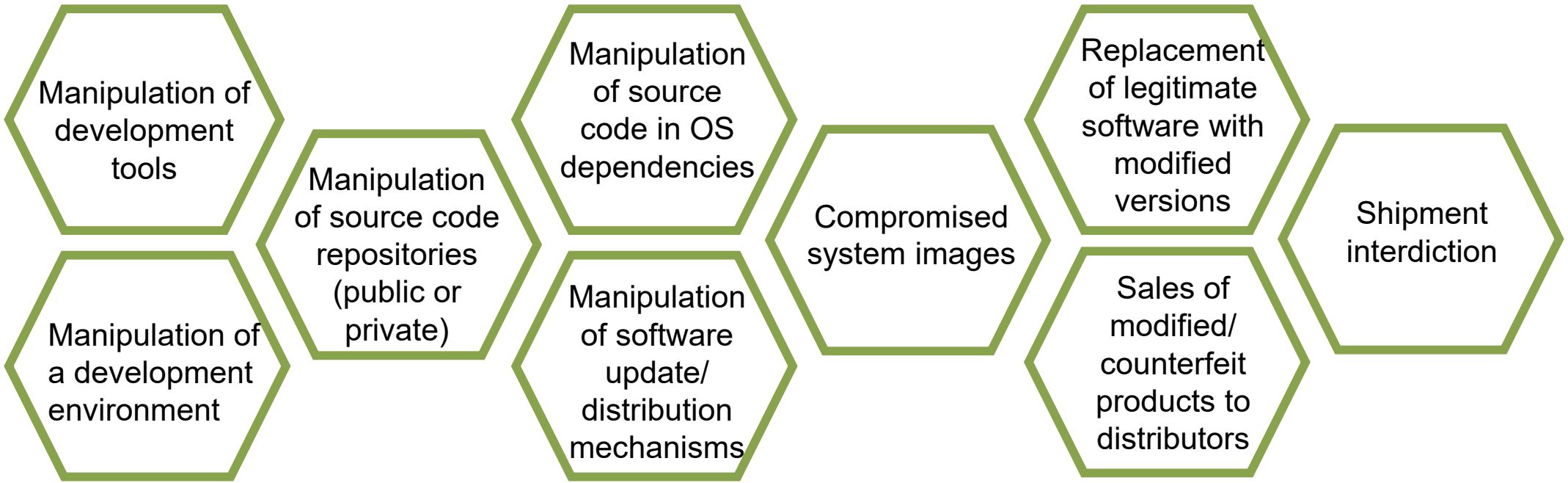


The ICT Supply Chain Lifecycle

- Software supply chains fit within the greater information and communications technology (ICT) supply chain framework.
- The ICT Supply Chain Lifecycle has six phases, each at risk from an attack



An attack can take place at any stage of the supply chain



Examples of risk at each phase of the ICT supply chain cycle

Design

- **Hijacked Cellular Devices. 2016** – A foreign company designed software used by a U.S. cell phone manufacturer. The phones made encrypted records of text and call histories, phone details, and contact information and transmitted that data to a foreign server every 72 hours.

Development & Production

- **SolarWinds. 2020** – An IT management company was infiltrated by a foreign threat actor who maintained persistence in its network for months. The threat actor left the network only after it had compromised the company's build servers and used its update process to infiltrate customer networks.
- **Vendor:** Orion (network management platform)

Distribution

- **End-User Device Malware. 2012** – Researchers from a major U.S. software company investigating counterfeit software found malware preinstalled on 20 percent of devices they tested. The malware was installed in new desktop and laptop computers after they were shipped from a factory to a distributor, transporter, or reseller.

Acquisition & Development

- **Kaspersky Antivirus. 2017** – An overseas-based antivirus vendor was being used by a foreign intelligence service for spying. U.S. government customers were directed to remove the vendor's products from networks and disallowed from acquiring future products from that vendor.
- **Vendor:** NetSarang (network connectivity software)

Maintenance

- **Backdoors Embedded in Routine Maintenance Updates. 2020** – Thousands of public and private networks were infiltrated when a threat actor used a routine update to deliver a malicious backdoor.

