Carnegie Mellon University
Software Engineering Institute

Managing for Supply Chain Resilience

FEBRUARY 15, 2023

Dan Kambic
Cybersecurity Team Lead

Notice

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM23-0118

About Me

- Cybersecurity Team Lead, Cyber Assurance, CERT division of Carnegie Mellon University's (CMU) Software Engineering Institute (SEI)
- 30+ years of experience in IT security, architecture, applications, project delivery, and management
- Prior to SEI, managed rollout and execution of global logistics and transportation management solution for worldwide manufacturer
- Before that held progression of global IT positions at separate worldwide manufacturer
- B.S. and M.S. in Electrical Engineering, University of Pittsburgh
- Certified Information Systems Security Professional (CISSP)
- Forrester Zero Trust
- ITIL v3 certification

Agenda

- Why is Supply Chain Risk Management a Cybersecurity Issue?
- Evolving from Security to Resilience
- Understanding External Dependencies
- An Engineering Approach to Managing Supply Chain Risk
- Food for Thought
- Takeaways

Managing for Supply Chain Resilience

Why is Supply Chain Risk Management a Cybersecurity Issue?

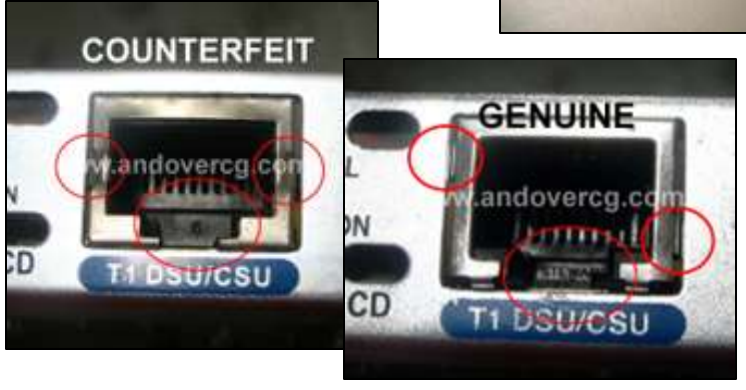
Carnegie Mellon University
Software Engineering Institute

SCRM Challenge: Growing Complexity

There are more than a dozen suppliers in a dozen nations involved in supplying just the primary airframe components needed to construct the Dreamliner. Each of these partnerships requires a level of connectivity and relies on information systems. Complex supply chains run in complex IT infrastructures.

