

Risk Management: Supply Chain Audit

Managing risk to minimize organization disruption
Thursday, February 17, 2022

Ron Woerner, CISSP, CISM



RON WOERNER

- >20 years of IT and security experience
- President and Chief Security Evangelist at Cyber-AAA
- Noted educator, consultant, keynote speaker and writer in the security industry
- Established the Cybersecurity Studies program at Bellevue University
- CISSP and CISM certified

Linktr.ee: <https://linktr.ee/cyberron>

Supply Chain Risk Management (SCRM)
Cyber Supply Chain Risk Management (C-SCRM)
Third-Party Risk Management (TPRM)



Hackers leak 190GB of alleged Samsung data, source code

By [Ionut Ilascu](#)

March 4, 2022 05:15 PM

2



<https://www.bleepingcomputer.com/news/security/hackers-leak-190gb-of-alleged-samsung-data-source-code/>



Source: <https://www.enisa.europa.eu/news/enisa-news/understanding-the-increase-in-supply-chain-security-attacks>

Supply Chain Key Elements

- **Supplier:** is an entity that supplies a product or service to another entity.
- **Supplier Assets:** are valuable elements used by the supplier to produce the product or service.
- **Customer:** is the entity that consumes the product or service produced by the supplier.
- **Customer Assets:** are valuable elements owned by the target.

A supply chain attack is a combination of at least two attacks.

