INFORMATION AND COMMUNICATIONS TECHNOLOGY SUPPLY CHAIN RISK MANAGEMENT TASK FORCE

Threat Evaluation Working Group: Threat Scenarios

Version 2.0

January 2021

This page is intentionally left blank.

Executive Summary

This latest report from the Threat Evaluation Working Group adds the assessment of Impacts and Mitigating Controls to each of the Supplier Threat Scenarios originally provided in version one released in February 2020. These additional sections are included in Appendix C, Threat Scenarios, of this report. The Working Group chose to include these updates as a standalone report to benefit the audience by providing a complete report without the need to include numerous references to the original report. The Working Group will release additional revisions to this report in the future to include Supply Chain Risk Management threat evaluations for Products and Services as well.

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) 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 (SCRM) 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 WG2 Co-chairs leveraged the National Institute of Standards and Technology (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.

The general steps depicted in the figure below, and described in the following paragraphs, were used in the development and analysis of 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 complied by the WG2 membership. Each phased deliverable is a standalone report that builds upon the effort in 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 of 2020 focused specifically on Suppliers only, The WG2 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 WG2 members.

Each of the identified threats was then reviewed by the WG2 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 WG2 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 reduce the threat data and identify common elements for further evaluation using a scenario development process.

This grouping and descriptive titles were shared with the WG2 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 WG2 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 this revision to the original delivered report, the WG2 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. The objective 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 SCRM 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	December 2020	Supplier 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

Co-Chair:	Drew Morin	T-Mobile
	Tommy Gardner	HP
	Angela Smith	GSA
Project Manager:	Julian Humble	DHS/CISA (SED)
Admin Support:	James Alvarez	Contract Support DHS/CISA (SED)
	Jaime Fleece	Contract Support DHS/CISA (SED)

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	CenturyLink
David Mazzocchi, Dwight Steiner, Melissa Brocato-Bryant	CenturyLink
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
Mike Funk	Quincy Media

Greg Holzapfel	Sprint
Brad Minnis	Juniper
Tanya Kumar	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
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, 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 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, designed 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 Communications and Information Technology 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 and can be found at: (www.cisa.gov/publication/ict-scrm-task-force-interim-report).

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. way the source interacted with the weakness 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 a particular 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 or 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)

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 C-SCRM Task Force).

The WG2 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 Task Force WG2, 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 C-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: Cyber Supply Chain Risk Management (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 means:

- 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 Internet of Things/Operational Technology (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 WG2 initially conducted a survey of threat information from the diverse WG2 membership. The only constraint on the identification of threats was to focus on supplier threats in accordance with our initial proposed scoping.

[i] See, NIST definition of C-SCRM, available at: https://csrc.nist.gov/Projects/Supply-Chain-Risk-Management. 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 our initial supplier threat evaluation process will be repeatable in future iterations as the WG2 proceeds to expand our scope to include products and services.

Once the threats were identified, the WG2 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 WG2 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	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	Impact	*Description of potential impacts to Supply Chain or consequences of exploiting the vulnerability*
	Likelihood	
	Risk Score (Impact x Likelihood)	
	Acceptable Level of Risk	
Mitigation	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 WG2 represent the asset specific data that are captured to assess risk; something that will vary considerably depending on the specific supplier/product/service. This will result in a work product that will be consistent with NIST guidance concerning threats, and flexible enough to be used by industry and public sector for a variety of purposes.

The WG2 executed using 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 WG2 members considered C-SCRM threats from a variety of sources including industry Subject Matter Experts (SME), 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 WG2 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. Our purpose was to initially cast a wide net to capture a broad sample of threat inputs for analysis.

Each threat submitted was presented by the WG2 member that sourced the information to the broader membership. The discussion enabled the WG2 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

[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.

