CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

INFORMATION AND COMMUNICATIONS TECHNOLOGY SUPPLY CHAIN RISK MANAGEMENT TASK FORCE

Threat Evaluation Working Group: Supplier, Products, and Services Threat Evaluation (to include Impact Analysis and Mitigation)

Version 3.0

July 2021

This page is intentionally left blank.

Executive Summary

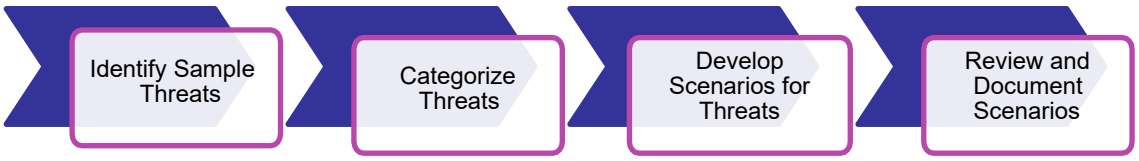
This latest report from the Threat Evaluation Working Group adds the assessment of Products and Services to include impacts and mitigating controls to each of the Supplier Threat Scenarios provided in the original version released in February 2020, and later augmented with impacts and mitigating controls in October 2020. These additional sections are included in Appendix C, Threat Scenarios, of this report. The Working Group (WG) chose to include these updates as a standalone report to benefit the audience without the need to include numerous references to the original reports.

Cyber Supply Chain Risk Management (C-SCRM) is the process of identifying, assessing, preventing, and mitigating the risks associated with the distributed and interconnected nature of Information and Communications Technology (ICT) (including the Internet of Things [IoT]) product and service supply chains. C-SCRM covers the entire life cycle of ICT, and encompasses hardware, software, and information assurance, along with traditional supply chain management and supply chain security considerations.

In October 2018, the Cybersecurity and Infrastructure Security Agency (CISA) launched the ICT Supply Chain Risk Management Task Force, a public-private partnership to provide advice and recommendations to CISA and its stakeholders on means for assessing and managing risks associated with the ICT supply chain. Working Group 2 (WG2), Threat Evaluation, was established for the purpose of the identification of processes and criteria for threat-based evaluation of ICT suppliers, products, and services.

WG2 focused on threat evaluation as opposed to the more comprehensive task of risk assessment, which considers threats as well as an organization's tolerance for risk, the criticality of the specific asset or business/mission purpose, and the impact of exploitation of specific vulnerabilities that might be exploited by an external threat. The WG Co-Chairs leveraged the National Institute of Standards and Technology (NIST) Risk Management Practices described in NIST SP 800-161 published in April 2015 to help guide the analysis of the threats, threat sources, and mitigating controls identified in this work effort.

The general steps depicted in the figure below, and described in the following paragraphs, were used in the development and analysis of Supply Chain Risk Management (SCRM) threats related to ICT suppliers, products, and services:



The threat evaluation work was phased over the charter of the ICT SCRM Task Force to provide interim deliverables compiled by the WG2 membership. Each phased deliverable is a standalone report that builds upon the effort of the previous phases. This notional versioning of the work product is captured in the Table of Revisions (following the Table of Contents) that describes the scope of each specific phased report work product.

The initial version delivered at the end of Phase 1 and published in February 2020 focused specifically on suppliers only. The WG membership were asked to identify a representative sample of the top SCRM threats specifically focused on suppliers in accordance with our initial proposed scoping. Once the threats were identified, the WG proceeded to compile additional information fields identified in NIST SP 800-161 as elements to capture and refine with the WG members.

Each of the identified threats was then reviewed by the WG to develop a proposed set of common groupings and category assignments to organize the identified threats. Based on the presentation and analysis of the threats submitted by the WG members, the threats were aggregated into a smaller, more manageable set of common "threat grouping" to aid in the evaluation process. The

objective of the aggregation was to consolidate the threat data and identify common elements for further evaluation using a scenario development process.

This grouping and descriptive titles were shared with the WG membership for review and comment. While consensus was not unanimous, it was determined that for the purposes of the evaluation scope, the list of nine categories represented a reasonable model for aggregation for this interim work product. These threat groupings served to guide the development of scenarios intended to provide insights into the processes and criteria for conducting supplier threat assessment.

For each category, the WG assembled teams to develop a narrative/scenario in a report format that included background information on the threat itself, the importance of this threat, and potential impact on the supply chain. Multiple scenarios were developed for each category if deemed appropriate by the writing teams. A common format was developed to ensure that each threat scenario presented a comprehensive view of the specific threat aligned to the requirements of the information fields identified from NIST SP 800-161.

For the next revision to the original delivered report (Version 2.0 delivered in October 2020), the WG membership revised the supplier scenarios to include scenario specific impacts. The scenarios were also edited to include potential threat mitigating strategies and possible SCRM controls to reduce these threat impacts.

In this latest release of the Threat Scenarios Report, the WG has repeated the threat evaluation methodology developed to assess threats and impacts to Products and Services in the supply chain. The first step in this process was to arrive at a consensus on the definition and scope of Products and Services. Following this step, the WG assessed the applicability of the original nine threat groupings to Product and Services threats. The WG also considered if there were additional threat groupings that might need to be added specific to Products and Services. In the end, the WG concluded that the categories of threats from earlier versions of the report were very much applicable, and that no additional groupings were needed to conduct a thorough evaluation. The final step in the process was to generate Products and Services scenarios to include impacts and mitigating controls. This version integrates the Products and Services scenarios into Appendix C, which is ordered by Threat Groups.

The objective of this work effort is to provide a practical, example-based guidance on Supplier SCRM threat analysis and evaluation that can be applied by procurement or source selection officials in government and industry to assess supply chain risks and develop practices/procedures to manage the potential impact of these threats. The process and resulting narratives not only serve as a baseline evaluation of specific SCRM threats, but further can be used as exemplary guidance on the application of the NIST Risk Management Framework. This process can be extended for evaluation of products and services, as well as replicated for other critical infrastructure providers. It also established a solid threat source evaluation that can be extended for specific products or services to drive the evaluation of supply chain risk.

This page is intentionally left blank.

Contents

FIGURES

TABLES

TABLE OF REVISIONS

VERSION	DATE	SCOPE
Original	February 2020	Supplier Threat Evaluation
Version 2.0	October 2020	Supplier Threat Evaluation to include Impact Analysis and Mitigation
Version 3.0	July 2021	Supplier, Products, and Services Threat Evaluation to include Impact Analysis and Mitigation

1.0 THREAT EVALUATION WORKING GROUP TEAM MEMBERS

Leadership team for WG:

TABLE 1—LEADERSHIP AND ADMINISTRATIVE SUPPORT FOR WORKING GROUP 2

POSITION	NAME	COMPANY
Co-Chair:	Drew Morin	T-Mobile
	Tommy Gardner	HP
	Angela Smith	GSA
Project Manager:	Julian Humble	DHS (SED)
Admin Support:	James Alvarez	Contract Support (SED)
	Aleida Baumgartner	Contract Support (NRMC)
	Jaime Fleece	Contract Support (SED)
	Donna Grace Moleta	Contract Support (NRMC)

WG consists of the members listed below:

TABLE 2—COMMUNICATIONS SECTOR WORKING GROUP MEMBERS

NAME	COMPANY
Rich Mosely, Jeff Huegel, Jon Gannon	AT&T
Chris Boyer, Brad Tonnesen	AT&T
Kathryn Condello, John Hayat, Fernando Boza	Lumen
David Mazzocchi, Dwight Steiner, Melissa Brocato-Bryant	Lumen
Savannah Schaefer	CompTIA
Stephen Boggs	Cox
Rob Cantu	CTIA
Mike Kelley	E.W. Scripps Company
Eric Neel	Hubbard Broadcasting
Michael Iwanoff	Iconectiv
Larry Walke, Kelly Williams	National Association of Broadcasters
Matt Tooley, Jesse Ward	NCTA
Shamlan Siddiqi	NTT
Chad Kliewer	Pioneer

NAME	COMPANY
Mike Funk	Quincy Media
Brad Minnis	Juniper
Tanya Kumar, Greg Holzapfel	T-Mobile
Chris Oatway	Verizon
Robert Mayer, Michael Saperstein	U.S. Telecom
Mike Kelley	Scripps

TABLE 3—INFORMATION TECHNOLOGY SECTOR WORKING GROUP MEMBERS

NAME	COMPANY
Tom Topping	FireEye
Robert Wharton, CJ Coppersmith, Jon Green	HPE
Mark Kelly, Melissa Bouilly, Jon Amis, Larry Senger	Dell
Trey Hodgkins	Hodgkins Consulting, LLC
John S. Miller/Courtney Lang	ITIC
Randi Parker	CompTIA
Ari Schwartz	Coalition for Cybersecurity Policy & Law
Marty Loy	Cisco
Jamie Brown, Chris Jensen, Robert Huber	Tenable
Brad Minnis	Juniper - ITIC
Nick Boswell, Charlotte Lewis	CDW-G
Peter McClelland	Threat Sketch
Tina Gregg, Amanda Craig	Microsoft
Jason Boswell	Ericsson
Steve Lipner	SAFECode
Eric Nelson, Corey Cunningham	Rehancement Group
Michael Aisenberg	MITRE
Alexander McLeod	ACT Online
Alvin Chan	HP
Tom Quillin, Audrey Plonk	Intel

NAME	COMPANY
Brett Bennet, Jennifer Kauffman	Cybercore Tech
Carol Woody	Carnegie Mellon
Travis Miller, David Flowers	Interos
Geoff Kahn, Mei Nelson	Accenture
Tommy Ross	BSA

TABLE 4—U.S. GOVERNMENT WORKING GROUP MEMBERS

NAME	COMPANY
Dennis Martin, Gwen Hess, Scott Friedman	DHS
Rebecca Adams, Charles Covel, Jillian Rucker	DHS
Ryan Orr, Ronald Clift	DHS
Debra Jordan, Kurian Jacob	FCC
Michael Van de Woude, Keith Nakasone, Kelley Artz	GSA
Jeffery Goldthorp	FCC
Rui Li	NRC
Celia Paulsen, Jon Boyens	NIST
Scott Morrison	DOJ
Stacy Bostjanick	DOD
Cherylene G. Caddy	DOE
Anita J. Patankar-Stoll	NSC
Evan Broderick, Megan Doscher	NTIA
Jason Geske, Evelyn Remaley	NTIA
Kanitra Tyler, Tosin Adegun, Mike Bridges	NASA
Adam Pastrich, Patrick Kelly, Austin Bower, John Bowler	Treasury
Jeremy McCrary	OMB

2.0 BACKGROUND

In October 2018, CISA launched the Information and Communications Technology Supply Chain Risk Management (ICT SCRM) Task Force, a public-private partnership to provide advice and recommendations to the CISA and its stakeholders on means for assessing and managing risks associated with the ICT supply chain.

The ICT SCRM Task Force provides a mechanism for representatives of industry and government to share information, explore challenges, and develop recommendations to manage ICT supply chain risks. The Task Force is led by representatives of Department of Homeland Security (DHS) and the ICT sectors.

Task Force membership and participation represents the public-private, cross-sector nature of the Task Force, with members drawn from both sectors and from across the government.

The Task Force summarized the results of its first year of work in the ICT SCRM Task Force Interim Report, which was released in September 2019. This Interim Report includes a description of the Task Force's progress and an initial set of recommendations derived from the individual reports of the Task Force's four WGs. The Interim Report and the reports of the subordinate WGs memorialize the work of these collaborative bodies, including consensus recommendations provided through the Critical Infrastructure Partnerships Advisory Council process to the federal agency participants. The activity of federal employees on the Task Force, including participation in discussions and votes, is intended to inform the Task Force's work through the individual experience of the participating members as subject matter experts and does not necessarily represent the official position of, or adoption of any recommendation by, the U.S. Government or any represented federal department or agency.

The Task Force evaluated multiple potential work streams and reached consensus on the establishment of four Task Force WGs and an Inventory WG. WG2, Threat Evaluation, was established for the purpose of the identification of processes and criteria for threat-based evaluation of ICT suppliers, products, and services. This proposed work stream is intended to provide ICT buyers and users with assistance and guidance for evaluating supply chain threats. Bringing uniformity and consistency to this process will benefit government and industry alike.

2.1 Relationship between Threat, Vulnerability, and Risk

A threat source interacts with a vulnerability, which results in a threat event. The way the source interacted with the is a threat vector. If the threat source was a human and the event intentional, it is an attack.

A vulnerability is a shortcoming or hole in the security of an asset. Risk represents the potential for loss, damage, or destruction of an asset as a result of a threat exploiting a vulnerability. Risk is the intersection of assets, threats, and vulnerabilities.

2.2 Relevant Definitions

Vulnerability: Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. (FIPS 200)

Threat: Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, or denial of service. Also, the potential for a threat-source to successfully exploit an information system vulnerability. (FIPS 200)

Threat event: An event or situation that has the potential for causing undesirable consequences or impact. (NIST SP 800-30)

Threat source/agent: The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability. (FIPS 200)

Attack: An attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity, availability, or confidentiality. (NIST SP 800-82 & CNSSI 4009)

Products: For the purposes of this ICT SCRM Threat Evaluation Working Group, an ICT product is defined as a commercial end-item that stores, retrieves, manipulates, transmits, or receives information electronically in an analog or digital form.

- End-Item: A system, equipment or assembled commodity ready for its intended use.
- Equipment: A type of ICT that is comprised of a combination of parts, components, accessories, attachments, firmware, or software that operate together to perform one or more functions of, as, or for an end-item or system. Equipment may be a subset of an end-item based on the characteristics of the equipment. Equipment that meets the definition of an end-item is an end-item. Equipment that does not meet the definition of an end-item is a component.
- Component. A component is any assembled element that forms a portion of an end-item.

Services: For the purposes of this ICT SCRM Threat Evaluation Working Group, an ICT service is defined as:

- an offering, or capability, or delivery of ICT functionality that does not require the user-or-customer to purchase, own, and operate the underlying ICT product, or;
- an offering, or capability, or delivery of manpower that directly supports an ICT product to include the planning, design, implementation, operation, security, optimization, or life cycle support.

3.0 OBJECTIVE, SCOPE, AND METHODOLOGY

WG2 is focused on Threat Evaluation as opposed to risk assessment since risk is specifically associated with an asset (product, service, supplier in the case of the charter for this ICT SCRM Task Force).

The WG Co-Chairs leveraged the NIST Risk Management Practices described in NIST SP 800-161 to help guide the analysis of the threats and threat sources identified in this work effort.

3.1 Objective

ICT SCRM Task Force WG, Threat Evaluation, was chartered with the identification of processes and criteria for threat-based evaluation of ICT supplies, products, and services. The objectives of this Threat Evaluation were defined as:

- Produce a set of processes and criteria for conducting supplier, product, and service threat assessments.
- The processes and criteria will initially be focused only on global ICT supplier selection, pedigree, and provenance. It will also address product assurance (hardware, software, firmware, etc.), data security, and supply chain risks.
- Finally, the process and criteria will establish a framework for a threat-based assessment of cyber supply chain risks that can be extended in future work products to address other critical infrastructure sectors.

3.2 Scope

The ICT SCRM Task Force agreed early on to leverage the NIST definition for C-SCRM and to scope according to the Federal Acquisition Supply Chain Security Act.

NIST definition: C-SCRM is the process of identifying, assessing, and mitigating the risks associated with the distributed and interconnected nature of ICT product and service supply chains. C-SCRM covers the entire life cycle of ICT:

- Encompasses hardware, software, and information assurance, along with traditional supply chain management and supply chain security practices.[i]

Covered articles are defined as:

- Information technology, including cloud computing services of all types (41 USC 4713(k)(2)(A));
- Telecommunications equipment or telecommunications service (41 USC 4713(k)(2)(B));
- The processing of information on a federal or non-federal information system, subject to the requirements of the Controlled Unclassified Information program (41 USC 4713(k)(2)(C));
- All IoT/OT – (hardware, systems, devices, software, or services that include embedded or incidental information technology). (41 USC 4713(k)(2)(D)).

3.3 Methodology

The WG initially conducted a survey of threat information from the diverse WG membership. The only constraint on the identification of threats was to focus on supplier threats in accordance with the initial proposed scoping.

[i] See, NIST definition of C-SCRM. For purposes of the ICT SCRM Task Force, the term "ICT" includes operational technology and "Internet of Things" devices and services.

The methods developed and applied in the initial supplier threat evaluation process were reused in future iterations as the WG expanded the scope to include products and services. For each of the Threat groupings identified in the initial threat evaluation report, the WG assessed applicability to Products and Services. In all cases, the threat groupings were deemed to be relevant to the expanded scope.

Once the threats were identified, the WG proceeded to complete the additional information captured in the fields highlighted in green from the NIST SP 800-161 spreadsheet in table 5 below as elements to capture and refine with the WG members. Information was captured in the current WG2 Supply Chain Threats by adding a few additional columns. This information was then used to inform the threat analysis process for supplier evaluation.

TABLE 5—TABLE DERIVED FROM NIST SP 800-161

Threat Scenario Component	Description
Threat Source	*Threat "actor" or category of threats*
Vulnerability	*Threat list working group has generated*
Threat Event Description	*Description of the method(s) of exploiting the vulnerability*
Outcome	*Outline the series of consequences that could occur as a result of each threat event*
Organizational units or processes affected	*This should reflect how or where in the supply chain the impact occurs*

Risk Component	Description
Impact	*Description of potential impacts to Supply Chain or consequences of exploiting the vulnerability*
Likelihood	
Acceptable Level of Risk	

Mitigation Component	Description
Potential Mitigating Strategies or SCRM Controls	*Identify supplier evaluation criteria that would reduce or mitigate the impact of the threat*
Estimated Cost of Mitigating Strategies	
Change in Likelihood	
Change in Impact	
Selected Strategies	
Estimated Residual Risk	

The remaining fields not completed by this WG represent the asset-specific data that are captured to assess risk; something that will vary considerably depending on the specific supplier/product/service. The result is a work product that will be consistent with NIST guidance concerning threat and flexible to be used by industry and public sector for a variety of purposes.

The WG executed an iterative process with interim deliverables shareable between the other Task Force WGs to inform their efforts. For example, the threats identified by WG2 were shared with and used to inform the Information Sharing WG on threat focus areas for information gathering and sharing. Similarly, the threats identified were leveraged to aid in assessing the inventory of standards and best practices that may be applicable to the evolving C-SCRM threat environment.

3.3.1 FOCUS ON SUPPLIER THREATS — DATA GATHERING PROCESS

This section describes the process used to generate the threats to SCRM suppliers and the sharing of those threats as inputs to the evaluation to follow. It should be noted that these threats are not considered comprehensive, but rather are representative, such that the evaluation WG could proceed through the exercise of threat evaluation put forward by the NIST Risk Management Framework.

The WG members considered C-SCRM threats from a variety of sources including industry subject matter experts (SMEs), Department of Defense (DoD), Intelligence Community (IC), DHS, and others to inform the development of risk-based criteria. The first data call conducted was a request from WG membership to provide supply chain threats that they recognize from their own experience or from their organization's perspective.[ii] The requested format of the data call was a bulleted list describing each threat. By casting a wide net, the Working Group was able to capture a broad sample of threat inputs for analysis.

Each threat submitted was presented by the WG member that sourced the information to the broader membership. The discussion enabled the WG to process additional details on each threat with the stated purpose of gaining a shared understanding of the specific threats identified. This process was repeated, and notes were captured for each of the identified threats. This set of information was compiled into a single data repository that was used in the Data Analysis phase of the process described below.

3.3.2 DATA ANALYSIS

The WG proceeded to review and categorize the collected data to develop useful insights into the current state of supplier threats in both public and private sectors. The threats identified by the WG members were then consolidated to provide a manageable and shareable set of threat groupings for further development of specific scenarios. These threat groupings served to guide the development of scenarios intended to provide insights into the processes and criteria for conducting supplier threat assessment.

As part of the analysis, the WG membership considered existing business due diligence indicators, such as those listed in General Services Administration's (GSA) Request for Information (RFI), Office of the Comptroller of the Currency (OCC) Third Party Risk Management guidance, and industry best practices identified as part of the inventory work product. Figure 1 below depicts the flow used by the WG to conduct the data analysis.

FIGURE 1—DATA ANALYSIS WORKFLOW

3.3.3 THREAT SCENARIO DEVELOPMENT

Once the WG has established supply chain threat categories, the WG assembled teams for each category. Each team then provided a narrative/scenario developed in a report format that includes background information on the threat itself, the importance of this threat, and potential impact on the supply chain. Multiple scenarios were

[ii] The working group data call requested each member to provide between five and ten supplier threats. The result was an initial set of over 250 specific threats.

developed for each category if deemed necessary by the writing teams. Each scenario also included details surrounding the:

- What (Description of the threat category. Text could include example threats associated with the category);
- Who (Who is likely to be the source of the threat [e.g., nation-state, organized crime] and who the likely target of the threat is);
- When – If applicable (When is the timing of the attack? Is it a denial of service or zero day? Is it persistent or a one-time event?);
- Why (Objective of threat actors: intellectual property theft, network disruption, etc.) and;
- Where (Where in the supply chain is the specific threat activity occurring).

A common format was developed to ensure that each threat scenario presented a comprehensive view of the specific threat and aligned to the requirements of the information fields identified from NIST SP 800-161, as described in Section 2.0 above.

3.3.4 PRODUCT AND SERVICES THREAT SCENARIO DEVELOPMENT

In this latest release of the Threat Scenarios report, the WG leveraged the supplier threat evaluation methodology described above to assess threats and impacts to Products and Services in the supply chain. The first step in this process was to arrive at a consensus on the definition and scope of Products and Services. Following this step, the WG assessed the applicability of the original nine threat groupings to Products and Services threats. The WG also considered if there were additional threat groupings that might need to be added specific to Products and Services. This assessment was intended to leverage the prior learnings of the WG to accelerate the process and still maintain integrity. In the end, the WG concluded that the categories of threats from an earlier version of the report were very much applicable and that no additional groupings were needed to conduct a thorough evaluation. The final step in the process was to generate Product and Services scenarios to include impacts and mitigating controls. This version integrates the Product and Services scenarios into Appendix C which is ordered by Threat Groups.

4.0 FINDINGS

4.1 Supplier, Products and Services Threat List

This section describes the threat information gathered and the specific information for each threat that was presented for evaluation by the WG membership.

4.1.1 TAXONOMY OF THREAT LIST

The initial data call from the WG members was for the identification of supplier threats. The scope of the threats was intentionally left broad to not restrict the identification process. A limited set of information was provided for each threat by the WG member that sourced the information.

- Threat description: Short text description of the specific supplier threat.
- Threat category (provided by source): Identification of the category that the WG member assigned to the identified threat.
- Threat source: Identification of the source or sources that might exploit the vulnerability identified by the threat.

4.1.2 THREAT LIST

The threats identified were presented to the entire WG to enable a common understanding of the information provided. The list was then consolidated based on common threat categories and reviewed by the WG membership in order to gain consensus.

4.2 Threat Data Analysis

4.2.1 CATEGORIZATION OF THREATS

Once the threat list was populated, the co-chairs reviewed the categories assigned to each of the threats to aggregate them into a smaller, more manageable set of common threat groups. The objective of the aggregation was to reduce the threat data and identify common elements for further evaluation using a scenario development process.

In order to aggregate the data, common threat categories were first identified. The next step of the analysis was to group the threats that shared common and related threat categories. Each of the identified threats were then reviewed by the WG to ensure that the common groupings and category assignments accurately reflected the threat. A few of those initially identified were dropped from the list as they did not actually represent a threat (for example, some were impacts or use case specific risks).

Once the threat category review was completed, the co-chairs proposed a set of threat groups to represent the set of common categories of threats identified. This grouping and descriptive titles were shared with the WG membership for review and comment. While consensus was not unanimous, it was determined that for the purposes of the evaluation scope, the list of nine categories represented a reasonable model for aggregation.

4.2.2 DESCRIPTION OF THREAT GROUPS

The evaluation of the threats submitted by the broad spectrum of WG members was consolidated into logical threat groups to aid in the evaluation process. The description of each of these groupings is provided in the following sections.

4.2.2.1 Counterfeit Parts

Insertion of counterfeits in the supply chain can have severe consequences in systems and services provided to downstream customers. These threats are associated with the replacement or substitution of trusted or qualified supplier components, products, or services with those from potentially untrusted sources.

4.2.2.2 External Attacks on Operations and Capabilities[iii]

This threat category represents those that result from the set of vulnerabilities associated with external attacks on suppliers' operations and capabilities. These threats are the result of an external actor exploiting a vulnerability. Alternatively, they are the result of an external actor planting malware with an objective of compromising the confidentiality, integrity, or availability of the supplier information, products, or services.

4.2.2.3 Internal Security Operations and Controls

This category of threats is closely related to external attacks identified above. The primary differentiator is that these threats are a result of challenges in internal supplier processes that enable the exploitation of weaknesses in basic cyber hygiene (e.g., software patching), user awareness (e.g., spear phishing), mishandling of sensitive

[iii] In Version 1.0 of the Threat Evaluation Working Group: Threat Scenarios report, this threat category was titled "Cybersecurity." It has been changed in this version of the report at the recommendation of working group membership. The identified threats in this category remain unchanged, only the title for the threat group is changed.

information, or internal cybersecurity process failures from the lack of a cybersecurity program based on best practices such as the NIST Cybersecurity Framework.

4.2.2.4 System Development Life Cycle (SDLC) Processes and Tools

This threat category represents those threats that impact the suppliers' ability to develop products or services that protect the confidentiality, integrity, and availability of products and services developed by the supplier. An example of this group of threats include failures in the development process to detect introduction of malware or unvetted code into software products through use of vulnerable open source libraries.

4.2.2.5 Insider Threats

This category of threats focuses on the vulnerability of the supplier to attack from trusted staff and partners that are embedded internal to the supplier operations. Most of the threats identified in this grouping are associated with intentional tampering or interference.

4.2.2.6 Economic Risks

Economic risks stem from threats to the financial viability of suppliers and the potential impact to the supply chain resulting from the failure of a key supplier as a result. Other threats to the supply chain that result in economic risks include, but are not limited to, vulnerabilities to cost volatility, reliance on single source suppliers, cost to swap out suspect vendors, and resource constraints as a result of company size.

4.2.2.7 Inherited Risk (Extended Supplier Chain)

This category of threats is a result of current supply chains that extend broadly across industries and geographies. These threats typically are associated with the challenge of extending controls and best practices through the entire supply chain due to its global nature. It also includes the vulnerabilities that can result from integration of components, products, or services from lower tier supplier where a prior determination of acceptable risk may not flow all the way through the development process to the end user supplier.

4.2.2.8 Legal Risks

This category of threats emanates from supplier vulnerabilities specific to legal jurisdiction. Some examples include weak anti-corruption laws, lack of regulatory oversight, weak intellectual property considerations. This also includes the threats that result from country specific laws, policies, and practices intended to undermine competition and free market protections such as the requirement to transfer technology and intellectual property to domestic providers in a foreign country.

4.2.2.9 External End-to-End Supply Chain Risks (Natural Disasters, Geo-Political Issues)

This category of threats is associated with broad based environmental, geopolitical, regulatory compliance, workforce and other vulnerabilities to the confidentiality, integrity, or availability of supplier information, products, or services.

4.2.3 THREAT LIST INCLUDING THREAT GROUPS

The threat list based on the data analysis presented is included as Appendix B to this document.

4.3 Threat Scenarios

4.3.1 SCENARIOS

The Threat Evaluation WG –Threat Scenarios developed for the ICT SCRM Task Force is included as Appendix C to this document. The developed scenarios with impacts and mitigating controls are presented with supplier scenarios listed first, followed by Products and Services scenarios – ordered by Threat Groupings.

5.0 CONCLUSIONS

The WG kicked off this evaluation with a blank sheet and focused on leveraging the diversity of its membership to provide a broad base of threats for analysis and evaluation. The WG membership determined that the same threat groupings can be applied to suppliers, products and services. As a result, the methods developed and applied in the initial supplier threat evaluation process was repeatable in future iterations as the WG expanded its scope to include Products and Services.

The WG recommends that the task force consider a continuation of the charter for this effort, with a focus on conducting a deep dive into a specific scenario in order to conduct a comprehensive threat analysis—prioritized by membership—as an example of how to leverage this threat assessment as an information feed into a company specific risk management program.

APPENDIX A: ACRONYM LIST

AI	Artificial Intelligence
ATO	Authority to Operate
BGP	Border Gateway Protocol
BIA	Business Impact Analysis
BOM	Bill of Materials
CAD	Computer-Assisted Design
CCTV	Close-Circuit Televisions
CERT	Computer Emergency Readiness Team
CFIUS	Committee on Foreign Investment in the United States
CIPAC	Critical Infrastructure Partnerships Advisory Council
CIS	Center for Internet Security
CISA	Cybersecurity and Infrastructure Security Agency
COTS	Commercial-Off-the-Shelf
COVID-19	Coronavirus Disease
CSRIC	Communication, Security, Reliability, and Interoperability Council
C-SCRM	Cyber Supply Chain Risk Management
CVE	Common Vulnerability and Exposure
DDoS	Distributed Denial of Service
DHS	Department of Homeland Security
DMZ	Demilitarized Zone
DNS	Domain Name System
DoD	Department of Defense
DOJ	Department of Justice
EAS	Emergency Alert System
FAR	Federal Acquisition Regulation
FCC	Federal Communications Commission
FIPS	Federal Information Processing Standards
GRC	Governance, Risk, and Compliance

GSA	General Services Administration
HPE	Hewlett-Packard Enterprises
IAAA	Identification, Authentication, Authorization, Auditing, and Accounting
IC	Intelligence Community
ICS	Industrial Control Systems
ICT	Information and Communications Technology
ID	Identification
IP	Internet Protocol
IP	Intellectual Property
ISO	International Organization for Standardization
ISP	Internet Service Provider
IT	Information Technology
ITAM	Information Technology Asset Management
ITIC	Information Technology Industry Council
ITP	Insider Threat Program
KPI	Key Performance Indicator
KRI	Key Risk Indicator
LAN	Local Area Network
MAC	Media Access Control
MANRS	Mutually Agreed Norms for Routing Security
MSSP	Managed Security Service Provider
NASA	National Aeronautics and Space Administration
NDA	Non-Disclosure Agreement
NIST-SP	National Institute of Standards and Technology (NIST) Special Publication
NTIA	National Telecommunications and Information Administration
OCC	Office of the Controller of the Currency
OEM	Original Equipment Manufacturer
OMB	Office of Management and Budget
OS	Operating System
OT	Operational Technology

PAM	Privileged Access Management
PC	Personal Computer
PCB	Printed Circuit Board
PM	Program Management
POS	Point-of-Sale
PWB	Printed Wiring Board
RFI	Request for Information
RFP	Request for Proposal
SAM	Software Asset Management
SC	Semiconductor
SBOM	Software Bill of Materials
SCA	Security Controls Assessment
SCRM	Supply Chain Risk Management
SDK	Software Development Kit
SDLC	System Development Life Cycle
SED	Stakeholder Engagement Division
SLTT	State, Local, Territorial, and Tribal
SMB	Small and Medium-sized Business
SME	Subject Matter Expert
SNMP	Simple Network Management Protocol
SPVM	Sourcing, Procurement and Vendor Management
SQL	Standardized Query Language
SSH	Secure Shell
TAA	Trade Agreements Act
TIA	Telecommunications Industry Association
U.S.	United States
USB	Universal Serial Bus
VPN	Virtual Private Network
WG	Working Group
WG2	Working Group 2: Threat Evaluation

APPENDIX B: THREAT LIST

Note: WG members were asked to identify a representative sample of the top SCRM threats specifically focused on suppliers in accordance with the initial proposed scoping. Based on presentation and analysis of the threats submitted by the WG members, the items were aggregated into a smaller, more manageable set of common threat groupings to aid in the evaluation process. The objective of the aggregation was to identify common elements for further evaluation using a scenario development process. The threats identified represent the output produced by this methodology, and do not represent an official or consensus documentation of supply chain threats. The threat list is intended to document the WG's work and provide input for future policy discussions.

Threat list in Appendix B represents the "raw" data gathered from the WG members. The description for each threat entry was provided by the WG members in their own words and refined through discussion with the WG membership. This data was used as a critical data input to drive the development of the Threat Groups used for scenario development. In the table below, the Threat Group number references the corresponding description in Section 4.2.2 of this report.

In general, revisiting the list of individual threats captured in Appendix B is not deemed necessary for every version of the report since the purpose of the threat list exercise was to identify and gain consensus on the threat categories only. No changes are recommended for this Version 3.0 release.