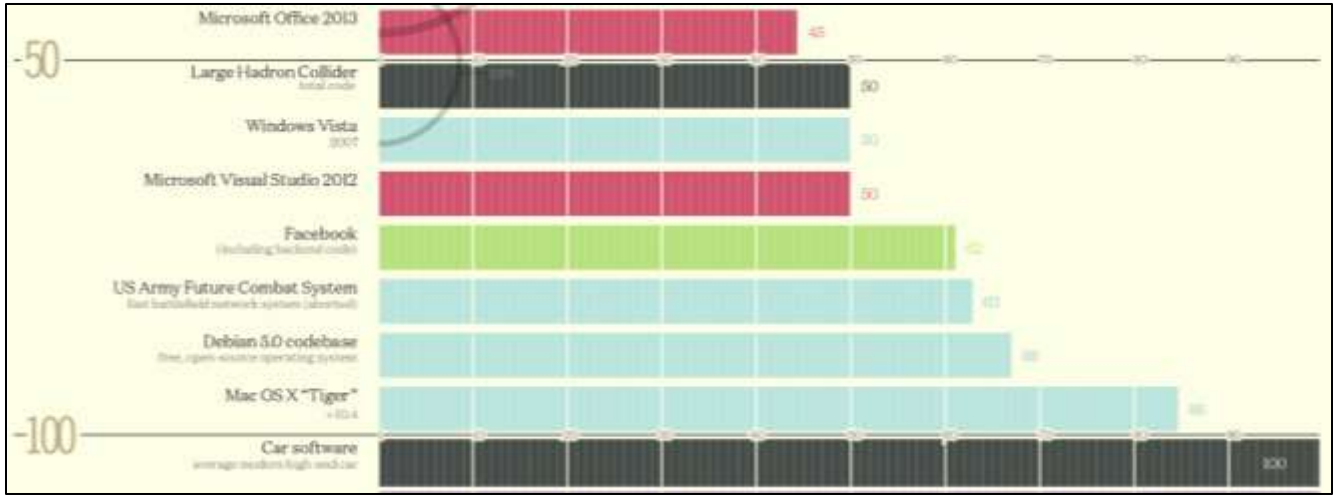
Source: www.boeing.com

SCRM Challenge: Component Provenance



The supply chain contains often **difficult-to-detect counterfeit components**

SCRM Challenge: Software is Everywhere



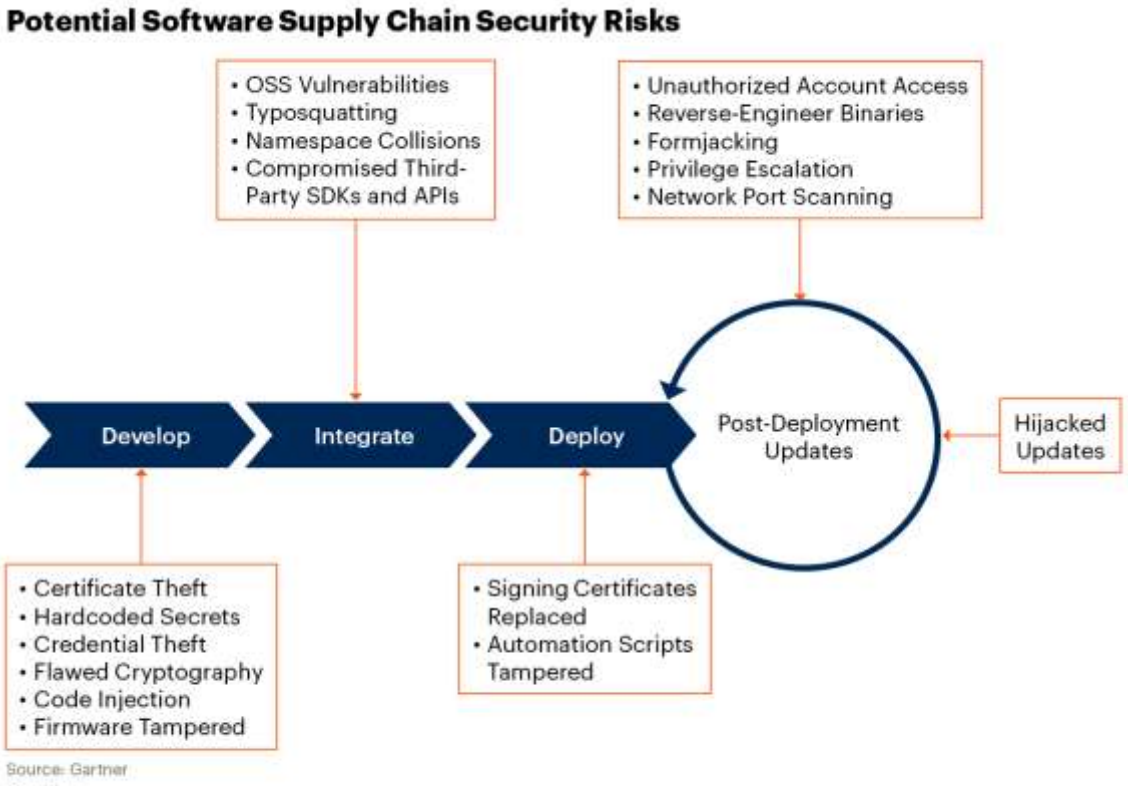
Source: https://informationisbeautiful.net/visualizations/million-lines-of-code/

"In short, software is eating the world."

Marc Andreesen, co-founder, Netscape

Software is growing in size and is being deployed on an increasing array of devices (e.g., software-defined radios)

Potential Software Supply Chain Security Risks



SCRM Challenge: Cyber-Physical Convergence

July 2017

INTERNET OF THINGS

Enhanced Assessments and Guidance Are Needed to Address Security Risks in DOD

GAO Highlights

Highlights of GAO-17-668, a report to congressional committees

Why GAO Did This Study

Congress included provisions in reports associated with two separate statutes for GAO to assess the IoT-associated security challenges faced by DOD. This report (1) addresses the extent to which DOD has identified and assessed security risks related to IoT devices, (2) assesses the extent to which DOD has developed policies and guidance related to IoT devices, and (3) describes other actions DOD has taken to address security risks related to IoT devices.

GAO reviewed reports and interviewed DOD officials to identify risks and threats of IoT devices faced by DOD. GAO also interviewed DOD officials to identify risk assessments that may address IoT devices and examined their focus areas. GAO further reviewed current policies and guidance DOD uses for IoT devices and interviewed officials to identify any gaps in policies and guidance where security risks may not be addressed.

What GAO Recommends

GAO recommends that DOD (1) conduct operations security surveys that could address IoT security risks or address operations security risks posed by IoT devices through other DOD risk assessments; and (2) review and assess its security policies and guidance affecting IoT devices and identify areas, if any, where new DOD policies may be needed or where guidance should be updated. DOD reviewed a draft of this report and concurs with GAO's recommendations.

View GAO-17-668. For more information, contact Joseph W. Kirschbaum at (202) 512-9971 or KirschbaumJ@gao.gov.

What GAO Found

The Internet of Things (IoT) is the set of Internet-capable devices, such as wearable fitness devices and smartphones, that interact with the physical environment and typically contain elements for sensing, communicating, processing, and actuating. Even as the IoT creates many benefits, it is important to acknowledge its emerging security implications. The Department of Defense (DOD) has identified numerous security risks with IoT devices and conducted some assessments that examined such security risks, such as infrastructure-related and intelligence assessments. Risks with IoT devices can generally be divided into risks with the devices themselves and risks with how they are used. For example, risks with the devices include limited encryption and a limited ability to patch or upgrade devices. Risks with how they are used—operational risks—include insider threats and unauthorized communication of information to third parties. DOD has developed IoT threat scenarios involving intelligence collection and the endangerment of senior DOD leadership—scenarios that incorporate IoT security risks (see figure). Although DOD has begun to examine security risks of IoT devices through its infrastructure-related and intelligence assessments, the department has not conducted required assessments related to the security of its operations.