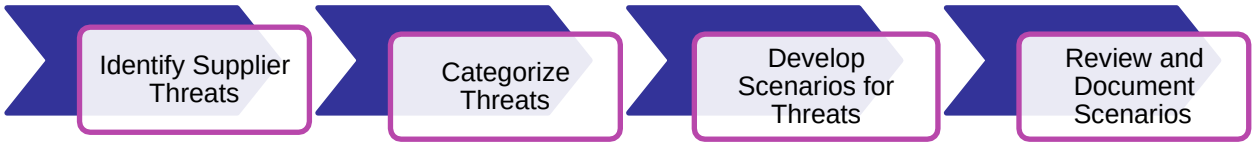
notes were captured for each of the identified threats. This set of information was compiled into a single data repository that was used in the Data Analysis phase of the process described below.

3.3.2 DATA ANALYSIS

The WG2 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 WG2 members were then consolidated and grouped to provide a manageable and shareable set of threat groupings for further the 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 our analysis, the WG2 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 WG2 to conduct the data analysis.

FIGURE 1—DATA ANALYSIS WORKFLOW



3.3.3 THREAT SCENARIO DEVELOPMENT

Once the WG2 established supply chain threat categories, the WG2 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 developed for each category if deemed necessary by the writing teams. Each scenario also includes 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 (What is the timing of the attack? Is it Denial of Service or zero day? Is it persistent or a one-time event? Etc.),
- Why (Objective of threat actors, intellectual property theft, network disruption…), and
- Where (Where in the Supply chain the specific threat activity is occurring).

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 as described in Section 2.0 above.

4.0 FINDINGS

4.1 Supplier Threat List

This section describes the supplier threat information gathered and the specific information for each threat that was presented for evaluation by the WG2 membership.

4.1.1 TAXONOMY OF THREAT LIST

The initial data call from the WG2 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 WG2 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 WG2 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 WG2 to enable a common understanding of the information provided concerning each specific threat. The list was then consolidated based on common threat categories and reviewed with the WG2 membership 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 specific threats 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 was then reviewed by the WG2 to ensure that the common groupings and category assignments accurately reflected the threat. A few of the threats initially identified were dropped from the list as they did not actually represent threats (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 WG2 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 WG2 members was consolidated into logical threat groups to aid in the evaluation process. The description of each of these threat 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 or planting malware attack such as zero day or 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 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.

[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.

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 compiled 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 WG2 – Supplier Threat Scenarios developed for the ICT SCRM Task Force is included as Appendix C to this document.

5.0 CONCLUSIONS

The WG2 kicked off this evaluation with a blank sheet and focused on leveraging the diversity of our membership to provide a broad base of threats for analysis and evaluation. This interim report and threat evaluation is limited to supplier threats only. The WG2 membership recognize that some of these threats are also applicable to products and services. The methods developed and applied in our initial supplier threat evaluation process will be repeatable in future iterations as the WG2 proceeds to expand our scope to include products and services.

The WG2 struggled with the specific threat groupings used, including proposal for further aggregation of the threat groupings into common sets to provide further clarification of the definition of each threat grouping. There were also some concerns that the threats identified may have also included risks. Due to time constraints, the co-chairs captured this information but decided to defer this to potential follow on work on products and services. This assumes that the task force supports the WG2 guidance to continue this work effort in the next iteration of WG2 outputs.

The WG2 recommends that the task force continue the charter for this effort with a focus on addressing products and services, review of categorization of threats, and possibly to provide risk assessments of some specific threats, prioritized by membership, as examples of how to leverage this threat assessment as an information feed into a company specific risk management program.

APPENDIX A: ACRONYM LIST

BGP	Border Gateway Protocol
BIA	Business Impact Analysis
CAD	Computer-Assisted Design
CCTV	Close-Circuit Televisions
CERT	Computer Emergency Readiness Team
CFIUS	Committee on Foreign Investment in the United States
CIS	Center for Internet Security
CSRIC	Communication, Security, Reliability, and Interoperability Council
C-SCRM	Cyber Supply Chain Risk Management
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
GSA	General Services Administration
HPE	Hewlett-Packard Enterprises
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
MAC	Media Access Control
MANRS	Mutually Agreed Norms for Routing Security

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
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
PWB	Printed Wiring Board
SAM	Software Asset Management
SC	Semiconductor
SCRM	Supply Chain Risk Management
SDLC	System Development Life Cycle
SED	CISA's Stakeholder Engagement Division

SMB	Small and Medium-sized Business
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

APPENDIX B: THREAT LIST

Note: 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. 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 member 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.