THREATS	THREAT CATEGORIES OR EVENT	THREAT SOURCE OR ACTOR
4.2.2.1 Counterfeit Parts		
Counterfeit product or component with malicious intent to cause unwanted function	Adversarial: Craft or create attack tools	Nation-State; organization; individual (Outsider/Insider)
Component elements included in product, software, or service	Adversarial: Craft or create attack tools	Nation-State; organization; individual (Outsider/Insider)
Virtualization and encapsulation hiding access	Adversarial: Craft or create attack tools	Nation-State; organization; individual (Outsider/Insider)
A malicious supplier employee inserts hostile content at the product or component manufacturing, or distribution stage, to affect supplier products or components delivered to a subset (potentially a targeted subset) of downstream customers (tampering or counterfeiting)	Adversarial: Craft or create attack tools	Nation-State; organization; individual (Outsider/Insider)
Sales of modified or counterfeit products to legitimate distributors	Adversarial: Craft or create attack tools	Nation-State; organization; individual (Outsider/Insider)
Insert tampered critical components into organizational systems	Adversarial: Deliver, insert, or install malicious capabilities	Nation-State; organization; individual (Outsider/Insider)
Insert counterfeit or tampered hardware into the supply chain	Adversarial: Deliver, insert, or install malicious capabilities	Nation-State; Organization; Individual (Outsider/Insider)

THREATS	THREAT CATEGORIES OR EVENT	THREAT SOURCE OR ACTOR
Counterfeit product or component without malicious intent to cause unwanted function	Accidental: User; privileged user	Individual (Insider)
Create counterfeit or spoof website	Adversarial: Craft or create attack tools	Nation-State; Organization; Individual (Outsider/Insider)
Craft counterfeit certificates	Adversarial: Craft or create attack tools	Nation-State; Organization
Embedded HW/SW threats from non-OEM source(s)	Adversarial: Craft or create attack tools	Nation-State; Organization; Individual (Outsider/Insider)
4.2.2.2 External Attacks on Operations and Capabilities		
Data breaches and unauthorized access to sensitive data (at rest and in transit)	Adversarial: Achieve results	Nation-State; Organization; Individual (Outsider/Insider)
Loss of critical information from vendor	Adversarial: Achieve results	Nation-State; Organization; Individual (Outsider/Insider)
Obtain unauthorized access	Adversarial: Achieve results	Nation-State; Organization; Individual (Outsider/Insider)
Data – Impacts to confidentiality, integrity or availability	Adversarial: Achieve results	Nation-State; Organization; Individual (Outsider/Insider)
Malware, unauthorized access, theft	Adversarial: Achieve results	Nation-State; Organization; Individual (Outsider/Insider)
Cause unauthorized disclosure or unavailability by spilling sensitive information	Adversarial: Achieve results	Nation-State; Organization; Individual (Outsider/Insider)
Login Attacks (Brute force, Dictionary attacks, Password spraying)	Adversarial: Conduct an attack	Nation-State; Organization; Individual (Outsider)
Credential Compromise	Adversarial: Conduct an attack	Nation-State; Organization; Individual (Outsider)
Supplier solution architecture allows for manipulation and extraction of data and services (not due to a system vulnerability)	Accidental: User, privileged user	Nation-State; Organization; Individual (Outsider/Insider)
Phishing, spear phishing, or whaling	Adversarial: Craft or create attack tools	Nation-State; Organization
Malware, unauthorized access, theft	Adversarial: Craft or create attack tools	Nation-State; Organization
Deliver known malware to internal organizational information systems (e.g., virus via email)	Adversarial: Deliver, insert, or install malicious capabilities	Nation-State; Organization; Individual (Outsider)
Compromise of integrity of product through intrusion	Adversarial: Exploit and compromise	Nation-State; Organization; Individual (Outsider)
External cyber attacker threats	Adversarial: Exploit and compromise	Nation-State; Organization; Individual (Outsider)

THREATS	THREAT CATEGORIES OR EVENT	THREAT SOURCE OR ACTOR
Embedded malware or virus attacks in delivered products	Adversarial: Craft or Create Attack Tools	Nation-State; Organization; Individual (Outsider/Insider)
Inappropriate modification of device, software, or service through network update	Adversarial: Craft or Create Attack Tools	Nation-State; Organization; Individual (Outsider/Insider)
Embedded HW/SW threats (from manufacturing)	Adversarial: Craft or Create Attack Tools	Nation-State; Organization; Individual (Outsider/Insider)
A malicious supplier employee inserts hostile content at the product or component manufacturing or distribution stage, to affect supplier products or components delivered to a subset (potentially a targeted subset) of downstream customers (tampering or counterfeiting)	Adversarial: Craft or Create Attack Tools	Nation-State; Organization; Individual (Outsider/Insider)
Embedded Malware. Virus Attacks in hosted services websites	Adversarial: Craft or create attack tools	Nation-State; Organization; Individual (Outsider/Insider)
Malware disguised as driver updates or system patches on compromise vendor web site	Adversarial: Craft or create attack tools	Nation-State; Organization; Individual (Outsider/Insider)
Intrusion or compromise of customer through service	Adversarial: Craft or create attack tools	Nation-State; Organization; Individual (Outsider/Insider)
Inappropriate modification of device, software, service through network update	Adversarial: Craft or create attack tools	Nation-State; Organization; Individual (Outsider/Insider)
Product vulnerabilities (intended) in hardware and software	Adversarial: Craft or create attack tools	Nation-State; Organization; Individual (Outsider/Insider)
Product vulnerabilities (unintended) in hardware and software	Accidental: User, privileged user	Individual (Insider)
Resource depletion	Accidental: User, privileged user	Individual (Insider)
Pervasive disk error	Accidental: User, privileged user	Individual (Insider)
Advanced Persistent Threats	Adversarial: Maintain a presence	Nation-State; Organization
DNS attack	Adversarial: Conduct an attack	Nation-State; Organization
DoS/DDoS	Adversarial: Conduct an attack	Nation-State; Organization
Threat actor impacts app store availability impacting end user ability to do job	Adversarial: Conduct an attack	Nation-State; Organization; Individual (Outsider)
Threat actor hacks cloud environment or telco making service unavailable	Adversarial: Conduct an attack	Nation-State; Organization; Individual (Outsider)

THREATS	THREAT CATEGORIES OR EVENT	THREAT SOURCE OR ACTOR
Threat actor breaks ability of information provider to deliver information	Adversarial: Conduct an attack	Nation-State; Organization; Individual (Outsider)
Man in the middle attack	Adversarial: Achieve results	Nation-State; Organization; Individual (Outsider)
Obtain information by externally located interception of wireless network traffic	Adversarial: Achieve results	Nation-State; Organization; Individual (Outsider)
Incorrect BGP routing at a level above your network	Adversarial: Achieve results	Nation-State; Organization; Individual (Outsider)
Replay attack	Adversarial: Conduct an attack	Nation-State; Organization; Individual (Outsider)
Spoofing	Adversarial: Conduct an attack	Nation-State; Organization; Individual (Outsider)
URL injection	Adversarial: Conduct an attack	Nation-State; Organization; Individual (Outsider)
Intentional specific software security threats or vulnerabilities exploitation (long list of specific types not included for brevity)	Adversarial: Craft or create attack tools	Nation-State; Organization; Individual (Outsider/Insider)
Threat actor compromises or hacks it software	Adversarial: Craft or create attack tools	Nation-State; Organization; Individual (Outsider/Insider)
Unintentional specific software security threats or vulnerabilities exploitation (long list of specific types not included for brevity)	Accidental: User, privileged user	Individual (Insider)
System misconfiguration	Accidental: User, privileged user	Nation-State; Organization; Individual (Outsider/Insider)
Zero-Day exploits	Adversarial: Craft or create attack tools	Nation-State; Organization
Conduct supply chain attacks targeting and exploiting critical hardware, software, or firmware	Adversarial: Conduct an attack (i.e., direct or coordinate attack tools or activities)	Nation-State; Organization
Perform malware-directed internal reconnaissance	Adversarial: Perform reconnaissance and gather information	Nation-State; Organization
Craft attacks specifically based on deployed information technology environment	Adversarial: Craft or create attack tools	Nation-State; Organization
Deliver modified malware to internal organizational information systems	Adversarial: Deliver, insert, or install malicious capabilities	Nation-State; Organization; Individual (Outsider/Insider)

THREATS	THREAT CATEGORIES OR EVENT	THREAT SOURCE OR ACTOR
Deliver targeted malware for control of internal systems and exfiltration of data	Adversarial: Deliver, insert, or install malicious capabilities	Nation-State; Organization; Individual (Outsider/Insider)
Deliver malware by providing removable media	Adversarial: Deliver, insert, or install malicious capabilities	Nation-State; Organization; Individual (Outsider/Insider)
Insert malicious scanning devices (e.g., wireless sniffers) inside facilities	Adversarial: Deliver, insert, or install malicious capabilities	Nation-State; Organization
Exploit split tunneling	Adversarial: Exploit and compromise	Nation-State; Organization
Exploit vulnerabilities in information systems timed with organizational mission/business operations tempo	Adversarial: Exploit and Compromise	Nation-State; Organization; Individual (Outsider/Insider)
Violate isolation in multi-tenant environment	Adversarial: Exploit and Compromise	Nation-State; Organization
Compromise information systems or devices used externally and reintroduced into the enterprise	Adversarial: Exploit and Compromise	Nation-State; Organization
Coordinate campaigns across multiple organizations to acquire specific information or achieve desired outcome	Adversarial: Maintain a presence or set of capabilities	Nation-State; Organization
Coordinate cyber-attacks using external (outsider), internal (insider), and supply chain (supplier) attack vectors	Adversarial: Maintain a presence or set of capabilities	Nation-State; Organization
Purchasing of equipment with known critical security vulnerabilities and little expectation of patching by vendor	Accidental: User, privileged user	Individual: Insider
Compromise of integrity of virtualization	Adversarial: Exploit and compromise	Nation-State; Organization; Individual (Outsider/Insider)
Access through service contract	Adversarial: Maintain a presence or set of capabilities	Nation-State; Organization
Quantum computing threat to commercial cryptography	Adversarial: Exploit and compromise	Nation-State
Crypto jacking	Adversarial: Exploit and compromise	Nation-State; Organization
Ransomware	Adversarial: exploit and compromise	Nation-State; Organization
Conduct physical attacks on infrastructures supporting organizational facilities	Adversarial: Conduct an attack	Nation-State; Organization; Individual (Outsider/Insider)

THREATS	THREAT CATEGORIES OR EVENT	THREAT SOURCE OR ACTOR
Physical compromise of specific device	Adversarial: Conduct an attack	Nation-State; Organization; Individual (Outsider/Insider)
Physical access through presence of device	Adversarial: Exploit and compromise	Nation-State; Organization; Individual (Outsider/Insider)
Physical network control or access	Adversarial: Exploit and compromise	Nation-State; Organization; Individual (Outsider/Insider)
Physical control of infrastructure	Adversarial: Exploit and compromise	Nation-State; Organization; Individual (Outsider/Insider)
Threat actor activity overwhelms organization's ability to deal with attacks, IT supply chain services unable to surge to meet need	Adversarial: Conduct an attack	Nation-State; Organization
4.2.2.3 Internal Security Operations and Controls		
Lack of knowledge (suppliers or subcontractors, especially SMBs, not knowing what their vulnerabilities are)	Accidental: Deliver, insert, install malicious capabilities	Nation-State; Organization; Individual (Outsider/Insider)
Product vulnerabilities (advertent or inadvertent) in hardware and software	Adversarial or Accidental: Deliver, insert, or install malicious capabilities	Nation-State; Organization; Individual (Outsider/Insider)
Vulnerability Exploitation	Adversarial or Accidental: Deliver, insert, or install malicious capabilities	Nation-State; Organization; Individual (Outsider/Insider)
Supplier Has Weak Controls to Detect or Prevent Social Engineering	Accidental: Deliver, insert, or install malicious capabilities	Nation-State; Organization; Individual (Outsider)
Spill sensitive information	Accidental: User; privileged user	Individual (Insider)
Data and Media Disposal is not Secure, Allowing Disclosure of Sensitive Data	Adversarial: Achieve results	Nation-State; Organization; Individual (Outsider)
Obtain information by opportunistically stealing or scavenging information systems/components	Adversarial: Achieve results	Nation-State; Organization; Individual (Outsider)
Exploit insecure or incomplete data deletion in multi-tenant environment	Adversarial: Exploit and Compromise	Nation-State; Organization; Individual (Outsider)
Data breaches post disconnect	Adversarial: Exploit and Compromise	Nation-State; Organization; Individual (Outsider)
Poor Employee/Contractor/Vendor Access Controls	Adversarial: Achieve results	Nation-State; Organization; Individual (Outsider/Insider)
Supplier System Does Not Have Controls to Validate and Authorize Escalation of Privileges	Adversarial: Achieve results	Nation-State; Organization; Individual (Outsider/Insider)

THREATS	THREAT CATEGORIES OR EVENT	THREAT SOURCE OR ACTOR
Staff using vulnerable unpatched personal computer systems from home to contact agency resources	Accidental: Individual	Individual (Outsider/Insider)
Large enterprise (~$10 billion/year) that supplies key components for mission projects continues to experience cyberattack and illicit technology transfer events	Adversarial: Exploit and Compromise	Nation-State; Organization; Individual (Outsider)
ICT Devices with default passwords	Accidental: Deliver, insert, or install malicious capabilities	Organization
(Removal of) Hard-set accounts in devices and software	Accidental: Deliver, insert, or install malicious capabilities	Organization
Devices that do not auto-update firmware	Accidental: Deliver, insert, or install malicious capabilities	Organization
Mishandling of critical or sensitive information by authorized users	Accidental: Individual	Individual (Insider)
Incorrect privilege settings	Accidental: Individual	Individual (Insider)
The nuclear power section has a maturing cyber program or defense architecture and regulatory requirements, but sophisticated offensive groups with nation-state capabilities are threats	Accidental: Deliver, insert, or install malicious capabilities	Nation-State; Organization; Individual (Outsider)
4.2.2.4 Compromise of SDLC Processes and Tools		
Malware coded, inserted, or deployed into critical ICT throughout the design, development, integration, deployment or maintenance phase of components	Adversarial: Craft or create attack tools	Nation-State; Organization; Individual (Outsider/Insider)
Manipulation of development tools	Adversarial: Craft or create attack tools	Nation-State; Organization; Individual (Outsider/Insider)
Manipulation of a development environment	Adversarial: Craft or create attack tools	Nation-State; Organization; Individual (Outsider/Insider)
Manipulation of source code repositories (public or private)	Adversarial: Craft or create attack tools	Nation-State; Organization; Individual (Outsider/Insider)
Manipulation of software update/distribution mechanisms	Adversarial: Craft or create attack tools	Nation-State; Organization; Individual (Outsider/Insider)
Compromise design, manufacture, or distribution of information system components (including hardware, software, and firmware)	Adversarial Supply Chain Threat: Exploit and compromise	Nation-State; Organization; Individual (Outsider/Insider)

THREATS	THREAT CATEGORIES OR EVENT	THREAT SOURCE OR ACTOR
Compromised/infected system images (multiple cases of removable media infected at the factory)	Adversarial: Exploit and Compromise	Nation-State; Organization; Individual (Outsider/Insider)
Replacement of legitimate software with codified versions	Adversarial: Deliver, insert, or install malicious capabilities	Nation-State; Organization; Individual (Outsider/Insider)
Insert untargeted malware into downloadable software or into commercial information technology products	Adversarial: Deliver, insert, or install malicious capabilities	Nation-State; Organization; Individual (Outsider/Insider)
Insert targeted malware into organizational information systems and information system components	Adversarial: Deliver, insert, or install malicious capabilities	Nation-State; Organization; Individual (Outsider/Insider)
Insert specialized malware into organizational information systems based on system configurations	Adversarial: Deliver, insert, or install malicious capabilities	Nation-State; Organization; Individual (Outsider/Insider)
Introduction of vulnerabilities into software products from open source	Accidental: Individual	Individual (Outsider/Insider)
Software integrity and does the product include open source code	Accidental: Individual	Individual (Outsider/Insider)
Foreign developed computer code or source code	Accidental: Individual or privileged user	Nation-State; Organization; Individual (Outsider/Insider)
Foreign companies controlled or influenced by a foreign adversary	Adversarial: Maintain a presence or set of capabilities	Nation-State
4.2.2.5 Insider Threat		
Lone wolf (disgruntled employee)	Adversarial: Conduct an attack	Individual: Insider
Insider threats	Adversarial: Deliver, insert, or install malicious capabilities	Nation-State; Organization; Individual (Outsider/Insider)
Threat actor recruits onsite IT services personnel with gambling debts to spy	Adversarial: Deliver, insert, or install malicious capabilities	Nation-State; Organization; Individual (Outsider/Insider)
IT services supply chain sends spy onsite	Adversarial: Deliver, insert, or install malicious capabilities	Nation-State; Organization; Individual (Outsider/Insider)
Insert subverted individuals into organizations	Adversarial: Deliver, insert, or install malicious capabilities	Nation-State; Organization; Individual (Outsider/Insider)
Insert subverted individuals into privileged positions in organizations	Adversarial: Deliver, insert, or install malicious capabilities	Nation-State; Organization; Individual (Outsider/Insider)
Internal: Personnel Threat	Adversarial: Deliver, insert, or install malicious capabilities	Nation-State; Organization; Individual (Outsider/Insider)

THREATS	THREAT CATEGORIES OR EVENT	THREAT SOURCE OR ACTOR
Conduct internally based session hijacking	Adversarial: Conduct an attack	Individual: Privileged Insider
Tampering while on hand	Adversarial: Conduct an attack	Individual (Outsider/Insider)
Tampering while being deployed or installed	Adversarial: Conduct an attack	Individual (Outsider/Insider)
Tampering while being maintained	Adversarial: Conduct an attack	Individual (Outsider/Insider)
Tampering while being repaired	Adversarial: Conduct an attack	Individual (Outsider/Insider)
4.2.2.6 Economic		
Viability of financially weak suppliers	Economic: Financial stability	Nation-State; Organization
Financial stability	Economic: Financial stability	Nation-State; Organization
Economic risk (i.e., a supplier or sub-contractor of a supplier will be economically devastated by a breach)	Economic: Financial stability	Nation-State; Organization
Limited visibility into business and sustainability practices of suppliers beyond the first tier	Economic: Financial stability	Organization
Cost volatility	Economic: Financial stability	Organization
No vendor support when a company transfers ownership or closes	Economic: Financial stability	Organization
Operational disruptions due to source being acquired by a far larger company with questionable security	Economic: Financial stability	Organization
Very small, privately held company “one-man show” with inadequate quality management and history of delivery delays; security concerns contracted to product components on the critical path of multiple mission projects	Economic: Financial stability	Organization
Young entrepreneurial business identified as a potential subcontractor for key mission components but has no discoverable facility for production, integration, test, nor quality management	Economic: Financial stability	Organization
SMB often lack the ability to heavily influence vendors to correct issues	Economic: Production problems	Organization
Little control over what applications or devices customers use or connect with via provider-services	Economic: Production problems	Organization; Individual (Outside)

THREATS	THREAT CATEGORIES OR EVENT	THREAT SOURCE OR ACTOR
If a vendor is compromised, some providers that use the same equipment or software across their entire system do not have the resources to continue operations or switch to another vendor	Economic: Production problems	Nation-State; Organization; Individual (Outsider/Insider)
Threat Actor determines how to manipulate decisions by delivering too much or too little information; inaccurate yet somehow changes decisions	Economic: Production problems	Nation-State; Organization; Individual (Outsider/Insider)
Industry discovers vulnerability in IT Product X resulting in freeze in using that product until fixed	Economic: Production problems	Nation-State; Organization; Individual (Outsider/Insider)
SMBs do not have the resources or expertise to evaluate the security of all devices and software that are purchased by the company	Economic: Production problems	Organization
Most small and medium sized providers do not proactively monitor customer-based equipment for anomalous behaviors, and as such are unable to diagnose a security issue unless notified by other means	Economic: Production problems	Organization
4.2.2.7 Inherited Risk (Extended Supplier Chain)		
Inherited risk (extended supplier chain)	Adversarial / Accidental: Deliver or insert malicious capabilities	Nation-State; Organization; Individual (Outsider/Insider)
Inherited risk generally	Adversarial / Accidental: Deliver or insert malicious capabilities	Nation-State; Organization; Individual (Outsider/Insider)
Mid-supply chain insertion of counterfeit parts	Adversarial / Accidental: Deliver or insert malicious capabilities	Nation-State; Organization; Individual (Outsider/Insider)
Depth of the supply chain and who is supplying the supplier	Adversarial / Accidental: Deliver or insert malicious capabilities	Nation-State; Organization; Individual (Outsider/Insider)
Domestic companies	Adversarial / Accidental: Deliver or insert malicious capabilities	Nation-State; Organization; Individual (Outsider/Insider)
Lack of enforced traceability	Adversarial / Accidental: Deliver or insert malicious capabilities	Nation-State; Organization; Individual (Outsider/Insider)
Supplier incorporates hostile content in product or component	Adversarial / Accidental: Deliver or insert malicious capabilities	Nation-State; Organization; Individual (Outsider/Insider)
Threat of upstream intrusions in supply chain and lack of traceability from component to finished product	Adversarial / Accidental: Deliver or insert malicious capabilities	Nation-State; Organization; Individual (Outsider/Insider)

THREATS	THREAT CATEGORIES OR EVENT	THREAT SOURCE OR ACTOR
Supplier has malicious intent and incorporates hostile content in product or component. This scenario applies to hardware or software providers (including both proprietary and open source software)	Adversarial / Accidental: Deliver or insert malicious capabilities	Nation-State; Organization; Individual (Outsider/Insider)
Trustworthy supplier inadvertently creates a product or component that is vulnerable to attack and delivers it to downstream customers. This scenario applies to hardware or software providers (including both proprietary and open source software)	Adversarial / Accidental: Deliver or insert malicious capabilities	Nation-State; Organization; Individual (Outsider/Insider)
Tampering while in transit	Adversarial: Conduct an attack	Nation-State; Organization; Individual (Outsider/Insider)
Shipment interdiction	Adversarial: Conduct an attack	Nation-State; Organization; Individual (Outsider/Insider)
Vendor noncompliance	Adversarial: Deliver, insert, or install malicious capabilities	Nation-State; Organization; Individual (Outsider/Insider)
Lack of Certification of component safety or quality at each appropriate level of the value chain of a product	Adversarial: Deliver, insert, or install malicious capabilities	Nation-State; Organization; Individual (Outsider/Insider)
Integrity of integrated third-party components	Adversarial: Deliver, insert, or install malicious capabilities	Nation-State; Organization; Individual (Outsider/Insider)
Lack of oversight or security standards for imported devices	Adversarial: Deliver, insert, or install malicious capabilities	Nation-State; Organization; Individual (Outsider/Insider)
Agency/enterprise does not have direct authority over third party suppliers	Adversarial: Deliver, insert, or install malicious capabilities	Nation-State; Organization; Individual (Outsider/Insider)
Lack of required disclosure of component manufacturer origin	Adversarial or Accidental: Deliver, insert, or install malicious capabilities	Nation-State; Organization; Individual (Outsider/Insider)
Lack of disclosure of origin	Adversarial or Accidental: Deliver, insert, or install malicious capabilities	Nation-State; Organization; Individual (Outsider/Insider)
Create and operate false front organizations to inject malicious components into the supply chain	Adversarial: Craft or create attack tools	Nation-State; Organization
IT information provider delivers intentionally bad or misleading data (e.g. DNS/BGP)	Adversarial: Achieve results	Nation-State; Organization; Individual (Outsider/Insider)
A malicious supplier employee inserts hostile content at the product or component design or software coding stage, to affect many supplier products or components (tampering)	Adversarial: Achieve results	Individual (Insider)

THREATS	THREAT CATEGORIES OR EVENT	THREAT SOURCE OR ACTOR
An upstream supplier to the trustworthy supplier serves as a vehicle (witting or unwitting) for introduction of hostile content into a hardware or software component that the trustworthy supplier in turn integrates into its product or component and delivers to downstream customers (tampering or counterfeiting)	Adversarial: Achieve results	Nation-State; Organization; Individual (Outsider/Insider)
An external threat actor penetrates the trustworthy supplier's design or manufacturing systems and inserts hostile content into a product or component that the trustworthy supplier delivers to downstream customers (tampering)	Adversarial: Achieve results	Nation-State; Organization; Individual (Outsider)
4.2.2.8 Legal risks		
Legal: IP or licensing violation	Legal: IP or Licensing violation	Nation-State; Organization; Individual (Outsider/Insider)
Suppliers operating in countries with weak intellectual property protection laws	Legal: IP or Licensing violation	Nation-State; Organization; Individual (Outsider/Insider)
Liability for purchaser	Legal: Lawsuits	Nation-State; Organization
Supplier fear liability impact could devastate participants in supply chain, particularly SMBs	Legal: Lawsuits	Nation-State; Organization; Individual (Outsider/Insider)
Privacy regulations	External: Government compliance and political uncertainty	Nation-State; Organization
Legislation and compliance	External: Government compliance and political uncertainty	Nation-State; Organization
Known to engage in financial crimes (e.g. fraud, bribery, money laundering)	External: Legal noncompliance or ethical practices	Organization
Known to have violated U.S. sanctions	External: Legal noncompliance or ethical practices	Organization
4.2.2.9 External, End-to-End Supply Chain Risks		
Natural disaster causing supply chain disruptions	External: Natural disasters	Environmental: Natural
Natural disaster	External: Natural disasters	Environmental: Natural
Natural disruptions	External: Natural disasters	Environmental: Natural

THREATS	THREAT CATEGORIES OR EVENT	THREAT SOURCE OR ACTOR
Geo-political uncertainty	External: Government compliance and political uncertainty	Nation-State; Organization
Manmade disruptions: sabotage, terrorism, crime, war	External: Government compliance and political uncertainty	Nation-State; Organization
Labor issues	External: Government compliance and political uncertainty	Nation-State; Organization
Supply chain disruptions and price spikes due to protectionism in global trade	External: Government compliance and political uncertainty	Nation-State
Lack of legislative governance enforcing traceability within the manufacturing and assembly process	External: Government compliance and political uncertainty	Nation-State; Organization
Nation-State control over foreign suppliers	External: Government compliance and political uncertainty	Nation-State
Diminishing contribution of U.S. companies in technology standards bodies and open source software	Adversarial: Maintain a presence or set of capabilities.	Nation-State

APPENDIX C: THREAT SCENARIOS

CONTENTS

This page is intentionally left blank.

1 THREAT CATEGORY: COUNTERFEIT PARTS

1.1 SCENARIO: COUNTERFEIT/FRAUDULENT PARTS

1.1.1 BACKGROUND

Counterfeit parts are a form of fraud. Counterfeiters prey on customers seeking high-quality parts from reputable manufacturers and instead are unknowingly sold substandard or defective parts. A counterfeiter's "intent to deceive" is the difference between a counterfeit part and a faulty part which has defects that are unknown to the manufacturer or the distributor.

1.1.2 THREAT SOURCES

Most counterfeit items seized while entering the United States come from Asia. Some 87 percent of seized counterfeit items came from China or Hong Kong.[iv]

1.1.3 THREAT IMPACT

Electronics are an indispensable part of everyday life. Between travel and communications, electronic components enable most cornerstones of modern existence. Unfortunately, electronic components in consumer products are increasingly being counterfeited. Fake components can easily cause product failures and even cause personal injury or death.

As an example, in 2012 the Senate Armed Services Committee uncovered more than 1,800 cases of "bogus parts" in the Pentagon supply chain.[v] The suspected components were identified in computers, missiles, military aircraft, and helicopters. Seventy percent of the counterfeit parts were manufactured in China.

That said, the Department of Defense is not the only victim. Consumer and industrial businesses are losing hundreds of billions of dollars annually. The automobile industry and the semi-conductor industry are losing billions of dollars annually.[vi]

As organizations have become aware of counterfeit parts, one of the responses is to test upon acceptance or prior to receipt. However, testing alone may not detect all counterfeits, so additional counterfeit detection techniques should be pursued such as: (1) assessing the electronic component measurements against the manufacturer's specifications; (2) assessing for marking authenticity (i.e., 'blacktopping'); (3) x-ray inspections; and, (4) decapsulation or 'de-lidding' of the electronic component(s). The consequences of weak supply chain monitoring, and the impact on costs, reliability, and reputation are negatively impacted by counterfeit parts and components.

1.1.4 VULNERABILITY

Counterfeit parts and materials adversely affect the global supply chain because parts produced for aerospace and defense also support consumer industries including automotive, aviation, computers, medical devices, security systems, and telecommunications.

[iv] U.S. Customs and Border Patrol, "Intellectual Property Rights Seizure Statistics Fiscal Year 2015," 2016.
[v] U.S. Senate Committee on Armed Services, "Senate Armed Services Committee Releases Report on Counterfeit Electronic Parts," 2012.
[vi] Gary Bamossy and Debra L. Scammon (1985) ,"Product Counterfeiting: Consumers and Manufacturers Beware", in NA - Advances in Consumer Research Volume 12, eds. Elizabeth C. Hirschman and Moris B. Holbrook, Provo, UT : Association for Consumer Research, Pages: 334-339.

The manufacture and sale of counterfeit products is a widespread problem that affects manufacturers, distributers, and retailers in virtually every industry. According to the International Anti-Counterfeiting Coalition (IACC), the global trade in counterfeit has increased from $5.5B in 1982 to approximately $600B annually today. In the U.S. alone, the economic impact of counterfeit goods on businesses is estimated to be $200B to $250B annually.[vii]

Software counterfeiting is a huge criminal industry that is as lucrative as the drug trade and, like the drug trade, transcends national borders.[viii] Moreover, media reports suggest that, like other forms of organized crime, the counterfeiting industry has begun to turn violent. Truly effective anti-counterfeiting efforts will require far more aggressive and sophisticated tactics than government, law enforcement authorities, and software vendors have used to date.

1.1.5 OUTCOME

The vulnerability has gone undetected in the software team's code, and the threat actor is able to compromise the software through the inserted vulnerability. The resulting effect on the code (and ultimately the end customer) can take a variety of forms, from being an inconvenience, to impacting system performance, to the loss of data.

1.1.6 ORGANIZATIONAL UNITS / PROCESSES AFFECTED – TAKEN FROM UNDER WRITERS LAB - MITIGATING THE RISK OF COUNTERFEIT PRODUCTS

Legitimate companies have the most to lose from counterfeit products. Yet, despite widespread counterfeiting activities, many companies are unaware that they have a potential problem. Therefore, it's important to conduct an initial analysis of potential counterfeiting risks that exist within a given industry, and with certain types of products. Here are some of the key product factors that often lead to the greatest counterfeiting risks:

- High-volume, low-cost products - popular, low-cost products that can be easily copied and sold in large numbers.
- Products in high demand - A product that's in demand, regardless of its price, will attract the attention of counterfeiters.
- Products with large market share - A product or group of products with a large market share is an ideal target for counterfeiters.
- Luxury products - Often, savvy counterfeiters will focus on counterfeiting expensive luxury products.
- Products that lack security features - Security features, such as holographic labels or custom colors, deter counterfeiters since they make counterfeit products difficult to replicate and easier to identify. Legitimate products without such security features are easier to counterfeit.
- Complex, loosely controlled supply and distribution chains - Companies with a long and complex supply or distribution chain present multiple opportunities for counterfeiting, since there are multiple points at which a counterfeiter can enter or manipulate the chain.
- Purchasing components and materials based on price alone - Often, even product components are targets for counterfeit producers. Low-priced components may be attractive to legitimate manufacturers, but counterfeit components present the same risks as counterfeit finished products.
- Products sold on the Internet - Selling products online means a potential loss of control over distribution, making it easier for counterfeiters to sell counterfeit products without a manufacturer's knowledge.

[vii] Nathan Vardi, "The World's Biggest Illicit Industries," 2010, Forbes.
[viii] Ibid.

1.1.7 MITIGATING STRATEGIES/SCRM CONTROLS

Many fake and counterfeit products are so identical in look and feel to genuine parts that it is getting harder to distinguish them visually. Procurement of safety-critical replacement parts can be a serious challenge and make you vulnerable to a catastrophic risk of failure from unknowing use of counterfeit components. Moreover, conventional quality control efforts are found to be inadequate to address the challenge of counterfeit products. Whether you are a manufacturer, contractor, distributor, or a retailer, counterfeit products can affect your profits, market share, and brand reputation, and present a serious product liability risk from bodily injury and property damage.

Although specific strategies may vary by type of products, industry segment, and procurement process, anti-counterfeiting experts and organizations recommend implementation of a comprehensive strategy to help reduce the risk of counterfeit products. The strategy should address two aspects. The first one is related to the procurement and related processes, and the second one is related to detection and screening for counterfeit products. The following are some of the suggested elements in the development of a prevention and mitigation strategy to combat this risk:

- Always know your source for procurement of critical products and components. Buying from authorized/certified distributors provides at least some assurance of product quality and integrity of authentic parts. Buying on the Internet or other alternate sources (gray or black market) or importing directly increases your chance of becoming a victim of counterfeit product frauds.
- If you are forced to procure a critical part from an alternate source because a part is not available from an authorized distribution channel, it is important to increase your own verification efforts to ensure the integrity of parts by additional testing efforts. Sometimes, reconditioned and salvaged parts may be sold as new, but may not meet specifications as represented.
- Do not buy on lowest cost criteria alone. In tough economic times, there is temptation to buy at lowest cost. If the price offered is a deeply discounted bargain basement price compared to known price range for branded products, it should raise suspicion alerting further investigation.
- Report suspected counterfeit products and distribution channels to law enforcement authorities and brand manufacturers. Ignoring knowledge about specific counterfeit products and sources of distribution can perpetuate this risk with potential for tragic consequences.

The second part of the strategy should address detection and screening of incoming goods before they are used. U.S. Customs Services and authorities in many countries have portside inspection of incoming import shipments, but compared to the volume of imports, they cannot be relied upon to stop imports of fake counterfeit products into the country. Many counterfeit products are deceptively like authentic parts with logos, trademarks, and other “look and feel” characteristics, and are getting harder to distinguish visually. However, they lack the product integrity and performance quality of genuine parts. Although this does present a challenge, experts suggest some tips that may be helpful in this screening effort.

- Unusual packaging or box
- Inconsistent appearance, color, dimensions with specifications
- Variations in items in a package
- Modifications, touch up and cosmetic beautification of old/salvaged parts
- Altered or worn manufacturer's markings such as name plate, model, serial/part numbers
- Incomplete or inconsistent information on name plate, product markings or certification
- Irregularities in documentation:
    - Shipping papers
    - Certification and technical data

- Lacking signatures and other required authentication of certain documents
- Chemical and material test report and certification documents with handwritten entries or other indication (whiteout) of possible alterations

Using multiple counterfeit detection techniques such as those listed in Section 1.2.3 to examine incoming electronic components allow organizations to stand a better chance of minimizing the risk of suspect devices entering the supply chain. Furthermore, the use of such techniques would provide the end user with greater confidence that when purchasing an electronic component and installing it alongside their equipment, it will work as expected.

PRODUCTS AND SERVICES THREAT SCENARIO

1.2 Scenario: Foreign Counterfeit/Fraudulent Parts

1.2.1 BACKGROUND

A foreign national is directing the shipment of counterfeit computer networking equipment into the Southern District of Texas. “Buy Lo Enterprises” is a technology provider owned and operated by a foreign national. They operate primarily out of Arlington, Texas, but they also provide products throughout the United States to commercial and public sector clients.

1.2.2 THREAT SOURCES

Foreign national selling computing components to federal agencies.

1.2.3 THREAT IMPACTS

The adverse effects of permitting the sale of technology equipment and services purchased by federal agencies through companies owned and operated by foreign nationals presents opportunities for malicious actors to compromise agency systems, networks, and the national security of the United States.

1.2.4 VULNERABILITY

Counterfeit parts and materials adversely affect the global supply chain because parts produced for aerospace and defense also support consumer industries including automotive, aviation, computers, medical devices, security systems, and telecommunications.

The manufacture and sale of counterfeit products is a widespread problem that affects manufacturers, distributers, and retailers in virtually every industry. According to the International Anti-Counterfeiting Coalition (IACC), the global trade in counterfeit has increased from $5.5B in 1982 to approximately $600B annually today. In the U.S. alone, the economic impact of counterfeit goods on businesses is estimated to be $200B to $250B annually.

Software counterfeiting is a huge criminal industry that is as lucrative as the drug trade and, like the drug trade, transcends national borders. Moreover, media reports suggest that, like other forms of organized crime, the counterfeiting industry has begun to turn violent. Truly effective anti-counterfeiting efforts will require far more aggressive and sophisticated tactics than government, law enforcement authorities, and software vendors have used to date.

1.2.5 COUNTERFEIT EVENT DESCRIPTION

From 2014 through 2020, Lo Ying directed the shipment of counterfeit computer networking equipment into the Southern District of Texas. Initially selling to a separate retailer in Arlington, Texas, and expanding to law enforcement acting in an undercover capacity. Over this time period, Mr. Ying sold counterfeit networking products through several business entities, often hiding behind layers of personal and corporate aliases to evade detection. Mr. Ying also used various means to conceal this unlawful conduct, including sending and receiving payments using accounts, seemingly unrelated publicly, to companies trafficking in illicit products. Mr. Ying and his customers would also agree to mislabel packages, break up shipments into separate components, alter destination addresses and use multiple forwarding companies based in the United States. When Herbert Falcon was notified by the Incident Response team that the switches purchased seemed to have an unusual number of defects and the screws may have been tampered with, the team decided to escalate the issue internally.

1.2.6 OUTCOME

A foreign-owned company is selling counterfeit IT equipment to federal agencies garnering huge profits while providing inferior products causing significant adverse network issues. The CIA has been notified and federal agencies have been prohibited from continued business with the vendor and affiliates.