Notional Internet of Things (IoT) Scenarios Identified by Department of Defense (DOD)

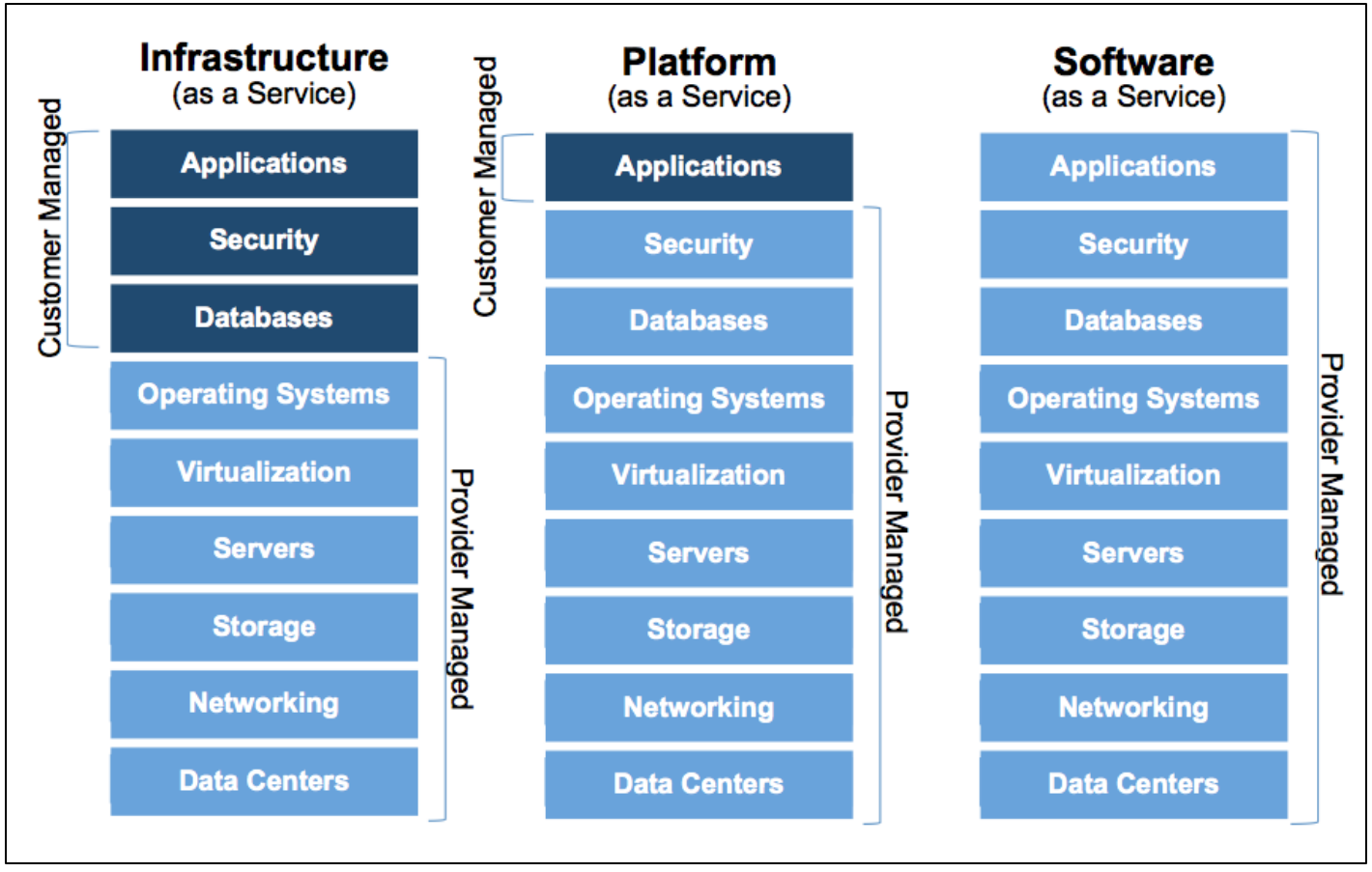
DOD has issued policies and guidance for IoT devices, including personal wearable fitness devices, portable electronic devices, smartphones, and infrastructure devices associated with industrial control systems. However, GAO found that these policies and guidance do not clearly address some security risks relating to IoT devices. First, current DOD policies and guidance are insufficient for certain DOD-acquired IoT devices, such as smart televisions in unsecure areas, and IOT device applications. Secondly, DOD policies and guidance on cybersecurity, operations security, information security, and physical security do not address IoT devices. Lastly, DOD does not have a policy directing its components to implement existing security procedures on industrial control systems—including IoT devices. Updates to DOD policies and guidance would likely enhance the safeguarding and securing of DOD information from IoT devices.

This is an unclassified version of a sensitive report GAO issued in June 2017

United States Government Accountability Office

The growth of the Internet of Things (IoT) is **outpacing** supply chain **risk management practices**