For future versions of this report (e.g., Version 3.0 which includes Products and Services), the WG2 will assess the Threat Groups to determine if there were any new additions required as a result of change in scope. 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 2.0 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		
Virtualization and encapsulation hiding access		
Sales of modified or counterfeit products to legitimate distributors		
A malicious supplier employee inserts hostile content at the product or component manufacturing or distribution stage so as to affect supplier products or components delivered to a subset (potentially a targeted subset) of downstream customers. (Tampering or counterfeiting)		

Insert tampered critical components into organizational systems	Adversarial: Deliver, insert, or install malicious capabilities	
Insert counterfeit or tampered hardware into the supply chain		Nation-state; Organization; Individual (Outsider/Insider)
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		
Obtain unauthorized access		
Data - Impacts to confidentiality, Integrity or availability		
Malware, unauthorized access, theft		
Cause unauthorized disclosure or unavailability by spilling sensitive information		
Login Attacks (Brute force, Dictionary attacks, Password spraying)	Adversarial: Conduct an attack	Nation-state; Organization; Individual (Outsider)
Credential Compromise		
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		
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		
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		
Embedded HW/SW threats (from manufacturing)		
A malicious supplier employee inserts hostile content at the product or component manufacturing or distribution stage so as to affect supplier products or components delivered to a subset (potentially a targeted subset) of downstream customers. (Tampering or counterfeiting)		
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		
Intrusion or compromise of customer through service		
Inappropriate modification of device, software, service through network update		
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		
Pervasive disk error		
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	
Threat actor impacts app store availability impacting end user ability to do job		Nation-state; Organization; Individual (Outsider)
Threat actor hacks cloud environment or telco making service unavailable		
Threat actor breaks ability of information provider to deliver information		
Man in the middle attack	Adversarial: Achieve results	Nation-state; Organization; Individual (Outsider)
Obtain information by externally located interception of wireless network traffic		
Incorrect BGP routing at a level above your network		
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		
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)
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 (example: nearly all Android based cellphones) 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)
Physical compromise of specific device		
Physical access through presence of device	Adversarial: Exploit and compromise	Nation-state; Organization; Individual (Outsider/Insider)
Physical network control or access		
Physical control of infrastructure		
Threat actor activity overwhelms organizations 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,	

Vulnerability Exploitation	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.		
Exploit insecure or incomplete data deletion in multi-tenant environment.	Adversarial: Exploit and Compromise	Nation-state; Organization; Individual (Outsider)
Data breaches post disconnect		
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		
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) Hardset accounts in devices and software		
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-states 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		
Manipulation of a development environment		
Manipulation of source code repositories (public or private)		
Manipulation of software update/distribution mechanisms		
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)
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 modified 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.		
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		

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		
IT services supply chain sends spy onsite		
Insert subverted individuals into organizations		
Insert subverted individuals into privileged positions in organizations		
Internal: Personnel Threat		
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		
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		
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)
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 decision by delivering too Much, too little, or type of information. it's not inaccurate, yet it 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 or Accidental: Deliver, insert, or install malicious capabilities	Nation-state; Organization; Individual (Outsider/Insider)
Inherited risk generally		
Mid supply chain insertion of counterfeit parts		
Depth of the supply chain and who is supplying the supplier		
Domestic Companies		
Lack of enforced traceability		
Supplier incorporates hostile content in product or component		
Threat of upstream intrusions in supply chain and lack of traceability from component to finished product		
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)		
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).		
Tampering while in transit	Adversarial: Conduct an attack	Nation-state; Organization; Individual (Outsider/Insider)
Shipment interdiction		