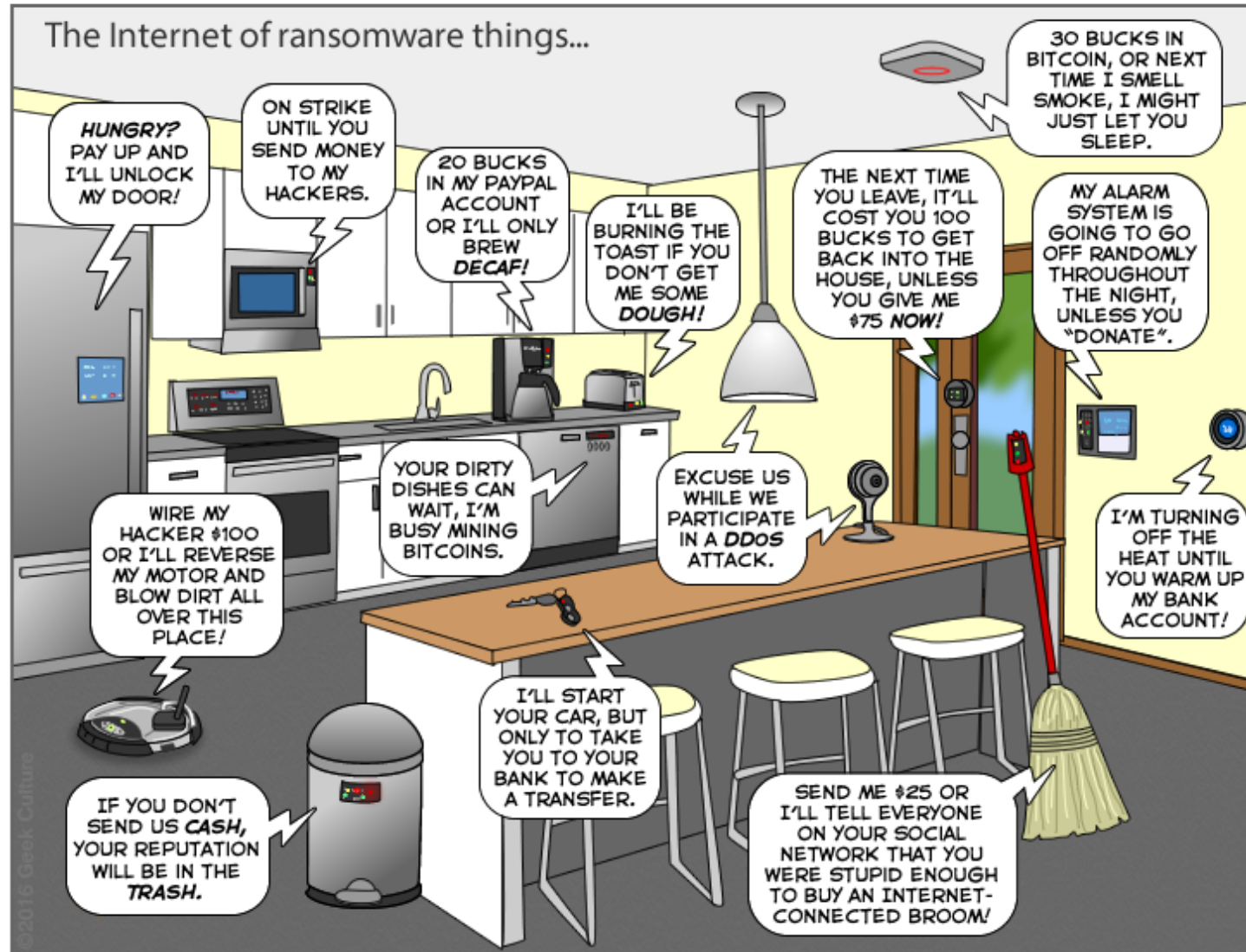
ENISA Taxonomy for Supply Chain Attacks

SUPPLIER		CUSTOMER	
Attack Techniques Used to Compromise the Supply Chain	Supplier Assets Targeted by the Supply Chain Attack	Attack Techniques Used to Compromise the Customer	Customer Assets Targeted by the Supply Chain Attack
Malware Infection	Pre-existing Software	Trusted Relationship [T1199]	Data
Social Engineering	Software Libraries	Drive-by Compromise [T1189]	Personal Data
Brute-Force Attack	Code	Phishing [T1566]	Intellectual Property
Exploiting Software Vulnerability	Configurations	Malware Infection	Software
Exploiting Configuration Vulnerability	Data	Physical Attack or Modification	Processes
Open-Source Intelligence (OSINT)	Processes	Counterfeiting	Bandwidth
	Hardware		Financial
	People		People
	Supplier		

© European Union Agency for Cybersecurity (ENISA), 2021

Cyber Supply Chain Risks – Shadow IT and IoT

The Joy of Tech™ by Nitrozac & Snaggy



You can help us keep the comics coming by becoming a patron!
www.patreon/joyoftech