SCRM Challenge: New Service Delivery Models



The rise of **cloud** computing is rapidly altering **service delivery models**

Managing for Supply Chain Resilience

Evolving from Security to Resilience

Carnegie Mellon University
Software Engineering Institute

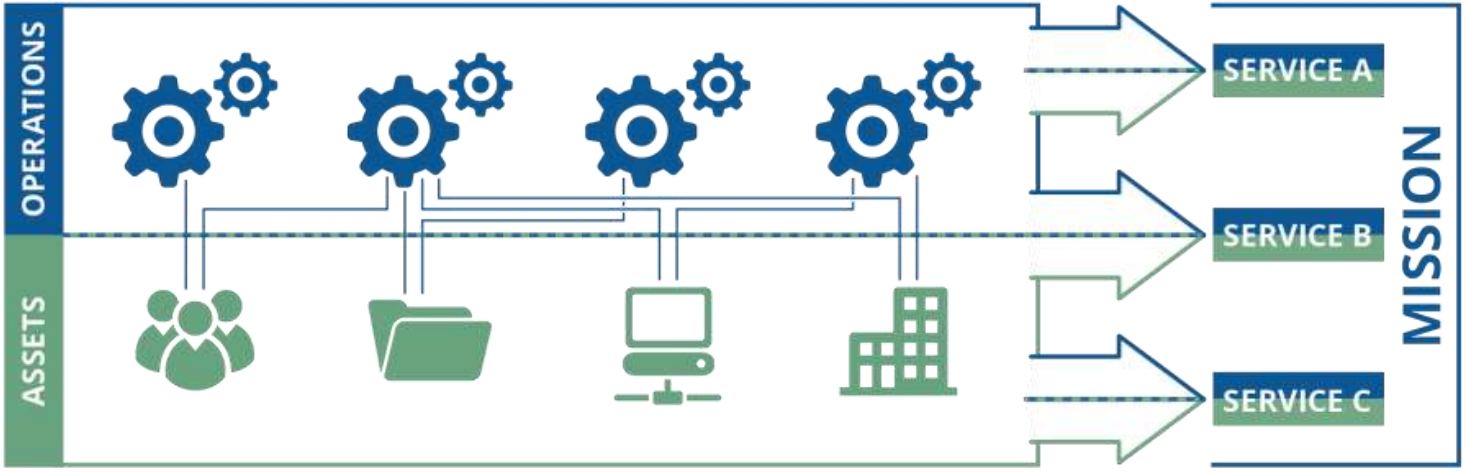
Operational Resilience Defined

Resilience: The physical property of a material when it can return to its original shape or position after deformation that does not exceed its elastic limit [wordnet.princeton.edu]

Operational resilience: The emergent property of an organization that can continue to carry out its mission after disruption that does not exceed its operational limit [CERT-RMM*]

*Carnegie Mellon University Software Engineering Institute CERT Resilience Management Model

Asset Support Services



People: those who operate and monitor the service

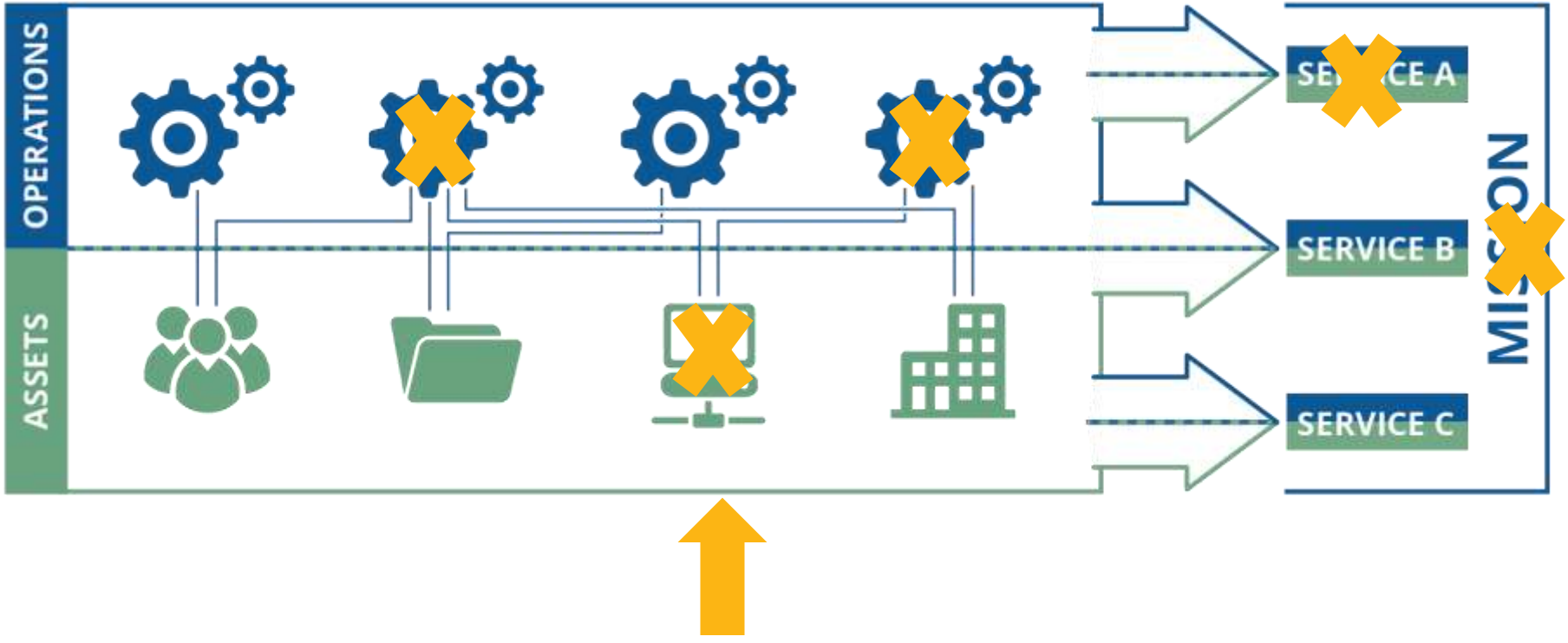
Information: data associated with the service