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		
Integrity of integrated third-party components		
Lack of oversight or security standards for imported devices		
Agency/enterprise does not have direct authority over third party suppliers.		
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		
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 so as to affect a large number of supplier products or components. (Tampering)	Adversarial: Achieve results	Individual (Insider)
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	

Suppliers operating in countries with weak Intellectual Property (IP) protection laws		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, etc.)	External: Legal noncompliance or ethical practices	Organization
Known to have violated U.S. sanctions		
4.2.2.9 External, End-to-End Supply Chain Risks		
Natural disaster causing supply chain disruptions	External: Natural disasters	Environmental: Natural
Natural disaster		
Natural disruptions		
Geo-Political uncertainty	External: Government compliance and political uncertainty	Nation-state; Organization
Man Made 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

Tables of Contents

This page is intentionally left blank.

1 THREAT CATEGORY: COUNTERFEIT PARTS

1.2 SCENARIO: COUNTERFEIT/FRAUDULENT PARTS

1.2.1 BACKGROUND

Counterfeit parts look just like regular parts and 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.

1.2.2 THREAT SOURCES

Most counterfeit items seized while entering the United States come from Asia. Some 87% of seized counterfeit items came from China or Hong Kong.[1] This data represents where the goods were shipped from, not necessarily where they were made. But it is likely most of them came from China.

1.2.3 THREAT IMPACT

Electronics are an indispensable part of our lives. Whether you're flying an airplane or driving a car, talking on your phone or using your tablet or desktop, a majority of our life is enabled by electronic components. Unfortunately, electronic components in consumer components, cars, and commercial planes are increasingly being counterfeited. Counterfeit components can easily cause product failures and even cause personal injury or death.

As an example, some time ago, the Senate Armed Services Committee uncovered more than 1 million "bogus parts" in the Pentagon supply chain. The suspected components were identified in computers, missiles, military aircraft and helicopters. Seventy percent of the counterfeit parts were manufactured in China.

That said, 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.

As organizations have become aware of counterfeit parts, one of the responses is to test upon acceptance or prior to receipt. But 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, the impact on costs, reliability and reputation are negatively impacted by counterfeit parts and components.

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 manufactures, 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 $200 and $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 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 annoying to impacting system performance to the loss of data.

1.2.6 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

1.2.7 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 failure and damage to systems or persons 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 product type, 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 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 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 similar to 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 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.

2 THREAT CATEGORY: EXTERNAL ATTACKS ON OPERATIONS AND CAPABILITIES

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
- 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 cyber-attacks
- 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 used for inter-domain routing on the Internet. BGP relies on mutual-trust among operators of gateway routers to ensure the integrity of the Internet routing infrastructure.[2] 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 cyber-attacks 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 colocation company leaked routes to a foreign Tier 1 Internet Service Provider (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 thru 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 Internet Service Providers 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:

- 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.
- https://www.bleepingcomputer.com/news/security/us-payment-processing-services-targeted-by-bgp-hijacking-attacks/

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 actually 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 cyber-attacks by malicious actors. For example, companies may fall victim to ransomware attacks multiple times during a year. Ransomware attacks are 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 USB drives near the organization 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 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 with. The targets browser opened the web page which contained malicious code that infects the targets 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 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 http://www.washingtonpost.com/wp-dyn/content/article/2010/08/24/AR2010082406495.html
- Krebs On Security article July 2018: https://krebsonsecurity.com/2018/07/state-govts-warned-of-malware-laden-cd-sent-via-snail-mail-from-china/

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 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. In this example, 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.