1.2.7 ORGANIZATIONAL UNITS / PROCESSES AFFECTED – TAKEN FROM UNDERWRITER LABS – MITIGATING THE RISK OF COUNTERFEIT PRODUCTS

Legitimate companies have the most to lose from counterfeit products. Yet, despite widespread counterfeiting activities, many companies are unaware that they have a potential problem. Therefore, it's important to conduct an initial analysis of potential counterfeiting risks that exist within a given industry, and with certain types of products. Here are some of the key product factors that often lead to the greatest counterfeiting risks:

- High-volume, low-cost products - popular, low-cost products that can be easily copied and sold in large numbers.
- Products in high demand - A product that's in demand, regardless of its price, will attract the attention of counterfeiters.
- Products with large market share - A product or group of products with a large market share is an ideal target for counterfeiters.
- Luxury products - Often, savvy counterfeiters will focus on counterfeiting expensive luxury products.
- Products that lack security features - Security features, such as holographic labels or custom colors, deter counterfeiters since they make counterfeit products difficult to replicate and easier to identify. Legitimate products without such security features are easier to counterfeit.
- Complex, loosely controlled supply and distribution chains - Companies with a long and complex supply or distribution chain present multiple opportunities for counterfeiting, since there are multiple points at which a counterfeiter can enter or manipulate the chain.
- Purchasing components and materials based on price alone - Often, even product components are targets for counterfeit producers. Low-priced components may be attractive to legitimate manufacturers, but counterfeit components present the same risks as counterfeit finished products.
- Products sold on the Internet - Selling products online means a potential loss of control over distribution, making it easier for counterfeiters to sell counterfeit products without a manufacturer's knowledge.

1.2.8 MITIGATING STRATEGIES/SCRM CONTROLS

Many fake and counterfeit products are so identical in look and feel to genuine parts that it is getting harder to distinguish them visually. Procurement of safety-critical replacement parts can be a serious challenge and make

you vulnerable to a catastrophic risk of failure from unknowing use of counterfeit components. Moreover, conventional quality control efforts are found to be inadequate to address the challenge of counterfeit products. Whether you are a manufacturer, contractor, distributor, or a retailer, counterfeit products can affect your profits, market share and brand reputation and present a serious product liability risk from bodily injury and property damage. Although specific strategies may vary by type of products, industry segment, and procurement process, anti-counterfeiting experts and organizations recommend implementation of a comprehensive strategy to help reduce the risk of counterfeit products. The strategy should address two aspects:

- The first aspect is related to the procurement and related processes:
    - Always know your source for procurement of critical products and components. Buying from authorized/certified distributors provides at least some assurance of product quality and integrity of authentic parts. Buying on the Internet or other alternate sources (gray or black market) or importing directly increases your chance of becoming a victim of counterfeit product frauds.
    - If you are forced to procure a critical part from an alternate source because a part is not available from an authorized distribution channel, it is important to increase your own verification efforts to ensure integrity of parts by additional testing efforts. Sometimes, reconditioned and salvaged parts may be sold as new but may not meet specifications as represented.
    - Do not buy on lowest cost criteria alone. In tough economic times, there is temptation to buy at lowest cost. If the price offered is a deeply discounted bargain basement price compared to known price range for branded products, it should raise suspicion alerting further investigation.
    - Report suspected counterfeit products and distribution channels to law enforcement authorities and brand manufacturers. Ignoring knowledge about specific counterfeit products and sources of distribution can perpetuate this risk with potential for tragic consequences.
- The second part of the strategy should address detection and screening of incoming goods before they are used. U.S. Customs Services and authorities in many countries have portside inspection of incoming import shipments, but compared to the volume of imports, they cannot be relied upon to stop imports of fake counterfeit products into the country. Many counterfeit products are deceptively like authentic parts with logos, trademark and other look and feel characteristics and are getting harder to distinguish visually. However, they lack product integrity and performance quality of genuine parts. Although this does present a challenge, experts suggest some tips that may be helpful in this screening effort.
    - Unusual packaging or box
    - Inconsistent appearance, color, dimensions with specifications
    - Variations in items in a package
    - Modifications, touch up and cosmetic beautification of old/salvaged parts
    - Altered or worn manufacturer's name plate, model, serial numbers
    - Incomplete or inconsistent information on name plate, product markings, or certification
    - Irregularities in documentation:

        – Shipping papers

        – Certification and technical data

        – Lacking signatures and other required authentication of certain documents

        – Chemical and material test report and certification documents with handwritten entries or other indication (whiteout) of possible alterations

2 THREAT CATEGORY: EXTERNAL ATTACKS ON OPERATIONS AND CAPABILITIES (CYBERSECURITY)

2.1 SCENARIO: ATTACKER EXPLOITS KNOWN VULNERABILITIES IN SUPPLIER SYSTEMS CONNECTED TO CRITICAL INFRASTRUCTURE ORGANIZATION NETWORKS

2.1.1 BACKGROUND

A critical infrastructure organization allows a supply chain vendor to access its network to process IT functions. The supply chain vendor lacks basic security controls that provide visibility into the range and numbers of assets connecting to its network. Further, the supply chain vendor only scans for vulnerabilities on an annual basis, as part of a compliance requirement. The supply chain vendor also fails to plan and prioritize its vulnerability mitigation practices.

As more devices are connected, the attack surface expands, often in unexpected places, such as building management systems and CCTVs. These systems perform multiple functions, such as managing access to specific doors, controlling door alarms, creating the photo IDs that allow facility access and monitoring for access.

2.1.2 THREAT SOURCE

Vulnerability exploits can be performed by hacktivists, cyber criminals and criminal organizations, or nation-state actors. The threat actor will compromise the supply chain vendor's IT environment/network and then gain access to the IT environment/network of the critical infrastructure organization.

2.1.3 THREAT IMPACT

The security program of the supply chain vendor is generally assessed on an annual basis in which significant trust is assumed contractually via supplier security controls. Coupled with the minimal annual assessment for vulnerabilities by the supplier, there exists significant period for which vulnerable systems remain unpatched.

In this instance, the adversary has gained unfettered physical and logical access to the critical infrastructure provider. The adversary will have the ability to operate at will within the critical infrastructure networks and systems, to include operational technologies that may result in denial of service, disruption of service, or life safety issues.

Given the lack of fundamental security controls at the supply chain vendor, they will have no insight into the attacker's path, likely requiring a complete rebuild of their IT systems and networks to a known good baseline. Depending upon the types of services provided by the supply chain vendor, the critical infrastructure organization may also be impacted by the remediation and recovery activity within the supply chain vendor's environment.

2.1.4 VULNERABILITY

The vulnerability from the critical infrastructure providers perspective is the supply chain vendor with inadequate security controls. The vulnerability from the supply chain vendor's perspective are the system vulnerabilities that should be appropriately managed and mitigated. The supply chain vendor's hardware, firmware, and software components of IT systems must be kept patched or otherwise mitigated.

2.1.5 THREAT EVENT DESCRIPTION

Coupling together three vulnerabilities in the past year, an attacker could setup a Zoom video conference, for example, with any target at the critical infrastructure organization. Once connected, the attacker can control the

attendee's screen by exploiting a vulnerability in Zoom, allowing them to download and install malware on the target's computer. With access to the target computer, the attacker can then exploit the building management system allowing physical access to the building. Now that the attacker can access the facility, the last step is to ensure the CCTV does not record their intrusion by exploiting the CCTV system.

In this scenario, an attacker could exploit software vulnerabilities to gain administrator rights within the critical infrastructure provider's systems, enabling them to create fraudulent IDs, disable door locks and alarms, access sensitive authorized user data, and delete video footage.

2.1.6 OUTCOME

The threat actor has secured the ability to physically access the facilities of the critical infrastructure organization. The threat actor could destroy elements within the facility making it impossible for the critical infrastructure provider to keep this facility operational.

2.1.7 ORGANIZATIONAL UNITS / PROCESSES AFFECTED

Physical security/inability to trust cyber-physical systems.

Information security/incident response - Limited insight into the nexus of the security events due to supplier systems that are ephemeral on the provider network, as well as limited visibility into the security of the supplier devices.

Operational technology or operations/physical access to critical systems.

2.1.8 MITIGATING STRATEGIES / SCRM CONTROLS

When evaluating a supply chain vendor, assess their Vulnerability Management program, by which the organization can track, assess, prioritize, and remediate known vulnerabilities across their entire attack surface in a timely manner before they can be exploited. Strategies to help prevent the exploitation of known vulnerabilities include:

- Identify business operations and assets most vulnerable to cyber-attacks, to include third party, OT, and IoT assets; for many organizations, the most critical assets are those that have the highest monetary value attached to them; for the government, this may be those deemed most mission critical.
- Utilize continuous threat intelligence to prioritize remediation efforts considering the overwhelming number of new vulnerabilities; organizations should use contextual factors including asset criticality and whether there are exploits available for specific vulnerabilities, in prioritization.
- Frequent scanning and reporting are critical because out-of-date data can be just as damaging as inaccurate data. The Center for Internet Security (CIS) Control 3.1 recommends automatically scanning all systems on a weekly or more frequent basis.
- However, organizations also need to make sure their reporting is aligned with their patch remediation cycle so that reporting and updates are relevant.
- Identify the security gaps and opportunities to reduce complexity in the IT security infrastructure that leaves organizations vulnerable to cyberattacks.
- Measure the value of responding to vulnerabilities through automation and machine learning.
- Designate and document security staff overseeing the most critical assets.
- Better utilize IT security staff and resources to improve the efficiency of vulnerability management.

2.2 SCENARIO: INCORRECT BGP ROUTING

2.2.1 BACKGROUND

The **Border Gateway Protocol** (**BGP**) is a standardized exterior gateway protocol designed to exchange routing and reachability information among autonomous systems (AS) on the internet. By design, routers running BGP accept advertised routes from other BGP routers by default. This allows for automatic and decentralized routing of traffic across the Internet, but it also leaves the Internet potentially vulnerable to accidental or malicious disruption, known as *BGP hijacking*.

In this example scenario, the internet traffic between the organization, a municipality, and the internet is rerouted for several hours.

2.2.2 THREAT SOURCE

Nation-state actors conducting espionage activity and cyber criminals are potential perpetrators of this type of attack. For example, in 2018, cyber criminals conducted BGP hijacking and DNS cache poisoning in an apparent attempt to steal payment card data or conduct reconnaissance for future targeting of either payment processors or merchant point-of-sale (POS) networks.

In this example, the attacker is a cyber-criminal seeking to discover all the partner organizations that this municipality has regular communications with. The cyber-criminal will then seek to hack into one of the partner organization and gain access to the municipality via the partner IT environment.

2.2.3 THREAT IMPACT

The threat impacts are both immediate and longer term. The immediate impact is that all internet traffic to and from the municipality is slowed while this attack is underway. The longer-term impact is that the municipality becomes incrementally more exposed to ransomware and other cyberattacks because the threat-actor now knows which organizations the municipality has regular network-to-network communications with.

2.2.4 VULNERABILITY

All Internet Service Providers (ISPs) have not implemented measures to ensure BGP announcements are coming from a legitimate source.

2.2.5 THREAT EVENT DESCRIPTION

Users initially noticed a delay in certain internet traffic. The municipalities networking team investigates the traffic delays. A traceroute shows a route that normally takes two or three hops is now taking more than ten and is routing via China. Further investigation shows that a co-location company leaked routes to a foreign Tier 1 ISP. The ISP then announced these routes on to the global internet redirecting the municipality's internet traffic through China Telecom's network.

2.2.6 OUTCOME

The incorrect routes were in circulation for several hours. During this time traffic was routed through China. This routing gave the threat-actors the ability to copy the traffic, analyze it and determine which organizations the municipality had established network-to-network connections.

Once the incorrect routes were discarded, internet routing traffic returned to normal.

2.2.7 ORGANIZATIONAL UNITS / PROCESSES AFFECTED

In this example, all organizations that had traffic rerouted could have noticed their internet traffic slow down during the attack. Additionally, all these organizations could also be subsequently attacked by the same, or other, threat actors, because of what was learned by the analysis of the rerouted traffic.

2.2.8 MITIGATING STRATEGIES / SCRM CONTROLS

Organizations evaluating ISPs can inquire about the policies, procedures, and ability to detect and prevent such traffic rerouting attacks. The service provider can be asked if they are a member of the Internet Society's Mutually Agreed Norms for Routing Security (MANRS) project.

This threat scenario, is addressed in:

- CSRIC Working Group 3 -- Report on Best Practices and Recommendations to Mitigate Security Risks to Emerging 5G Wireless Networks
- NIST, Protecting the Integrity of Internet Routing: Border Gateway Protocol (BGP) Route Origin Validation

References:

- Border Gateway Protocol - Security
- Craig Timberg (2015-05-31). "Quick fix for an early Internet problem lives on a quarter-century later". The Washington Post. Retrieved 2015-06-01.
- BGP hijacking
- DNS spoofing
- Lawrence Abrams, "U.S. Payment Processing Services Targeted by BGP Hijacking Attacks," 2018.

2.3 SCENARIO: RANSOMWARE

2.3.1 BACKGROUND

Ransomware is a type of malware where the target's computer is rendered unusable, typically by locking the user out of their system(s) or encrypting some, or all, of the data on their system(s). The attacker then demands a monetary (bitcoin, etc.) ransom so that the target can receive the key to recover their data or access their system. Ransomware is also used as a cyber red-herring to give responders something to focus on while the attacker has other objectives within the organizations systems. Lastly, cyber attackers have been seen using ransomware's encryption capabilities to permanently lock victim systems with the ultimate intent to destroy those systems and force the victim into a lengthy and expensive recovery process.

2.3.2 THREAT SOURCE

As supply chains have become more digitized, companies have occasionally fallen short of ensuring that they have the necessary measures to deal with cyberattacks by malicious actors. For example, companies may fall victim to ransomware attacks multiple times during a year. Ransomware attacks are most typically propagated by individuals or groups seeking monetary gain. These attackers may be non-nation-state threat actors operating either with or without host government approval, nation-state threat actors, or nation-state threat actors conducting ransomware attacks in their off hours.

This threat scenario will address the use case where the threat actors are financially motivated.

2.3.3 THREAT IMPACT

The impacts of ransomware attacks are becoming increasingly consequential. Threat actors are now conducting these potentially destructive attacks against governments, hospitals, and critical infrastructure. Another recently implemented tactic is for the ransomware attacker to steal data from the organization and threaten to release that stolen data in order to further compel the victim organization to pay the ransom. For those organizations that choose to not pay the ransom, the process of rebuilding their IT Infrastructure can take months and potentially lead to permanent data loss, thus directly impacting the time that IT-based services and operations are off-line.

In this threat scenario, the attacker has stolen data and encrypted the organizations systems, the organization has chosen not to pay the ransom and now must deal with both the destruction of their systems as well as the public release of citizen Personally Identifiable Information (PII).

2.3.4 VULNERABILITY

Ransomware can establish a foothold within an organization in a variety of methods; these include, broadly distributed spray-and-pray attacks, specifically targeted attacks, and self-propagating ransomware such as that used in the 2017 WannaCry attacks. Additionally, attackers continue to utilize email-based attacks, watering-hole attacks, public-facing web server attacks, social engineering, and even dropping malware-laden Universal Serial Bus (USB) drives near the organization that they wish to attack.

Ransomware attackers have also utilized the email attack vector to deliver fictitious invoices to deliver malware-laden documents to recipients. If received by the right person, a fictitious invoice, from a supply chain partner might be effective at getting the recipient to open the document or install a specific piece of malware.

The attack vectors here are many; ransomware is typically delivered after an initial system has been exploited by one of the methods listed above. Once the system is exploited, the attackers can then download additional tools to further explore the organizations network and IT environment or they can download ransomware to conduct the attack against that first compromised system.

It is very common to find that an organization that has a ransomware event had systems that were unpatched. Vulnerabilities, therefore, may exist in many elements within the enterprise IT systems as well as its people.

2.3.5 THREAT EVENT DESCRIPTION

In this example ransomware scenario, the threat actor is specifically targeting a government contractor organization. The threat actor uses email and a phone message to pose as a conference organizer with information about a conference that will be heavily attended by the leadership from the government contractor's largest customer. The email and voice mails are specifically coordinated to target at a few people within the government contractor organization. The voice mail notifies the targets to expect the email. The email contains a URL to a web page designed to look like a legitimate conference webpage. The government contractor target opened the email and clicked on the URL which contained malicious code that infects the target's computer thus giving the threat actor their first electronic foothold within the victim IT environment.

Once the victim's system was exploited, the attacker was able to remotely control that system. This control allowed the threat actor to download additional malware, explore the enterprise IT environment, steal valuable data, determine which systems were most valuable, and finally launch the ransomware.

2.3.6 OUTCOME

In this example the threat actor had the victim's core business systems disabled. The threat actor further demonstrated that they also possessed sensitive data that the victim would not want released to the public. The victim organization then had to make the pay/no-pay decision.

Regardless, if the victim organization pays the ransom, or not, the victim organization is compelled to conduct a full incident response (IC) to ensure that the threat actor is fully removed from the organization's systems.

In this example, the victim organization decided to not pay the ransom. An abbreviated list of the outcomes for the organization follows, the victim organization had to:

- Rebuild the systems that were destroyed by the ransomware.
- Stand up manual interim processes to enable the organization to continue to operate.
- Restore old data from backup.
- Integrate the data from the manual process period.
- Report the incident and the loss of sensitive data.
- Deal with fines and lawsuits regarding the loss, and release, of the sensitive data.

This restoration and recovery process took the organization months and resulted in a substantial loss of citizen goodwill for this municipality. Having many systems offline for weeks or months also resulted in loss of income and substantial unexpected expenses.

2.3.7 ORGANIZATIONAL UNITS / PROCESSES AFFECTED

The organizational units impacted by this attack include nearly every component of the victim organization as the supporting IT infrastructure had to be restored, recovered from backup, etc. Additionally, the citizen data that was released potentially impacted those citizens.

Processes affected include the victim organization's core business processes. Therefore, while the incident response was being conducted and the restoration and recovery were being conducted, the organization had to operate on manual or temporary systems.

2.3.8 MITIGATING STRATEGIES / SCRM CONTROLS

A ransomware attack is a cyberattack regardless of whether it's targeted or how it's delivered.

Therefore, ransomware prevention strategies are part of the organization's overall cyber risk management strategies. Organizations should follow well known risk management strategies such as those presented in the NIST Risk Management Framework.

A ransomware event can bring additional challenges to the victim organization.

These additional challenges, and their respective example management documents from NIST are:

- Data Protection - SP 1800-11(Draft) Data Integrity: Recovering from Ransomware and Other Destructive Events
- Disaster Recovery - SP 800-34 Rev. 1 Contingency Planning Guide for Federal Information Systems
- Incident Response Planning - SP 800-61 Rev. 2 Computer Security Incident Handling Guide

2.4 SCENARIO: REMOVAL MEDIA ATTACK

2.4.1 BACKGROUND

Threat Actors have utilized removable media, such as USB thumb-drives and CDs, to insert malware into an organization's computer systems. Examples of such methods and attacks are:

- Operation Buckshot Yankee
- Krebs On Security, "State Govts. Warned of Malware Laden CD Sent Via Snail Mail from China," 2018.

For organizations that do not have the appropriate security controls in place, when removable media is inserted into a computer, that system can look for executable files and attempt to run those programs. This can result in malware bypassing all network perimeter defenses and getting installed on the victim's computer.

2.4.2 THREAT SOURCE

Nation-state cyber threat actors have been behind the news-worthy events of these removable media attacks. Other cyber attackers, such as cyber criminals and cyber hacktivists, can also easily use this attack method. If the victim organization is within the supply chain of another organization the attacker can leverage the relationships and connectivity between the two organizations to move up and down the supply chain.

2.4.3 THREAT IMPACT

Potential impacts include:

- Disruption of supply chain delivering their products and services.
- Supply chain organizations being breached exposing their data and systems to theft and destruction.
- Threat actor moving to partner, supplier, and customer networks to conduct data manipulation, data theft, and data/system destruction.
- Threat actor using a supply chain organization as platform from which to launch attacks against others beyond those listed above.
- Unexpected financial impacts can include remediation, penalties, fines, lawsuits, falling stock value, etc.

2.4.4 VULNERABILITY

The vulnerability is that there is no prevention of, or pre-scanning of the malicious removable media prior to the removable media being read by the internal computer system. Removable media is delivered to an employee and that media is inserted into a computer system that can be compromised by the malware contained in/on the removable media.

2.4.5 THREAT EVENT DESCRIPTION

In this example scenario, the threat actor is attempting to compromise the products of the supply chain organization. The products are physical security systems being manufactured by the supply chain organization. The threat actor seeks to be able to remotely monitor and control the physical security systems of the supply chain organization's customers.

The threat actor drops many USB drives, containing malware into the parking lot of the supply chain vendor. The USB drives are labeled with the supply chain organization's logo, and the USB drives contain file objects that appears to be related to the supply chain vendor's business.

Many employees pick up the USB drives, carry them into the organization, and insert them into the USB ports of their computers. Some employees seek to return the USB drives; others are curious about the USB drive contents. In one study,[ix] 48 percent of the distributed USB drives were inserted into the organization's computers.

Once inserted, the computer can "autorun" the malware installation program. The employee can also attempt to open files, some with an alluring file name, thus allowing the malware to start running, become installed, open an electronic backdoor into the computer, and beacon to the external attacker. This activity results in the attacker gaining access to that system.

Once the threat actor has persistent backdoor access into one of the supply chain vendor's systems, the threat actor can continue the attack.

2.4.6 OUTCOME

The threat actor is successful with their mission of compromising the physical security systems being manufactured by the supply chain organization. The supply chain organization's customers are now purchasing systems that can be remotely controlled by the foreign military-intelligence organization. The supply chain organization is providing software updates to their existing customers, and these updates contain the malicious capabilities as well.

The attacker is now able to remotely monitor and control their customer's entire physical security systems.

The attacker now also has a foot hold in each of the supply chain organizations customer's networks. This can enable the attacker to launch additional attacks into each of those organizations.

2.4.7 ORGANIZATIONAL UNITS / PROCESSES AFFECTED

The supply chain organization is compromised, and the attacker can move freely within their network and systems. The supply chain organization's products have been compromised; therefore, their customers are also potentially affected. The compromised physical security system is now a platform from which the attacker can begin to attack each organization where their security system is installed.

2.4.8 MITIGATING STRATEGIES / SCRM CONTROLS

The buyer organization, conducting this analysis, would evaluate:

- The extent to which potential supplier organizations protect themselves from removable media type attacks.
- The extent to which the organizations are connected electronically.
- The extent to which the supply chain organization has a security training program and mature security-focused software development and distribution practices.
- Internal security controls, such as micro segmentation, so that such a compromised system would not be able to move electronically throughout the IT environment or communicate outside of the organization.

This threat scenario, removable media, is addressed in:

- NIST SP 800-53 Rev 4 Security Control: Media Protection.

[ix] Robert Lemos, "How to keep USB thumb drive malware away from your PC," PC World, 2016.

- NIST SP 800-161 [Supply Chain Risk Management Practices for Federal Information Systems and Organizations] references NIST SP 800-53 Rev 4 Security Control: Media Protection.

2.5 SCENARIO: RESOURCE DEPLETION

2.5.1 BACKGROUND

Unintentional/accidental resource depletion is a non-adversarial threat resulting from system misconfigurations or lack of resource planning. System events resulting in resource depletion/accidental shutdown may vary from misconfiguration of information systems and network connectivity to improper software updates within production environments.

Organizations operating without the appropriate security controls in place will experience regular system and network outages inadvertently caused by uncontrolled/unmanaged changes to their environments. This will cause a reduction in the organizations overall systems and network availability.

2.5.2 THREAT SOURCE

Internal; non-malicious.

2.5.3 THREAT IMPACT

The lack of resource planning or proper configuration management policies and procedures creates a direct and indirect impact to the availability of key information technology systems within the organization's supply chain. Indirect impacts may include delayed delivery of products and or solutions, while direct impacts may be the loss of services within active environments. Specific examples for provided services would be failed service level agreements with cloud providers, managed security service providers (MSSPs), and systems integrators. Physical examples would be the lack of power or environmental support to expand a technical footprint within a data center.

2.5.4 VULNERABILITY

The vulnerability is the lack of (or lack of enforcement of) change management and configuration management policies and procedures within the organization.

2.5.5 THREAT EVENT DESCRIPTION

When analyzing this threat scenario, the organization creates a fictitious, or potential, threat source described as an internal employee with non-malicious intentions.

In this scenario, the supply chain organization recently hired a new network engineer who identified some inefficiencies in the existing network configurations. The network engineer updates the system routing configurations and applies the updates to the production network without recording the updated configurations.

2.5.6 OUTCOME

The internal employee unintentionally caused an accidental network unavailability. The unavailable network impacted the availability of the supply chain organization's enterprise applications, in-turn creating a negative impact on the supply chain organization's ability to deliver products or services.

2.5.7 ORGANIZATIONAL UNITS / PROCESSES AFFECTED

The supply chain organization may experience productivity inefficiencies caused by system or network outages possibly impacting their ability to support or deliver on their contracts. The supply chain organization's customers may also experience impacts to their existing operations through system/service availability or product supply.

2.5.8 MITIGATING STRATEGIES / SCRM CONTROLS

The buyer organization, conducting this analysis, would evaluate:

- The presence of configuration management policies and procedures that are in place and actively enforced.
- Assess the overall impact of vendor system or network outages will have on the organizations operations.
- Assess the overall impact of vendor system or network outages will have on the vendors ability to meet contractual requirements.

PRODUCTS AND SERVICES THREAT SCENARIO

2.6 SCENARIO: CYBERSECURITY (TRUSTED CONTRACTOR)

2.6.1 BACKGROUND

One key component of supply chain risk management is the supply chain of contract workers. Corporations, enterprises, organizations, agencies, etc. (collectively referred to as organizations in this section) often engage contract and temporary workers in the fields of IT, cybersecurity, as well as other parts of the business. These contractors bring significant risk comprising both internal and external components. The contracted individuals may also be temporary workers or "1099's" (hourly, or non-employees) to their contracting agency. These risks can result in threats that include insider threat, espionage, and increased vulnerability. This section addresses some of these risks, threats, vulnerabilities and mitigations.

2.6.2 THREAT SOURCES

Trusted contractors are often provided with extensive access to a company and its resources and may be treated as employees. That level of access and trust results in substantially increased risk. Often contractors (and other temporary help) have less rigorous vetting processes than full time employees, they and are often provided by agencies who are relied on to provide the vetting. Those contractors and their agencies become part of an organization's supply chain. Moreover, the contractor may have a new, informal, or periodic relationship with the contracting agency. Thus, both the contractor and their supplying agency become part of the supply-chain risk to an organization.

In addition, and due to the considerations above, an organization may have more limited recourse or control of management of a situation where a risk or vulnerability is exploited by a contractor.

The sources of the threat and risk of malicious trusted insiders are manifold. Organizations often manage cost by keeping their full-time employee staffing as lean as possible, then fill the production needs with temporary and contract workers. Organizations adopting new technologies, new products, new operational models, or new business areas often bring on temporary staff and contractors to get them over the hump of adapting, adopting, and integrating the new elements. Astute and vigilant bad actors can watch for such opportunities and position themselves to be brought in at the time when outside help is most needed.

In another section, espionage is discussed as a component of supply chain risk. It is described as a problem that costs the American economy hundreds of billions of dollars per year and puts national security at risk. Please refer to that section for further discussion on this topic.

2.6.3 THREAT IMPACT

Trusted contractors are a subsect of "insider threats." Insider threats have proven to be a major risk to organizations as they have access and opportunity, impeded only by proper motivations and effective risk management controls. An insider with bad motivations and inadequate security controls has an opportunity to wreak havoc on an organization, or act as a saboteur. The impact can be exfiltration of intellectual property, personal identifiable information, and other sensitive restricted information. The other legs of the platform can also be impacted. An insider can detrimentally affect confidentiality of information, communications, and operations. An insider can also affect the integrity of information, communications, and operations. Such impacts from a trusted contractor, gone rogue, can be catastrophic to an organization, its employees, its customers, its partners, as well as the other parts of its entire ecosystem.

Trusted contractors can also effect, facilitate, or exacerbate an external threat. An insider can feed the malicious external threat actor the information they need to compromise an organization's systems. Such information can include network architectures, security architectures, credentials, processes, procedures, etc. Even on the physical security side, a malicious insider can both figuratively and literally leave the door open to threat actors. Many medium-risk threats can escalate to high-risk when an insider has direct access to physical systems and networks. Many organizations still, either purposely or inadvertently, follow a hard-shell/soft-center security control model.

2.6.4 VULNERABILITY

Organizations are vulnerable to the threat of malicious trusted contractors. The key factor is that their guard can be down because the contractors or other temporary employees are "trusted." Someone walking in from the street, with no working relationship to the organization, would not be allowed to roam freely in the organization, nor would they be allowed free and unfettered access to the data, information, networks, processes, or organizational operations. But the "trusted" contractor or temporary employee does have access that no stranger would be granted. This situation illustrates the vulnerability that organizations have to the risk of trusted contractors. And, again, there is a propensity to architect networks, processes, operations, and even physical systems in a hard-shell/soft-center paradigm.

2.6.5 EVENT DESCRIPTION

The possible consequences from a malicious trusted contractor, trusted temporary, trusted insider have been described above. These events are only the tip of the iceberg. A smart and imaginative insider with malicious intent can wreak havoc in numerous ways. An analogy would be the threat model of innumerable bad-actors, or hackers, attacking an organization with a limited number of defenders; the ratio of attackers to the defenders demands more creative approaches to mitigations. Such mitigations are described below.

2.6.6 OUTCOME

The threat if unanticipated, undetected, and unmitigated can cause catastrophic outcomes resulting in loss of reputation, business, sensitive or restricted information, money, or legal action as a result of negligence.

2.6.7 ORGANIZATIONAL UNITS / PROCESSES AFFECTED

All organizational units in an organization are vulnerable to and possibly affected by the threats and impacts of malicious trusted contractors. Moreover, a malicious contractor, as with other insider threats, can often move laterally within an organization to other organizational units. This movement can be physical or virtual. Virtual

lateral movement may be accomplished by means of corporate networks, local area networks (LANs), cloud services, and other organizational resources available to authorized insiders.

2.6.8 MITIGATING STRATEGIES / SCRM CONTROLS

- The principal strategic approach to risk mitigation is adopting a zero-trust model. It provides the broadest protection against a malicious insider threats as well as that of malicious contractors.
- Second, implement least privilege principles. Least privilege can limit the damage from insider threat.
- Third, rigorous Identification, Authentication, Authorization, Auditing, and Accounting (IAAA) –access controls to support both least privilege and zero-trust.
- In addition to the "accounting" aspect of IAAA, implement appropriate comprehensive logging of systems and network traffic.
- Implement comprehensive air-gapped backups to facilitate recovery in case of ransomware, as well as for more routine disaster recovery or business continuity purposes.
- If possible, implement pre-forensics technologies to facilitate incident response, threat actor tracking, and recovery, and develop and test an incident response (IR) plan.

In addition to the technical controls listed above, supply-chain controls and mitigations should be implemented to manage the risk of a malicious contract worker. Some of these strategies and controls include using known and vetted suppliers of contract workers, performing background checks and reference checks on the contract worker independent of those done by the provider, documenting and implementing legal and contractual controls on the provider, etc.

3 THREAT CATEGORY: INTERNAL SECURITY OPERATIONS AND CONTROLS

3.1 SCENARIO: POOR ACCESS CONTROL POLICY

3.1.1 BACKGROUND

An organization has a small legacy network, which has been maintained over a period of 10+ years but has not been assessed for risk or security threats in quite some time. The network is mostly static in nature, in both configuration and system level/type (operating system, patch, function, applications, etc.). Over that period, the team responsible for monitoring and managing the security of this network has changed several times, with no update or re-check of policies and procedures.

The organization has decided to perform some routine network checks prior to upgrading other portions of the infrastructure and has called in a pre-existing vendor to verify systems and configurations.

3.1.2 THREAT SOURCE

The systems involved are part of legacy wireless infrastructure which still routes traffic in certain areas and is also available as fallback for emergency or backup situations.

While the current infrastructure has been through audits and assessments over time, the legacy infrastructure has largely been signed off as status quo.

3.1.3 THREAT IMPACT

With the right kind of elevated privilege access, a malicious user could cause catastrophic impacts on a system, but even low-level user rights can typically allow enough permissions to cause harm or use the compromised host

as a beachhead, launching attacks into other systems. A lack of proper access controls can not only result in unauthorized access and subsequent destruction, manipulation, and other malicious activity, but also make incident response investigations difficult or impossible due to the inability to trace back the activity. Thus, impact across a group of assets could be wider than the actual attack scope; if the company lacks proof that hosts or data were accessed, one might be required to assume that they were compromised due to breach notification (or similar) laws.

3.1.4 VULNERABILITY

While the network routes a relatively small amount of traffic, it does have access to a large amount of subscriber information that is maintained for the current infrastructure. The systems control access to sensitive user data, Domain Name System (DNS) function and routing of user traffic in, out, and through the legacy network.

3.1.5 THREAT EVENT DESCRIPTION

Due to weak access control policies, years-old user accounts from the equipment vendor are still functional. Some of these user accounts allow root or privileged access and are not uniquely identifiable as belonging to an individual or even to a certain company. The credentials for these accounts have become compromised and a malicious attacker has used them to gain access to the legacy network, where additional attacks can be sourced from.

3.1.6 OUTCOME

The following illustrates some of the weaknesses exposed in an attack chain that could be sourced from this supplier:

- Some equipment is accessible directly from the enterprise network, not via a firewall or Demilitarized Zone (DMZ);
- User accounts are not uniquely identifiable, reviewed or changed;
- User sessions are not controlled and vulnerable to typical brute force account access methods; and
- Potential violations of user access are not alerted.

Given the above factors, an attack would not only likely be successful but also would go undetected for a long time unless service was otherwise impacted (e.g., user traffic stopped passing or was degraded). Simple dictionary or brute force attacks would likely be successful due to access control and account management policies. Thus, theft or manipulation of data, either through man-in-the-middle or exfiltration would be possible. In addition, other defenses or mitigations set up elsewhere in the network could be negatively impacted or changed from within.

3.1.7 MITIGATING STRATEGIES / SCRM CONTROLS

Carnegie Mellon's eleven essential practices for cyber hygiene should help mitigate the risk associated with this scenario. Proper access control means protection of system resources against unauthorized access; a process by which use of system resources (e.g., executable programs, network configuration data, application file systems, network databases, etc.) is regulated according to a security policy and is permitted only to authorized entities (users, programs, processes, or other systems) according to that policy.

Authentication and authorization are basic security methods, which provide the means to ensure the identity of users and limit their use of network resources to predefined activities or roles. They can thus be used to protect network operators against any unauthorized use of the network's services.

Furthermore, user authentication provides a basic mechanism for logging and auditing the management activities, which makes it possible to track activities afterwards. Providing each user with a unique user identification (ID) and password together with a certain profile (privilege level) makes it possible to limit user's access to only those management activities they require in order to perform their task.

Enforcing the strong password selection, password aging (which enforces the users to change their passwords at predefined intervals), two-factor authentication, and the encryption of the files containing the user ID and password data (to prevent unauthorized users to obtain sensitive data) provide additional security.

It is also recommended to implement restrictions on the rate of login attempts, concurrent login attempts, and lockout periods for incorrect login attempts and monitored alerts for incorrect login attempts.

Security event logs or audit trails are of fundamental importance to an operator in detecting malicious activities by defining the indicators of such behavior. The log also establishes accountability for malicious users committing internal fraud or sabotage. The security event logging should be compliant to open standards to permit the administrator to perform archival and analysis of logs and for post-incident evidence gathering and investigation.