Technology: tools and equipment that automate and support the service

Facilities: where the service is performed

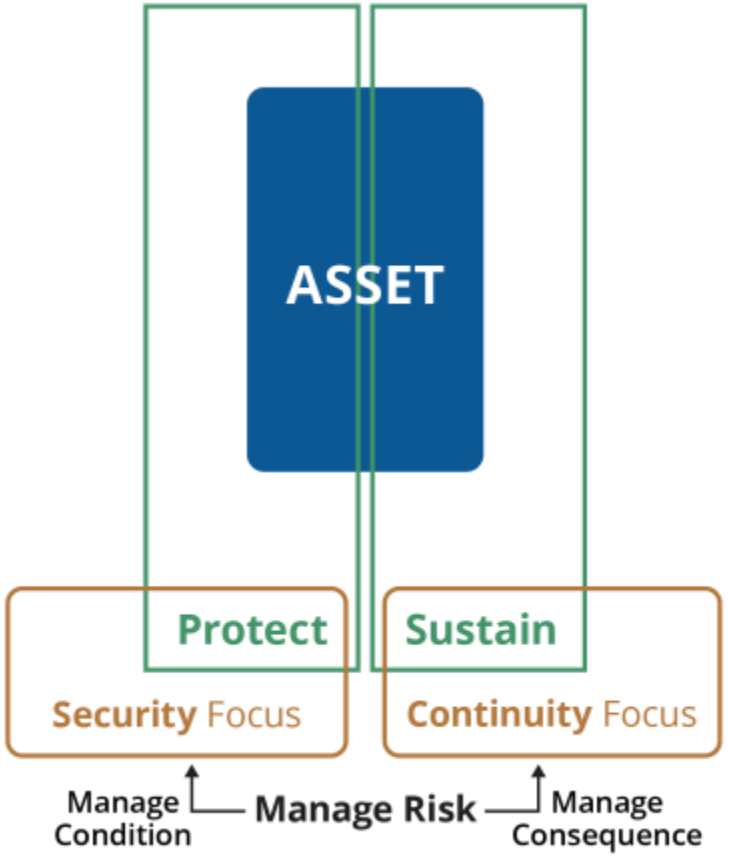
Assets derive their value from their importance in meeting the service mission, and we must understand their resilience requirements.

Disruption of Assets Can Lead to Mission Failure



Realized operational risk resulting in asset disruption

Operational Resilience Starts at the Asset Level



Ideally optimal mix of protection and sustainment strategies

Depends on the **value** of the asset to the service and the
cost of deploying and maintaining the strategy

The management challenge of operational resilience

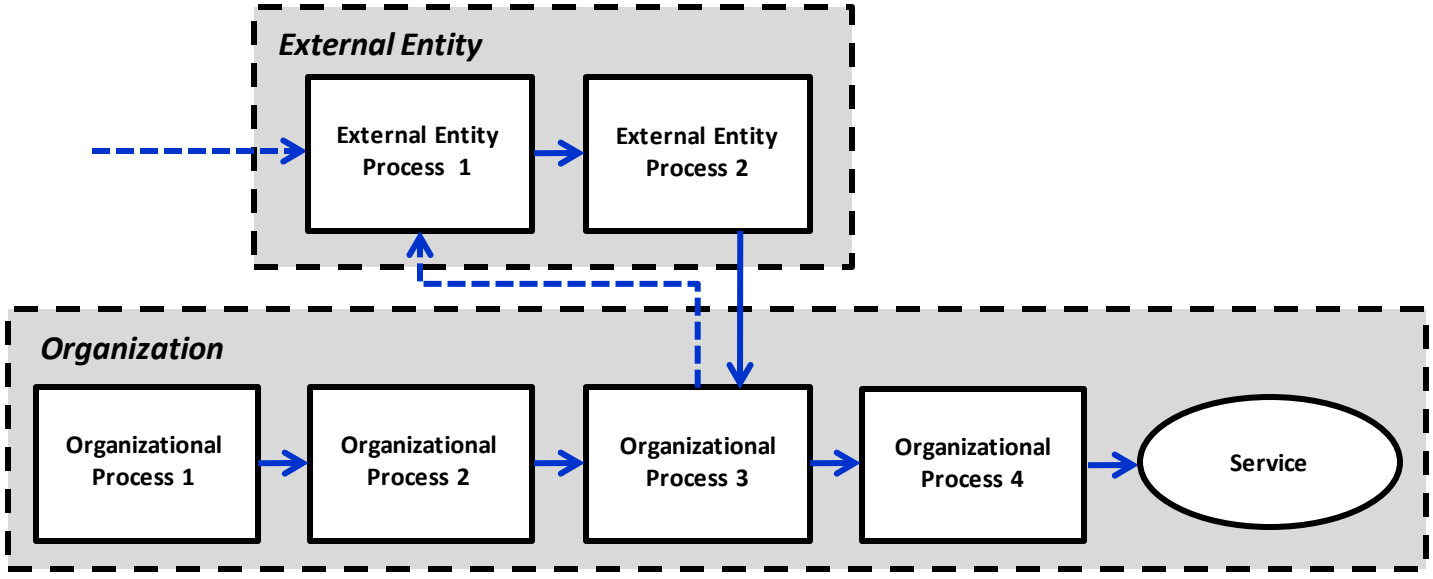
Carnegie Mellon University
Software Engineering Institute

Managing for Supply Chain Resilience

Evolving from Security to ResilienceUnderstanding External Dependencies

EXD: Defining External Dependencies

An external dependency exists when an entity that is external to the organization has access to, control of, ownership in, possession of, responsibility for (including development, operations, maintenance, or support), or other defined obligations related to one or more services or assets of the organization.