joyoftech.com

Key Cyber Supply Chain Risks

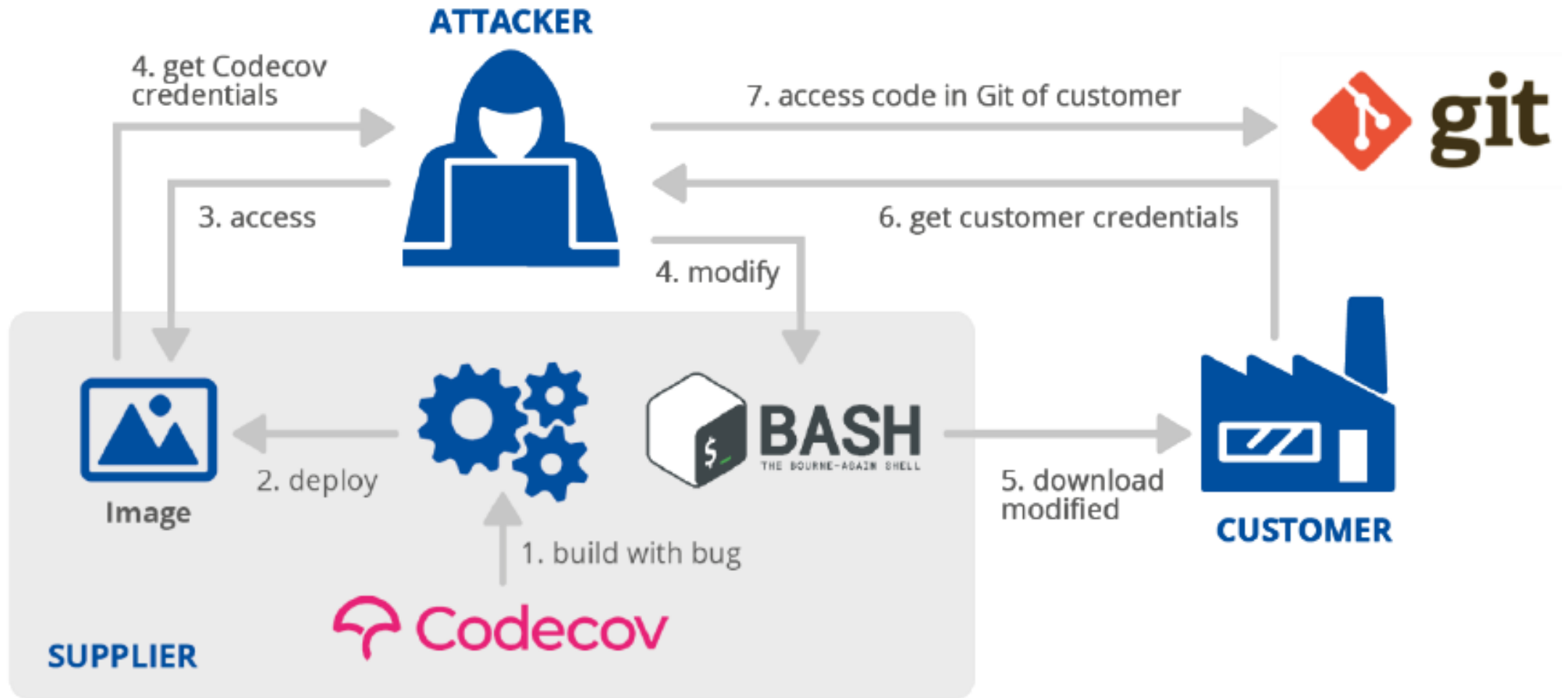
What keeps you up at night?

- Third party service providers or vendors
- Poor information security practices by lower-tier suppliers.
- Compromised software or hardware purchased from suppliers.
- Software security vulnerabilities in supply chain management or supplier systems.
- Counterfeit hardware or hardware with embedded malware.
- Third party data storage or data aggregators.