The first step to detect harmful activities is to know the indicators for such behavior. The earlier such an activity is detected, the more time is left to take appropriate countermeasures.

3.2 SCENARIO: DEVICES THAT DO NOT AUTO-UPDATE FIRMWARE (IMBEDDED SPINAL CORD STIMULATOR WITH A HAND-HELD CONTROLLER)

3.2.1 BACKGROUND

Failing to update your software does not just mean you will not have the latest version; it means you could be exposed to major security vulnerabilities that could also affect your physical wellbeing. There is medical technology today that allows patients to control their comfort levels by carrying a hand-held device to monitor and control implantable medical devices. After numerous, unsuccessful surgeries, a patient received a surgically implanted spinal cord stimulator to address years of chronic back pain. The stimulator tricks the brain to thinking the pain is gone.

3.2.2 THREAT SOURCE

Unauthorized individuals potentially accessing the device and changing the setting that control and monitor the comfort level of a patient. The hacker could turn the controller completely off making it impossible for the patient to active the device and receive the benefits provided by the device to manage pain.

3.2.3 THREAT IMPACT

In cases where a device is assumed to only be in a domain with authorized access allowed (the opposite of Zero Trust environments), malicious actions can result in significant impacts to both the device/service and the user/host. Potential impacts in this scenario are financial impact to the device company, harm to the reputation of the medical services company, and potential physical harm to the patient(s) involved.

3.2.4 VULNERABILITY

Hand-held devices do not auto-update and requires live conversation with a help desk and, in some instances, a trip to the patient's health care provider must take place to update the firmware and sync the device.

3.2.5 THREAT EVENT DESCRIPTION

Unauthorized individuals accessing the device and changing the settings that control/monitor the comfort level of a patient. The hacker could turn the controller completely off making it impossible for the patient to activate the device and receive the benefits provided by the device to manage pain. Conversely, the hacker could turn the controls up or down making the pain encountered by the patient intolerable.

3.2.6 OUTCOME

Since the device does not appear to allow hackers to gain access to a patient's medical/personal history, the primary threat is controlling the device itself, which in some instances (i.e., pacemaker) could be life altering.

3.2.7 MITIGATING STRATEGIES / SCRM CONTROLS

- To mitigate the seriousness of such an attack, patients who have an imbedded device that require updates from time to time should ensure that their contact information is kept up to date with the manufacturer of the medical device, as well as their health care providers so that the patient can be notified when an update to a device is required;
- Periodically, contact the manufacturer of the device for firmware updates; and
- Make regular appointments with healthcare provider to ensure the device is working properly.

3.3 SCENARIO: MISHANDLING OF CRITICAL OR SENSITIVE INFORMATION

3.3.1 BACKGROUND

An energy company supplier, Griffon Power, routinely handles marketing and technical information on industrial components used throughout their network. These are sometimes internal in nature but are generally marked as such. Recently, a small team within the company reviewed confidential external information from a domestic supplier on parts that were proposed for new turbines. These documents were highly sensitive in nature and shared under a non-disclosure agreement (NDA).

3.3.2 THREAT SOURCE

As part of the project analysis, the team set up a shared network drive to distribute and review information. All information related to the project was stored within this folder, which was only accessible internally. Griffon Power ultimately decided not to go forward with the new turbine offering and moved on with other business. About a year later, as part of a network cleanup and upgrade effort, network storage was decommissioned and sold off to an offshore company for parts.

Much of the NDA-level information shared between Griffon Power and the potential supplier has not been properly handled and is now exposed to a third-party company.

3.3.3 THREAT IMPACT

When intellectual property is left completely exposed, the financial impact could be as minimal as the total value of the asset, or as high as the value of an entire business unit, product line, or future business plans, depending on the nature of the data.

3.3.4 VULNERABILITY

Not having a process to properly decommission network storage, which was eventually sold off to an offshore company for parts.

3.3.5 THREAT EVENT DESCRIPTION

Proprietary information on the inner workings and specialty parts of turbines that are used throughout energy companies has been made available and sold on the dark web. This could be used for economic or blackmail purposes or by foreign competitors to gain an unfair advantage in the market.

3.3.6 OUTCOME

Some of the weaknesses exposed in Griffon Power's policies on the handling of data are:

- Failure to wipe data that is no longer used;
- Failure to classify data – then handle and protect according to the classification;
- Failure to implement document-level encryption for sensitive data; and
- Failure to audit systems prior to decommissioning.

3.3.7 MITIGATING STRATEGIES / SCRM CONTROLS

Data management policies can have a broad range of useful steps that could prevent such risks in this scenario. All data should be classified according to its intended use, who can access it, and if or how it can be shared. In addition, data tags could be set according to whether it is Public, Limited Release, Internal or Confidential (for example). Depending on how the data are classified, it may need to be encrypted and have access to the data controlled and monitored.

Separately, companies should have a process and policy for decommissioning equipment and perform regular audits before any such equipment is released, sold or distributed. At a minimum, any non-public data should be removed from any systems; in most cases, it is advisable to perform a complete wipe of data or destruction of storage devices to a sufficient level that data cannot be recoverable later.

3.4 SCENARIO: LACK OF ASSET VISIBILITY AND VULNERABILITY EXPLOITATION

3.4.1 BACKGROUND

An organization in the supply chain lacks visibility into the range and numbers of assets connecting to its network. Further, this organization only scans for vulnerabilities on an annual basis, as part of a compliance requirement. The organization also fails to plan and prioritize its vulnerability mitigation practices.

3.4.2 THREAT SOURCE

Many high-profile incidents, including the Equifax breach and WannaCry, could have been prevented through better cyber hygiene. Fifty-seven percent of enterprises that experienced a breach in the past two years state that a known, unpatched vulnerability was the root cause.[x]

The discovery and disclosure of vulnerabilities continue to grow in volume and pace. In 2018 alone, an average of 45 new vulnerabilities were published every single day, for a total of 16,500, up from 15,038 in 2017.[xi]

With 59 percent of all vulnerabilities in 2018 rated as Critical or High severity, security organizations are challenged to determine which vulnerabilities truly represent a risk and prioritize the most critical vulnerabilities

[x] "State of Security Response," Ponemon/ServiceNow, 2018
[xi] Primary Research, Tenable Vulnerability Intelligence

to maximize limited remediation resources. After all, the proportion of Common Vulnerabilities and Exposures (CVEs) with a publicly available exploit was seven percent in 2018, down one percentage point from 2017.

3.4.3 THREAT IMPACT

In scenarios where Governance, Risk and Compliance (GRC) policies are not followed and asset inventory is therefore unknown and exposed, an attacker could exploit vulnerabilities, compromise data, and then cover their tracks without evidence. Without a proper asset valuation and inventory, it is not possible to assess risk, and it must be assumed that maximum impact is possible to the organization or assets.

3.4.4 VULNERABILITY

The vulnerability in the scenario is that the organization in the supply chain lacks visibility into the range and numbers of assets connecting to its network.

3.4.5 THREAT EVENT DESCRIPTION

As more devices are connected, the attack surface expands, often in unexpected places, such as building management systems and Close-Circuit Televisions (CCTVs). These systems perform multiple functions, such as managing access to specific doors, controlling door alarms, creating the photo IDs that allow facility access and monitoring for access.

Coupling together three vulnerabilities in the past year, an attacker could setup a Zoom video conference, for example, with any target at the organization. Once connected, the attacker can control the attendee's screen by exploiting a vulnerability in Zoom[xii] allowing them to download and install malware on the target's computer.

With access to the target computer, the attacker can then exploit the building management system[xiii] allowing physical access to the building. Now that the attacker can access the facility, the last step is to ensure the CCTV does not record their intrusion by exploiting the CCTV system.[xiv] In this scenario, an attacker could exploit software vulnerabilities to gain administrator rights, enabling them to create fraudulent IDs, disable door locks and alarms, access sensitive authorized user data and delete video footage.

3.4.6 OUTCOME

Building management contractors, just like IT managers, must consider cyber risk associated with all computer systems and networks within their scope of responsibility. Often, building management systems and CCTV are outside the control or purview of organization IT departments. A disciplined vulnerability management program, by which the organization can track, assess, and remediate known vulnerabilities across their entire attack surface in a timely manner, before they can be exploited is necessary.

3.4.7 MITIGATING STRATEGIES / SCRM CONTROLS

- Identify business operations and assets most vulnerable to cyberattacks, to include third party, operational technology (OT), and IoT assets; for many organizations, the most critical assets are those that have the highest monetary value attached to them; for the government, this may be those deemed most mission critical;

[xii] "Tenable Research Discovers Vulnerability in Zoom that Could Lead to Conference Hijacking," Tenable, 2018.
[xiii] "Multiple Zero-Days in PremiSys IDenticard Access Control System," Tenable, 2019.
[xiv] "Tenable Research Discovers "Peekaboo" Zero-Day Vulnerability in Global Video Surveillance Software," Tenable, 2018.

- Utilize continuous threat intelligence to prioritize remediation efforts considering the overwhelming number of new vulnerabilities; organizations should use contextual factors including asset criticality and whether there are exploits available for specific vulnerabilities, in prioritization;
- Frequent scanning and reporting are critical, because out-of-date data can be just as damaging as inaccurate data. The Center for Internet Security (CIS) Control 3.1 recommends automatically scanning all systems on a weekly or more frequent basis;
- Organizations need to make sure their reporting is aligned with their patch remediation cycle so that reporting and updates are relevant;
- Identify the security gaps and opportunities to reduce complexity in the IT security infrastructure that leave organizations vulnerable to cyberattacks;
- Measure the value of responding to vulnerabilities through automation and machine learning; and
- Utilize IT security staff and resources to improve the efficiency of vulnerability management.

3.5 SCENARIO: ICT DEVICES WITH DEFAULT PASSWORDS

3.5.1 BACKGROUND

All ICT devices ship with default passwords, not changing the administrator password can result in the attacker to easily identify and access ICT systems. It is imperative to change default manufacturer passwords and restrict network access to critical and important systems.

3.5.2 THREAT SOURCE

One of the first things a hacker checks is whether the default account and password are enabled on a device. Websites such as www.defaultpassword.com list the default credentials, old and new, for a wide variety of devices:

- Routers, access points, switches, firewalls, and other network equipment
- Databases
- Web applications
- Industrial Control Systems (ICS) systems
- Other embedded systems and devices
- Remote terminal interfaces like Telnet and Secure Shell (SSH)
- Administrative web interfaces
- Enterprise Resource Planning systems

In 2014, Trustwave released the results of an analysis of 691 data breaches and concluded that one third were due to weak or default passwords.[xv] In 2018, it was reported that less than 8 percent of analyzed breaches were due to weak or default credentials.[xvi] While the trend suggests that password security is improving, it remains crucial to have a process in place for dealing with new equipment which may still be configured with the manufacturer's passwords.

[xv] Trustwave, "2014 Trustwave Global Security Report," 2014.
[xvi] Trustwave, "2018 Trustwave Global Security Report," 2018.

3.5.3 THREAT IMPACT

Theft or manipulation of data could result from device compromise through improper password use; this could result in minor to major financial impact to the company, depending on the scale of compromise. Additionally, and especially in the case of IoT devices, this could also lead to significant disruption of services due to a Distributed Denial of Service (DDoS) attack launched from multiple compromised devices. Such DDoS incidents have resulted in significant loss of revenue or damage to company reputation, as well as legal or financial penalties.

3.5.4 VULNERABILITY

For devices shipped with default passwords, not changing the administrator password can result in the attacker easily identifying and accessing ICT systems. It is imperative to change default manufacturer passwords and restrict network access to critical and important systems.

3.5.5 THREAT EVENT DESCRIPTION

A small Internet Service Provider has been breached by an attacker that has gained access to the enterprise network through a router with the factory default password.

3.5.6 OUTCOME

The attacker with knowledge of the password and network access to a system can log in, usually with root or administrative privileges. Further consequences depend on the type and use of the compromised system.

Examples of incident activity involving unchanged default passwords include:

- Internet Census 2012 Carna Botnet distributed scanning;
- Fake Emergency Alert System (EAS) warnings about zombies;
- Stuxnet and Siemens SIMATIC WinCC software;
- Kaiten malware and older versions of Microsoft Standardized Query Language (SQL) Server;
- SSH access to jailbroken Apple iPhones;
- Cisco router default Telnet and enable passwords; and
- Simple Network Management Protocol (SNMP) community strings.

3.5.7 MITIGATING STRATEGIES / SCRM CONTROLS

- As part of good cyber hygiene practices and to reduce the risk of security breaches through default credentials which have been left configured on network devices, it's best to implement a process to change the passwords, and if possible, account names, when new equipment is installed.
- Identify software and systems that are likely to use default passwords. Regularly perform vulnerability network scans to identify systems and services using default passwords. Additionally, utilize good password management including:
    - Change Default Passwords - Change default passwords as soon as possible and absolutely before deploying the system on an untrusted network such as the Internet. Use a sufficiently strong and unique password. See the United States-Computer Emergency Readiness Team (U.S.-CERT) Security Tip ST04-002 and Password Security, Protection, and Management for more information on password security;

- Use Unique Default Passwords - Vendors can design systems that use unique default passwords. Such passwords may be based on some inherent characteristic of the system, like a Media Access Control (MAC) address, and the password may be physically printed on the system;
- Use Alternative Authentication Mechanisms - When possible, use alternative authentication mechanisms like Kerberos, x.509 certificates, public keys, or multi-factor authentication. Embedded systems may not support these authentication mechanisms and the associated infrastructure;
- Force Default Password Changes - Vendors can design systems to require password changes the first time a default password is used. Recent versions of DD-WRT wireless router, Linux-based firmware operate this way; and
- Restrict Network Access - Restrict network access to trusted hosts and networks. Only allow internet access to required network services, and unless necessary, do not deploy systems that can be directly accessed from the Internet. If remote access is required, consider using Virtual Private Network (VPN), SSH, or other secure access methods and be sure to change default passwords.

- Vendors can design systems to only allow default or recovery password use on local interfaces, such as a serial console, or when the system is in maintenance mode and only accessible from a local network.

3.6. SCENARIO: INCORRECT PRIVILEGE SETTINGS, AUTHORIZED PRIVILEGED USER, OR ADMINISTRATOR ERRONEOUSLY ASSIGNS USER EXCEPTIONAL PRIVILEGES OR SETS PRIVILEGE REQUIREMENTS ON A RESOURCE TOO LOW

3.6.1 BACKGROUND

Organizations employ least privilege for specific duties and information systems. The principle of least privilege is also applied to information system processes, ensuring that the processes operate at privilege levels no higher than necessary to accomplish required organizational missions or business functions. Organizations consider the creation of additional processes, roles, and information system accounts as necessary, to achieve least privilege. Organizations also apply least privilege to the development, implementation, and operation of organizational information systems.

3.6.2 THREAT SOURCE

Access controls that define specific sets of privileges linked to individuals are a fundamental security practice. However, these same principals are not always applied to the high-privilege access administrative accounts that have massive control over business-critical IT functions.

High-privilege access may be the most sensitive aspect of IT. Administrative accounts can make widespread changes to IT systems on which the business may depend. If misused, these capabilities can cause extensive damage ranging from security threats and compliance violations to incidents that tarnish the reputation of the business itself.

3.6.3 THREAT IMPACT

With the right kind of elevated privilege access, a malicious user could cause catastrophic impacts on a system, but even low-level user rights can typically allow enough permissions to cause harm or use the compromised host as a beachhead, launching attacks into other systems. A lack of proper access controls can not only result in unauthorized access and subsequent destruction, manipulation, and other malicious activity, but also make incident response investigations difficult or impossible due to the inability to trace back the activity. Thus, impact across a group of assets could be wider than the actual attack scope; if the company is unable to prove hosts or data were not accessed, one might be required to assume that they were compromised due to breach notification (or similar) laws.

3.6.4 VULNERABILITY

The vulnerability is that the company until recently had no formal Information Security Policy (ISP), or related procedures. There has been no policy for assigning system privileges, leading to many users having administrative or super user system privileged access which are not required for their current job. In this scenario, a user was granted root access to a UNIX system, in which the operating system does not apply access controls to the user root. That user can terminate any process and read, write, or delete any file.

3.6.5 THREAT EVENT DESCRIPTION

Acme Packet is a midsized manufacturing company which has doubled its enterprise product offering and number of employees. When the company first started, it had less than 25 employees, many of which had multiple responsibilities. One example includes the office manager also serving as their IT department.

Additionally, the company until recently had no formal information security policy or related procedures. There has been no policy for assigning system privileges, leading to many users having administrative or super user system privileged access which are not required for their current job.

In this scenario, a user was granted root access to a UNIX system, in which the operating system does not apply access controls to the user root. That user can terminate any process and read, write, or delete any file.

3.6.6 OUTCOME

The scenario above presents multiple risks to the supply chain ranging from insider risks to cyber espionage. Additionally, the easiest way for a cyber attacker to gain access to sensitive data is by compromising an end user's identity and credentials. Things get even worse if a stolen identity belongs to a privileged user, who has even broader access, and therefore provides the intruder with *the keys to the kingdom*. By leveraging a *trusted* identity, a hacker can operate undetected, gaining access to sensitive data and system access with little or no indications to the attack.

3.6.7 MITIGATING STRATEGIES / SCRM CONTROLS

- Conduct a security review of all users physical and system access adjusting user access to least privileged access, the minimum access needed to perform the job.
- Establish an Information Security Policy (ISP) based off industry standards and best practices.
- Deploy a Privileged Access Management (PAM) system for monitoring and protection of super user accounts. This is one of the most important aspects of Identity and Access Management (IAM), and cybersecurity at large today. With a PAM solution in place, an organization can dramatically reduce the risks discussed above.
- The Best Practices for PAM utilize the Four Pillars of PAM. Gartner outlines key challenges and makes clear recommendations that emphasize the critical role of people, processes and technology in effectively mitigating PAM risk and making purchase decisions, including:
    - Track and Secure Every Privileged Account;
    - Govern and Control Access;
    - Record and Audit Privileged Activity; and
    - Operationalize Privileged Tasks.
- Establishing a Zero Trust Architecture (ZTA) or similar protocols where all resource authentication and authorization is dynamic and strictly enforced before access is allowed. Under such an architecture,

access to data resources is granted when the resource is required, and authentication (both user and device) is performed before the connection is established.

PRODUCTS AND SERVICES THREAT SCENARIOS

3.7 SCENARIO: POOR PRODUCTS AND SERVICES ACCESS CONTROL POLICY

3.7.1. BACKGROUND

A widget sales organization, WidgCo, receives a set of new enterprise routers, which it installs throughout multiple field offices. New admin credentials are created, but the company is unaware that pre-existing admin accounts with default passwords exist. These routers are exposed to the open Internet, and they may not generally be locally monitored.

3.7.2. THREAT SOURCE

The systems involved are part of wireless infrastructure which handles Peripheral Component Interconnect (PCI) traffic as well as other sensitive information for multiple customers. While the infrastructure has been through audits and assessments over time, these new routers have not been a part of the most recent review.

3.7.3. IMPACT

With the right kind of elevated privilege access, a malicious user could cause catastrophic impact on a system, but even low-level user rights can typically allow enough permissions to cause harm or use the compromised host as a beachhead, launching attacks into other systems. A lack of proper access controls can not only result in unauthorized access and subsequent destruction, manipulation, and other malicious activity, but also make incident response investigations difficult or impossible due to the inability to trace back the activity. Thus, impact across a group of assets could be wider than the actual attack scope; if the company lacks proof that hosts or data were accessed, one might be required to assume that they were compromised due to breach notification (or similar) laws.

3.7.4. VULNERABILITY

Default admin/password credentials that are not removed or exist but are not disclosed by a vendor can be easily exploited in the wild if outside network access is available.

3.7.5. THREAT EVENT DESCRIPTION

Due to weak access control policies, pre-existing accounts from the equipment vendor are still functional. Some of these user accounts allow root or privileged access and are not uniquely identifiable as belonging to an individual or even to a certain company. The credentials for these accounts have become compromised and a malicious attacker has used them to gain access to the network, where additional attacks can be sourced from.

These attacks could also be initiated at a service level, where limited access is granted for a special project or time period but then not removed.

3.7.6. OUTCOME

The following illustrates some of the weaknesses exposed in an attack chain that could be initiated against exposed equipment or services:

3.7.1.1 Some equipment is accessible directly from the enterprise or an outside network, not via a firewall or DMZ;

3.7.1.2 User accounts are not uniquely identifiable, reviewed or changed;

3.7.1.3 User sessions are not controlled and vulnerable to typical brute force account access methods; and

3.7.1.4 Potential violations of user access are not alerted.

Given the above factors, an attack would not only likely be successful but also would go undetected for a long time unless service was otherwise impacted (e.g., user traffic stopped passing or was degraded). Simple dictionary or brute force attacks would likely be successful due to access control and account management policies. Thus, theft or manipulation of data, either through man-in-the-middle or exfiltration would be quite possible. In addition, other defenses or mitigations set up elsewhere in the network could be negatively impacted or changed from within.

3.7.7. POTENTIAL MITIGATING STRATEGIES / SCRM CONTROLS

Proper access control means protection of system resources against unauthorized access; a process by which use of system resources (e.g., executable programs, network configuration data, application file systems, network databases, etc.) is regulated according to a security policy and is permitted only to authorized entities (users, programs, processes, or other systems) according to that policy.

Authentication and authorization are basic security methods, which provide means to ensure the identity of users and limit their use of network resources to predefined activities or roles. They can thus be used to protect network operators against any unauthorized use of the network's services.

Furthermore, user authentication provides a basic mechanism for logging and auditing the management activities, which makes it possible to track activities afterwards. Providing each user with a unique user ID and password together with a certain privilege level makes it possible to limit a user's access to only those management activities they require in order to perform their task.

Enforcing strong password selection, password aging (which enforces the users to change their passwords at predefined intervals), two-factor authentication, and the encryption of the files containing the user ID and password data (to prevent unauthorized users to obtain sensitive data) provide additional security.

Upon receipt/installation of new equipment or the instantiation of a new service, due diligence for reviewing policies, scanning, checking for pre-existing accounts, etc. should be undertaken as soon as possible and not just "on the next audit cycle," which could result in months or years of risk exposure.

It is also recommended to implement restrictions on the rate of login attempts, concurrent login attempts, and lockout periods for incorrect login attempts and monitored alerts for incorrect login attempts.

Security event logs or audit trails are of fundamental importance to an operator in detecting malicious activities by defining the indicators of such behavior. The log also establishes accountability for malicious users committing internal fraud or sabotage. The security event logging should be compliant to open standards to permit the administrator to perform archival and analysis of logs and for post-incident evidence gathering and investigation.

The first step to detect harmful activities is to know the indicators for such behavior. The earlier such an activity is detected, the more time is left to take appropriate countermeasures.

3.8 SCENARIO: PRODUCTS AND SERVICES MISHANDLING OF CRITICAL OR SENSITIVE INFORMATION

3.8.1. BACKGROUND

An energy company supplier, Griffon Power, routinely handles marketing and technical information on industrial components used throughout their network. These are sometimes internal in nature but are generally marked as such. Recently, a small team within the company reviewed confidential external information from a domestic supplier on parts that were proposed for new turbines. These documents were highly sensitive in nature and shared under an NDA. All data and resources should be made available by authorized users securely as they become available.

3.8.2. THREAT SOURCE

As part of the project analysis, the team set up a shared network drive to distribute and review information. All information related to the project was stored within this folder, which was only accessible internally. Griffon Power ultimately decided not to go forward with the new turbine offering and moved on with other business. About a year later, as part of a network cleanup and upgrade effort, network storage was moved due to a network virtualization project which was completed by AstroNet. It is expected that access to these new storage areas is strictly through secure network slices provisioned by AstroNet.

Much of the NDA-level information shared between Griffon Power and the potential supplier has not been properly handled and is now exposed to a third-party company.

3.8.3. IMPACT

Isolation is a fundamental feature of network slicing. The better the isolation, the more secure the slicing solution is; multiple slices may coexist by sharing the same infrastructure and resources. Data separation and resource (compute, storage, memory) isolation is therefore of critical importance, especially if the service is used by multiple entities. This coexistence is determined by the minimum requirements set for each slice. When network slicing is not configured correctly in completely isolating slices end-to-end, access to the slices is potentially compromised and data contained is at risk.

When intellectual property is not properly segmented and protected that data is exposed and poses the risk of theft both internally and externally. The financial impact could be as minimal as the total value of the asset, or as high as value of an entire business unit, product line or future business plans, depending on the nature of the data.

3.8.4. THREAT EVENT DESCRIPTION

Poor data or resource isolation can lead to exposure of sensitive or proprietary information, even if protective measures are taken elsewhere in the network. While the slices at the operator level were configured such that traffic isolation occurs within the network, the accessibility of sensitive data has been generically assigned to all users. A contractor who has been granted temporary access and a company phone has found that they are able to access all parts of the internal network when connecting over their mobile connection. Proprietary information on the inner workings and specialty parts of turbines that are used throughout energy companies has been compromised or stolen, then sold on the dark web. This could be used for economic or blackmail purposes or by foreign competitors to gain an unfair advantage in the market.

3.8.5. OUTCOME

Although a fundamental premise of network slicing is that the network is carved into discrete, self-contained units, in many cases each slice may still leverage network-wide resources. As such, while unique security

parameters can be defined for network slices individually, there are security parameters that must be applied to shared network resources. As such, the opportunity exists for incongruences to exist between a network-wide security policy and a security policy that must be applied to an individual slice.

AstroNet's deployment of Griffon Power's network virtualization exposed some weaknesses in their overall handling of sensitive data;

- Failure to audit systems prior to and post deployment of network slices.
- Lapses in network and configuration management.
- Lapses in access controls.
- Failure to set unique security parameters between network slices and shared network resources.
- Failure to classify data – then handle and protect according to the classification, traceability and retention.

3.8.6. POTENTIAL MITIGATING STRATEGIES / SCRM CONTROLS

Security policy management can provide a security by design framework for establishing effective isolation of network resources, protecting an organization's digital assets from malicious or unintentional harm.

Vulnerability testing is and can be an effective process for validating the availability and integrity of the deployed solution, often identifying threats that maybe used in theft of company IP.

Data management policies can have a broad range of useful steps that could prevent such risks in this scenario. All data should be classified according to its intended use, who can access it, and if or how it can be shared. In addition, data tags could be set according to whether it is Public, Limited Release, Internal or Confidential (for example). Depending on how the data are classified, it may need to be encrypted and have access to the data controlled and monitored.

3.9 SCENARIO: PRODUCTS AND SERVICES LACK OF ASSET VISIBILITY AND VULNERABILITY EXPLOITATION

3.9.1. BACKGROUND

A software vendor lacks visibility into the open source or proprietary software libraries and components utilized in its products. Further, this organization lacks an effective secure software development lifecycle process, and regularly ships software products which may contain exploitable vulnerabilities. The organization also fails to plan and prioritize its product vulnerability mitigation practices.

Organizations which fail to plan and prioritize vulnerability mitigation practices are at risk of dedicating time and resources towards mitigation of lower risk vulnerabilities, leaving them potentially exposed to more significant attacks with a higher likelihood of exploitation. Attackers could also target the source code of their products, the release executables, etc. thereby impacting their entire customer base.

Without a secure development lifecycle or adequate response process, it is likely that vulnerabilities are discovered in the products of the vendor by attackers and might be exploited in the wild (zero-day vulnerabilities).

Many high-profile incidents could have been prevented through better asset management and cyber hygiene practices and processes. Fifty-seven percent of enterprises that experienced a breach in the past two years state that a known, unpatched vulnerability was the root cause.[xvii]

Further, the discovery and disclosure of vulnerabilities continue to grow in volume and pace. In 2019 alone, an average of 47 new vulnerabilities were published every single day, for a total of 17,306, up from 16,511 in 2018.[xviii]

With 52 percent of all vulnerabilities in 2019 rated as Critical or High severity, security organizations and software vendors are challenged to determine which vulnerabilities truly represent a risk and prioritize the most critical vulnerabilities to maximize limited remediation resources. After all, the proportion of CVEs with a publicly available exploit was about six percent in 2019, down one percentage point from 2018.[xix]

3.9.2. THREAT SOURCE

Organizations that do not have full visibility into where and how open source libraries and components are utilized in their products will not be prepared to mitigate the impacts of newly discovered vulnerabilities in those libraries and components. This will deeply impact all their customers as well as they will not be able to determine their true cyber exposure.

3.9.3. IMPACT

An exploit of a known, unpatched vulnerability in the software products of a financial services firm could result in the theft of financial, credit or other sensitive data for customers and individuals. This impact can be magnified significantly if the firm lacks visibility into the software libraries, frameworks, and components used in its products.

According to a survey conducted in 2018 by the Ponemon Institute, 56 percent of organizations had a breach that was caused by one of their vendors. For example, the Ripple20 vulnerabilities caused complications in the OT world as the Treck stack has been used in hundreds of products over the years, and numerous high severity vulnerabilities were found in the library. If an enterprise is not patching vulnerabilities in components used in their products, they are opening the attack surface area for all their customers.

3.9.4. VULNERABILITY

The vulnerability in this scenario is that a software or hardware vendor ships a product to a customer which lacks visibility or knowledge of which open source or proprietary components are utilized in their products and how these components are utilized. In addition, the lack of the secure development lifecycle and adequate vulnerability response process elevates the risk of vulnerabilities being discovered in its products (post release) as a result of insecure design and coding practices.

3.9.5. THREAT EVENT DESCRIPTION

An attacker develops or utilizes existing exploit code to attack a newly discovered (or known, unpatched) vulnerability in a widely deployed open source library software component. An attacker could utilize this exploit to perform a remote code execution against an organization that has failed to mitigate the vulnerability. This threat

---

[xvii] "State of Security Response," Ponemon/ServiceNow, 2018

[xviii] "National Vulnerability Database: Statistics Results," NIST, 2020.

[xix] Primary Research, Tenable Vulnerability Intelligence

is further exacerbated if the enterprise customer lacks visibility into which components are used in the software products it acquires, thereby putting all its customers at risk.

3.9.6. OUTCOME

Outcomes of successful attacks against known, unpatched vulnerabilities in hardware and software products include impacts against the full range of confidentiality, integrity, and availability of data and systems.

In addition, the same impact can be expected of vulnerabilities that are not discovered prior to release as a result of the lack of implementation of the secure development lifecycle. Vulnerabilities discovered post release can cost up to 20 times more to fix when compared to being discovered earlier in the product development lifecycle.

3.9.7. POTENTIAL MITIGATING STRATEGIES / SCRM CONTROLS

- The enterprise ensures its vendor utilizes an effective secure software development lifecycle program, including either an internal or external software bill of materials (SBOM), threat modeling, software composition analysis tools and capabilities, security training for developers, penetration testing and a process to track and remediate vulnerabilities in third party products that have been integrated.
- The enterprise has a codified security response process to deal with vulnerability disclosures in their products.
- The enterprise utilizes continuous threat intelligence to prioritize remediation efforts considering the overwhelming number of new vulnerabilities; organizations should use contextual factors including asset criticality, availability of workarounds, and whether there are exploits available for specific vulnerabilities, in prioritization.

4 THREAT CATEGORY: COMPROMISE OF SYSTEM DEVELOPMENT LIFE CYCLE (SDLC) PROCESSES & TOOLS

4.1 SCENARIO: DEVELOPMENTAL PROCESS OF HARDWARE AND SOFTWARE

4.1.1 BACKGROUND

Both hardware (printed circuit boards and computer chips) and software (source or object code and firmware) are highly reliant upon automated development tools. A Printed Wiring Board (PWB) (the circuit board to which components are soldered) is composed of hundreds, if not tens of thousands of circuit traces and component connections. A much smaller instance of this is the computer chip which can contain thousands of transistors and other elemental circuit components. Likewise, on the software side, computer code in its source form can constitute thousands or millions of lines of instructions, and often integrates dozens of third-party components. Once compiled, this can reach megabytes of binary code.

Given the complexity of both hardware and software development processes, threat actors may seek to introduce vulnerabilities into the hardware or software through development processes or tools, or by compromising the development environment.

4.1.2 THREAT SOURCE

Manipulation of development tools and development environments can come by way of a variety of different threat actors: nation-state, organization or individual (outsider or insider).

4.1.3 THREAT IMPACT

Compromise of development environments could have an array of different impacts on suppliers and customers, including:

- Loss of data, including sensitive data;
- Exposure of sensitive intellectual property;
- Disruption or disablement of system operations;
- Customer loss of trust in products/services/systems; or
- Loss of market share by vendors.

4.1.4 VULNERABILITY

Development tools and processes can introduce vulnerabilities into hardware and software products and services in a variety of ways, including unintentionally and intentionally. Unintentional vulnerabilities may be introduced when development tools are not configured for security, or when development processes lack adequate controls to identify and mitigate errors. Malicious actors may seek to intentionally introduce vulnerabilities by exploiting development tools in a variety of ways. Recently, malicious actors have targeted software supply chains by compromising servers issuing updates and patches to deployed software, enabling the attackers to transmit malware to hundreds of thousands of individual software copies and their users at once.[xx] Software supply chain vulnerabilities may also arise when an organization maintains insufficient controls to secure its development environment, enabling actors to access and manipulate source code under development, or when an organization has insufficient processes to securely integrate third-party components, enabling actors to compromise software by compromising components integrated into that software.

4.1.5 THREAT EVENT DESCRIPTION

In this example scenario, the threat actor compromises a server used to issue updates and patches to software embedded on commonly used consumer devices. After compromising the server, the actor transmits malware, in the guise of a software patch, to all deployed devices, which are configured to receive automatic updates.

4.1.6 OUTCOME

The malware deployed through the update server enables the attacker to access credentials and other sensitive data on individual infected devices, effectively giving the attacker the ability to control and disrupt these devices, and to access and manipulate data.

4.1.7 ORGANIZATIONAL UNITS / PROCESSES AFFECTED

The end user customer is directly impacted by the malware. Additionally, the incident undermines customer trust in the update services of the vendor, leading customers to turn off automatic update configuration settings and reject future updates, leaving the devices vulnerable to future attacks.

4.1.8 MITIGATING STRATEGIES / SCRM CONTROLS

Strategies to help prevent the unintended introduction of vulnerabilities through the development environments of hardware and software suppliers include:

[xx] Director of National Intelligence, "Software Supply Chain Attacks," 2019.

- Observe all SDLC practices.
- Establish robust processes for selecting, vetting, testing, and tracking third-party components.
- Maintain strong access controls and authentication mechanisms via ZTA or like govern access to development environments, and use change management tools to track identity, time/date, type of change, and other relevant information for all changes.
- Configure development tools, such as compilers, to secure settings.
- Adopt best practices for providing secure updates, including code-signing, and provide notifications to customers detailing the key information about the content of all updates.

PRODUCTS AND SERVICES THREAT SCENARIOS

4.2 SCENARIO: FAULTY THIRD-PARTY COMPONENTS

Supplier's development process includes the incorporation of a product/system which has third-party components that are now determined to be faulty.

The supplier can track hardware part numbers and the version numbers of its software in the product/system but does not keep track of the third-party software components.

When a faulty third-party hardware component is identified as having been utilized it can track where it was used and who has the impacted product/system.

For faulty third-party software components, the supplier is unaware what its developers used the faulty components and no remedial actions are taken, leaving its customers exposed to the potential failures with security, safety, availability, and reliability consequences.