In this scenario, 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 48% of the distributed USB drives were inserted into the organization's computers.[3]

Once inserted, the computer can autorun the malware installation program. Or, the employee can attempt to open files, some with an alluring file name, thus allowing the malware to start running and install, open an electronic backdoor into the computer, and signal a point of entry 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, 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 suppliers are also potentially compromised. 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 and/or communicate outside of the organization

This threat scenario, Removable Media, is addressed in:

- NIST SP 800-53 Rev 4 Security Control: Media Protection
- 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 or accidental resource depletion is a non-adversarial threat resulting from system misconfigurations or lack of resource planning. System events resulting in resource depletion or 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 or 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 a 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 or service availability and 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

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 or type (OS, 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 untouched.

3.1.3 THREAT IMPACT

With the right kind of elevated privilege access, a malicious user could cause catastrophic impacts on a system. 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.

3.1.4 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

Implementation of cyber-hygiene practices should help mitigate the risk associated with this scenario (For additional details, visit: https://insights.sei.cmu.edu/insider-threat/2017/11/cyber-hygiene-11-essential-practices.html). 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 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 DON'T AUTO-UPDATE FIRMWARE (IMBEDDED SPINAL CORD STIMULATOR WITH A HAND-HELD CONTROLLER)

3.2.1 BACKGROUND

Failing to update your software doesn't just mean you won't have the latest version; it means you could be exposed to major security vulnerabilities that could also affect your physical wellbeing. There's 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

The 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 and 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 don't 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 doesn't appear to allow hackers to gain access to a patient's medical or personal history, the primary threat is control of the device itself, where the compromise of the imbedded device 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 requires 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 marketing and technical information. 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 is allowed to 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. 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. [4]

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 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.[5]

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 allowing them to download and install malware on the target's computer.[6]

With access to the target computer, the attacker can then exploit the building management system allowing physical access to the building.[7] 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.[8] In this scenario, an attacker could exploit software vulnerabilities to gain administrator rights, enabling them to create fraudulent ID's, 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 organizations IT department. 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 crucial.

3.4.7 MITIGATING STRATEGIES / SCRM CONTROLS

- Identify business operations and assets most vulnerable to cyber-attacks, 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;
- Utilize continuous threat intelligence to prioritize remediation efforts in light of 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 cyber-attacks;
- 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 (ERP) 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. In 2018, it was reported that less than 8 percent of analyzed breaches were due to weak or default credentials. 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.

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 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 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 absolutely 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 level 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 laws (or similar).

3.6.4 VULNERABILITY

The vulnerability is that 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.

3.6.5 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 based off industry standards and best practices
- Deploy and 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, and cybersecurity at large today. With a PAM solution in place, an organization can dramatically reduce the risks discussed above.
- The Best Practices for Privileged Access Management 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 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.

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; and/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. 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:

- 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 similar, to govern access to development environments, and use change management tools to track identity, time and 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

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.[iv]

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, 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,

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

		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 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.

5.1.4 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 Risk Management Framework. See the following for more information: https://csrc.nist.gov/projects/risk-management/risk-management-framework-(rmf)-overview

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 or 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 (SC) 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 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 insiders 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 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. Impact is Low
Harm to Assets	Low	Due to limited access to IP and the requirement of encrypted data at rest and in transit, we believe the IP aspects of this are low impact.
Harm to Individuals	Very Low	There is no personal information shared during this agreement, Impact is very low
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 and 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 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. Itis 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 with Chip Inc from an acquisition standpoint. Make those POCs clear to Chips Inc and give the POC's 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 or classified data or impact to a company's critical systems and services.

Outlined in NIST Special Publication 800-53, NIST defines an insider as: One who will use her or 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, and 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 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, 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 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 who is instrumental in sourcing candidates for employment, and of which 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 Supply Chain Risk Management (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 Risk Management Framework. See the following for more information: https://csrc.nist.gov/projects/risk-management/risk-management-framework-(rmf)-overview

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.

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 (Ex. intellectual property theft)

- Monetary loss for the enterprise, and potentially the extended supply chain [v]
- 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:

Development of an Insider Threat Program[9]

- 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[10]
- 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

---

v 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.