Example: Apache Log4j Vulnerability

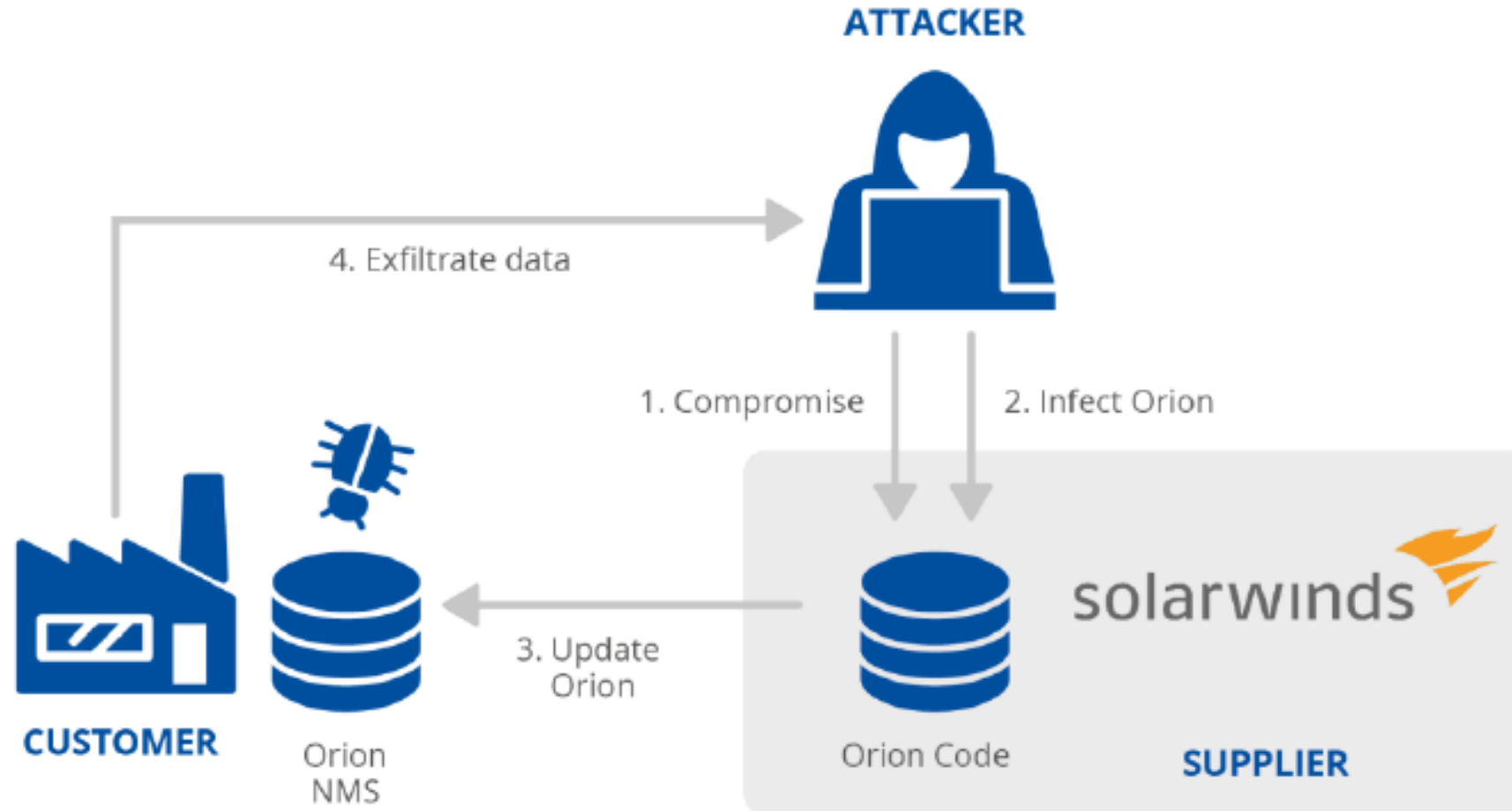
- Common Java software library for logging
- Critical remote code execution (RCE) vulnerability ([CVE-2021-44228](#))
- Log4Shell Exploit
- CISA Guidance: <https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance>
- Apache's [Log4j Security Vulnerabilities page](#)
- FR Secure CVE-2021-44228: Log4j Vulnerability Blog: <https://frsecure.com/blog/cve-2021-44228>
Uses <https://log4shell.huntress.com/>

Codecov Compromise



© European Union Agency for Cybersecurity (ENISA), 2021

SolarWinds Compromise



© European Union Agency for Cybersecurity (ENISA), 2021

Supply Chain Attacks

■ Supplier Attack Techniques

- ◆ Unknown – 66%
- ◆ Exploiting Software Vulnerabilities – 16%

■ Assets Targeted

- ◆ Code – 66%
- ◆ Data – 20%
- ◆ Processes – 12%

■ Customer Attack Techniques

- ◆ Abusing the trust of the customer in the supplier – 62%
- ◆ Malware – 62%

■ Goal of gaining access to:

- ◆ Customer Data – 58%
- ◆ Key People – 16%
- ◆ Financial Resources – 8%

Need for Cyber Supply Chain Risk Management



Supply Chain Management Processes

SC processes identified by The Global Supply Chain Forum:

- Customer Relationship Management
- Supplier Relationship Management
- Customer Service Management
- Demand Management
- Order Fulfillment
- Manufacturing Flow Management
- Product Development and Commercialization
- Returns Management