4.2.1 BACKGROUND

A shipped system in operation in the field has a component from an outside supplier that is determined to be faulty and in need of update/replacement. For hardware items this would include physical swapping of smallest replaceable unit. For software items this would be an update via the items update mechanism. For some operational technologies that are not networked, the software update may require physical access to the unit to connect to the device with an upgrade unit or swapping out a memory device with the new software.

4.2.2 THREAT SOURCES

Attackers with knowledge of the deployed devices can learn about the faulty item and leverage its condition by making use of a vulnerability or causing unsafe and unreliable operation at a time of their choosing. Discovery of where an organization deployed devices in systems may be from network reconnaissance, social engineering, or open source analysis.

4.2.3 THREAT IMPACT

Depending on the failure mode of the faulty item and the items role in the deployed system, there can be security, safety, availability, or reliability impacts with anywhere from negligible to catastrophic consequences. In operational technologies like the control system of a chemical plant, a security fault that allows unauthorized operation of the item could cause a chemical leak or explosion/fire with many harmful consequences unless the safety systems intervene. However, if there is also a safety aspect to the failure it could curtail the safety systems effectiveness.

4.2.4 VULNERABILITY

The underlying third-party network stack component PBsleeps used in BUTROS 5 SCADA Controller is affected by eleven vulnerabilities known as UR-GENT/11. The BUTROS 5 SCADA Controller supplier is unaware they are using that third-party network stack component PBsleeps.

The impact on the BUTROS 5 SCADA Controller Ethernet plug-in communication modules and devices from these vulnerabilities will allow an attacker to leverage various attacks (e.g., to execute arbitrary code over the network).

4.2.5 EVENT DESCRIPTION

Attacker scans an ethernet network at SUN Global Chemical Works. Attacker recognizes the footprint of the PBsleeps network stack component and knows about the UR-GENT/11 vulnerabilities. They perform probing attacks until they are able to successfully gain control of the BUTROS 5 SCADA Controller and change its programming.

4.2.6 OUTCOME

SUN Global Chemical Works has a catastrophic chemical reaction that destroys a chemical reactor and surrounding equipment and expels a toxic chemical plume into the surrounding countryside.

4.2.7 ORGANIZATIONAL UNITS / PROCESSES AFFECTED

Product/System acceptance procedure at SUN Global Chemical Works did not require a SBOM with equipment deliveries. Such a practice would have identified the lack of insight of the supplier of the BUTROS 5 SCADA Controller into what third-party software they used. If the SBOM had been available and delivered with the product/system, SUN Global Chemical Works would have been in a position to recognize that the vulnerability advisories about UR-GENT/11 applied to the BUTROS 5 SCADA Controller, and network segmentation mitigations could have been put in place while waiting for the firmware patches to fix the faulty software components.

4.2.8 MITIGATING STRATEGIES / SCRM CONTROLS

Recommending all suppliers to have a SBOM for the products/systems they supply would give insights into the maturity of their software development practices and configuration management.

Recommending all suppliers to provide a SBOM with delivered items and all updates would provide the SUN Global Chemical Works operations staff the ability to proactively monitor published vulnerability information that could impact their systems and put in place mitigations while working with their suppliers for a long-term remediation.

4.3 SCENARIO: THIRD PARTY COMPONENT SECURITY ISSUE

The supplier's development process includes the incorporation of a product/system with component installed that is now prohibited based upon new security concerns.

The supplier can track hardware part numbers and the version numbers of its software in the product/system but does not keep track of the third-party software components.

When a prohibited third-party hardware component is identified as having been utilized, it can track where it was used and who has the impacted product/system.

For prohibited third-party software components, it is unaware what its developers used the components and no remedial actions are taken, leaving its customers exposed to the consequences of the prohibited component.

4.3.1 BACKGROUND

Pelican State Power provides electricity to a major region of the United States. It has numerous generating stations with massive electric generators. A control system in operation in the field has a component (AXIOM-3) that is now determined to be prohibited based on new security concerns. Pelican State now has the problem to determine where in their network this item has been deployed (for most companies, this is a large problem - once in the field it's usually forgotten). They must determine a replaceable component for AXIOM-3 and then determine where, in their network, AXIOM-3 resides.

4.3.2 THREAT SOURCES

Adversaries have an awareness of the vulnerabilities of this prohibited component. They can surreptitiously gain access to the Pelican State Power's network to learn about the faulty item and its locations within the network. They are then able to cause issues at a time of their choosing. This can be in the form of causing the component to fail by making use of a known vulnerability in the component, or modifying the software code within the component causing it to execute "B" rather than "A" when a specific condition is met. This can result in an unsafe and unreliable operation or worse.

4.3.3 THREAT IMPACTS

The impact on Pelican State Power from these vulnerabilities allows an attacker to leverage various attacks, such as executing arbitrary code over their network. This would cause control systems in their electric generating stations to execute commands that would either shut down electric generators, or speed them up. Either way, it would cause severe damage to the generators in terms of either destroying the equipment, or causing explosions rendering the generating station unusable and causing wide-spread blackouts in their service territory. These massive generators are custom built, and to replace them requires a lead time of several years.

4.3.4 VULNERABILITY

The vulnerability on Pelican State Power generating stations due to the prohibited component modules and devices from these vulnerabilities will allow an attacker to leverage numerous attacks by executing arbitrary code over the network.

4.3.5 SDLC EVENT DESCRIPTION

The adversary is aware of the prohibited component and that Pelican State Power has that component in their control network. They gain access to Pelican state Power's control network through surreptitious means and can examine the network and recognize that the prohibited components are in a vital piece of a control module for the generators. They can successfully gain access to the control module and alter its program to execute "B" instead of "A" at a time the adversary selects.

The adversary determines that the greatest damage would be done by destroying the massive generators during the peak of either a heat wave or a cold snap. On August 22nd, amid record breaking temperatures, they executed their plan. AXIOM-3 is commanded to speed up the generators by 15 percent - far in excess of their ability to continue to operate. This causes 35 percent of all generators in the Pelican State system to immediately overspeed and be torn apart. The remaining generators not affected by the prohibited component are unable to pick up the slack, thus tripping circuit breakers throughout the electric grid and causing an immediate blackout across the whole service territory.

4.3.6 OUTCOME

The heat is oppressive and soon customers are inundating Pelican State's call centers wanting to know when service will be restored. There is no hope to restore service for several years now until new massive generators

can be built and delivered. Neighboring electric utilities can offer no assistance as their systems are already strained to capacity due to the current heat wave. Meanwhile, currently, and for the foreseeable future, air conditioners stop running, no gas can be pumped, ATMs will not work, traffic signals are inoperative, and all cash registers are dead. Civil unrest begins to occur.

4.3.7 ORGANIZATIONAL UNITS / PROCESSES AFFECTED

The acceptance procedures at Pelican State Power did not require a Bill of Material (BOM) with their equipment deliveries. This would have identified the component, and would have provided a method of tracking which generating stations that component had been installed in. If the Bill of Material had been delivered with the product/system, Pelican State would have been able to recognize where the prohibited component was installed and been in a better position to replace them. As it was, they scrambled to determine which stations had the prohibited component, wasting valuable time.

4.3.8 MITIGATING STRATEGIES / SCRM CONTROLS

Request all of Pelican State's suppliers to provide a Bill of Material for software and hardware of the systems they deliver would provide them with the ability to identify which generating stations had the prohibited component. This would have allowed them to quickly determine the extent of the problem and give additional lead time to find a replacement for the component.

Keeping apprised of hardware and software threats by subscribing to such warning sites as ERAI, and if possible, GIDEP to stay informed on the latest known hardware threats would have given Pelican State Power additional time to find replacement parts for the AXIOM-3 component (ERAI has the world's largest database of suspect counterfeit and nonconforming electronic parts).[xxi]

A clause in each of their RFI/Request for Proposals (RFPs) and contracts that states "The contractor shall notify Pelican Power Company whenever there is a change in subcontractors or suppliers at any point during design, development, fabrication, testing, or deployment." Also, the clause "Do not use grey market suppliers under any circumstances." Numerous additional contract clauses will help mitigate the problem caused by a warning of a prohibited component.

4.4 SCENARIO: THIRD PARTY SOFTWARE LEGAL ISSUE

Supplier's development process includes the incorporation of a product/system with prohibited component installed and misrepresented them as legal.

Supplier has hardware part numbers visible in the product and the version numbers of its software in the product/system but does not make available a list of third-party software components utilized.

A visual examination of the product can identify prohibited third-party hardware components by part numbers and visual identification.

For prohibited third-party software components, the customer is unaware that such components were used, and is exposed to the consequences of the prohibited components.

[xxi] ERAI's Nonconforming Parts Photo Database

4.4.1 BACKGROUND

ICU Enterprises is a long-time manufacturer and distributer of office printers, copiers, scanners, and projectors. It has been supplying federal customers for more than five years and has had good reviews. While verifying the serial number during a routine inventory, one customer discovered that one of the products, a copier/scanner (copier), included an operating component provided by a Russian company with ties to the Russian Intelligence Service. The component, along with its controlling software, allows the vendor to access the copiers through a dedicated connection across the Internet for diagnosis, maintenance, and updates to the machines' operating software. The vendor did not mention the use of the Russian-provided components in any of its literature or sales presentations. The local sales representative claims that he was unaware of the origin of the component/software in question. The copiers are deployed in 15 offices across the organization. They may also be deployed in other offices across the Federal Government, and within State, Local, Territorial, Tribal, and Local (SLTT) government offices and their contractors.

4.4.2 THREAT SOURCES

The component in question provides remote access to all operational aspects of the copier, which is required in order to allow the vendor to conduct remote diagnosis and maintenance. There is a high risk that Russian or other foreign intelligence services will be able to access the copiers from anywhere in the world and receive digital copies of any copied or scanned documents.

4.4.3 THREAT IMPACT

Even though the copiers are not authorized for use on classified materials, many of the documents contain sensitive information. This sensitive information can be aggregated to provide insight into the inner workings of the agency or, more broadly, into federal or SLTT government plans or activities.

4.4.4 VULNERABILITY

The vulnerability on ICU Enterprise copiers will not only allow an attacker to leverage its connection to gather information, but this open path provides a further conduit by which to penetrate deeper into government networks.

4.4.5 SDLC EVENT DESCRIPTION

The foreign intelligence service gains access to several copiers and begins to receive digital copies of all scanned and copied documents. Through aggregation of information, it learns of a new technology being developed that could be of interest to the foreign nation-state. Through further analysis, the foreign service can discern the name and location of the industry partners leading the development, the location of the research, development and testing facilities, and the names of the key government and industry personnel working on the project. It also learns that some of these government and industry officers employ the same model copier and begins the process of accessing these copiers in order to gather additional information. It also alerts its field agents of the name and location of the facilities and key personnel so that they may begin penetrating the facilities.

4.4.6 OUTCOME

The foreign intelligence service now has direct access to sensitive information regarding the new technology, and its field agents have developed cordial relationships with key and other personnel within the project facilities. They are soon able to extract additional important information from these and other personnel through social engineering and other methods commonly employed by intelligence services. They are able to gather additional information regarding the technology, as well as insight on how best to penetrate the facility and place agents inside, initially as general support, maintenance and janitorial staff, with a longer-term goal of placing more direct support agents within the facilities.

4.4.7 ORGANIZATIONAL UNITS / PROCESSES AFFECTED

The procurement procedures at the affected federal or SLTT government agencies did not include a requirement for a SCRM plan from the vendor, and the agencies did not have SCRM plans of their own. Additionally, the agencies did not require non-processing equipment to undergo full Security Controls Assessments (SCA) as part of their Authority to Operate (ATO) or risk management programs. Doing so would have identified the components in question and subsequent vulnerabilities before the copiers were purchased and installed.

4.4.8 MITIGATING STRATEGIES / SCRM CONTROLS

Require all manufacturers to provide SCRM plans on all of the items included in their proposals, as well as SCRM plans from all of their major suppliers, including the origin of all parts or services received and a trace to the firms' top-level owners and controlling body (the procuring agencies will determine what constitutes a major supplier and include instructions as part of their proposal requests). This should be included as part of the organization's overall SRCM plan.

Require organizations to conduct full type SCAs and issue type ATOs on any item that will be connected to government networks prior to final procurement and installation. This should be included as part of the agency's overall SRCM plan.

Require manufacturers/vendors to notify customers whenever there is a change in subcontractors or suppliers at any point during design, development, fabrication, testing, or deployment.

Require manufacturers/vendors to inform the customer of all changes in a product design or substitution of operational components so that the customer can determine if another SCA is required prior to shipping of the new equipment. This should be included as part of the agency's overall SRCM plan.

Keeping apprised of hardware and software threats by subscribing to such warning sites as US-CERT and ERAI to stay informed on the latest known hardware/software threats.

4.5 SCENARIO: MALICIOUS SUPPLIER INSERTS HOSTILE CONTENT

4.5.1 BACKGROUND

A software supplier, NMT-Com provides network management infrastructure for numerous global companies. Recently, several customers have complained about products that have ended up failing certain security scans upon receipt, although most customers have had no reported issues.

4.5.2 THREAT SOURCE

NMT-Com has software developers around the world, with a dozen different code compiler locations, at their primary development centers. Software packages and libraries are uploaded for review and security scanning, and then stored where they can be utilized by developers within the region; customer support is handled by the regional center that supplies the software load.

Product packages are intended to be consistent across customers for easier support, patching, and development. Release testing is done on a periodic basis in the development cycle at each center.

4.5.3 THREAT IMPACT

Malicious or nefarious suppliers or rogue supplier employees are a major concern and can lead to a compromised supply chain. In addition, suppliers controlled by a country of concern can lead to nation-state initiatives to produce malicious software or manipulated hardware components. Impacts range from multiple cybersecurity

risks, including malware, botnets, unauthorized access, privacy, loss of data including intellectual property, industrial control, and national security threats.

4.5.4 VULNERABILITY

According to the scenario presented, since NMT-Com has a dozen different code compiler locations, there is the potential for a bug to be inserted into the code, thus creating a vulnerability.

4.5.5 THREAT EVENT DESCRIPTION

A malicious supplier employee inserts hostile content at the product or component manufacturing or software compilation stage to affect supplier products or components delivered to a targeted subset of downstream customers.

4.5.6 OUTCOME

Due to the disconnect between the process of where software is scanned and where it is compiled and released, there is a potential for insertion of malicious software. There is an assumption of trust at the compiler locations and no re-scanning is done, except on the full release on a periodic basis (rather than every time it is changed and before it is signed).

This could leave customers of the supplier open to backdoor exploits, software injection attacks, data manipulation, data exfiltration, or any number of attacks possible if the very code itself is compromised.

4.5.7 MITIGATING STRATEGIES / SCRM CONTROLS

- The supplier should implement, monitor and audit a comprehensive security assurance framework as part of their software development process;
- All software should be compiled in trusted locations, such as where it is also verified, scanned and signed. This would also serve as a logical central distribution point. Whenever software is changed and re-compiled, there could be a potential for injection of malicious code; thus, security scanning should be performed on each of these loads; and
- Static and dynamic code inspection is commonly used to verify the security and integrity of software. Static testing involves checking the code from an internal standpoint, executing code paths and routines to ensure they are operating as expected. Dynamic (black box) testing involves mimicking attacker behavior from the outside, detecting known vulnerabilities and simulating theoretical ones to determine if the product is vulnerable to different kinds of exploits.
- Consider keeping code repositories and compiling functions in the cloud.

5 THREAT CATEGORY: INSIDER THREAT

5.1 SCENARIO: CONTRACTOR COMPROMISE SCENARIO

5.1.1 BACKGROUND

Nation-state threat actors have always utilized people to help them conduct their intelligence gathering operations. In some cases, they attempt to infiltrate people into an organization. In other cases, the threat actors attempt to compromise people already working at the organization of interest. These people might be employees or onsite contractors.

Additionally, there are non-nation-state, ideologically driven, organizations that attempt to recruit individuals that could be onsite contract employees.

The risks presented by this type of attack are compounded when organizations outsource some of the work that needs to be accomplished. The risk is compounded because often it's the company that is hired that is screening the employees that will be onsite performing the work.

This sample threat scenario is the case where an onsite IT contractor employee is compromised, or recruited, by a threat actor and becomes an insider threat. For scope purposes within this document, we will assume this is a low to mid-level employee in a non-critical position.

This scenario will not address all the potential negative actions the insider could take. This scenario will focus on mitigating the chances that such a compromised insider, from the supply chain, can remain undetected once the compromise takes place.

5.1.2 THREAT SOURCE

The threat source, in this example, is an onsite contract employee that becomes compromised, or recruited, by a threat actor. The contract employee then becomes an onsite tool of the threat actor.

5.1.3 THREAT IMPACT

Using NIST SP 800-30, we worked through the impact assessment and we have come to the following assessment.[xxii]

TYPE OF IMPACT	IMPACT ASSESSMENT	NOTES
Harm to Operations	Low-Medium	An insider threat can have limited impact depending on their limited role and accesses. This tends to be limited for most low to midlevel employees due to maturity of processes, limited roles, and layers of oversight. Some decisions or actions may require management oversight.
Harm to Assets	Low-Medium	The low to mid-level employee is limited to how they access facilities and are limited in their information technology assets accesses. They can willfully click on malicious attachments or files in emails, but systems are geared to monitor and address such a scenario. This insider could damage systems or components, but given oversight, separation of roles, monitoring of processes and feedback from customers, impact should remain low in most cases.

[xxii] This risk assessment framework is an example. There are other frameworks and reference tools that can be used instead of NIST 800-30.

TYPE OF IMPACT	IMPACT ASSESSMENT	NOTES
Harm to Individuals	Low	There are few roles at the low- to mid-level that involve the handling of personal information of employees or customers. Mature processes, security controls, and monitoring are essential to mitigating impacts. Contractors hired for these limited roles go through background checks and monitoring. These roles tend to have more extensive management oversight and auditing.
Harm to Other Organizations	Low	Due to limited scope and separations of roles of low- to mid-level employees and contractors, an insider would have limited impact in this space to either products or the ability to affect reputation. Good quality control and monitoring with customer engagement should keep any impacts low. This can help with addressing who or what is the cause of any issues as well.
Harm to the Nation	Very Low	Most companies have limited to no impact to national security. This is by design for most sensitive government programs' concept of operational security. For programs that have limited impact to possible national security, additional measures are taken to limit the opportunity for impact or the impact itself. Company processes would limit who has knowledge of any processes or components that could have an impact national security.

5.1.4 VULNERABILITY

The vulnerability in this example is the inability to detect that an employee has become compromised, or recruited, by a threat actor.

5.1.5 THREAT EVENT DESCRIPTION

A full-time contract employee is providing IT Services to an enterprise. The enterprise is the target of the threat actor. The threat actor may wish to steal/change/destroy/hold hostage data, or the threat actor may wish to disrupt operations.

The relevant threat event is the successful recruitment of the contractor individual and the fact that the individual then attempts to undertake the malicious activity. The outcome is an undetected malicious insider, that is a contract IT employee, and the activity that the undetected malicious insider undertakes.

5.1.6 ORGANIZATIONAL UNITS / PROCESSES AFFECTED

The affected organization has the onsite IT contractor working within their environment. Depending upon the specific bad activity, other potential impacts could occur for other business partners of the enterprise.

5.1.7 MITIGATING STRATEGIES / SCRM CONTROLS

The potential mitigating strategies would be an element of the Risk Management Process as described by the NIST Risk Management Framework.

Potential Mitigating Strategies could include:

- Requiring contractors to have the same background and periodic security check that employees must undergo. Additionally, the contractor company would be required to share the results of these checks with the buyer/hiring organization.
- Delivering insider awareness training to enterprise employees, and contractors, would better enable the insider-contract-employee to be identified.
- Establishing a ZTA or similar where all resource authentication and authorization is dynamic and strictly enforced before access is allowed. Under such an architecture, access to data resources is granted when the resource is required, and authentication (both user and device) is performed before the connection is established.

5.2 SCENARIO: NEW VENDOR ONBOARDING

5.2.1 BACKGROUND

Reaching out to new semiconductor companies can give manufacturers a performance or pricing edge, especially when the market has lean margins and must compete for government contracts.

Chips Inc., a semiconductor company used by the organization to produce military and aerospace systems, is considering a partnership with American Systems Co. to leverage their fabrication facility. This would represent a significant change in the supply chain related to a critical system element. American Systems Co. formed a task force in conjunction with Chips Inc., to help identify risks in the potential partnership and how they can be mitigated by both companies and their contractors.

5.2.2 ENVIRONMENT

American Systems Co. is concerned about the intellectual property and their patents regarding the Chips Inc. fabrication facility. They would like to monitor and control for chip over-production and mitigate loss of intellectual property (IP) or extra chips that might end up in their competitor's hands. These critical capabilities are currently innovative and a key driver of American Systems Co.

Additionally, Chips Inc. is in Hong Kong. In reviewing the financial viability of the company, American Systems Co. found that they receive considerable government subsidies to encourage technical sector companies in Hong Kong. This risk is that Chips Inc. could lose their government subsidy, which keeps the company viable. This may result in the sale of sensitive IP that belongs to American Systems Co.

Chips Inc. provides field service teams in 15 countries to service the chips and platforms manufactured by them. Within the U.S., the field services are provided by a contractor who outsources to subcontractors in various geographical locations to provide coverage in the U.S. The contractors and subcontractors all wear the same TechServices polo shirts and name badges when they are performing onsite services. Through these support contracts, TechServices personnel can access American Systems Co.'s field sites across the country, including sensitive or critical facilities. The contractors always have unlimited access to spare parts as some of the response times for customer outages have a 2-hour performance window.

5.2.3 THREAT IMPACT

Using NIST SP 800-30, we worked through the impact assessment and we have come to the following assessment.

TYPE OF IMPACT	IMPACT ASSESSMENT	NOTES
Harm to Operations	Low	American Systems Co. will have personnel at Chips Inc. to monitor a production run and disposal of any over production. Logistical shipment tracking is in place, and access to data is removed when the production run is over.
Harm to Assets	Low	Low impact due to limited access to IP and the requirement of encrypted data at rest and in transit.
Harm to Individuals	Very Low	There is no personal information shared during this agreement.
Harm to Other Organizations	Very Low	Financial costs to configure and run equipment is an impact on Chips Inc. only. American Systems Co. does have the option to return to its previous chip fabricator.
Harm to the Nation	Very Low	These components have no impact on National Security Systems. Chips Inc. subcontractor, TechServices personnel go through a background clearance check to be able to service any sensitive sites.

5.2.4 ORGANIZATIONAL UNITS / PROCESSES AFFECTED

The risks of bringing aboard a new vendor are critical, and the challenge of working with a vendor that supports their products directly requires a more extensive vetting and monitoring.

This vendor onboarding process includes parts and components that involve sensitive American Systems Co. intellectual property. Chips Inc. has direct access to the electronic circuit design, testing, and packaging aspects of American Service Co's intellectual property. They will have unique access to supply/demand data as they will know how much product American Service Co.'s buys and where the company requests shipments to be delivered. Since Chips Inc takes care of shipment and delivery of the products, they have exceptional knowledge of the processes that American Service Couse to receive, integrate, and support the products they make.

Finally, Chips Inc. supports customers deployments of their fabricated chips and technologies by way of TechServices. TechServices has a value-added service which maintains replacement parts and maintains technicians on a 24/7 basis to respond to customer outages and problems very rapidly. While the parts are stored separately from the technicians, Chips Inc. does provide the service and has extensive knowledge and access to American Service Co.'s sensitive operational facilities, internal processes and extensive access to spare parts. Since TechServices has subcontracted other companies, higher risk personnel may be the ones delivering services. This would allow them to gain access to critical facilities and parts before they are installed into

American Service Co.'s systems. It is likely that TechServices can also provide services to American Service Co.'s competition and may share data verbally or otherwise with their competition.

5.2.5 MITIGATING STRATEGIES / SCRM CONTROLS

A broad-based team focus and engagement strategy to work with Chips Inc. is essential to identify all the potential risks and then develop risk mitigation strategies. NIST SP 800-30 Rev. 1, and 800-171 or ISO IEC 27036 can be used to conduct risks assessments and perform risk management functions.

5.2.6 MITIGATING STRATEGIES COULD INCLUDE

- Phasing of the onboarding of services. Services to fabricate chips should be developed first. Additional services provided by Chips Inc., such as TechServices, can be phased in after initial risks and monitoring are in place.
- For delivery and distribution, American Service Co. can keep its existing distribution center to receive deliveries and monitor parts from Chips Inc. for compliance. The common distribution center can effectively shield much of American Service Co.'s infrastructure and operations from Chips Inc.
- American Service Co. can work with Chips Inc. procedures and work to update any lost or non-compliant chips and products.
- Limit American Service Co.'s POCs that with Chip Inc. from an acquisition standpoint. Make those POCs clear to Chips Inc. and give the POCs training to identify what data and types of data to share with Chips Inc.
- Agree to security measures for transmission, encryption, storage, retention, destruction, and required paperwork of intellectual property shared with Chips Inc.
- When American Service Co. decides to utilize support services from TechServices, American Service Co. can request TechService employees have a background check before being allowed to perform work. The same request can be made for Chips Inc. employees that interact with American Service Co.
- American Service Co. should monitor the financial performance of Chips Inc. on a quarterly or bi-annual basis to monitor for changes in the company's financial performance or leadership.

References:

- CMU National Insider Threat Center – Common Sense Guide to Mitigating Insider Threats
- ISO 27002
- NIST 800-53 rev 4
- Insiderthreatdefense.us

5.3 SCENARIO: THREATS WS – INSIDER CATEGORY – STAFFING FIRMS USED TO SOURCE HUMAN CAPITAL

5.3.1 BACKGROUND

Nation-state threat actors utilize a myriad of vectors to insert, influence, turn, or threaten company insiders into a compromising position, often resulting in the loss of a company's confidential/classified data or impact to a company's critical systems and services.

NIST defines an Insider as: "One who will use her/his authorized access, wittingly or unwittingly, to do harm to the security of the entity they work for. This threat can include damage through espionage, terrorism, unauthorized disclosure, or through the loss or degradation of entity resources or capabilities."

While it is common for a nation-state threat actor to apply leverage to an existing company insider in order to achieve a specific goal, the unwilling or untrained insider threat can often be more easily identified as compared to a purposefully planted insider. In any case, companies should have an operational Insider Threat Program (ITP) [NIST 800-53 & 800-171] wherein they employ active controls and awareness training to collect automated and manual notifications of potential insider threats.

In addition to the internal controls for the detection and prevention of insider threats, companies must also consider the insider threats stemming from their supply chain in the following scenario – the focus is the sourcing of employees/contractors/consultants.

5.3.2 THREAT SOURCE

The threat source, in this example, is a nation-state having influence over a staffing firm used by a company to source human capital. Staffing firms are often leveraged for two primarily purposes; (1) to source employee candidates, and (2) to provide skilled contractors/consultants as part of fixed-priced services. In either case, the sourcing of candidates performed by the staffing firms can be manipulated to ensure certain qualified candidates (who are also insider threat agents) gain the first opportunities for employment. If selected for employment or contractor/consulting services, the threat agents begin to leverage access permissions to escalate privileges and acquire/disseminate data to unauthorized entities.

5.3.3 THREAT IMPACT

Using NIST SP 800-30, we worked through the impact assessment and we have come to the following assessment.

TYPE OF IMPACT	IMPACT ASSESSMENT	NOTES
Harm to Operations	Low-Medium	An insider threat can have limited impact depending on their limited role and accesses. This tends to be limited for most low- to mid-level employees due to maturity of processes, limited roles, and layers of oversight. Some decisions or actions may require management oversight.
Harm to Assets	Low-Medium	The low- to mid-level employee is limited to how they access facilities, are limited in their information technology assets accesses. They can willfully click on malicious attachments or files in emails. But systems are geared to monitor and address such a scenario. This insider could damage systems or components, but given oversight, separation of roles, monitoring of processes and feedback from customers, impact should remain low in most cases.
Harm to Individuals	Low	There are few roles at the low- to mid-level that involve the handling of personal information of employees or customers. Mature processes, security controls and monitoring are essential to mitigating impacts. Contractors hired for

TYPE OF IMPACT	IMPACT ASSESSMENT	NOTES
		these limited roles go through background checks and monitoring. These roles tend to have more extensive management oversight and auditing.
Harm to Other Organizations	Low	Due to limited scope and separations of roles of low- to mid-level employees and contractors, an insider would have limited impact in this space to either products or the ability to affect reputation. Good quality control and monitoring with customer engagement should keep any impacts low. This can help with addressing who or what is the cause of any issues as well.
Harm to the Nation	Very Low	Most companies have limited to no impact to national security. This is by design for most sensitive government programs concept of operational security. For programs that have limited impact to possible national security, additional measures are taken to limit to opportunity for impact or the impact itself. Company processes would limit who has knowledge of any processes or components that could have an impact national security.

5.3.4 VULNERABILITY

The vulnerability in this example involves the partnership with a third-party staffing firm that is instrumental in sourcing candidates for employment, and the staffing firm can be leveraged by a nation-state to manipulate the recruitment and candidate sourcing to a company. In many of these cases, the staffing firm has offices around the world, while also having a recruitment/candidate database that can be accessed and modified by the staffing firm's international associates, with the intent of strategically planting insider agents into the recruitment process of a company.

Background checks can be effective for preventing the hiring of known malicious characters, but they may not detect willing insider threat agents. While it is important to maintain controls that detect and stop insider threat activity, preventing the hiring of an insider threat agent can help mitigate this risk. This requires the adoption of SCRM controls at staffing firms.

5.3.5 THREAT EVENT DESCRIPTION

An Insider Threat Agent successfully navigates the hiring process and secures employment (full-time, part-time, contractor, or consultant) with the target company. The insider agent uses their authorized access to acquire confidential/classified data and attempts to escalate their access privileges to acquire data when access is not currently granted. The insider agent utilizes a slow and undetectable process for data exfiltration. This activity could last for years without detection. If finally detected years later, the investigation could find that the agent was sourced from the company's staffing firm. Background checks at the time of hire did not uncover anything to highlight the potential threat.

5.3.6 ORGANIZATIONAL UNITS / PROCESSES AFFECTED

The affected organization is the one that sources candidates from the staffing firm which had an unknown international presence. The insider agent can affect the company's competitive edge, customer market percentage, reputation, and result in financial and regulatory penalties.

5.3.7 MITIGATING STRATEGIES / SCRM CONTROLS

The potential mitigating strategies would be an element of the Risk Management Process as described by the NIST Risk Management Framework.

Potential Mitigating Strategies could include:

- Performing SCRM assessment on all staffing firms used to source candidates for privileged access roles; the assessment should ensure the staffing firm does not have an international database which allows remote locations to influence the candidate hire dataset for a company.
- Perform background checks on all workers, including employees, contractors, and consultants; background checks for resources who have privileged access should be performed with repetition.

PRODUCTS AND SERVICES THREAT SCENARIO

5.4 SCENARIO: CONTRACTOR COMPROMISE

5.4.1 BACKGROUND

Nation-state threat actors have always utilized people to help them conduct their intelligence gathering operations. In some cases, they attempt to infiltrate people into an organization. In other cases, the threat actors attempt to compromise people already working at the organization of interest. These people might be employees or onsite contractors.

Additionally, there are non-nation-state, ideologically driven, organizations that attempt to recruit individuals that could be onsite contract employees.

The risks presented by this type of attack are compounded when organizations outsource some of the work that needs to be accomplished. The risk is compounded because often it's the company that is hired that is screening the employees that will be performing the work.

This sample threat scenario is a case where an onsite IT contractor employee is compromised, or recruited, by a threat actor and becomes an insider threat.

This scenario will not address all the potential negative actions the insider could take. This scenario will focus on mitigating the chances that such a compromised insider, from the supply chain, can remain undetected once the compromise takes place.

5.4.2 THREAT SOURCE

The threat source, in this example, is an onsite contract employee that becomes compromised, or recruited, by a threat actor. The contract employee then becomes an onsite tool of the threat actor.

5.4.3 THREAT IMPACT

Potential impact of insider threat may include:

- Compromise of the integrity of the enterprise and potentially, the extended supply chain.
- Compromise of the confidentiality of the enterprise and potentially, the extended supply chain (e.g., intellectual property theft).
- Monetary loss for the enterprise, and potentially the extended supply chain.[xxiii]
- Unauthorized disclosure of national security information (when considering nation-state threat actors).
- Corporate espionage

5.4.4 VULNERABILITY

The vulnerability in this example is the inability to detect that an employee has become compromised, or recruited, by a threat actor.

5.4.5 THREAT EVENT DESCRIPTION

A full-time contract employee is providing IT Services to an enterprise. The enterprise is the target of the threat actor. The threat actor may wish to steal, change, destroy, or hold hostage data or the threat actor may wish to disrupt operations, or corrupt or sabotage a product.

The relevant threat event is the successful recruitment of the contractor individual and the fact that the individual then attempts to undertake the malicious activity.

5.4.6 OUTCOME

The outcome is an undetected malicious insider that is a contract IT employee, coupled with activity that the undetected malicious insider undertakes.

5.4.7 ORGANIZATIONAL UNITS / PROCESSES AFFECTED

The affected organization is the organization that has the onsite IT Contractor working within their environment. Depending upon the specific bad activity, other potential impacts could occur for other business partners of the enterprise.

5.4.8 MITIGATING STRATEGIES / SCRM CONTROLS

Potential Mitigating Strategies could include: [xxiv]

Development of an Insider Threat Program:

- Establish an insider threat oversight body that includes senior executives from the company's HR, security, legal, privacy, ethics, incident response team, IT, and public relations departments.

[xxiii] According to Ponemon Institute's April 2018 Cost of Insider Threats study, insider threat incidents cost the 159 organizations they surveyed an average of $8.76 million in a year. Malicious insider threats are more expensive than accidental insider threats. Incidents caused by negligent employees or contractors cost an average of $283,281 each, whereas malicious insider credential theft costs an average of $648,845 per incident.

[xxiv] NIST'S Preliminary Examination of Insider Threat Programs in the U.S.A. Private Sector, 2013

- Implement a formal insider threat incident response plan. This plan should include current and former employees, contractors, and business partners.
- Whenever possible, include staff members on the insider threat team who already have experience in dealing with insider threats and foreign intelligence threats, such as experienced counterintelligence staff. This selection of experienced staff is especially important for companies in which mishandling of classified, proprietary, trade secret, and intellectual property material could culminate in law enforcement action.
- Include the following components in an insider threat program: employee monitoring, awareness training, and identification and monitoring of critical assets and intellectual property. Technologies should include access controls, logging, data loss prevention, and host-based monitoring.
- Implement a program that tracks metrics to compare them to industry benchmarks (which may not exist yet) and assess the effectiveness of the program over time.
- Implement a behavioral monitoring program on an organization's network.
- Delivering insider awareness training to enterprise employees and contractors, would betterenable the insider-contractor-employee to be identified.
- Integrated Risk Management Program – Development of an organization-wide approach to manage cybersecurity risk.[xxv]

Incident Response and Management:

- Consider the full range of disciplinary actions, including legal action, if warranted, against malicious insiders. Simply firing an employee pushes a potentially serious problem to another unsuspecting organization.
- Contractually requiring contractors to have the same background and periodic security check that employees must conform to. Additionally, the contractor company would be required to share the results of these checks with the buyer or hiring organization. Furthermore, properly implemented ZTA strategies, information security and resiliency policies, and best practices reduce the risk of an insider attack. ZTA does prevent a compromised account or system from accessing resources outside of its normal purview or normal access patterns. See NIST SP 800-207 for additional information.