- 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
- 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

Training and Awareness

- Delivering insider awareness training to enterprise employees, and contractors, would better enable the insider-contract-employee to be identified
- Integrated Risk Management Program – Development of an organization-wide approach to manage cybersecurity risk[11]

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

Organizational Hygiene

- 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[12]
- 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

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 3rd 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	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

		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 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
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

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 a number of 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[13]

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.

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. 55% 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[14]
- 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 time. For example, a supplier's receivables may be growing, but that could mean its credit and collection standards are weak[15]
- It's important to have internal metrics for the CISO 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 collocated 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 aren't.

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 and integrity of the supply chain
- Financial compromise due to the lack of supplier compliance

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[16]
    - 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 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[vi]

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

6.3 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 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 been a successful 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 a majority 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. Committee on Foreign Investment in the United States (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.[17]

In 2018, the USA 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 start with.

6.4.2 THREAT SOURCE

The value of currency and politically volatile events can have serious implications on taxes (tariffs) and the 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 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[18]
- 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 a number of 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

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

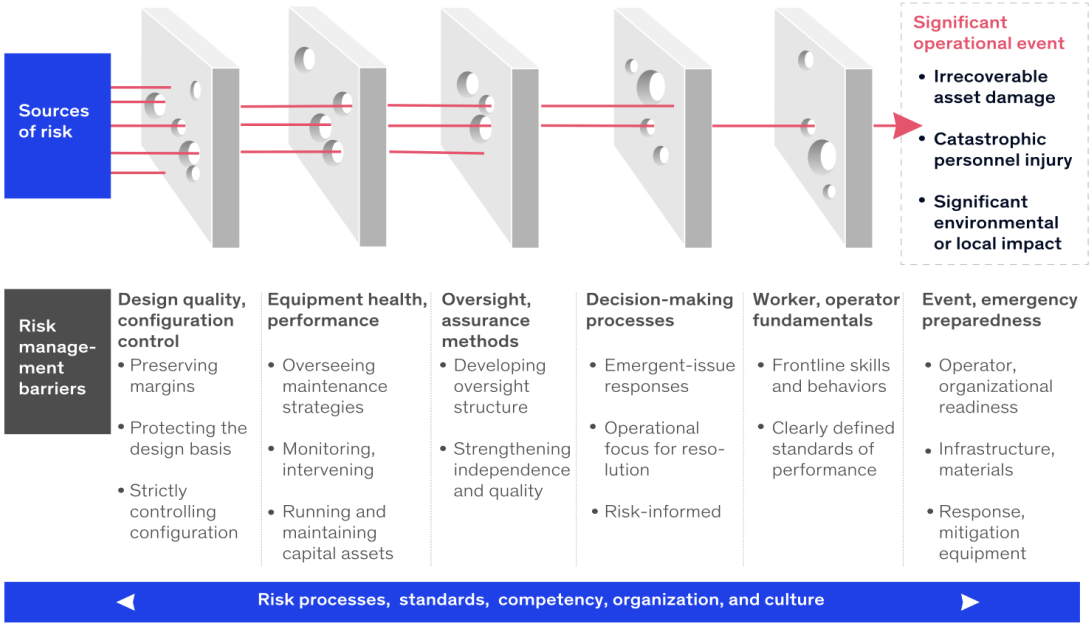
6.4.5 OUTCOME

The ability for U.S. or other countries to invest in Chinese mines has been 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're 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 obtained 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[19]
- With a global supply chain, transparency (internally in the organization and throughout the supply chain) is difficult but 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[20]
    - 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[21]
- 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
- 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[22]

Layers of defenses help organizations manage unknown risks.



McKinsey & Company

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 putting 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[vii]
- Device tampering and data spoofing[viii]
- Corporate espionage
- DoS Attacks[ix]
- Destruction of hardware
- 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 CFO's 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

[vii] 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.

[viii] 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.

[ix] 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.

SDLC:

- Creation of a secure embedded design and development lifecycle for hardware equipment. ENISA'S Hardware Threat Landscape and Good Practice Guide Report[23] provides an example of guidelines of particular 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
- 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[24]

Agency wide Compliance:

- Industry 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 and 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

7.1.9 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.