The Supply Chain Management Processes
Keely L. Croxton, Sebastián J. García-Dastugue,
Douglas M. Lambert, Dale S. Rogers
The International Journal of Logistics Management
ISSN: 0957-4093
Article publication date: 1 July 2001

Cyber Supply Chain Security Principles

- Assume breach when developing defenses
- Security is a **people, process and technology** problem
- Security is Security. Physical and Cyber

- Zero Trust
- Least privilege
- Fail-safe defaults

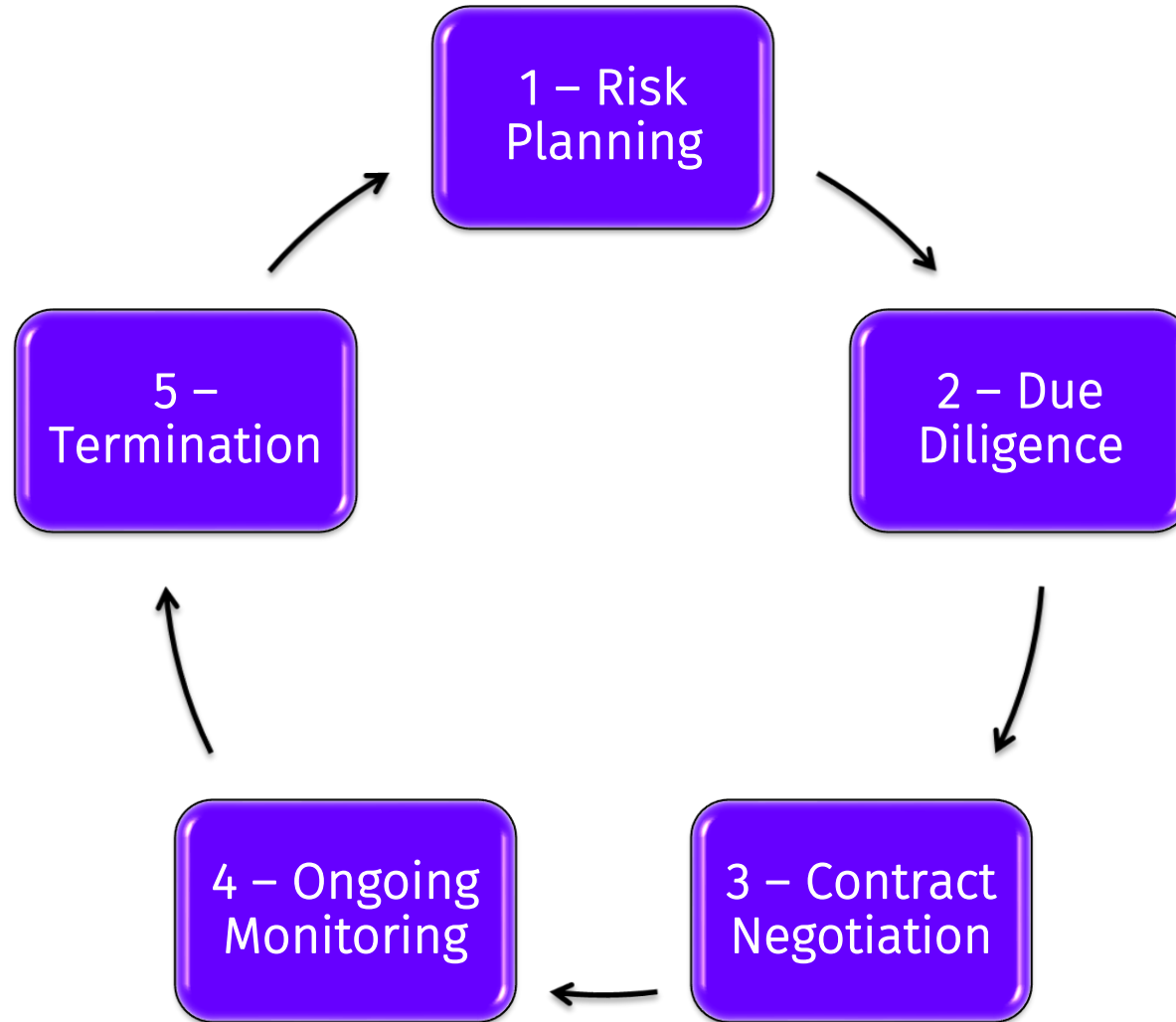
ICT SCRM Program Basics

- Identify the people & functions
- Manage security & compliance
- Assess the components (hardware, software, services)
- Know your suppliers (and their suppliers)
- Verify assurance of third-parties
- Evaluate your SCRM program

Source:

https://www.cisa.gov/sites/default/files/publications/ict_scrm_essentials_508.pdf

Third Party Risk Management Framework



C-SCRM Key Practices

1. Integrate C-SCRM Across the Organization
2. Establish a Formal C-SCRM Program
3. Understand the Organization's Supply Chain
4. Know, Manage, and Collaborate with Critical Suppliers
5. Include Key Suppliers in Resilience and Improvement Activities
6. Assess and Monitor Throughout the Supplier Relationship
7. Plan for the Full Life Cycle

Source: NISTIR 8276, Key Practices in Cyber Supply Chain Risk Management: Observations from Industry, <https://doi.org/10.6028/NIST.IR.8276>

Monitoring Supply Chain Cyber Security

A supplier assessment conducted prior to bringing a supplier on board is a snapshot in time that becomes obsolete before it is completed.

NISTIR 8276, p. 11