Disposal

- **Sensitive Data Spillage. 2019** – A researcher bought old computers, flash drives, phones and hard drives, and found only two properly wiped devices out of 85 examined. Also found were hundreds of instances of personally identifiable information (PII) spillage, including Social Security numbers, passport numbers, and credit card numbers.

Source: "Defending Against Software Supply Chain Attacks" – Cybersecurity and Infrastructure Security Agency (Apr. 2021)

REGULATORY ENVIRONMENT

Regulatory Environment EU and ROW

- Legal Framework
  - GDPR
  - NIS Directive (and the sequel NIS 2)
- Supranational Co-operation
  - ENISA & EU Cyber Security Agency
  - Critical Entities Resilience (CER) Directive
  - Security Operations Centres Network
  - EU Cyber Diplomacy Toolbox.
  - What about Brexit?
- Contracting considerations



Regulatory Environment U.S.



- Federal
  - Federal contracting requirements
  - Federal agencies (FTC, OCR, SEC)
- State
  - Data security laws
  - Breach notification laws
  - State Agencies (NY DFS, AGs, DOIs)
- Contracting considerations

U.S. Securities and Exchange Considerations



SEC's heightened scrutiny of cyber risk disclosures

- First American Financial Corporation Enforcement Action
- Pearson PLC Enforcement Action

2018 SEC Cybersecurity Disclosure Guidance

- "…it is critical that public companies take all required actions to inform investors about material cybersecurity risks and incidents in a timely fashion."
- Far-reaching definition of materiality

PROACTIVE PREPARATION



How do you proactively prepare?

- Diligence and contracting
  - Risk shifting and liability caps
  - International considerations (e.g., effect on transfer impact assessment?)
- Program for ongoing monitoring and review
  - **Internally**: maintain HVA program and network segmentation; patch management; vulnerability scans; physical assessments of hardware
  - **Externally**: Strong vendor management program; look for vendors with strong SDLC; conduct code reviews where needed; push down internal controls to address risks that are "downstream of downstream"
- Cyber insurance



Risk Management Framework



Summary

Managing Known Risks

- Identify, understand and document risks
- Build a risk assessment framework
- Monitor risks
- Regular review

Managing Unknown Risks

- A good offense is the best defence
- Create a culture of risk management—it is EVERYONE's job

DETECTION AND RESPONSE



Detection Considerations

- Take a programmatic approach (defined roles and responsibilities, policies and procedures, technology where appropriate, checks and balances)
  - Software
    - Use verification of distributed binaries through hash checking or other integrity checking mechanisms
    - Scan downloads for malicious signatures
    - Test software and updates prior to deployment
  - Hardware
    - Physical inspections using baseline to look for tampering or anomalies
- Zero-day considerations

Response Considerations

- Preserve privilege of investigation
- Preserve evidence
- Determine if:
  - A vulnerability was actually introduced into the environment?
  - That vulnerability was exploited?
  - There was credential compromise, lateral movement, data exfiltration?
  - If the compromise led to the access, acquisition, use, or disclosure of personal information or protected health information?
- If possible, follow the threat actor to determine "attribution" and potential additional reporting obligations

Response Considerations

- Notifications:
  - To regulators
  - To businesses (if a vendor)
  - To consumers
  - To credit reporting agencies
- Contractual obligations
  - Assess timing obligations and possible regulator notification triggers for certain entities (e.g., covered entities under HIPAA, insurance companies)
- SEC disclosure obligations (for public companies)
  - Consider recent enforcement history when making disclosures
- Evaluate how it could impact ESG reporting cybersecurity

Response Considerations

- Remediation
  - Patch vulnerability
  - Examine processes that led to the vulnerability
  - Evaluate if policies or procedures need to be updated
  - Evaluate response to incident to identify any areas that could be improved
- Document remediation activities in case of regulatory inquiries

QUESTIONS?