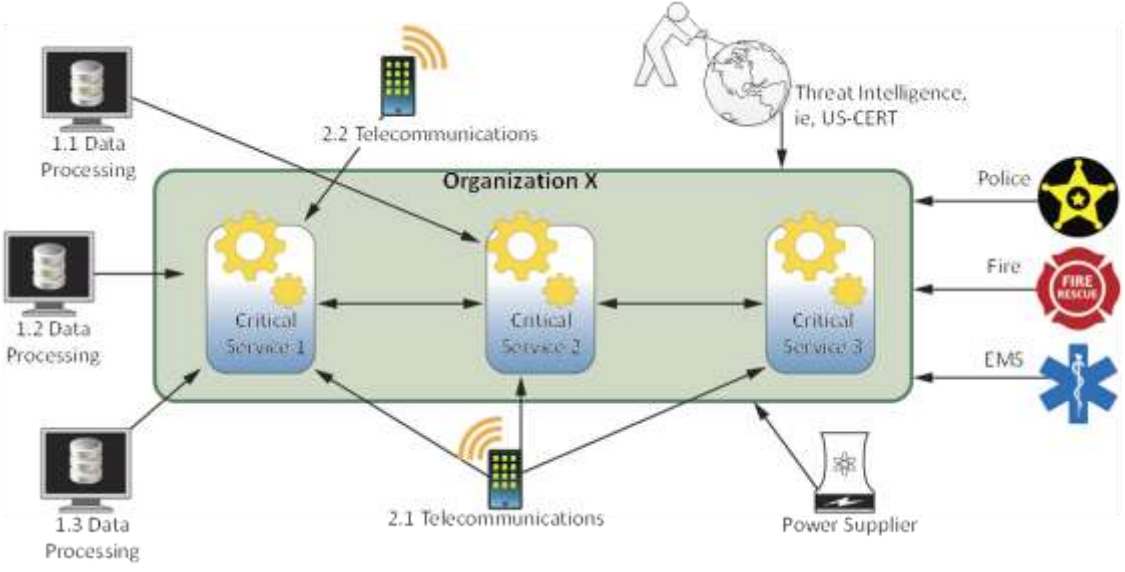
"One caveat of outsourcing is that you can outsource business functions, but you cannot outsource the risk and responsibility to a third party. These must be borne by the organization that asks the population to trust they will do the right thing…"

– Verizon Data Breach Investigations Report

EXD and Mission Achievement

Managing the risk of depending on external entities to support your organization's high value services.

External Dependency Management focuses on external entities that provide, sustain, or operate Information and Communications Technology to support your organization.



Watch Your EXD Assumptions!

- The supplier is better at security than we are
- Suppliers are flexible and accommodating
- Do we have acceptable alternatives to our current supplier(s)?
- “They’re ‘compliant,’ so we’re secure”
- “The contract terms auto-renew”
- Do not assume SBOM replaces other key cyber practices (vulnerability management, vendor risk assessment)*

* Source: NIST SP 800-161r1, “Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations”

Service Level Agreement (SLA) ITTLv2

A formal, negotiated document that defines (or attempts to define) in quantitative (and perhaps qualitative) terms the service being offered to a Customer. Confusion must be avoided over whether the quantitative definitions constitute thresholds for an acceptable service, targets to which the supplier should aspire or expectations that the supplier would strive to exceed. Any metrics included in a Service Level Agreement (SLA) should be capable of being measured on a regular basis and the SLA should record by whom. Typically, it will cover service hours and service availability. Customer support levels, throughputs and responsiveness, restrictions, functionality and the service levels to be provided in a contingency. It may also include information on security, charges and terminology.

Source: http://www.knowledgetransfer.net

Standard SLAs and Contracts

Basic reasons to have a contract (partial list)

- Risk allocation
- Drive behavior
- Define breach
- Recover damages

However, in practice Cyber SLAs can be

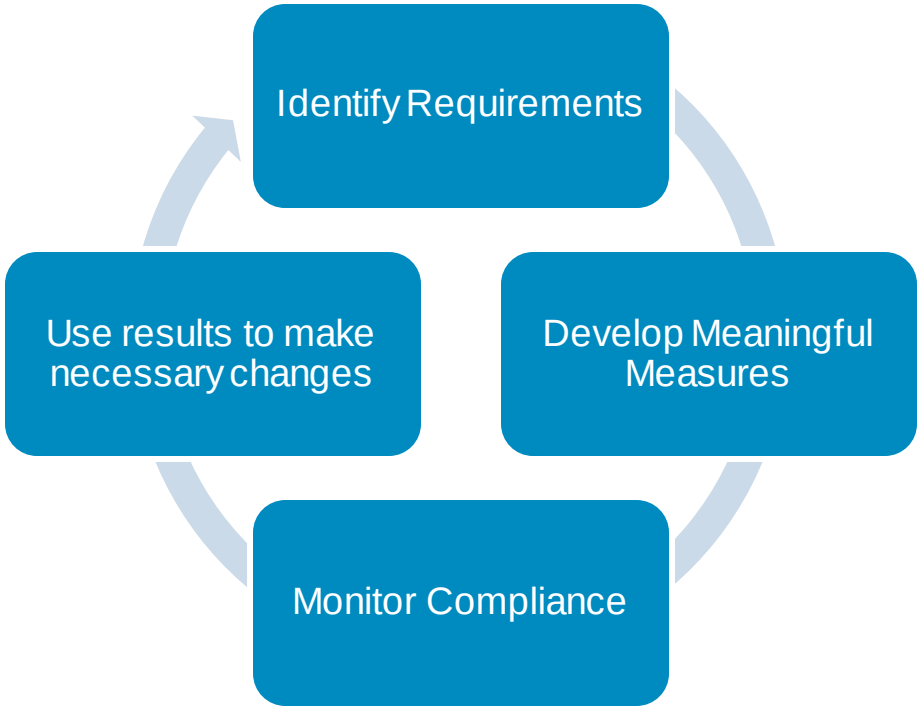
- Unidirectional (often written by the vendor, and smaller customers may have trouble negotiating or changing them)
- Lacking specific measures, apart from availability metrics
- Frequently indemnify the provider to the greatest extent possible, limiting the provider's exposure.