- Establish continual supplier-monitoring programs
- Cover entire supplier relationship life-cycle
- Monitor a variety of supplier risks (not just cyber / technical)

Monitoring Supply Chain Cyber Security

Assessment / Monitoring Mechanisms

- Supplier attestation
- Self-assessment
- Third-party assessments
- Formal certifications
 - SOC2
 - FedRAMP
- Site visits

Assessing / Auditing Supply Chain Cyber Security



Common Criteria for Frameworks

- Privacy and Security Program Management
 - ◆ Physical / environmental
 - ◆ Data / network / systems
 - ◆ Related Standard Operating Procedures (SOPs)
 - ◆ Users access / authorization
 - ◆ Information sharing and transmission
- Data and information governance and risk management
 - ◆ Security and privacy policies
 - ◆ Data retention and disposal
- Supplier contractual agreements
- Education, awareness and training

Assessing SCRM / ITRM – NIST CSF



<https://www.nist.gov/cyberframework>

CIS Controls



The Cloud Security Alliance Cloud Controls Matrix (CSA CCM)

- Provides fundamental security principles to be used to assess the overall security risk of a cloud provider
 - Guide for cloud vendors
 - Assists prospective cloud customers
- CCM is not a mandated industry standard
- CCM is a framework for governance, risk management and compliance security controls tailored to the cloud industry

- Cloud Security Alliance: <https://cloudsecurityalliance.org/>
- CSA CCM: <https://cloudsecurityalliance.org/research/cloud-controls-matrix/>
- Cloud Security Posture Management (CSPM): <https://github.com/opencspm/opencspm>