5.4.9 NIST SP 800-53 (REV. 4) RELEVANT CONTROLS

PM-12 Insider Threat Program

- The organization implements an insider threat program that includes a cross-discipline insider threat incident handling team. [xxvi]
- Family – PM (Program Management)
- Related NIST SP 800-53 Controls : AC-6, AT-2, AU-6, AU-7, AU-10, AU-12, AU-13, CA-7, IA-4, IR-4, MP-7, PE-2, PS-3, PS-4, PS-5, PS-8, SC-7, SC-38, SI-4, PM-1, PM-14

[xxv] NIST Cyber Security Framework
[xxvi] NIST Risk Management Framework

NIST CYBER SECURITY FRAMEWORK (CSF) RELEVANT CORE FUNCTIONS AND CONTROLS

FUNCTION	CONTROL/NAME	DESCRIPTION	NIST SP 800-53 (REV. 4) RELATED CONTROLS	INFORMATIVE REFERENCES
IDENTIFY	ID.AM-5 Asset Management (subcategory ID.AM-5)	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with them relative importance to organizational objectives and the organization's risk strategy ID.AM-5: Cybersecurity Roles and Responsibilities for the Entire Workforce and third-party Stakeholders	CP-2, PS-7, PM-11	CIS CSC 17, 19 COBIT 5 APO01.02, APO07.06, APO13.01, DSS06.03 ISA 62443-2-1:2009 4.3.2.3.3 ISO/IEC 27001:2013 A.6.1.1
IDENTIFY	Governance (ID.GV):	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	PS-7, PM-1, PM-2, SA-2, PM-3, PM-7, PM-9, PM-10, PM-11	CIS CSC 19 COBIT 5 APO01.02, APO10.03, APO13.02, DSS05.04 ISA 62443-2-1:2009 4.3.2.3.3 ISO/IEC 27001:2013 A.6.1.1, A.7.2.1, A.15.1.1
IDENTIFY	Supply Chain Risk Management	Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk	SA-9, SA-12, PM-9	CIS CSC 4 COBIT 5 APO10.01, APO10.04, APO12.04, APO12.05, APO13.02, BAI01.03, BAI02.03, BAI04.02 ISA 62443-2-1:2009 4.3.4.2

FUNCTION	CONTROL/NAME	DESCRIPTION	NIST SP 800-53 (REV. 4) RELATED CONTROLS	INFORMATIVE REFERENCES
		decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess, and manage supply chain risks.		ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2
PROTECT	Awareness and Training	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity related duties and responsibilities consistent with related policies, procedures, and agreements.	AT-2, PM-13	CIS CSC 17, 18 COBIT 5 APO07.03, BAI05.07 ISA 62443-2-1:2009 4.3.2.4.2 ISO/IEC 27001:2013 A.7.2.2, A.12.2.1
DETECT	Continuous Monitoring	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures. Subcategory DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events.	AC-2, AU-12, AU-13, CA-7, CM-10, CM-11	CIS CSC 5, 7, 14, 16 COBIT 5 DSS05.07 ISA 62443-3-3:2013 SR 6.2 ISO/IEC 27001:2013 A.12.4.1, A.12.4.3
RESPOND	Response Planning (RS.RP)	Response Planning (RS.RP): Response processes and procedures are	CP-2, CP-10, IR-4, IR-8	CIS CSC 19 COBIT 5 APO12.06, BAI01.10 ISA 62443-2-1:2009 4.3.4.5.1

FUNCTION	CONTROL/NAME	DESCRIPTION	NIST SP 800-53 (REV. 4) RELATED CONTROLS	INFORMATIVE REFERENCES
		executed and maintained, to ensure response to detected cybersecurity incidents.		ISO/IEC 27001:2013 A.16.1.5
RESPOND	Mitigation (RS.MI)	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	IR-4, CA-7, RA-3, RA-5	CIS CSC 19 COBIT 5 APO12.06 ISA 62443-2-1:2009 4.3.4.5.6 ISA 62443-3-3:2013 SR 5.1, SR 5.2, SR 5.4 ISO/IEC 27001:2013 A.12.2.1, A.16.1.5
RECOVER	Recovery Planning (RC.RP)	Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	CP-10, IR-4, IR-8	CIS CSC 10 COBIT 5 APO12.06, DSS02.05, DSS03.04 ISO/IEC 27001:2013 A.16.1.5

5.5 SCENARIO: DISGRUNTLED CONTRACTOR

5.5.1 BACKGROUND

Contract employee ("Sally") has been a long-time employee of her company, Services LLC, and is presently providing database-related support services via a sub-contract engagement with an Integrator Firm, who is the prime contractor with the Acme Organization.

The period of performance of this contract is ending in half a year and Acme Organization is in the final stages of re-competing the contract. The incumbent Integrator Firm has informed the Services LLC Management Team that they are submitting a bid, but they have decided they no longer will be using Services LLC as a subcontractor. As a result, the Services LLC Management Team is considering laying off the handful of the Services LLC employees that have been supporting the Acme Organization – to include Sally – shortly after this contract ends. Sally learns about the potential layoffs from a friend and work colleague who is a direct report to one of the Services LLC managers.

Sally is upset that she might be losing her job and angry that she had to learn about this "through the grapevine," and even more angry that the management team of Services LLC does not regard her as an asset to the company. Sally no longer feels motivated to perform her work to the typical high standard she used to apply to

herself. With three more months left on the current contract, Sally learns that the Integrator Firm has been awarded the new contract.

With a few weeks left before the contract ends, Sally's stress level has increased substantially as she is unclear about if or when she will be losing her job and is worried about how she will pay her bills. Her Services LLC supervisor has been telling her that they are hoping to assign her to a new project team, but she is not sure if this is true or not. She has been applying for other jobs but has been unsuccessful. She is distracted and depressed and "lashes out" at the Integrator Firm program manager when he asks her to document her day-to-day processes for the purpose of supporting a "smooth and seamless transition" of her work responsibilities to the new, incoming Integrator Firm team member.

5.5.2 THREAT SOURCE

The threat source, in this example, is a contract employee responsible for providing database-related support services to the Acme Organization. The employee performs her work by remotely connecting into Acme Organization's production system. She also has access to the development and testing environments for this system and is the primary person who is responsible for ensuring backups are performed. Because of the nature of the access that the contract employee has to the organization's information technology system, as well as knowledge the employee has gained about the data within this system, the contract employee is well positioned to cause harm.

5.5.3 VULNERABILITY

There are several actual or potential vulnerabilities (or control gaps or weaknesses) highlighted in this example. The Service LLC subcontractor may be held to a different set of requirements and level of oversight from that of the prime contractor. Sally's emotional state and concerns about her financial situation have likely made her more vulnerable to making mistakes. Her changes in demeanor, behavior, and the quality of her work performance are indicators that she may be disgruntled. While a disgruntled employee should not be equated to be an insider threat, there is a greater likelihood that a disgruntled employee can become an insider threat. Sally is part of a contractor support team from multiple companies and conducts most her work remotely. As a result, it is likely no one noticed these indicators, viewed them as a concern, nor viewed them as their responsibility to report or address especially since the contract was nearing its end. The way Sally became aware of the Service LLC's Management Team's plan to potentially let her go, and their insufficient communications with her about whether she would be reassigned, were factors that contributed to Sally's disgruntlement and the actions she took. Lastly, the request by the Integrator Firm Program Manager revealed there were likely insufficient controls in place related to Sally's duties and responsibilities and suggests a level of blindness, ignorance, or disregard about the personal impact to Sally.

5.5.4 THREAT EVENT DESCRIPTION

Sally's distress reached a new high after the incident with the Integrator Firm employee. She felt she had no control over her situation and began obsessing about how she felt she was being mistreated and unappreciated. With a few days left on the job, she decided she could "get back" at the Integrator Firm program manager by altering some of the content, in several key fields, for a select number of the records in the database. Sally also made sure that the same changes were made to the backup database files. She was also careful in choosing to make changes that she knew would likely go unnoticed for many months, and Sally believed it was highly unlikely that the changes she made to the records would ever be attributed to her.

By making the changes to the data, Sally felt like she still had a little bit of control over something in her life. She did not want to do anything bad, but it gave her some pleasure knowing that "justice might be served" if and when the altered content was discovered—as she believed it would–it would create a situation where the integrity of all the database records would then be called into question. When this occurred, she believed that it would be blamed on the Integrator Firm program manager, and the person who replaced her and "took" her job from her.

5.5.5 ORGANIZATIONAL UNITS / PROCESSES AFFECTED

The affected organizations are the organization that has contracted for support services and the contractor firm providing the services. Depending upon the specific value and purpose of the data that was affected, other potential impacts could occur for other stakeholders of users of the system or the information associated with the system. Reputations could be negatively impacted. There could be substantial costs incurred as well.

5.5.6 MITIGATING STRATEGIES / SCRM CONTROLS

Potential mitigating strategies could include:

- Close review of employee network activities, especially during the time period in which an employee's relationship with a given organization will be ending soon
- Conduct an exit interview or increase communications with an employee who will be leaving or will be terminated to assess their frame of mind
- Ensure employees are reminded of their legal obligations to protect information or not to disclose information and the consequences for violating those obligations
- Terminate access once an employee has been told they will be terminated, or when the employee has given notice that they are leaving
- Ensure account access for the employee is removed
- Perform a "transition" audit
- The ACME Corp. could review relevant standards documents for information and methods relevant to managing this risk. For example:
    - NIST SP 800-37
    - NIST SP 800-53
    - NIST SP 800-161
    - NIST SP 800-171
- The ACME Corp. could have an operational Insider Threat Program (ITP) wherein they employ active controls and awareness training to collect automated and manual notifications of potential insider threats.
- The ACME Corp. could require, or evaluate, an Insider Threat Program implemented by their contractors.
- The ACME Corp. could evaluate how ACME contractors implement SCRM practices for their contractors; in this scenario that would be Services LLC.
- The ACME Corp. could implement access control policies and controls to ensure that IT System users only have access to what is required to conduct their job.

5.6 SCENARIO: SUPPLY CHAIN SOFTWARE BUILD LIBRARY POISONING

5.6.1 BACKGROUND

Organizations utilize Information and Communications Technology (ICT) systems to build networks, interconnect systems/locations, provide voice/video/data communications, as well as provide internet connectivity. These systems are comprised of both hardware and software. The software within these systems is typically proprietary, yet the software often contains significant amounts of open-source software components not actually developed by the equipment manufacturer. If the software within these systems contains malicious capabilities or exploitable vulnerabilities, unapproved functionality might enable threat actors to copy, block, or modify the traffic

flowing through this equipment. The presence of malicious capabilities or exploitable vulnerabilities, within these systems, presents a risk to the normal operation of the ICT equipment, and therefore to the enterprise.

In this scenario (Supply Chain, ICT Product, Insider) a malicious insider, within an Information or Communications Technology (ICT) vendor organization modifies the software build process to replace an element of the product's software build. The products software image will now built contain malicious software that an adversary, or threat actor, can utilize to impact the operations of the businesses that utilize the relevant ICT product.

The substituting of one software build element, for another, is the focus of this ICT Equipment Supply Chain Insider Threat. An example of this type of substitution occurred in 2017 when the official repository for the widely used Python programming language was tainted with modified code packages.[xxvii]

5.6.2 THREAT SOURCE

The threat source is the software running on the ICT equipment. This software has the potential to contain malicious capabilities or vulnerabilities that can be exploited by attackers.

In this scenario, an insider, within the multi-level supply chain of the ICT equipment vendor, modifies the software build process to cause malicious software, or a vulnerability, to be included as an element of the ICT equipment software.

5.6.3 THREAT IMPACT

The threat impacts of a compromised software supply chain are the same as the threat impacts of vulnerable, or already malicious, software.

An example of a successful software supply chain attack can be found in the ShadowPad attacks.[xxviii]

5.6.4 VULNERABILITY

The vulnerability in this instance is the lack of awareness and oversight into the software components that comprise the software from trusted ICT equipment vendors.

5.6.5 THREAT EVENT DESCRIPTION

Today's software development methodologies reflect software development environments where many developers or teams-of-developers each develop system elements which are brought together to build a product software image. Additionally, components of the software build can include software from external vendor software libraries, other third-party software libraries, as well as open source libraries such as GitHub.

The software build process contains a list of the component software elements that will comprise the build image. By modifying the build list, the insider can replace a software build element with alternate software that contains vulnerabilities or malicious capabilities.

This activity of modifying the build process to ultimately insert vulnerabilities, or malicious software, can happen at various places along the supply chain. For example, the manufacturer of ICT network equipment might include software elements from the manufacturer of a system component. In the same manner, the manufacturer of the

---

[xxvii] Dan Goodin, "Devs unknowingly use "malicious" modules snuck into official Python repository," ArsTechnica, 2017.
[xxviii] SecureList, "Popular server management software hit in supply chain attack," 2017.

system component might also include software elements from a supplier of a chip on the system component. Each of these entities likely also includes open source software as elements of their software builds.

5.6.6 OUTCOME

The outcome of this scenario is that an organization can be operating ICT equipment that is vulnerable or contains embedded malicious software. Threat actors might then be able to utilize the embedded malicious software or exploit the existing vulnerability to gain access to the enterprise IT environment.

5.6.7 ORGANIZATIONAL UNITS / PROCESSES AFFECTED

The organizational units or processes affected depend upon what roll in the Enterprise IT/OT infrastructure the ICT equipment fulfills. This assessment must be made on a case by case basis.

5.6.8 MITIGATING STRATEGIES / SCRM CONTROLS

Software supply chain risk management is undergoing rapid evolution and progress. The following mitigating strategies will likely also evolve as government regulations and standards evolve over the coming years. Today enterprises should consider one or more of the following mitigating strategies:

- Require ICT equipment manufacturers to disclose their software supply chain risk management practices. Assess those practices.
- Require ICT equipment manufacturers to disclose their insider risk management programs. Assess those practices.
- Require ICT equipment manufacturers to provide SBOMs for their systems. The SBOMs should include a roll up of all the software elements from the ICT equipment manufacturers supply chain as well as all open-source software elements.
- Establish a program or process to continuously assess the risk of the software supply chain software inventory. Note: the enterprise should also be doing this same software inventory continuous monitoring function for in-house software development efforts, as well as for contracted software development services. This will enable the enterprise to conduct its own risk assessments for the ICT equipment being utilized. Note that multiple services are available to automatically assess the risk introduced by each software element.
- Require ICT equipment manufacturers to immediately disclose identified vulnerabilities, or compromised software, of any element of the ICT equipment software regardless of whether the software was written by the ICT equipment manufacturer or it came to them from their supply chain.

5.7 SCENARIO: AGENCY EMPLOYEE COMPROMISED

5.7.1 BACKGROUND

Federal agencies have been focused on identifying and preventing agency employees with security clearances from becoming insider threats by leaking information, intentionally or otherwise. Now, agency Insider Threat programs are expanding to all employees—past or present—who have had any kind of access to agency information.

NIST defines an Insider as: One who will use her/his authorized access, wittingly or unwittingly, to do harm to the security of the entity they work for. This threat can include damage through espionage, terrorism, unauthorized disclosure, or through the loss or degradation of entity resources or capabilities.

In addition to the internal controls for the detection and prevention of insider threats, companies must also consider the insider threats stemming from their supply chain; in this scenario – the focus is the sourcing of employees/contractors/consultants.

5.7.2 THREAT SOURCE

The threat source, in this example, is a federal employee having influence over a sensitive database storing legal documents used in a lawsuit against a major U.S. IT Corporation. The agency is responsible for preventing unfair methods of competition in commerce and to police anticompetitive practices. In this case, employees have access to active case information being levied against major U.S. corporations. If selected for employment, the threat agent begins to leverage access permissions to acquire and disseminate data to unauthorized entities.

5.7.3 VULNERABILITY

The vulnerability in this example involves a privileged employee who was approached by a major U.S. corporation to acquire privileged information instrumental in evading prosecution by the agency. Although the employee passed initial background checks, a recent financial hardship due to bad investments, medical emergency, gambling, drug addiction, etc. has left the employee open to compromise.

Background checks can be effective for preventing the hiring of known malicious characters, but they may not detect insider threat agents after they are hired. While it is important to maintain controls that detect and stop insider threat activity, detecting the changes in employee risk factors can help mitigate the risk of insider threats. This requires the adoption of Supply Chain Risk Management (SCRM) controls to be applied to employees on a recurring basis as outlined below in 5.7.6 Potential Mitigating Strategies/SCRM Controls.

5.7.4 THREAT EVENT DESCRIPTION

An Insider Threat Agent successfully navigated the hiring process and secured employment (full-time, part-time, contractor) with the target agency. The insider agent uses their authorized access to acquire confidential/classified data and attempted the exfiltration the data undetected. Due to the impending case, the insider agent quickly grabbed the data in the performance of their daily duties but did not cover their tracks. This activity went undetected and during the court proceedings, the defending corporation used the privileged data to circumvent court proceedings. When the agency investigates how the corporation was prepared for their actions with privileged information, the investigation found that the insider agent was a privileged account technician of the agency. Background checks at the time of hire did not find anything to highlight the potential threat.

5.7.5 ORGANIZATIONAL UNITS / PROCESSES AFFECTED

The agency's privileged data handling processes and authorized privileged employee monitoring, hiring, and job performance processes would be affected. Network security settings, controls and requirements would need to be modified to detect and prevent future occurrences.

5.7.6 POTENTIAL MITIGATING STRATEGIES / SCRM CONTROLS

While it is uncommon for an agency employee to leverage their authorized access in order to achieve a specific personal goal, incidents do occur. Thus, agencies should have an operational Insider Threat Program (ITP) [NIST 800-53 & 800-171] wherein they employ active controls and awareness training to collect automated and manual notifications of potential insider threats.

The potential mitigating strategies would be an element of the Risk Management Process as described by the NIST Risk Management Framework.

Potential Mitigating Strategies could include:

- Scheduling new alerts that trigged any time data is added to, removed from, or modified on their secure servers
- Alerts could generate when authorized employees logged into and out of their privileged accounts
- Background checks could be performed annually
- New risk-based questions could be added to the employees' annual and mid-term evaluations
- Limiting the need-to-know privileges of the employees

6 THREAT CATEGORY: ECONOMIC

6.1 SCENARIO: FINANCIAL STRENGTH OF THE SUPPLIER

6.1.1 BACKGROUND

Each company is different in capability to respond to financial problems. This depends on several factors including personnel, size, scope of the company, access to capital, and even geographic location. At any point in time, this capability can change.

6.1.2 THREAT SOURCE

There is significant overhead in maintaining a secure operational environment within a business enterprise. Some firms operating on razor-thin margins or startups struggling to make a profit will be tempted to cut corners or accept risks that can open attack vectors to a threat.

6.1.3 THREAT IMPACT

- Lack of adequate assessments and financial strength can lead to a supplier failure.
- Lack of financial strength can lead to bankruptcies.
- Acceptance of high-volatile risks can lead to financial/security-based compromises and threats.
- Compromise of the confidentiality, integrity, and availability of the organization and the supply chain.
- Lack of financial strength may lead to usage of dated software/hardware materials. This can lead to compromise of integrity of the supply chain and various threats noted in section 11.0.
- Declining revenues can pinch on cash flows and on labor requirements. Increasing price sensitivity may erode margins.[xxix]

6.1.4 VULNERABILITY

The vulnerability in the scenario was created by not spending funds on using protective software.

6.1.5 THREAT EVENT DESCRIPTION

A company struggling to survive under heavy financial stress just to meet payroll may cut IT staff, stop using protective software, or even share protected files or data with an unauthorized buyer just to stay afloat.

[xxix] Craig Guillot, "Managing supply chain risk in an economic downturn," Supply Chain Dive, 2019.

6.1.6 OUTCOME

These potentially bad results are predicated on weakness in financial strengths of a supplier. Unpredictable or surge orders or customers shifting to a new supplier can cause a company to rebalance to match income with expenses.

6.1.7 MITIGATING STRATEGIES / SCRM CONTROLS

- Transparency and collaboration are necessary for supply chain risk mitigation. Fifty-five percent of respondents to a recent Procurement Intelligence Unit survey said supplier insolvency would be the leading risk they face over the next 12 months. The key is to see potential problems, such as trends indicating a company may be close to being insolvent, before they arise and when an organization still has time to address the issues with the supplier.[xxx]
- To mitigate monetary compromises, financial risk assessments require evaluation of all financial statements. Understanding a supplier's financial health requires a deep dive into the supplier's financials to see how several factors have changed over a period. For example, a supplier's receivables may be growing, but that could mean its credit and collection standards are weak.[xxxi]
- It's important to have internal metrics for the Chief Information Security Officer to conduct predictive analytics of the economic viability of the organization. Cross communication amongst the technology and finance organizations are needed when considering supply chain risk.
- Understanding the financial position of your suppliers can help deciding on the need for changes, mitigation strategies, or discussions on how you can help or advise suppliers on improving their operations. Reviewing financial reports from public companies, looking at reports from organizations like Dun & Bradstreet, or having a one-on-one personal discussion and review can also help. A close personal relationship with suppliers will also help mitigate risk.

6.2 SCENARIO: INFORMATION ASYMMETRIES

6.2.1 BACKGROUND

There will always be a difference between what the supplier knows and what the customer knows. Even for customers, who have people co-located with suppliers, this difference of insights or information can cause decision making that will open potential threat vectors.

6.2.2 THREAT SOURCE

The problem from different knowledge or understanding of a supplier's financial status or economic conditions in the marketplace can create assumptions that everything is going fine, when in fact they are not.

6.2.3 THREAT IMPACT

- Lack of communication with the supplier and customer.
- Lack of preparedness when managing supplier/vendor risk.
- Potential compromise of the confidentiality, availability, and integrity of the supply chain.
- Financial compromise due to the lack of supplier compliance.

[xxx] "Supplier Financial Risk: Health Assessment Report," Rapid Ratings.
[xxxi] Ibid.

6.2.4 VULNERABILITY

Lack of oversight from the customer's perspective - built into contracts with the supplier.

6.2.5 THREAT EVENT DESCRIPTION

The supplier is not following the processes or procedures in securing the product from either physical compromise or digital security of the design. The customer is not aware of their lack of compliance.

6.2.6 OUTCOME

The lack of information or the partial gathering of information can cause problems from the customer making assumptions that things are proceeding on plan and with approved and documented processes, but when the supplier knows that these efforts are not being maintained.

6.2.7 MITIGATING STRATEGIES / SCRM CONTROLS

- Place people at the site of a suppliers' production or assembly to monitor or validate. This will incur additional costs but is a control step that reduces or mitigates risk in supply chain compromise.
- Customer organizations should develop and implement a cohesive supplier/vendor risk management program. Organizations need to be able to develop a standardized risk management framework by clearly defining consistent risk assessment procedures, establishing controls, defining forward-looking risk metrics, and implementing risk mitigation strategies. An effective risk management framework helps in flagging vendor risk and enables organizations to react to risk or compliance issues on time.[xxxii]
    - A major oversight in many supplier risk management frameworks is the supplier's optimization of technology. Cross communication amongst the technology and C-suite, strategy, and finance sectors are very important for this process to be successful.
- Customer organizations should leverage technology when developing and implementing a supplier/customer relationship. Technology enables companies to standardize and streamline their processes for managing and mitigating vendor risk. It facilitates a shift from reactive to proactive risk management, and enables a forward-looking vendor governance program which, in turn, strengthens compliance.
    - One of the most important controls in risk management is legal and contractual protection. Technology provides the ability to store large volumes of vendor contracts, documents, service-level agreements, clauses, and non-compliance penalties in an integrated, structured, and easily accessible manner. This helps companies avoid legal liabilities, while also simplifying vendor onboarding.[xxxiii]
- Evaluating vendors regularly through surveys, assessments, and well-defined metrics such as KPIs (key performance indicators) and KRIs (key risk indicators) allows companies to drive continuous improvement in the risk management process.[xxxiv]
- Trend analysis and reporting tools facilitate effective supplier risk and performance tracking. Customer organizations should use these tools to combine data and mitigate oversight.

[xxxii] "Managing Vendor Risk: A Critical Step toward Compliance," Metric Stream.
[xxxiii] Ibid.
[xxxiv] Ibid.

6.3 SCENARIO: OWNERSHIP CHANGE

6.3.1 BACKGROUND

Ownership of a supplier can change hands at any time. New investors will be brought into a small business or start up. Successful businesses will be acquired or merged with larger or equal size businesses. If the ownership change involves foreign entities, this can be problematic to the information security of the company.

6.3.2 THREAT SOURCE

Large amounts of cash generated by a successful business requires reinvestment. Often cash accumulation is used to acquire companies in vertical or horizontal markets.

6.3.3 THREAT IMPACT

- Potential threat to the confidentiality, availability, and integrity of the supply chain.
- Potential threat to national security when considering suppliers linked to foreign entities.
- Potential monopolization of international market power.
- Potential organizations driven to unfair competition.
- Ripple effect of price volatility, excess inventory, and compromises to the security of the supply chain.
- Oversight in security upgrades and compliance with new ownership.

6.3.4 VULNERABILITY

Lack of oversight from the customer's perspective - built into contracts with the supplier.

6.3.5 THREAT EVENT DESCRIPTION

A large Chinese firm has successful been a supplier to numerous companies across the globe. This firm targets a U.S. firm in the same market that is considered a competitor for acquisition. This allows for horizontal integration at the same time as a reduction in global competition.

6.3.6 OUTCOME

The acquisition of firms that control most of the market can be considered an anti-trust violation in many countries. This concept or legal restriction does not apply worldwide. Firms that are controlled, subsidized or financially supported by governments can have an unfair advantage in the marketplace.

6.3.7 MITIGATING STRATEGIES / SCRM CONTROLS

The U.S. Government should protect U.S. firms undergoing unfair competition. CFIUS should restrict sales of U.S. firms to foreign firms, where the acquisition would create a risk to the supply chain or a transfer of control of a critical market to oversight by a hostile or unfriendly government.

Supply chain visibility is critical when considering the potential of an ownership change and its implications. Supply chain visibility is the ability of all stakeholders through the supply chain to access real time data related to the order process, inventory, and potential supply chain disruptions.[xxxv]

In 2018, the U.S. Government stood up multiple agencies and task forces to address global supply chain risk (including DHS CISA and the Protecting Critical Technology Task Force at the DoD). When considering global diplomacy in the supply chain, public and private partnership is important for seeking methodology when assessing and monitoring risk.

6.4 SCENARIO: COST VOLATILITY

6.4.1 BACKGROUND

Outside of the suppliers' control, there can be governmental or economic drivers that will affect the cost of a specific product. While minor price increases or drops are usually accounted for in the markup of products at each stage of the supply chain, successful companies still have challenges when monetary policy (value of the local currency) is less than stable or when market related events occur (i.e., tariffs are employed for political purposes or economic downturn causes businesses to react differently). This can be quite problematic for multiple parts of the supply chain. This is especially true for ICT supply chain, which works on thin margins to begin with.

6.4.2 THREAT SOURCE

The value of currency and politically volatile events can have serious implications on taxes (tariffs) and the true cost of trade across multiple currencies. One way around this is to diversify your supply chain sources to develop contingencies should volatility arise on supply costs. This is part of a good supply chain risk management strategy.

6.4.3 THREAT IMPACT

- Potential implications to national security of the customer's end product.
- Potential compromise of the confidentiality, availability, and integrity of nation-states, organizations, and the supply chain.
- Lack of transparency, compliance, and security of the supply chain.
- Potential modification of hardware/software devices while in transit through the supply chain. As more software components are outsourced and volatile events occur, there are more opportunities for third-party tampering and the likelihood of malware or coding vulnerabilities being inserted.[xxxvi]
- Potential risks of financial loss for organizations of the supply chain.

6.4.4 THREAT EVENT DESCRIPTION

The Chinese government is suspected of limiting output of the rare earth element, neodymium, to several external suppliers. Neodymium is essential in the manufacturing of permanent magnets. Various countries have various amounts of Neodymium stockpiled for multiple industries. Neodymium has fluctuated extensively in price over the past 5 years and affects the pricing of hard drives and other electronics that much of the world counts on from Vietnam, China, and other Asian countries. Since China has over 90 percent of the earth's known quantity of

[xxxv] "Supply chain visibility software and solutions," IBM.
[xxxvi] Victor Ng, "Mitigating against supply chain cyber risks," Cybersec Asia, 2019

Neodymium, at various times, they have taken political actions that cause dramatic volatility in the price and amount of Neodymium available worldwide.

6.4.5 OUTCOME

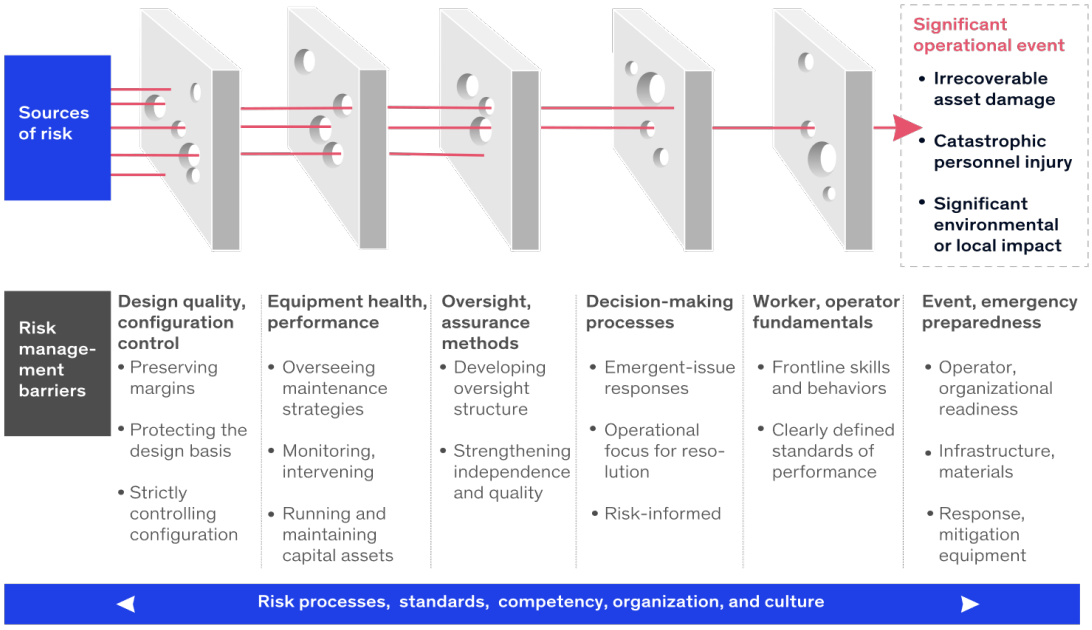
The ability for U.S. or other countries to invest in Chinese mines has been very limited to non-existent by the Chinese government. Chinese firms have sought to invest in the companies that use the rare earths to expand their ability to control more of the technology marketplace. These firms are backed by the Chinese government, and they are usually state owned or managed companies. They can use rare earths to affect prices outside the country (initiate volatility) and ensure supply and low cost for state owned companies (inside China) to affect the volatility, price, and supply chains for various products.

6.4.6 MITIGATING STRATEGIES/SCRM CONTROLS

- U.S. companies need to work with businesses and countries outside of China to diversify their supply chains and lower supply chain risks. R&D needs to consider possible replacements for rare earths that are politicized. Supply chains can, likely at additional cost, work to obtain and seek out rare earths from other sources. Additionally, some rare earths can be obtained at a lower price if they are provided before they are separated but will incur some cost for the separation of the rare earths from their source. The goal from these mitigations will likely yield a diversified source of products that can obtain needed Neodymium at a more stable price structure than competitors. Competitors will likely have to add margin to deal with the multiple variables that will add excess market costs to their supply chain.
- Organizations within the supply chain should consider a "Security by Design" approach with products integrated with firmware management systems. For an added layer of protection, production codes are vetted, stored, and safeguarded to prevent hardware from being modified, unless the code is retrieved.[xxxvii]
- With a global supply chain, transparency (internally in the organization and throughout the supply chain) is difficult, but very important.
    - Leaders must clearly define and communicate an organization's risk tolerance. Risk mitigation often has an associated incremental cost, and so it is important to align on which risks need to be mitigated and which can be borne by the organization.[xxxviii]
    - Various organizations, such as IBM, recommend the leveraging of technology when wanting to access real-time data within each node of the supply chain. Embedded AI capabilities provide real time intelligence and actionable recommendations to reduce disruption mitigation from days to hours.[xxxix]
- A typical approach for risk identification is to map out and assess the value chains of all major products. Each node of the supply chain—suppliers, plants, warehouses, and transport routes—is then assessed in detail. Risks are entered on a risk register and tracked rigorously on an ongoing basis. In this step, parts of the supply chain where no data exist, and further investigation is required should also be recorded.[xl]
- With volatile components it is important for customer organizations to "Build Strong Defenses." McKinsey and Company outlines typical layers of defense organizations employed to against volatile risks via the figure below.[xli]

[xxxvii] Ibid.
[xxxviii] Tucker Bailey et al., "A practical approach to supply-chain risk management," McKinsey, 2019.
[xxxix] "Supply chain visibility software and solutions," IBM.
[xl] Tucker Bailey et al., 2019.
[xli] Ibid.

Layers of defenses help organizations manage unknown risks.



McKinsey & Company

PRODUCTS AND SERVICES THREAT SCENARIOS

6.5 SCENARIO: COMPROMISED PRODUCT QUALITY TESTING BY SUPPLIERS DUE TO FINANCIAL STRESSES

6.5.1 BACKGROUND

During the testing of hardware components, sometimes exceptions are taken when verifying the quality of the products. If the organization is financially instable and is looking for means to avoid costs, lack of due diligence during the product assessment phase can be common. Weak product testing procedures can lead to an approval of defected or potentially counterfeit products. As these faulty products are integrated into equipment, the integrity of the end item can be compromised.

6.5.2 THREAT SOURCES

A supplier's financial instability and the decisions that come from it can lead to a disparity of information shared between the customer and supplier. Organizations struggling to make profits may accept risks and allow for low quality testing procedures. When allowing an organization to be part of the supply chain, due diligence from each member of the chain includes the evaluation of problems that could affect the equipment's reputation and integrity. Not doing so can lead to an opening for attack vectors and threats.

6.5.3 THREAT IMPACT

- Inherited risk of potentially faulty, dated, or counterfeit products
- Lack of product integrity
- Reputational risks for the manufacturer of the end product

- Product liability concerns for the consumer of the end product

6.5.4 VULNERABILITY

The distribution of low-quality products integrated into an end product is a widespread problem that affects manufactures, distributers, and retailers in any and every industry. The vulnerability comes from the supplier who chose to inadequately test the parts due to financial stresses.

6.5.5 THREAT EVENT DESCRIPTION

The supplier is not following the adequate processes in securing the product from potential physical compromise. The customer is not aware of their lack of compliance.