Managing for Supply Chain Resilience

An Engineering Approach to Managing Supply Chain Risk

Carnegie Mellon University
Software Engineering Institute

A Better Management Process: Plan, Do, Check, Act



Identify Requirements

- Create detailed service description
- Translate internal security requirements into EXD requirements

Develop Meaningful Measures

- Negotiate and agree specific SLAs

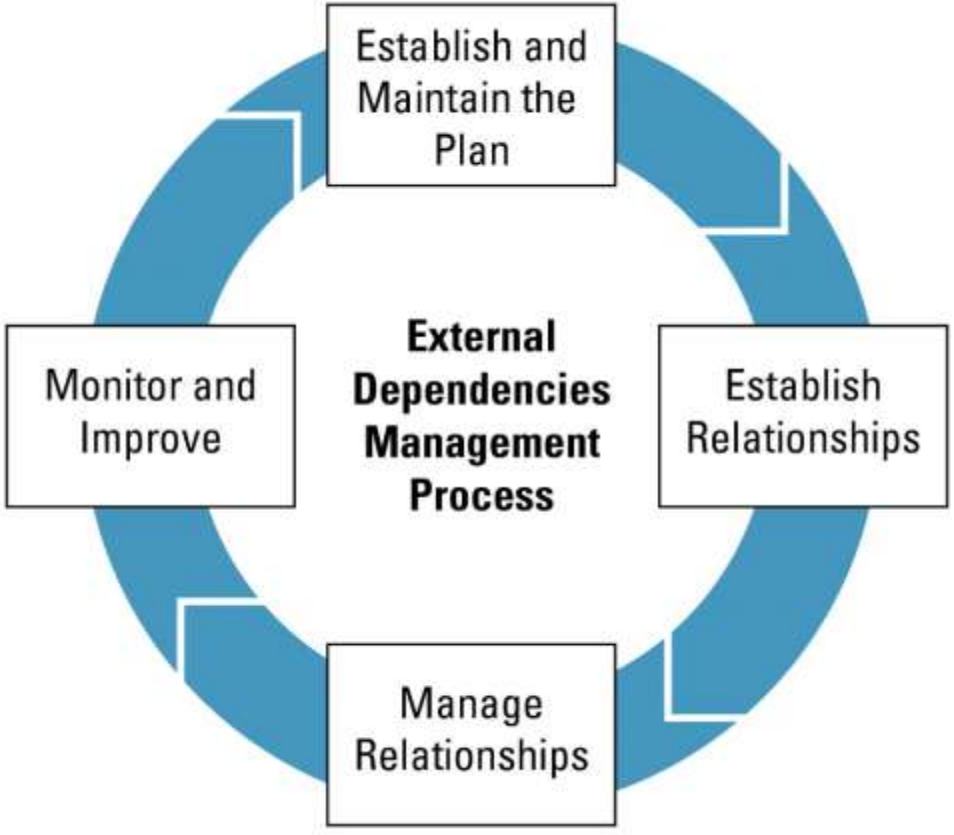
Monitor Compliance

- Independently monitor and verify provider
- Conduct periodic service reviews using SLAs
- Invoke penalties for SLA violations as required
- Conduct RCA as required on service security issues
- Manage corrective actions to resolution as specified in SLAs

Use Lessons Learned to

- Update SLAs
- Ensure relationships continue to meet your business needs

External Dependency Management Program



Key Goals

- Identify program objectives
- Identify Critical Services
- Prioritize Critical Services
- Identify enterprise and service resilience requirements
- Plan relationship formation and management

Managing for Supply Chain Resilience

Food for Thought

Carnegie Mellon University
Software Engineering Institute

Consider a Cyber Resilience Assessment (CRA) – 1

Carnegie Mellon University Software Engineering Institute

The CRA is a single-day assessment of an organization's cyber resilience practices, based on the CERT® Resilience Management Model (CERT® RMM), a process improvement model for managing operational resilience.