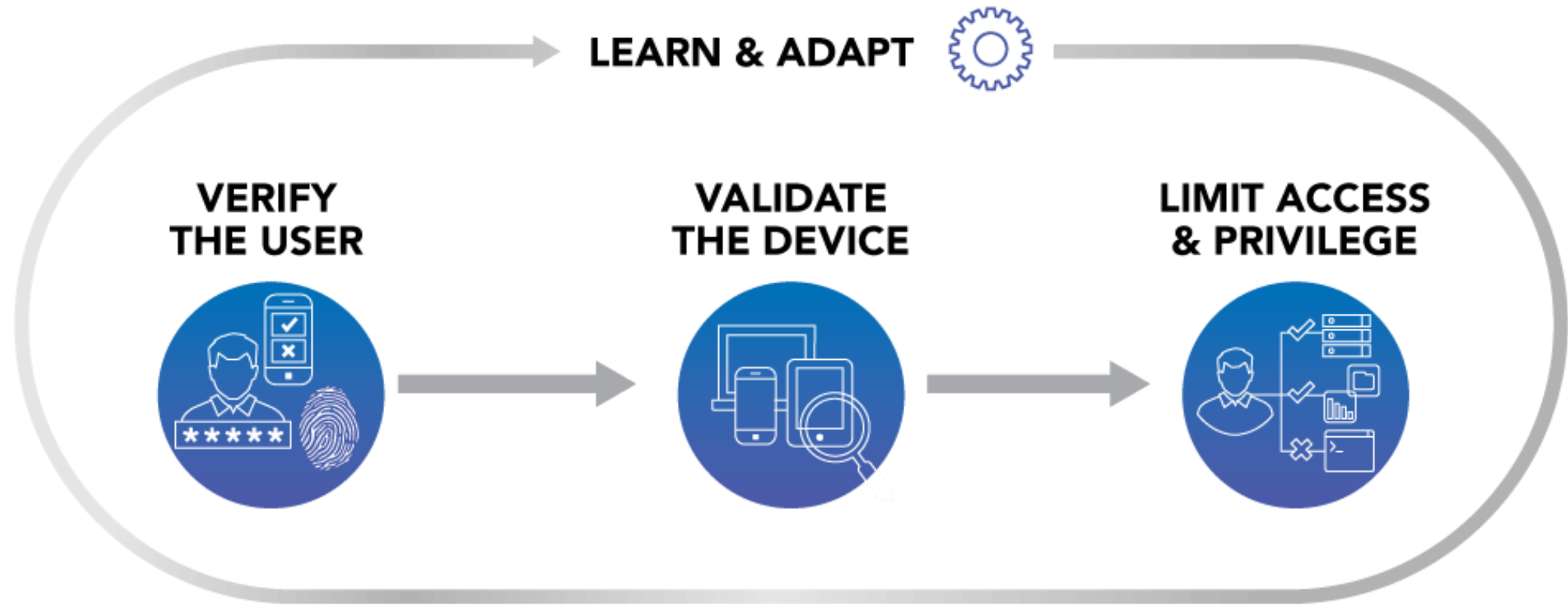
Common Vendor Security Compliance templates

- Vendor Security Alliance (VSA):
<https://www.vendorsecurityalliance.org/> (Free)
- HITRUST Alliance Cyber Security Framework (CSF):
<https://hitrustalliance.net/product-tool/hitrust-csf/> (Licensed)
- Shared Assessments, Standardized Information Gathering (SIG) Questionnaire: <https://sharedassessments.org/sig/> (Purchase)

Cyber Supply Chain Best Practices

- Security requirements are included in every RFP and contract
- Component purchases are tightly controlled
- Source code is available or certified for all purchased software
- Legacy systems and support
- Access control for service vendors

Zero Trust Architecture



Software Bill of Materials (SBOM)

SOFTWARE BILL OF MATERIALS

A “Software Bill of Materials” (SBOM) is a nested inventory for software, a list of ingredients that make up software components. The following documents were drafted by stakeholders in an open and transparent process to address transparency around software components, and were approved by a consensus of participating stakeholders. More information about the NTIA multistakeholder process on software component transparency is available [here](#).

Introduction to SBOM

[SBOM at a Glance \(2021\)](#)

This resource provides an introduction to the practice of SBOM, supporting literature, and the pivotal role SBOMs play in providing much-needed transparency for the software supply chain. ([Japanese translation](#))

[SBOM FAQ \(2021\)](#)

This document outlines detailed information, benefits, and commonly asked questions.

[SBOM Myths vs. Facts \(2021\)](#)

This document is intended to help the reader to understand and dispel common, often sincere myths and misconceptions about SBOM.