6.5.6 OUTCOME

The lack of information can cause problems because the customer is assuming the supply chain is proceeding on plan with adequate and diligent processes. Potential vulnerabilities have gone undetected in the product's design. The resulting effect can take a variety of forms, from impacting the performance of the equipment to a potential compromise of the authentication and integrity of the product. The worst-case scenario would be the introduction of components that cause product failure due to lack of compliance with design specifications or by providing threat actors with malicious intent access to networks

6.5.7 ORGANIZATIONAL UNITS / PROCESSES AFFECTED

Any supply chain member that integrates products without adequate vetting and authentication can open doors to potential cybersecurity threats. From a business perspective, quality testing procedures are often conducted to reduce overall project costs, protect an organization's reputation or brand, reduce litigation expenses, conform to regulatory requirements, and to verify that all products are legitimate.

As an example, an office that is part of a larger enterprise acquires laptops for their employees that will connect to the networks of the enterprise. One of the suppliers purchased laptop batteries from a third party. Testing the integrity and authentication for these batteries was an overhead cost the firm assumed they could avoid. The batteries were sold as brand-name new, genuine, original, Original Equipment Manufacturer (OEM) products. As these laptops were used in the office, employees realized that these laptops contained counterfeit lithium-ion laptop batteries. Such components can lack safeguards and pose physical threats for the enterprise.

6.5.8 MITIGATING STRATEGIES / SCRM CONTROLS

- Customer organizations should leverage technology when developing and implementing a supplier/customer relationship. Technology can streamline processes for managing and mitigating vendor risk.
- Evaluating vendors regularly through surveys, assessments, and well-defined metrics such as key performance indicators (KPIs) and key risk indicators (KRIs) allows companies to drive continuous improvement in the risk management process.[xlii]
- Specify performance measures that define the expectations and responsibilities for both parties including conformance with rules and expectations from members in the chain. Such measures can be used to motivate the third party's performance, provide further transparency for the customer along the chain, or potentially penalize poor performance.

[xlii] "Integrating KRIs and KPIs for Effective Technology Risk Management," ISACA, 2018.

- Trend analysis and reporting tools facilitate effective supplier risk and performance tracking. Customer organizations should use these tools to combine data and mitigate oversight.

6.6 SCENARIO: DEMAND VOLATILITY IN THE SUPPLY CHAIN

6.6.1 BACKGROUND

Demand volatility is a reality in many industries and supply chains. Not only are retailers serving consumers facing volatile demand, but this volatility is being passed on to manufacturers and distributors at different stages of the industry value chains. When demand spikes and fluctuates, members of the chain may not be able to maintain their consistency in manufacturing and distributing the quantity of products/services. Supply chain risks, lack of commodity availability, and potential loss of competitive edge can be a direct reason for price risks and insertion of third-party suppliers. Inadequate third-party suppliers may lead to insertion of faulty products in the chain.

6.6.2 THREAT SOURCES

Many factors contribute to demand volatility, including increased customer choices, product customization, rapid technological improvements, global competition and upstream supply fluctuations.[xliii]

Managing volatile demand efficiently in a demand driven environment is a significant challenge and requires companies to employ robust supply chain strategies.

The level of market turbulence has increased, bringing with it a reduction in the predictability of demand. According to various sources and economists, there are many reasons for this increased demand volatility.[xliv] Shorter life cycles, often driven by technology change, means that the risk of obsolescence increases. Higher levels of competitive activity lead to market disturbances to demand in many consumer markets (e.g., promotions, sales incentives, and the like). Increasing variety within product ranges further fragments demand and makes forecasts less reliable.

For a chain to maintain the need of the market, inserting various third-party suppliers may support the demand, but may open the doors to various cybersecurity threat vectors. Inadequately vetted suppliers may insert faulty, dated, or potentially counterfeit products into the chain.

6.6.3 THREAT IMPACT

Because companies are still largely forecast driven, with long planning horizons and long lead times of response, they are increasingly vulnerable to wild swings in demand. If faulty or counterfeit products are inserted into the chain, the impacts of the threat could be;

- Lack of product integrity
- Compromise of the confidentiality of the end product
- Reputational risks for the manufacturer of the end product
- Product liability concerns for the consumer of the end product

---

[xliii] Rajesh Gangadharan, "Supply Chain Strategies to Manage Volatile Demand," Supply & Demand Chain Executive, 2007.
[xliv] "Supply Chain Vulnerability Executive Report," Cranfield University School of Management, 2002.

6.6.4 VULNERABILITY

The vulnerability is largely coming from responding to the market demands via inserting other manufacturers, suppliers, distributers, etc. to the supply chain ecosystem of the end product. To maintain the pace and consistency of delivering products and services, adequate vetting of these new members and products may not occur.

6.6.5 THREAT EVENT DESCRIPTION

The supplier is not following the adequate processes in securing the product from potential security compromise due to the fluctuation in demand. New members are being inserted into the supply chain ecosystem to maintain the market's need without adequate vetting. The customer is not aware of their lack of compliance.

6.6.6 OUTCOME

According to various economists, often the focus of supply chain management strategies when addressing volatility tends to only be on one area of the chain (e.g., inventory optimization) without consideration of all aspects of products in the supply chain, resulting in sub-optimal results. The lack of volatile demand management can be a huge competitive differentiator for companies. Not being able to manage volatile demand in a cost-effective manner can lead to significant financial and security risks, ranging from premium supply chain costs to insertion of counterfeit products.

6.6.7 ORGANIZATIONAL UNITS / PROCESSES AFFECTED

As mentioned in the previous use case, any supply chain member that integrates products without adequate vetting and authentication can open doors to potential cybersecurity threats. From a business perspective, quality testing procedures are often conducted to reduce overall project costs, protect an organization's reputation or brand, reduce litigation expenses, conform to regulatory requirements, and to verify that all products are legitimate.

6.6.8 MITIGATING STRATEGIES / SCRM CONTROLS

Pragmatic mitigating strategies may include:

- **Maintaining an Inventory Buffer**: Various economists recommend utilizing an inventory buffer strategy to manage the volatility in demand. While maintaining high levels of inventory can be expensive and retaining low inventory levels can negatively impact customer service, a middle ground can be found by building carefully planned inventory levels. This right balance of planned inventory buffers (safety stock) can be designed to cushion most of the shocks from the volatility in demand.[xlv] A more attractive alternative to inventory buffers in many industries is the use of capacity buffers. Through internal or external resources, capacity buffers provide more flexibility to companies to manage unexpected variations in demand. The inventory kept in stock has also been accumulated following adequate security test vetting and can mitigate the insertion of cyber threats.
- **Collaborative Processes**: Responding quickly to changes in demand requires fast information flow with the suppliers and partners. Collaborating with suppliers enable the end user to send forecast data to its suppliers faster, enabling the suppliers to plan their supply chains and respond faster to demand changes passed on. This process can help members in the supply chain ecosystem be ready to their best ability for how to prepare.

[xlv] Rajesh Gangadharan, 2007.

6.7 SCENARIO: ECONOMIC/TRADE POLICIES & THE GLOBAL SUPPLY CHAIN

6.7.1 BACKGROUND

Economics and cybersecurity are increasingly intertwined. As this connectivity grows, however, so does exposure to the risks and costs of cyberattacks. Some proposed measures addressing cybersecurity risk are likely to constitute barriers to data flows and digital trade. These include data-flow restrictions and import restrictions on IT products, including software from countries or supply chains where cyber risk is high.[xlvi]

Countries may also resort to import restrictions including higher tariffs as a means of punishing and deterring cyberattacks. By treating goods, services, or data from high-risk countries less favorably than those from countries where cyber risk is lower, cybersecurity measures may violate international trade agreements and regulations. This can disrupt current global supply chains and having to acclimate to such large changes may insert threat vectors into the current chain when looking for substitute suppliers.

6.7.2 THREAT SOURCES

Security and trade have traditionally overlapped, and supply chains tend to be global in nature. Tariffs and trade wars can rattle markets, prompt uncertainty, and question whether supply chains and global operations are positioned to handle the speed, unpredictability, and interconnectedness of the global economy.

Global economic discourse leads to market volatility, disruption in the supply chain, and organizations having to consider new economic regulations, policies, etc. This can impact global supply chains vastly. When having to find new members to substitute or integrate into the chain to continue providing products/services, new threats can enter the chain with new suppliers and additional costs can incur to swap out current vendors.

6.7.3 THREAT IMPACT

- Lack of financial strength may lead to supplier failure/bankruptcy.
- New members in the supply chain may lead to lack of communication with the new suppliers and customer. This can lead to oversight in security compliance, etc. with new ownership.
- Potential threat to the confidentiality, availability, and integrity of the supply chain.
- Potential monopolization of market power when complying to international trade regulations.
- Potential insertion of faulty products as shifting to new suppliers.
- Potential inherited risk as new suppliers are integrated into the supply chain.

6.7.4 VULNERABILITY

As organizations comply to trade regulations, domestic policies, etc., it may lead to disparities with current global supply chains and their makeup. To maintain compliance, customers may reevaluate the current suppliers and shift to new stakeholders to substitute in the chain. New suppliers may open doors to inherited risk, faulty products, financial burdens, and various new threat vectors.

6.7.5 THREAT EVENT DESCRIPTION

Geopolitical and macro-economic uncertainty, highlighted by Brexit and the Italian budget crisis in Europe, and the simmering trade war between U.S. and China have major implications globally for supply chains and markets.

[xlvi] Joshua Meltzer and Cameron Kerry, "Cybersecurity and digital trade: Getting it right," Brookings Institute, 2019.

Sudden changes in tariff barriers, trade rules, and the economic outlook have the potential to disrupt supply chains, considerably increase costs, etc. Within the supply chain, companies need to reconsider their sourcing locations and how they move physical goods across the organization.[xlvii]

As organizations reconsider suppliers while maintaining the consistency and pace to distribute products, the chain may be susceptible to new cyber threat vectors.

6.7.6 OUTCOME

If members in the chain cannot adequately keep up with international trade agreements and do not have the financial stability to change suppliers and continue business, it is possible that the supply chain may fail and the competitive edge that organization had is now lost.

If the organization does find new members to substitute in the supply chain and continues business, the organization needs to be very cognizant of the potential inherited risks and security posture the new suppliers have. If not, potential cyber threat vectors may insert themselves into the chain, potentially leading to a vulnerability.

6.7.7 ORGANIZATIONAL UNITS / PROCESSES AFFECTED

When adding new members into the supply chain, the confidentiality, availability, and integrity of the original chain and its process is affected. The vetting of new suppliers is essential and communication between the end user and the suppliers is essential.

6.7.8 MITIGATING STRATEGIES / SCRM CONTROLS

Leveraging Distributed Ledger Technology: In today's world, businesses which fail to provide their customers with what they want, as soon as they want will lose market share. A digital supply chain provides real time visibility on the movement of goods across a company's supply and logistics networks, from product conception, to transit, to arrival at destination. Distributed ledger technology provides a single platform through which supply chain partners can share information and collaborate seamlessly. This technology facilitates teamwork, reduces misunderstandings, and expedites delivery timelines between businesses, logistics providers, and suppliers.

This can help when considering new members and the communication gap in the chain. Various use cases have been executed doing so.

McKinsey and Company assessed blockchain technology's value at stake for the supply chain world, and looked at three areas where it could add value:[xlviii]

- **Replacing slow, manual processes.** Although supply chains can currently handle large, complex data sets, many of their processes, especially those in the lower supply tiers, are slow and rely entirely on paper—such as is still common in the shipping industry.
- **Strengthening traceability.** Increasing regulatory and consumer demand for provenance information is already driving change. Moreover, improving traceability also adds value by mitigating the high costs of quality problems, such as recalls, reputational damage, or the loss of revenue from black- or grey-market products. Simplifying a complex supply base offers further value-creation opportunities (see sidebar, "A complex supply chain of unknown parties").

[xlvii] Peter Cunningham and Natasha Condon, "Trade Around the World: Mitigating Rising Supply Chain Risks in Evolving Economies," CItiBank.
[xlviii] "Blockchain technology for supply chains—A must or a maybe?" McKinsey, 2017.

- **Reducing supply-chain IT transaction costs.** At this stage, this benefit is more theoretical than actual. Bitcoin pays people to validate each block or transaction and requires people who propose a new block to include a fee in their proposal. Such a cost would likely be prohibitive in supply chains because their scale can be staggering. For example, in a 90-day period, a single auto manufacturer would typically issue approximately 10 billion call-offs just to its tier-one suppliers. Also, together all those transactions would significantly raise demand for data storage, an essential component of blockchain's distributed-ledger approach. In addition, creating and maintaining numerous copies of data sets would be impractical in the supply-chain environment, especially in permission-less blockchains.

7 THREAT CATEGORY: INHERITED RISK (EXTENDED SUPPLIER CHAIN)

This category of threats is a result of current supply chains that extend broadly across industries and geographies. These threats typically are associated with the challenge of extending controls and best practices through the entire supply chain due to its global nature. It also includes the vulnerabilities that can result from integration of components, products, or services from lower tier supplier where a prior determination of acceptable risk may not flow all the way through the development process to the end user supplier.

7.1 SCENARIO: SUB-AGENCY FAILURE TO UPDATE EQUIPMENT

7.1.1 BACKGROUND

A sub-agency had not upgraded their hardware supporting their network routers, switches, and hubs to ensure an adequate cybersecurity posture. As a result, this agency was unable to receive software updates, and therefore put their agency at a substantial risk and vulnerable position.

7.1.2 THREAT SOURCE

These disruptions have taken place across state and local agencies, the private sector, and even at home with personal routers. Threats can come from international unfriendly countries, hackers, etc. Furthermore, the attack can come at any time with persistence and can occur frequently if the condition is not fixed.

7.1.3 THREAT IMPACT

Potential impact of failure to update equipment:

- Hardware/device modification
- Traffic sniffing[xlix]
- Device tampering and data spoofing[l]
- Corporate espionage
- DoS Attacks[li]
- Destruction of hardware

[xlix] The access to network traffic is a common threat in typical IT environments. However, in the context of hardware-related attacks, traffic sniffing is not limited to network connections but can also be carried out on internal buses and connections, such as the memory or hard drive bus. Those bus systems traditionally do not assume threats from within those system/devices which are physically connected so that no compensating controls are implemented.

[l] Comparable to surveillance threats, the tampering or spoofing of data on mobile computing devices can have wider impact than typical data tampering: Spoofed location, audio, or visual data can lead to a variety of abuse scenarios.

[li] Denial-of-service of mobile/personal/embedded devices (e.g. the crash of a smartphone, the outage of a monitoring solution, or the error state of an alarm system).

- Lack of agency wide compliance in security
- Compromise of confidential nation-state information
- Compromise of the extended supply chain's integrity and confidentiality
- Compromised special code within the supply chain's hardware components

7.1.4 VULNERABILITY

Because this was a sub-agency on the entire agency's network, all sub-agencies became vulnerable. The software from a supplier is not being maintained to its current version across sub-agencies, which has created a vulnerability.

7.1.5 THREAT EVENT DESCRIPTION

This is a network category threat that business heads and Chief Financial Officers must be made aware of to understand that cutting budgets from network infrastructure may not be a viable option. This is due in large part because of the size and scope of the risk posed to an organization's network infrastructure.

7.1.6 OUTCOME

The objective of the threat actor can be network disruption, data theft, intellectual property and financial threats.

7.1.7 MITIGATING STRATEGIES / SCRM CONTROLS

Potential Mitigating Strategies include:

- Require flow-down controls and risk management for all sub-agencies to pass to any of their sub-agencies.
- Require audits or compliance reports and attestations.

SDLC:

- Creation of a secure embedded design and development lifecycle for hardware equipment. ENISA's Hardware Threat Landscape and Good Practice Guide Report[lii] provides an example of guidelines of relevance when considering this mitigation strategy:
  - Rely on stable software components
  - Secure coding guidelines must be specific for hardware related development and languages
  - Implementation of segregation of duties
  - Consideration of extra variable integrity validity checks on critical values

Secure Updates/Modification:

- Updates should be signed in a cryptographically secure way. Guidance on that can be found in NIST SP 800-89, NIST FIPS 186-3, or NIST SP 800-131A.
- The Root of Trust for Update (RTU) should be stored in a tamper-protected way (e.g., using hardware key stores). Those key stores must be properly closed after usage.

---

lii Enisa.europa.eu

- Use endpoint detection and response solutions to automatically detect and remediate suspicious activities.
- Develop your defenses based on the principle that your systems will be breached. When one starts from the premise that a breach is inevitable, it changes the decision matrix on next steps. The question becomes not just how to prevent a breach, but how to mitigate an attacker's ability to exploit the information they have accessed and how to recover from the breach.[liii]

Agencywide Compliance:

- Agency-wide secure development standards should be implemented. The network should work towards the maintenance of the network's compliance. Each sub-agency's compliance with guidelines, standards, etc. should be documented and shareable in an open and transparent way.
- Establishment of a chain of trust. It should be possible to establish a chain of trust from the initial hardware booting steps to the execution of the operating system.
- Stakeholders should work towards effective training/awareness programs and mappings to best practices for each node of the agency network.
- Security requirements are included in every Request for Proposal (RFP) and contract to assure compliance by suppliers.

7.1.8 RELEVANT CONTROLS

Refer to NIST CSF Relevant Core Functions and Controls in table below in section 7.4.9.

7.2 SCENARIO: SUB-AGENCY FAILURE TO UPDATE ENTERPRISE SOFTWARE

7.2.1 BACKGROUND

Enterprise software from a supplier is not being maintained to its current version across sub-agencies to ensure an adequate cybersecurity posture.

7.2.2 THREAT SOURCE

This threat is applicable across federal, state, and local agencies as well as the private sector. The threats could occur anywhere within the supply chain (i.e., OEMs, manufacturers, integrators, third parties, etc.).

7.2.3 THREAT IMPACT

- Lack of consistency and compliance through the supply chain ecosystem
- Vulnerabilities to security flaws and software vulnerabilities to the entire supply chain ecosystem
- Compromise of the integrity, confidentiality, or availability of the entire supply chain ecosystem

7.2.4 VULNERABILITY

Unpatched applications.

[liii] NIST Best Practices in Cyber Supply Chain Risk Management

7.2.5 THREAT EVENT DESCRIPTION

Software is the threat category. The sample threat mentioned above could be a threat to any agency that does not maintain supported software thresholds (usually 2 previous versions). Non-updated operating systems are also a threat. Some organizations are still running vulnerable and unsupported versions that were deprecated years ago.

7.2.6 OUTCOME

Intellectual property, network, and disruption are all applicable. Several cities have already had their networks locked up, and threat actors are demanding financial settlement to unlock their network and devices.

7.2.7 ORGANIZATIONAL UNITS / PROCESSES AFFECTED

Depending on the software, it could impact the OEM, the reseller, or the integrator. There could be cost implications, and the integrity of the company may be questioned. Out-of-date software (no longer supported by the OEM or third parties) places unnecessary risk on the agency. Unsupported software places security vulnerability upon the business and the agency. The threat is applicable at any time and persistent within the infrastructure.

7.2.8 MITIGATING STRATEGIES / SCRM CONTROLS

- Require supply chain organizations to keep their applications and operating systems up-to-date and patched within 72 hours of release of a new patch. Require attestations of compliance. Perform periodic audits.

Security Modifications/Protective Measures:

- Require each supply chain agency to patch their systems. Common attacks correlate to vulnerabilities with old or out-of-date software. Ensure all systems in the supply chain ecosystem have up-to-date patches.
- Require each supply chain agency to develop and maintain a robust incident response plan. This may cause limitations to the damage of the supply chain ecosystem when inflicted by an attack.
- Consider the integration of each sub agency's software security activities into the agency's SLDC.
- Consider the usage of proper network segmentation. This may limit the movement of attackers and helps limit the traffic to and from the critical data of the supply chain.
- Develop your defenses based on the principle that your systems will be breached – such as zero trust. When one starts from the premise that a breach is inevitable, it changes the decision matrix on next steps. The question becomes not just how to prevent a breach, but how to mitigate an attacker's ability to exploit the information they have accessed and how to recover from the breach.[liv]

Agency-wide Training and Compliance:

- Require and implement a set of key metrics/minimum baselines that are meaningful and relevant to the supply chain ecosystem's software security. Well defined baselines can help assess the supply chain's security posture and build a widespread understanding of current level of cyber hygiene.

[liv] NIST Best Practices in Cyber Supply Chain Risk Management

- Require and implement a minimum baseline for training and awareness on security for all stakeholders within the agency.
- Security requirements are included in every RFP and contract to assure compliance by suppliers.

7.2.9 RELEVANT CONTROLS

Refer to NIST Cybersecurity Framework Relevant Core Functions and Controls in table below in section 7.4.9.

7.3 SCENARIO: INHERITING RISK FROM THIRD PARTY SUPPLIER

7.3.1 BACKGROUND

During the development of components (software or hardware), sometimes exceptions are taken in test cases deemed *noncritical* to the operation of the subcomponent. These are not necessarily the wrong decisions in the testing process, but the failure results from not maintaining this information as the element flows up in the supply chain. This failure results in a lack of traceability as these elements are integrated into higher-level components, and eventually end products or systems. Furthermore, this failure can lead to cascading minor errors resulting in a vulnerability or IP license violation in the final product.

7.3.2 THREAT SOURCE

This threat is sourced from known and trusted suppliers. It is not intentionally targeting the end procuring agency, but it manifests at that level in the delivered system. This threat typically manifests as a one-time vulnerability in the form of a bug. It is not specific to only software or firmware, although that is more likely. This is an unintentional threat that results from inheriting acceptable risk decisions made by a supplier further down the chain from the end producer of the final product or service. The deeper into the supply chain it occurs, the more difficult it is to identify in advance.

7.3.3 THREAT IMPACT

Potential impact to the supply chain includes:

- Potential intellectual property violations in the final product
- Lack of product integrity
- Potential irreversible damage to the end product's brand/reputation.
- Lack of traceability and consistency through the supply chain
- Inadequate communication through the supply chain
- Potential hardware/software vulnerabilities
- Potential compromise of the supply chain's confidentiality

7.3.4 VULNERABILITY

Unlike a typical threat actor sourced attack on the supply chain, the inherited risk from a lack of transparency can be very difficult to identify and mitigate in advance. It is an accidental vulnerability that is part of the normal system development life cycle and is a known vulnerability, possibly mitigated through proper internal controls. This information is traced within the SDLC of the sourcing supplier, and typically provided in release notes to the procuring entity. The challenge is the compounding effect of numerous separate and distinct test exceptions as the complexity and scale of a system increases.

7.3.5 THREAT EVENT DESCRIPTION

This is an inherited risk as a result of the extended supply chain that is an accepted part of the supplier SDLC. It is possible that the subcomponent, assembly, or software is used in a system for which it was not initially intended. The resulting environmental changes or integration with other pieces results in the threat manifesting into an impactful failure.

7.3.6 ORGANIZATIONAL UNITS / PROCESSES AFFECTED

The lack of traceability as these elements are integrated into higher level components, and eventually end products or systems can lead to cascading minor errors resulting in a vulnerability or IP license violation in the final product. The objective is not to perpetuate a threat. It is the result of a common trade off in any engineering process concerning cost, schedule, and quality.

7.3.7 MITIGATING STRATEGIES / SCRM CONTROLS

- Proper engineering process will ensure that these decisions are documented, and traceability is provided vertically up the supply chain.
- Track and trace programs establish provenance of all parts, components, and systems. One example program specific to software product traceability is the NITA SBOM.
- Although it is not a technology that is currently used widely in the supply chain space, utilization of blockchain or distributed ledger technology has shown to be a promising method in maintaining provenance throughout the entire supply chain. Blockchain technology is a shared digital platform where each participant organization within the supply chain can store and share information which is verified and immutable. All this data is then available simultaneously and in real time.[lv]
- Require and implement a set of key metrics/minimum baselines that are meaningful and relevant to the supply chain ecosystem's hardware/software components. Well defined baselines can help assess the supply chain's security posture and build a widespread level of cyber hygiene.
- Once a vendor is accepted in the formal supply chain, an assessment and corrective actions as appropriate should be conducted (possibly on site) to address any vulnerabilities and security gaps.
- Require and implement a minimum baseline for training and awareness on security for all stakeholders within the agency.
- Security requirements are included in every RFP and contract to assure compliance by suppliers.

7.3.8 RELEVANT CONTROLS

Refer to NIST CSF Relevant Core Functions and Controls in table below in section 7.4.9.

7.4 SCENARIO: MID SUPPLY INSERTION OF COUNTERFEIT PARTS VIA SUPPLIER XYZ TO TRUSTED/VETTED VENDOR

7.4.1 BACKGROUND

During the supply chain process, it is possible that a third party, or upstream supplier ("Supplier XYZ") providing components (software or hardware) to a trusted vendor within a chain has not been vetted to the same caliber as

[lv] Accenture, "Tracing the Supply Chain," 2018.

the trusted vendor itself. This can lead to the opportunity of a threat agent delivering, installing, and inserting counterfeit elements to the trusted vendor.

7.4.2 THREAT SOURCE

The threat may be sourced by a variety of stakeholders, including the following:

- Nation-state actors;
- Cyber criminals;
- Extended stakeholders utilized via Supplier XYZ; and,
- Unvetted stakeholders in the extended supply chain, etc.

7.4.3 THREAT IMPACT

- Pathway for new and easier software/hardware vulnerabilities
- Compromise of the confidentiality, integrity, and availability of the supply chain
- Potential implications to national security, espionage, etc.
- Lack of transparency and traceability through the supply chain

7.4.4 VULNERABILITY

The inherited risk from Supplier XYZ can be difficult to detect because stakeholders within the extended supply chain may be hard to trace and enforce the same level of vetting scrutiny as a trusted vendor will be receiving. This vulnerability is the result of an extended supply chain with an unvetted or poorly vetted supplier that has been accepted by the stakeholders using it.

7.4.5 THREAT EVENT DESCRIPTION

This inherited risk effects the transit and integrity of the trusted supply chain. Supplier XYZ can serve as an incognito vehicle for introduction of hostile elements that the vetted supplier may integrate within a product or component that may be purchased by consumers. If Supplier XYZ had integrated counterfeit parts wittingly, they could have the ability to affect the reliability of the supply chain, products, or exploit consumer data.

7.4.6 OUTCOME

If intentional, Supplier XYZ's objective may be to negatively impact integrity or availability of products and services provided by the upstream trusted vendor. A secondary objective could be damage to the reputation of the trusted vendor. It is possible that supplier XYZ's objective is not intentional damage but is the result of poor vendor risk management processes.

7.4.7 ORGANIZATIONAL UNITS / PROCESSES AFFECTED

This threat affects hardware and software components within the supply chain. The threat described above is an inherited risk due to the accepted trust of an extended supply chain member that has not been vetted and trusted by the end buyer. This can lead to insertion of counterfeit products, as well as tampering of a legitimate and integral supply chain.

7.4.8 MITIGATING STRATEGIES / SCRM CONTROL

- This threat will persist until Supplier XYZ is identified as the source of the counterfeit materials and removed.
- Treating every supplier and their integration points in the network as a new security perimeter is critical if manufacturers want to be able to maintain operations in an era of accelerating cybersecurity threats.[lvi]
- Consideration of utilizing a zero-trust privilege approach to securing privileged access credentials.[lvii]
- Require and implement a set of key metrics/minimum baselines that are meaningful and relevant to the supply chain ecosystem. Well defined baselines can help assess the supply chain's security posture and build a widespread understanding of current level of cyber hygiene. Utilize these baselines for all third parties.
- Require and implement a minimum baseline for training and awareness on security for all stakeholders within the agency.
- Once a vendor (e.g., Supplier XYZ) is accepted in the formal supply chain, an assessment and corrective actions as appropriate should be conducted, possibly on site, to address any vulnerabilities and security gaps.
- Security requirements are included in every RFP and contract to assure compliance by suppliers.
- It is critical for supply chains to establish provenance programs for all parts, components, and systems.
- Tight controls on access by service vendors are imposed. Access to software is limited to a very few vendors. Hardware vendors are limited to mechanical systems with no access to control systems. All vendors are authorized and escorted.

7.4.9 RELEVANT CONTROLS

Refer to NIST CSF Relevant Core Functions and Controls in table below.

[lvi] Louis Columbus, "Why Manufacturing Supply Chains Need Zero Trust," Forbes, 2019.
[lvii] "What is Zero Trust Privilege?" Centrify.

NIST CSF RELEVANT CORE FUNCTIONS AND CONTROLS

FUNCTION	CONTROL/NAME	DESCRIPTION	NIST SP 800-53 (REV. 4) RELATED CONTROLS	INFORMATIVE REFERENCES
IDENTIFY	ID.AM-5 Asset Management (subcategory ID.AM-5)	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with them relative importance to organizational objectives and the organization's risk strategy ID.AM-5: Cybersecurity Roles and Responsibilities for the Entire Workforce and third-party Stakeholders	CP-2, PS-7, PM-11	CIS CSC 17, 19 COBIT 5 APO01.02, APO07.06, APO13.01, DSS06.03 ISA 62443-2-1:2009 4.3.2.3.3 ISO/IEC 27001:2013 A.6.1.1
IDENTIFY	Governance (ID.GV):	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	PS-7, PM-1, PM-2, SA-2, PM-3, PM-7, PM-9, PM-10, PM-11	CIS CSC 19 COBIT 5 APO01.02, APO10.03, APO13.02, DSS05.04 ISA 62443-2-1:2009 4.3.2.3.3 ISO/IEC 27001:2013 A.6.1.1, A.7.2.1, A.15.1.1
IDENTIFY	Supply Chain Risk Management	Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	SA-9, SA-12, PM-9	CIS CSC 4 COBIT 5 APO10.01, APO10.04, APO12.04, APO12.05, APO13.02, BAI01.03, BAI02.03, BAI04.02 ISA 62443-2-1:2009 4.3.4.2 ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2

FUNCTION	CONTROL/NAME	DESCRIPTION	NIST SP 800-53 (REV. 4) RELATED CONTROLS	INFORMATIVE REFERENCES
PROTECT	Awareness and Training (PR.AT)	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity related duties and responsibilities consistent with related policies, procedures, and agreements.	AT-2, PM-13	CIS CSC 17, 18 COBIT 5 APO07.03, BAI05.07 ISA 62443-2-1:2009 4.3.2.4.2 ISO/IEC 27001:2013 A.7.2.2, A.12.2.1
DETECT	Continuous Monitoring (DE.CM)	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures. Subcategory DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events.	AC-2, AU-12, AU-13, CA-7, CM-10, CM-11	CIS CSC 5, 7, 14, 16 COBIT 5 DSS05.07 ISA 62443-3-3:2013 SR 6.2 ISO/IEC 27001:2013 A.12.4.1, A.12.4.3
RESPOND	Response Planning (RS.RP)	Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	CP-2, CP-10, IR-4, IR-8	CIS CSC 19 COBIT 5 APO12.06, BAI01.10 ISA 62443-2-1:2009 4.3.4.5.1 ISO/IEC 27001:2013 A.16.1.5
RESPOND	Mitigation (RS.MI)	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	IR-4, CA-7, RA-3, RA-5	CIS CSC 19 COBIT 5 APO12.06 ISA 62443-2-1:2009 4.3.4.5.6 ISA 62443-3-3:2013 SR 5.1, SR 5.2, SR 5.4 ISO/IEC 27001:2013 A.12.2.1, A.16.1.5

FUNCTION	CONTROL/NAME	DESCRIPTION	NIST SP 800-53 (REV. 4) RELATED CONTROLS	INFORMATIVE REFERENCES
RECOVER	Recovery Planning (RC.RP)	Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	CP-10, IR-4, IR-8	CIS CSC 10 COBIT 5 APO12.06, DSS02.05, DSS03.04 ISO/IEC 27001:2013 A.16.1.5

PRODUCTS AND SERVICES THREAT SCENARIOS

7.5 SCENARIO: INHERITING RISK FROM THIRD PARTY SOFTWARE DEVELOPMENT TOOLKIT USED IN THOUSANDS OF APPLICATIONS

7.5.1 BACKGROUND

Mintegral, a popular iOS Software Development Kit (SDK) owned by Chinese company Mobvista is reported to contain malicious code used to perpetrate ad click fraud, and capture and upload sensitive information. The SDK is used in developing >1,200 Appstore apps with ~300 Million downloads per month and >1 billion mobile users.

7.5.2 THREAT SOURCE

The malicious code can spy on user activity by logging URL-based requests made through the app. This activity is logged to a third-party server and could potentially include personally identifiable information (PII) and other sensitive information. Furthermore, the SDK fraudulently reports user clicks on ads, stealing potential revenue from competing ad networks and, in some cases, the developer/publisher of the application. The Mintegral SDK presents itself as a tool to help app developers and advertisers build monetized ad-based marketing. It contains several anti-debug protections that appear to be designed to keep researchers from discovering the true behavior behind the application.

7.5.3 THREAT IMPACT

Potential impact to the product includes:

- Product failure
- Lack of product integrity
- Potential irreversible damage or compromise to a system using the end-product
- Lack of traceability and consistency through the supply chain making it difficult to discover the root cause of the product failure
- Potential hardware/software vulnerabilities

7.5.4 VULNERABILITY

Attacks are increasing significantly at the software supply level, so it is not surprising to see developer toolsets designed or compromised to act maliciously, especially when they are “free” or open source. Detected attacks in the development stage of next generation open source software increased approximately 1700 percent between July 2019 and May 2020 over the average for approximately the previous 4 years according to Sonatype. Information gleaned from devices can be compiled, retained, and exploited in big data platforms in such a way that the aggregated information is far more valuable/damaging than the parts. Uses may include developing Artificial Intelligence (AI), targeting influence operations, and blackmail.

7.5.5 THREAT EVENT DESCRIPTION

This is an inherited risk because of products being developed using tools with embedded vulnerabilities. It is possible that the software is integrated into a more sensitive system either through an IoT device, or as a mobile application used to access the system or services remotely. The resulting environmental changes or integration with other pieces results in the threat manifesting into an impactful failure.

7.5.6 OUTCOME

Next generation attacks like those posed by malicious code embedded into an SDK are strategic and can involve bad actors intentionally targeting and surreptitiously compromising “upstream” open source projects so they can subsequently exploit vulnerabilities when they inevitably flow “downstream” into the wild.

7.5.7 ORGANIZATIONAL UNITS / PROCESSES AFFECTED

Cyberattacks aimed at actively infiltrating open source software supply chains have quadrupled between July 2019 and May 2020 according to the Sonatype report. Adversaries can infect a single open source component or SDK that is then distributed “downstream” by unwitting developers for covert exploitation of end products or SaaS services.

While the use of open source offers benefits to enterprises and development teams in terms of time to market, cost, and reliability, it also can be the source of vulnerabilities that pose significant risk to application security. Many development teams rely on open source software to accelerate delivery of digital innovation. Both traditional and agile development processes frequently incorporate the use of prebuilt reusable open source software components. As a result, some organizations may not have accurate inventories of open source software dependencies used by their different applications, or a process to receive and manage notifications concerning discovered vulnerabilities or available patches from the community supporting the open source.

7.5.8 MITIGATING STRATEGIES / SCRM CONTROLS

In order to mitigate inherited threats from upstream software products, organizations should establish programs to document provenance of all parts, components, and systems; in the case of embedded open source code, these should include a SBOM that identifies all open source software and libraries.

Identification of all the applications where open source vulnerabilities may exist can be difficult. To address the identification and mitigation challenge requires an intentional effort that includes activities such as code inspection, dynamic security scanning, and vulnerability testing. These are the same techniques that should be applied to all software code repositories, whether open source or not.

There are enterprise specific products that offer a complete end-to-end solution for third party components and supply chain management with features such as licensing, security, inventory, and policy enforcement. These products are offered by vendors such as Black Duck Software, Sonatype, Nexus, and Protecode, to name a few.