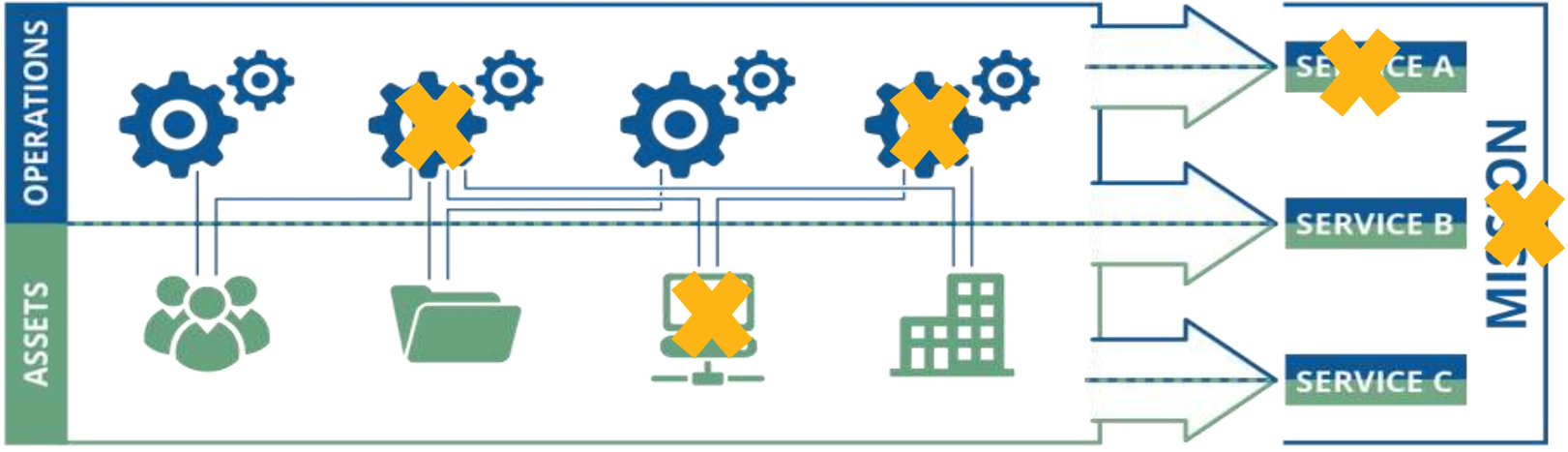
It examines key practices of an organization's cyber security program to

- Understand how well the organization manages cybersecurity risk by protecting and sustaining critical services
- Provide a resource-efficient roadmap for cybersecurity risk management and improvement informed by leading security practices
- Measure the process stability and maturity to produce consistent results over time, foster efficiencies and confidence, and integrate with overall enterprise risk management

Consider a Cyber Resilience Assessment (CRA) – 2

It is **not** a technical assessment or controls audit

It uses a service-oriented approach, focusing on a critical service identified by the organization. Critical services are sets of activities sufficiently critical that their disruption would severely impact continued operations or harm the organization's mission



The CRA Domains: What's Covered

Carnegie Mellon University Software Engineering Institute

- The ten domains in the CRA represent important areas that contribute to the cyber resilience of an organization
- The domains focus on **practices** an organization should have in place to assure the **protection and sustainment** of its critical services
- 42 goals, 169 cyber management practices
- Maturity Indicator Level (MILs) questions are also asked to nominally indicate process maturity
- Higher MIL scores generally translate to more stable processes that
  - produce predictable results over time and
  - are retained during times of stress (i.e., more resilient)

CRA Domains	
AM	Asset Management
CM	Controls Management
CCM	Configuration and Change Management
VM	Vulnerability Management
IM	Incident Management
SCM	Service Continuity Management
RM	Risk Management
EDM	External Dependencies Management
TA	Training and Awareness
SA	Situational Awareness

CRA Benefits

Carnegie Mellon University Software Engineering Institute

Provides an organization with a more robust awareness of its cybersecurity posture:

- Reviews the capabilities essential to managing disruptions of critical services during operational challenges and crisis
- Identifies areas for improvement to strengthen dependency cyber risk management and resilience
- Provides insight into an organization's supplier oversight and cybersecurity management practices
- Improves enterprise-wide awareness of the need for effective external dependency management
- Strengthens the organization's cybersecurity posture in support of its mission
- Provides a comprehensive final report that includes options for improvement

Snapshot of Example CRA Report

CRA Performance Summary

Domain Summary	MIL-1 Performed Domain practices are being performed.	MIL-2 Planned: Domain practices are supported by planning, policy, stakeholders, and standards.	MIL-3 Managed: Domain practices are supported by governance and adequate resources.	MIL-4 Measured: Domain practices are supported by measurement, monitoring, and executive oversight.	MIL-5 Defined: Domain practices are supported by enterprise standardization and analysis of lessons learned.
Asset Management	G1 G2 G3 G4 G5 G6 G7	Q1 Q2 Q3 Q4	Q1 Q2 Q3 Q4	Q1 Q2 Q3	Q1 Q2
Controls Management	G1 G2 G3 G4	Q1 Q2 Q3 Q4	Q1 Q2 Q3 Q4	Q1 Q2 Q3	Q1 Q2
Configuration and Change Management	G1 G2 G3	Q1 Q2 Q3 Q4	Q1 Q2 Q3 Q4	Q1 Q2 Q3	Q1 Q2
Vulnerability Management	G1 G2 G3 G4	Q1 Q2 Q3 Q4	Q1 Q2 Q3 Q4	Q1 Q2 Q3	Q1 Q2

Takeaways

- Supply chains are clearly becoming increasingly complex and cyber-dependent
- Understanding your critical services and the extent to which they depend on assets and external providers is essential
- Managing supply chain risks from external dependencies must be a key component of an organization's overall security strategy
- Supply chain risks are best addressed by adopting a resilience management approach
- Establish and manage appropriate processes to ensure the resilience of services dependent on the actions of external entities
- Question and keep your assumptions about your supply chain in check—trust but verify
- SLAs can be leveraged to start the discussion
- Consider tools like the Cyber Resilience Assessment to help you understand your resilience practices and relative 'maturity' level

Thank You

Visit the SEI website **https://www.sei.cmu.edu/**

My contact Information

Dan Kambic
Telephone 412 268 9164
Email djkambic@cert.org