[SBOM Explainer Videos on YouTube \(2020-2021\)](#)

This collection of videos provides a wide range of information about SBOM including introductory concepts, technical webinars, and proof of concept presentations.

<https://www.ntia.gov/SBOM>

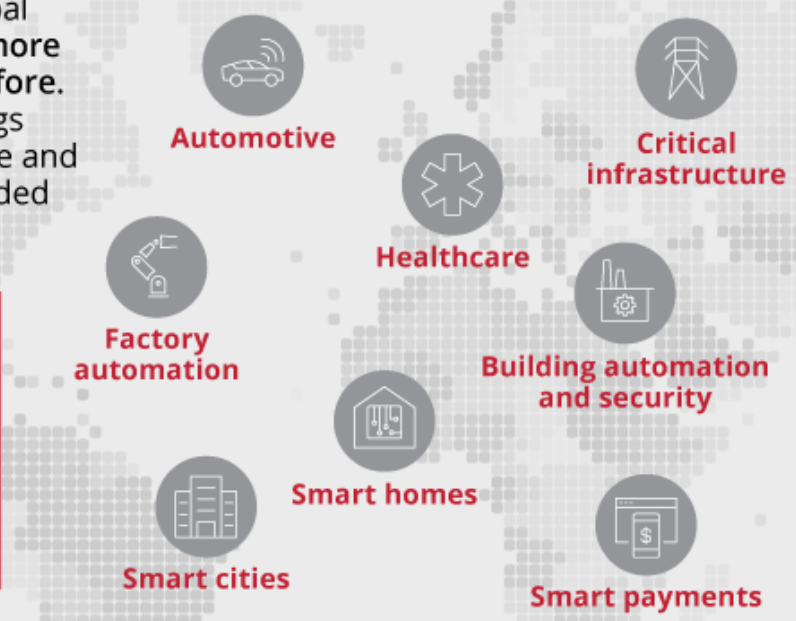
Underwriters Laboratory - Cyber

The world continues to connect on trust

Navigating today's global market is riskier and more complex than ever before. As the Internet of Things becomes more intricate and complex, it leads to added security vulnerabilities.

40 billion
CONNECTED
devices by 2027

Business Insider, "The Internet of Things 2020", March 2020.



- Automotive
- Critical infrastructure
- Healthcare
- Factory automation
- Building automation and security
- Smart homes
- Smart cities
- Smart payments

UL has deep cybersecurity expertise to help companies across the various ecosystems successfully implement cybersecurity into their products, systems and processes.

- A global network of IoT and OT security laboratories
- Over 500 security experts and advisors
- Specialized expertise in global security standards, frameworks and best practices

<https://www.ul.com/services/solutions/cybersecurity>

<https://www.ul.com/services/solutions/supply-chain-and-product-stewardship>

<https://www.ul.com/services/iot-device-security>

Supply Chain Risk Management (SCRM)
Cyber Supply Chain Risk Management (C-SCRM)
Third-Party Risk Management (TPRM)



Resources

- NIST, NISTIR 8276, Key Practices in Cyber Supply Chain Risk Management: Observations from Industry, <https://doi.org/10.6028/NIST.IR.8276>
- NIST, Best Practices in Cyber Supply Chain Risk Management: <https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-Supply-Chain-Best-Practices.pdf>
- NIST SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations, <https://csrc.nist.gov/publications/detail/sp/800-161/final>
- CISA Supply Chain: <https://www.cisa.gov/supply-chain>
- Vendor Security Alliance: <https://www.vendorsecurityalliance.org/>

RON WOERNER

- >20 years of IT and security experience
- President and Chief Security Evangelist at Cyber-AAA
- Noted educator, consultant, keynote speaker and writer in the security industry
- Established the Cybersecurity Studies program at Bellevue University
- CISSP and CISM certified

Linktr.ee: <https://linktr.ee/cyberron>
<https://www.linkedin.com/in/ronwoerner/>