7.6 SCENARIO: INHERITING RISK FROM THE ACQUISITION OF IT MAINTENANCE AND REPAIR SERVICES.

7.6.1 BACKGROUND

Today, many purchases of IT hardware offer maintenance and repair services as part of that purchase. These products can include mobile devices, printers, laptops and desktop computers, and mainframe computers. Many of these repair and maintenance offerings lack transparency about the technicians who will perform the services or the source of replacement components that will be used, if needed, in the provision of the service. The lack of transparency is particularly acute when the services are offered through small order sources, such as e-commerce portals at the time of purchase of the hardware.

When IT hardware fails, particularly in commercial or commercial-off-the-shelf (COTS) IT hardware products, vendors who offer IT maintenance and repair services frequently replace the component based on functional capabilities, availability and cost, and do not always consider supply chain risks. When enterprises or end users rely upon maintenance or repair services for IT hardware used on or in their information systems, they may inherit the risks associated with the source of repair components delivered as part of those services or the technicians that may deliver the service.

7.6.2 THREAT SOURCE

IT hardware repair or maintenance services which are not transparent about vendor attestation—or services that utilize non-OEM or non-authorized IT hardware components—can threaten any system or individual who uses them.

7.6.3 THREAT IMPACT

Potential impact to the product includes:

- Product failure
- Lack of product integrity
- Product performance degradation
- Potential irreversible damage or compromise to a system using the end-product
- Lack of traceability and consistency through the supply chain making it difficult to discover the root cause of the product failure
- Potential hardware/software vulnerabilities
- Access by non-vetted personnel to elements of IT system hardware

7.6.4 VULNERABILITY

IT hardware that is repaired or maintained using non-OEM or authorized sources of replacement components can create vulnerabilities for end users and enterprises. These vulnerabilities range from mere lack of vetting of the components to ensure products meet OEM performance parameters to intentional supply chain tampering to enable espionage or product failure during critical mission activities. Vulnerabilities can also come from acquiring IT hardware repair and maintenance services separate from the acquisition of the hardware to be maintained, or from a non-OEM authorized repair source. Either of these situations can exponentially increase the vulnerabilities by adding non-vetted personnel to the calculation of risk. When personnel are performing work, are they properly trained, or could they have malicious intent? Finally, another vulnerability can be found when a trusted supplier or vendor does not adequately mitigate risks from these types of sources and allows risk to enter their supply chain.

7.6.5 THREAT EVENT DESCRIPTION

This is an inherited risk because users of IT hardware repair and maintenance services may inadvertently be exposing their networks and enterprise to non-OEM or authorized source components and non-vetted service personnel by utilizing those services. These conditions can lead to failure of IT hardware products because they do not meet design specifications or serve to enable intentional failure, takeover, or manipulation of a hardware product when used. Non-vetted personnel providing the services can also deliver additional threats by accessing hardware used on an enterprise or network.

7.6.6 OUTCOME

The worst-case scenario of this inherited risk would be the introduction of components that cause hardware, network, or enterprise failure due to lack of compliance with design specifications or by providing threat actors with malicious intent access to networks. Other worst-case scenarios include unauthorized access to hardware, networks, or enterprises by non-vetted personnel who are providing the repair or maintenance services.

7.6.7 ORGANIZATIONAL UNITS / PROCESSES AFFECTED

Any organization that utilizes IT hardware repair or maintenance services without adequately vetting the vendor and the sources they use can fall victim to these possible threats.

As an example, an office that is part of a larger enterprise acquires laptops for their employees that will connect to the networks of the enterprise. As part of that acquisition, the extended warranty for the laptops, offered through a third-party provider, is purchased. During their useful life, the laptops experience several failures of components, like hard drives, modems, or network cards. Other users needed to increase the onboard memory of the laptops because of the specific tasks those users performed in their work.

As a result of using the service for repair and maintenance, several devices had non-OEM hardware components installed. These components can cause failure of the device or provide a threat vector for malicious actors to access the device or the networks it may connect to. Similar threats were created when the capabilities of other laptops were expanded. The vendor, who was a third-party unaffiliated with the OEM of the product or the channel partner, also gained access to all of those devices and could have used that access to alter the hardware or software of the device.

7.6.8 MITIGATING STRATEGIES / SCRM CONTROLS

In order to mitigate against inherited threats posed by the use of services providers offering repair or maintenance of IT hardware, organizations should ensure that those services are offered by OEM-authorized vendors who are properly vetted and trained to work on the devices, and who will use replacement components that meet the original design specifications and are sourced responsibly.

7.7 SCENARIO: INHERITING RISK FROM COMPONENTS PRODUCED WITH KNOWN AND DEEMED MITIGATED OR NONCRITICAL FAULTS

7.7.1 BACKGROUND

During the development of components (software or hardware), sometimes exceptions are taken in test cases deemed *noncritical* to the operation of the component. These are not necessarily the wrong decisions in the testing process, but the failure is a result of not maintaining this information as the component flows up in the supply chain. This results in a lack of traceability as these elements are integrated into higher level equipment and eventually end-items or products. Furthermore, this can lead to cascading minor errors resulting in a vulnerability or intellectual property (IP) license violation in the final product.

7.7.2 THREAT SOURCE

This threat is sourced from known and trusted suppliers. It is not a failure in the system development process used, but rather is a result of a failure in the communications chain from the origin of a specific component to the ultimate supplier of the final product and ultimately consumer of the product. It is not intentionally targeting the end procuring agency, but it manifests at that level in the delivered system. This threat typically manifests as a one-time vulnerability in the form of a bug. It is not specific to only software or firmware, although that is more likely. This is an unintentional threat that results from inheriting acceptable risk decisions made by suppliers further down the chain from the end producer of the final product or service. The deeper into the supply chain this occurs, the more difficult it is to identify in advance or trace back to take corrective action. This is especially true if the latent defect deemed non-service impacting is amplified by the specific way the component is used in the end product, or by other non-critical defects from other components assembled into the end-item.

7.7.3 THREAT IMPACT

Potential impact to the product includes:

- Product failure
- Lack of product integrity
- Potential irreversible damage or compromise to a system using the end-product
- Lack of traceability and consistency through the supply chain making it difficult to discover the root cause of the product failure
- Potential hardware/software vulnerabilities

7.7.4 VULNERABILITY

Unlike a typical threat actor sourced attack on the supply chain, the inherited risk from a lack of transparency can be very difficult to identify and mitigate in advance. It is an accidental vulnerability that is part of the normal system development life cycle and is a known vulnerability, possibly mitigated through proper internal controls. This information is traced within the SDLC of the sourcing supplier and typically provided in release notes to the procuring entity. The challenge is the compounding effect of numerous separate and distinct test exceptions across the entire supply chain involved in the delivery of an end-item or product as the complexity and scale of a system increases.

7.7.5 THREAT EVENT DESCRIPTION

This is an inherited risk because of the extended supply chain that is an accepted part of the supplier SDLC. It is possible that the subcomponent, assembly, or software is used in a system for which it was not initially intended. The resulting environmental changes or integration with other pieces results in the threat manifesting into an impactful failure.

7.7.6 OUTCOME

Product or system failure is the worst-case scenario if this threat manifests in a completed product. Other possible outcomes include performance degradation and even exposure to other cyber vulnerabilities depending on the nature of the latent defect.

7.7.7 ORGANIZATIONAL UNITS / PROCESSES AFFECTED

The lack of traceability as these elements are integrated into higher level components (and eventually end products or systems) can lead to cascading minor errors resulting in a vulnerability or latent defect in the final

product. The objective is not the result of an intention to perpetuate a threat. It is the result of a common trade off in any engineering process concerning cost, schedule, and quality.

In one example of this scenario, a latent defect resulted in the eventual failure of a critical database that caused a nationwide service outage. The defect was the result of a small memory leak that was deemed non-critical and the release notes mitigated the defect by requiring the system to be power cycled as part of weekly maintenance. However, when processing data at a massive scale, the memory leak unexpectedly accelerated exponentially resulting in catastrophic failure.

7.7.8 MITIGATING STRATEGIES / SCRM CONTROLS

- Good engineering process will ensure that these decisions are documented, and traceability is provided with the component vertically up the supply chain to provide visibility into customers of the final products or services.
- Track and trace programs establish provenance of all parts, components, and systems to include all documents, such as release notes, including an SBOM.
- Although it is not a technology that is currently used widely in the supply chain space, utilization of blockchain or distributed ledger technology has shown to be a promising method in maintaining provenance throughout the entire supply chain. Blockchain technology is a shared digital platform where each participant organization within the supply chain can store and share information which is verified and immutable. All this data is then available simultaneously and in real time.[lviii]

8 THREAT CATEGORY: LEGAL RISKS

8.1 SCENARIO: LAWS THAT HARM OR UNDERMINE AMERICAN ECONOMIC INTERESTS

8.1.1 BACKGROUND

Under U.S. federal and (most) state law, trade secrets have protected status, which helps to enable the cyber supply chain to flourish. This same type of legal protections does not exist in every country where a company – or entities in the company's supply chain - is located or transacts business.

"China has implemented laws, policies, and practices and has taken actions related to intellectual property, innovation, and technology that may encourage or require the transfer of American technology and intellectual property to enterprises in China or that may otherwise negatively affect American economic interests. These laws, policies, practices, and actions may inhibit United States exports, deprive United States citizens of fair remuneration for their innovations, divert American jobs to workers in China, contribute to our trade deficit with China, and otherwise undermine American manufacturing, services, and innovation."[lix]

8.1.2 THREAT SOURCE

State and quasi-state threat actors refer to hostile governments that want to disrupt American cyber supply chains for strategic or tactical advantage. It is also a reference to any governing authority that de facto acts as a state. Lack of diplomatic recognition as a state does not affect the actor's ability to operate as a supply chain threat. These actors are defined by their strategic or tactical reasons for wanting to disrupt American cyber supply chains and their ability to employ state or state-like powers to achieve that end, not the formalities of diplomacy, such as state-owned enterprises—who would look to steal American intellectual property. State-owned enterprises

---

[lviii] Accenture, "Tracing the Supply Chain," 2018.
[lix] Executive Office of the President, "Memorandum for the United States Trade Representative of August 14, 2017," 2017.

and similar quasi-state actors around the world seek advantage in the marketplace and in the operation of whatever end they are tasked by their associated government.

Quasi-state actors are largely synonymous with state-owned enterprises. These are businesses or organizations that operate independently of any government, at least on paper, but are influenced by a government to such a degree that the organization is either effectively owned or controlled by it. These quasi-state actors are different from state actors in that they have some private function—usually a market function— but they cannot escape government-given public functions. These public functions may include manufacturing of military equipment, maximizing employment, or dominating a sector seen as strategic to the state-actor's national interests.

8.1.3 THREAT IMPACT

The impact of this threat is to undermine the financial soundness and viability of cyber supply chains, making counterfeit, theft, and other hostile economic actions easier.

8.1.4 VULNERABILITY

Businesses operating in or desiring to sell their goods to nation-states, such as China, may be subject to legal requirements that could result in the loss of their intellectual property or the undermining of their market share.

8.1.5 THREAT EVENT DESCRIPTION

The state actor opts against enforcing (or not having) intellectual property protections and forces technology transfers. This allows a state actor to unleash non-state third parties and quasi-state actors to pursue their objectives to steal intellectual property without domestic legal consequence. A more overt method of obtaining IP is via forced technology transfers (a government-mandated transfer of intellectual property from the original owner to some other entity).

8.1.6 OUTCOME

This fundamentally harms trade secret protections. Further, once stolen intellectual property is in the wild and with few legal protections and remedies, it can result in counterfeit parts and sabotage that may cause disruptions in the cyber supply chain, denial of end products, and failure of the end products.

8.1.7 MITIGATING STRATEGIES / SCRM CONTROLS

Strategies to help mitigate this threat include:

- Setting up supply chain operations outside of countries without the needed legal protections.
- Routing the most sensitive/vulnerable parts of a supply chain out of such countries.
- Drafting contracts to include the relevant protections.

8.2 SCENARIO: LEGAL JURISDICTION-RELATED THREATS

8.2.1 BACKGROUND

Company A relies upon a foreign-based manufacturer to produce a key component of its product. The country the manufacturer is located is known for government corruption and weak oversight of its domestic businesses.

8.2.2 THREAT SOURCE

Supply chain entity is threat actor: Entities within the global supply chain can intentionally or unintentionally introduce threats into an end product deliverable. Actors may have nefarious intent, be profit-motivated, or simply negligent.

8.2.3 THREAT IMPACT

The impact of this threat is to undermine the financial soundness and viability of cyber supply chains, making counterfeit, theft, use of sub-standard quality parts, and other hostile economic actions easier.

8.2.4 VULNERABILITY

A threat actor can engage in nefarious behavior in a jurisdiction unlikely to punish or deter such behavior. The problem of security becomes more complex, and therefore more expensive.

8.2.5 THREAT EVENT DESCRIPTION

The manufacturer uses inferior material to produce the components for Company A while charging Company A for the costs of the more expensive, specified material and falsifying its financial records. Manufacturing company managers pocket the savings in costs they generate from using cheaper material. This introduces a weakness in the product that cannot be readily identified but will cause the component and to fail prematurely.

8.2.6 OUTCOME

Poor security from entities within a supply chain has potentially devastating implications for delivery of an end product. When the supply extends across multiple countries, differing legal jurisdictions introduce multiplied and varied threat opportunities.

8.2.7 MITIGATING STRATEGIES / SCRM CONTROLS

Strategies to help mitigate this threat include:

- Setting up supply chain operations outside of countries without the needed legal protections.
- Routing the most sensitive/vulnerable parts of a supply chain out of such countries.
- Randomized and systematic quality control testing.
- Drafting contracts to include the relevant protections all the way down the supply chain.

PRODUCTS AND SERVICES THREAT SCENARIO

8.3 SCENARIO: INCLUSION OF PROHIBTED COMPONENT(S) IN A PRODUCT

8.3.1 BACKGROUND

Several years ago, the ACME Company sourced parts from a foreign-based manufacturer for one its ACME-branded products. This product, along with other ACME Company products is then distributed and sold by various resellers. This manufacturer was recently identified as being controlled and influenced by an adversarial nation-state. This raised concerns that parts may pose an unacceptable cybersecurity and supply chain risk. A compromise of the product could allow for the interception and exfiltration of data transiting stored within this product. To protect national security interests, a law was enacted that prohibits the government from purchasing products or component parts produced by this manufacturer.

The ACME Company uses multiple different manufacturers to source these parts and recently ended its relationship with the problematic manufacturer. Only a subset of the portfolio of products offered by the ACME Company include components made by this manufacturer, but many of the products that include the parts from the problematic manufacturer remain available for sale in the marketplace. None of the marketing material or product description information include a comprehensive listing of the parts that comprise the end product, nor is there readily available information about the provenance of these parts.

8.3.2 THREAT EVENT DESCRIPTION

A reseller of ACME Company products continue to offer the full set of ACME Company products to government customers. The reseller company explains to the government that they are not offering any products, or products that contain component parts, that were produced by the problematic manufacturer.

One of the government customers purchases an ACME product from this reseller, and the customer discovers that it does include a part that was made by this problematic manufacturer. This customer notifies the contracting officer and submits a hotline report to the Office of the Inspector General that the reseller has been fraudulent in its representation.

8.3.3 THREAT SOURCE

The primary threat source is the adversarial nation-state that is wielding influence and control over a manufacturing company doing business in its country. Secondary and tertiary threat sources include the ACME Company, who did not remove these items from its inventory or disclose their component makeup to their resellers. The reseller also becomes a threat vector by unwittingly facilitating the sale of these products to the government.

8.3.4 VULNERABILITY

Several vulnerabilities contributed to this threat event: lack of visibility into the composition of an ICT product; reliance upon a foreign manufacturer doing business within an adversarial nation-state; insufficient due diligence to ensure that a legal representation was accurate.

8.3.5 THREAT IMPACT

An ICT product that includes compromised components – or components that can be compromised – be used as a threat vector by an adversary. The threat actor may be able to gain unauthorized access to sensitive information transiting or stored within the product. The component may also cause the product to malfunction or perform additional functions, not expected nor desired by the user.

8.3.6 ORGANIZATIONAL UNITS / PROCESSES AFFECTED

ACME Company's reputation may be impacted negatively. The reseller may suffer legal penalties, incur significant legal costs, loss of market-share, and be suspended or barred from doing business with the government. Government users who purchased and used a product that contained these prohibited parts may be exposed to a nefarious cyberattack.

8.3.7 STRATEGIES / SCRM CONTROLS

Potential mitigating strategies could include:

- Require disclosure of component parts and their provenance.
- Consult with legal counsel and conduct sufficient due diligence prior to making a legally binding representation.

- Examine the product/conduct product testing prior to installation and use.
- Source parts from trusted companies doing business in locations at low risk of adversarial foreign ownership, influence, or control.
- Establish robust processes to vet supply chain partners.

9 THREAT CATEGORY: EXTERNAL END-TO-END SUPPLY CHAIN

9.1 SCENARIO: NATURAL DISASTERS/PANDEMIC CAUSING SUPPLY CHAIN DISRUPTIONS

9.1.1 BACKGROUND

External events including natural disasters can have a large impact on the end to end supply chain ranging from destruction of manufacturing facilities, the ability to receive production materials to the ability of workers to get to work, to the ability to distribute final products to mention only a few. Depending on the size and scope of the event, the disruption to the end-to-end supply chain can have multiple impacts.

9.1.2 THREAT SOURCE

Natural disasters can have a severe impact on the global economy. According to Aon Benfield's 2016 Global Climate Catastrophe Report, the world saw $210 billion in economic losses because of 315 separate natural disasters. That's 21 percent above the 16-year average of $174 billion. In 2017, Hurricane Harvey victims saw over 178,000 homes lost, $669 million in damages of public property, around a quarter million vehicle losses, $200 million in Texas crop in livestock losses. Additionally, businesses saw significant and expensive losses due to flooding, electrical outage, and employees' inability to get to work, all causing temporary disruption of the flow of goods and services. But the impacts of natural disasters reach far beyond the local damages of affected areas. When these natural events happen, many businesses find their supply chains greatly impacted.

The Tohoku Earthquake and Tsunami in Japan and the Thailand Floods in 2011 are both examples of natural disasters that had expanded indirect economic effect. Both disasters caused severe disruption to global technology supply chains. After the Thai floods, there was a global shortage of computer hard drives that sent consumer prices skyrocketing until factories were able to resume operations. When the 2011 tsunami struck, several major until business operations were restored to normal. Car manufacturers were forced to shut down production at factories throughout Europe and the U.S. due to a lack of available parts from factories in Japan, setting off a supply chain reaction that impacted multiple suppliers of parts throughout the wider global economy.[lx]

At the time of writing this document, the global coronavirus disease (COVID-19) pandemic has had severe impacts in various areas including economic, societal, political, legal, and much more. It is not possible to estimate the total impact, but there is widespread agreement that it will be substantial and that it will likely take years to recover. The Working Group do not address this specific threat as a separate scenario in this report since these scenarios were originally developed prior to the COVD-19 outbreak.

9.1.3 THREAT IMPACT

Natural disasters can have a large impact on the end-to-end supply chain including destruction of manufacturing plants, warehousing and distribution locations. Impacts to infrastructure including impacts to roads, rail, sea and air capabilities resulting in delays in delivery of raw materials, components, and consumer goods as local

[lx] "How Natural Disaster Affects Supply Chains," Trinity Logistics, 2018.

communities recover from the disaster. Often multiple impacts can further delay delivery of products and services.

9.1.4 THREAT EVENT DESCRIPTION

A category 5 hurricane hit in Savanah, Georgia, and moved up the east coast and inland in Northern Virginia before becoming a tropical storm. The hurricane damaged or destroyed ports from Savanah, Georgia to Norfolk, Virginia, while also destroying roads and bridges. Critical infrastructure impacts were also widespread, specifically impacts to power and communications.

9.1.5 OUTCOME

The ever-growing reach of global supply chains exposes these networks to serious vulnerabilities. In this scenario, a medium-sized manufacturing company has been impacted in several ways. There are impacts to delivery of materials into the manufacturing plant and to distribution of finished products. This may further result in financial harm, such as unrecoverable loss of revenue or accounts receivable, contractual fines, and penalties. Other impacts include the inability to provide effective customer relations and regulatory reporting as well as damage to relationships, brand, or corporate reputation and confidence.

9.1.6 MITIGATING STRATEGIES / SCRM CONTROLS

Following established steps to identify potential risks to the supply chain and plan for business interruptions is critical for a company's survival in times of natural disasters.

The first step is to complete a Business Impact Analysis (BIA). This analysis provides a complete understanding of the business and its supply chain, allowing organizations to identify exposures and potential mitigation measures. It helps identify the most feasible and cost-effective strategies and solutions for business continuity and disaster recovery. In addition, reviewing insurance policies as they relate to business interruption enables companies to detect any areas requiring additional coverage.

Following the BIA, the second step is disaster recovery preparation. Based on the results of the impact analysis, this exercise finds critical business functions, resources and methods; reveals business unit, supplier and customer interdependencies; further identifies potential threats and exposures; and helps users ascertain potential losses and impacts, should a disaster occur. The process involves documenting recovery time objectives, IT interdependencies and manual procedures; evaluating existing recovery capabilities; and creating effective mitigation measures, including the recovery plan documenting who to call, where to go, and who will do what in the event of a disaster. It also identifies which tasks must be considered mission critical. The plan sets a schedule for periodic backups of all electronic and hard-copy documentation, which should be stored in an alternate location.

Focus on creating a stable, yet flexible, supply chain. Diversifying suppliers and methods of transport wherever possible is an effective strategy. Also consider alternate supplier teams and define roles both internally and externally to enable this emergency supply chain. Backup work locations, redundant IT systems should also be a priority.

The body of the recovery plan should include the following:

- Business assumptions;
- Incident-management team member including critical personnel from all areas of the company resources and recovery assignments;
- Recovery strategy and solution overview;
- Emergency response procedures;

- Incident reporting procedures;
- Recovery team notification, mobilization and assembly procedures;
- Detailed recovery procedures;
- Situation-assessment guidelines;
- Emergency contact information of key employees, vendors and customers;
- A summary of mission-critical business functions to be recovered; and
- Detailed procedures for transitioning back to business as usual.

Finally, the third step in the process is to regularly test the plan. A plan is only as good as its execution. A tabletop exercise is an effective way to test and validate the plan by ensuring all internal and external team members are familiar with their roles and responsibilities. Aside from assisting team members with practicing their roles and developing their confidence and expertise, it can also reveal any necessary gaps and needed updates.

9.2 SCENARIO: MAN MADE DISRUPTIONS: SABOTAGE, TERRORISM, CRIME, AND WAR

9.2.1 BACKGROUND

Man-made events such as fire, product defects, cyberattacks, labor and civil unrest, terrorism, utility failure, and piracy are frequent disruptors of supply chains, but typically have a lower severity than natural catastrophes.

9.2.2 THREAT SOURCE

The year 2016 saw several man-made disruptions, including the late summer Gap warehouse fire in Fishkill, New York, which destroyed 30 percent of Gap's total warehouse space and disrupted more than 10 percent of Gap's orders.[lxi] Another example is the Samsung Note cell phone battery recall, which was linked to problems in a battery supplier's supply chain and had far-reaching consequences for the Samsung brand and their customers.[lxii]

The past few years have seen an increasing prevalence of cyberattacks. Most of these incidents, such as the high-profile Equifax data breach that involved the personal information of some 143 million Americans, and the 2016 Dyn cyberattack which took down some of the world's most popular websites such as Twitter, Airbnb, and Netflix, do not directly affect supply chains. However, they raise major red flags for supply chain practitioners. It seems that cyber criminals have a growing number of avenues of attack at their disposal, especially given the exponential growth in the number of Internet-enabled devices and cloud-based communications networks.

9.2.3 THREAT IMPACT

Impacts from man-made disruptions may have a wider or narrower impact on the supply chain than natural disasters. For example, sabotage is typically narrowly directed as is crime, where terrorism and war may have broader implications. Man-made disruptions such as sabotage and terrorism can have an impact on the end to end supply chain ranging from destruction of manufacturing plants, warehousing and distribution locations, infrastructure including impacts to roads, rail, sea, and air capabilities. These impacts result in delays in the delivery of raw materials, components, and consumer goods to impacted communities as they recover from the disaster. While some areas of the supply chain may recover quicker than others, the end to end supply chain usually remains impacted.

[lxi] Lindsay Rupp, "Gap's Distribution-Center Fire Could Bring Holiday Headaches," Bloomberg, 2016.
[lxii] Edwin Lopez, "Samsung reveals cause of Galaxy Note7 defects, unveils new quality control checklist," Supply Chain Dive, 2017.

9.2.4 THREAT EVENT DESCRIPTION

The collision of carriers in the waterway ceased operations at the Twin Ports. The collision resulted in one of the vessels taking on water, which caused the vessel to capsize dropping the containerized units from the vessel into the waterway, destroying the products in the containerized units

The cargo carriers not affected in the collision sat idle until they received direction from the port authorities on how to proceed. The carriers were either directed up the coast to a different port or were instructed to stay put until they could resume operations and accept the cargo at the Twin Ports.

9.2.5 OUTCOME

Most of the overseas cargo comes from Asia, and therefore come into ports on the West Coast. Los Angeles and Long Beach handle over 40 percent of U.S imports from Asia. Due to the heavy cargo traffic, a collision of 2 cargo ships occurred in the waterways halting operations to the Twin Ports in Los Angeles and Long Beach.

9.2.6 ORGANIZATIONAL UNITS / PROCESSES AFFECTED

The collision created a delay in delivery of network components to the U.S. company. The components could have been destroyed if they were in a containerized unit that fell into the water, or a significant delay could occur if the components were on a ship that was re-routed to a different port due to the port closures at Twin Ports.

The U.S. company was able to track down their shipment and determined that it was taken to a port in New Jersey, then arranged for ground transportation to obtain the shipment and deliver to the U.S. company.

The U.S. company missed their committed lead times resulting in a delay in delivering their network equipment to customers. Due to the missed due dates, the U.S. company was expected to pay liquidated damages that were contractually agreed to with their customers.

9.2.7 MITIGATING STRATEGIES / SCRM CONTROLS

To avoid future scenarios such as the one described above, the ports should monitor the traffic 24/7 to avoid congestion of ships when approaching the ports.

Additionally, a protocol should exist amongst ships, that if any ship is within .5 miles from another ship, the ships communicate with one another and, based on the protocol, one ship remain idle until the other ship has cleared the port.

9.3 SCENARIO: LABOR ISSUES

9.3.1 BACKGROUND

An organization has decided to perform a threat scenario analysis of its resource and capacity planning. The scenario will focus on the sensitivity of the business to unforeseen fluctuations in the country's unemployment rate.

9.3.2 THREAT SOURCE

GoFast Auto Company is a 1.5 million square foot manufacturing facility that produces 45 million automotive parts per year. The company supplies mainly to after-market retailers but does have some direct contracts with major automotive manufacturers in the U.S. to produce proprietary parts. There are 35,000 employees, 28,000 of which are directly tied to production and run three full shifts. The production organization is made up of

machinists, technicians, inventory control, quality assurance, design engineering, and other occupations ranging in skill and education level.

9.3.3 THREAT IMPACT

Labor issues resulting in labor shortages can arise from the lack of availability of trained or qualified employees, labor strikes, and walkouts. Impacts can span the entire supply chain ranging from concept and design, to production and manufacturing, to distribution and sales. Typically, labor issues impact a specific segment of the supply chain but have downstream supply chain impacts.

9.3.4 THREAT EVENT DESCRIPTION

The organization has established the following fictitious threat for the analysis exercise:

Two years ago, there had been a lot of political momentum to enable better, higher-paying jobs in manufacturing and other blue-collar jobs. Due to this, a year ago, there were several programs that were funded by the U.S. Government to encourage bringing jobs back to the U.S. from overseas locations while also increasing wages. After three phases of these programs touching on different industries, the U.S. has seen its unemployment rate drop from 8.5 percent to 3.4 percent.

9.3.5 OUTCOME

With unemployment at low levels, there has been a lot of job movement, particularly in the manufacturing sector. As a result of this, GoFast has seen attrition at 3x the normal rate. Labor levels have dropped off to the point where the production of some components has had to be delayed or even halted. The reduction in volume produced has directly led to a drop in revenue, and one contract for proprietary parts was terminated. In 6 months, revenues have dropped 13 percent.

GoFast attempted to rectify some of the impact by moving employees into more critical roles, but generally the training time for a major role change is approximately 4 months. Additionally, GoFast has reached out to several consulting and staffing firms, but there are two issues with this. One issue is the personnel from these outlets would take even longer (6-8 months) to fully integrate as they are brand new to the company. the second issue is that staffing firms are having trouble attracting skilled talent.

9.3.6 MITIGATING STRATEGIES / SCRM CONTROLS

- Institute a standard rotation or cross-training process for all, or at least employees in critical roles;
- Offer more competitive packages for skilled people looking for new opportunities in the marketplace;
- Entice more employees to stay with perks, including wage increases, benefits, time off, educational and training opportunities, flexible hours, or other options that make sense for employee and employer;
- Simplify processes or improve related training and documentation to reduce transition or onboarding time for folks new to an area; and
- Work with local trade schools and universities to develop talent with specific skills that are currently lacking in the workforce.

9.4 SCENARIO: INFLUENCE OR CONTROL BY FOREIGN GOVERNMENTS OVER SUPPLIERS

9.4.1 BACKGROUND

An organization has decided to perform a threat scenario analysis of its Printed Circuit Board (PCB) suppliers. The scenario will focus on the sensitivity of the business to unforeseen fluctuations in component cost.

9.4.2 THREAT SOURCE

Apex PC Corporation designs, assembles, and ships 3.5 million personal computers per year. It has a global footprint, both in terms of customer and supply bases. Five years ago, to reduce the cost of goods sold, Apex shifted most of its PCB procurement to Southeast Asia. To not be single sourced, Apex finalized agreements with five different suppliers within the country and has enjoyed a positive partnership with each during this time.

9.4.3 THREAT IMPACT

Suppliers from countries of concern and other countries that have control or influence over suppliers can use manipulation of price of goods, manufacturing, production, and delivery timelines impacting the flow of components, products, and services throughout the supply chain. Additionally, foreign governmental influence, especially from countries of concern, can lead to a compromised supply chain leading to cyber and national security threat concerns.

9.4.4 THREAT EVENT DESCRIPTION

The organization has established the following fictitious threat for the analysis exercise:

Last year, the country where Apex does most of their PCB business has seen a new regime take over the government. This regime has been more focused on improving finances and the business environment within the country, allowing larger firms who set up headquarters and other major centers within country advantages to more easily and cost-efficiently do business with suppliers within the same region.

In February of 2019, this now-corrupt regime has passed new legislation that establishes an additional 20 percent tax on all electronic components and goods sold outside of the country. This new law was to take effect on June 1, 2019.

At the time the new law was announced, the current Apex inventory of PCBs was about 10 percent of yearly demand, which was the typical level of inventory they were comfortable with. Before June, Apex reached out to all five suppliers to order additional materials, but there was quickly a shortage due to higher demand from many foreign customers of these products. By June 1, 2019, the day the new tax law took effect, Apex was up to an inventory level of up to 15 percent of yearly demand.

9.4.5 OUTCOME

Between February and June 2019, Apex also looked to partner with new suppliers but identified several issues with this approach. For one, of the 10 new suppliers Apex reached out to, the lead time for ramping up to desired demand was anywhere from 6 months to 18 months. This would include work on Apex's end, to include testing samples of the supplier PCBs and working out logistics details, to supplier-side activities such as procurement of raw materials and acquisition of additional personnel, production space, etc. necessary to meet the new demand.

The second issue is due to the current contracts with all five current suppliers in Southeast Asia, there were minimum demand requirements, meaning Apex was committed to purchasing a minimum of 100,000 PCBs per month for the duration of the contracts (which ranged anywhere from 3 months to 24 months remaining). This would mean Apex could not easily avoid the cost implications of this new tax.

Could Apex absorb the cost of the PCBs? With a 20 percent cost increase, this eroded the margins of a PC from 13.5 percent down to 4.5 percent, on average. For some of the lower margin Apex offerings, it would likely mean discontinuing the line and using these now more expensive PCBs on higher-end models that could carry more margin.

9.4.6 MITIGATING STRATEGIES / SCRM CONTROLS

- Diversify suppliers not just by immediate location, but by country, region, and other factors;
- Build cost implications into supplier contracts, making it easier to walk away from suppliers when costs rise too high (whether its fault of the supplier or not);
- Adjust desired inventory levels to better account for unexpected shortage of demand at critical times; and
- Employ more resources in countries or regions of key suppliers in hopes of receiving advanced indication of a new legislature that may negatively affect business.

PRODUCTS AND SERVICES THREAT SCENARIO

9.5 SCENARIO: MALICIOUS SUPPLIER INSERTS HOSTILE CONTENT

9.5.1 BACKGROUND

A software supplier, NMT-Com, provides network management infrastructure for numerous global companies. Recently, several customers have complained about products that have ended up failing certain security scans upon receipt, although the majority of customers have had no reported issues.

9.5.2 THREAT SOURCE

NMT-Com has software developers around the world, with a dozen different code compiler locations, at their primary development centers. Software packages and libraries are uploaded for review and security scanning, and are then stored where they can be utilized by developers within the region; customer support is handled by the regional center that supplies the software load.

Product packages are intended to be consistent across customers for easier support, patching, and development. Release testing is done on a periodic basis in the development cycle at each center.

9.5.3 VULNERABILITY

According to the scenario presented, since NMT-Com has a dozen difference code compiler locations, there is the potential for a bug to be inserted into the code, thus creating a vulnerability.

9.5.4 THREAT EVENT DESCRIPTION

A malicious supplier employee inserts hostile content at the product or component manufacturing or software compilation stage to affect supplier products or components delivered to a targeted subset of downstream customers.

9.5.5 OUTCOME

Due to the disconnect between the process of where software is scanned and where it is compiled and released, there is a potential for insertion of malicious software. There is an assumption of trust at the compiler locations and no re-scanning is done, except on the full release on a periodic basis (rather than every time it is changed and before it is signed.

This could leave customers of the supplier open to backdoor exploits, software injection attacks, data manipulation, data exfiltration, or any number of attacks possible if the very code itself is compromised.

9.5.6 POTENTIAL MITIGATING STRATEGIES / SCRM CONTROLS

The supplier should implement, monitor, and audit a comprehensive security assurance framework as part of their software development process.

All software should be compiled in trusted locations, such as where it is also verified, scanned, and signed. This would also serve as a logical central distribution point. Whenever software is changed and re-compiled, there could be a potential for injection of malicious code; thus, security scanning should be performed on each of these loads.

Static and dynamic code inspection is commonly used to verify the security and integrity of software. Static testing involves checking the code from an internal standpoint, executing code paths and routines to ensure they are operating as expected. Dynamic (a.k.a. black box) testing involves mimicking attacker behavior from the outside, detecting known vulnerabilities and simulating theoretical ones to determine if the product is vulnerable to different kinds of exploits.

Consider keeping code repositories and compiling functions in the cloud.

DHS POINT OF CONTACT

National Risk Management Center
Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security
NRMC@hq.dhs.gov
For more information about NRMC, visit www.cisa.gov/national-risk-management

PDM21063