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, 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[25]

Agency Wide Training and Compliance:

- Require and implement a set of key metrics or 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
- 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 CSF 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 IP violations in the final product
- Lack of product integrity
- Potential irreversible damage to the end product's brand or reputation.
- Lack of traceability and consistency through the supply chain
- Inadequate communication through the supply chain
- Potential hardware or 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 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

- Good 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 Software Bill of Materials
- 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[26]
- Require and implement a set of key metrics or minimum baselines that are meaningful and relevant to the supply chain ecosystem's hardware and 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 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 criminal
- Extended stakeholders utilized via Supplier XYZ
- Unvetted stakeholders in the extended supply chain, etc.

7.4.3 THREAT IMPACT

- Pathway for new and easier software or 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 un-assumed 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[27]
- Consideration of utilizing a zero-trust privilege approach to securing privileged access credentials[28]
- Require and implement a set of key metrics or 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 any and 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 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

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 3rd 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

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
RECOVER	Recovery Planning (RC.RP)	Recovery Planning (RC.RP): Recovery processes and procedures are executed	CP-10, IR-4, IR-8	CIS CSC 10 COBIT 5 APO12.06, DSS02.05, DSS03.04

	and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	ISO/IEC 27001:2013 A.16.1.5

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 excel. 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 conducts 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." Excerpt from Presidential Memo to the U.S. Trade Representative, 2017.

8.1.2 THREAT SOURCE

State threat actors refer to hostile governments that want to disrupt American cyber supply chains for strategic or tactical advantage. Non-state threat actor is 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 ability to employ state or state-like powers to achieve their goals. State-owned enterprises and similar non-state actors around the world seek an advantage in the marketplace and in the operation of whatever they are tasked by their associated government.

Quasi-state actors are largely synonymous with state-owned or state-controlled 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 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 open 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 or 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

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 has the opportunity to engage in nefarious behavior in a jurisdiction unlikely to punish or deter such behavior. The problem of security become 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 multiple 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 or 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

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. 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 our 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, and $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 effects. 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 get back up and running. When the 2011 tsunami struck, several major industries were impacted. 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.

We are currently amid a global pandemic, coronavirus disease (COVID-19), which 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. We do not address this specific threat as a separate scenario in this report since these scenarios were originally

developed prior to the COVID-19 outbreak. The WG plans to specifically include this scenario in Version 3.0 of the report.

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 can result in delays in delivery of raw materials, components, and consumer goods as local communities recover from the disaster. Frequent and multiple impacts can further delay delivery of products and services.

9.1.4 THREAT EVENT DESCRIPTION

A category 5 hurricane hit Savanah, GA, and moved up the east coast and inland in northern VA before becoming a tropical storm. The hurricane damaged or destroyed ports from Savanah, GA to Norfolk VA while also destroying roads and bridges. Critical infrastructure impacts were 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 getting materials into the manufacturing plant and the ability to distribute finished products leading to financial harm. These may include unrecoverable loss of revenue or accounts receivable; contractual fines and penalties; inability to provide effective customer relations and regulatory reporting; and 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 during 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
- 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 practice their roles, develop confidence and expertise it can 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, cyber-attacks, 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. Another example is the Samsung Note cellphone 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.

The past few years have seen an increasing prevalence of cyber-attacks. Most of these incidents, such as the high-profile Equifax data breach that involved the personal information of some 143 million Americans, and the Dyn cyber-attack 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.

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 which time 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

The majority of overseas cargo comes from Asia and therefore come into ports on the West Coast. Los Angeles and Long Beach handle over 40 % of U.S imports from Asia. Due to the heavy cargo traffic, a collision of two 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 and 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 half a mile 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 United States 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 brining jobs back to the U.S. from oversees 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 %.

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 three times 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 %.

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 four months. Additionally, GoFast has reached out to several consulting and staffing firms, but there are two issues with this. One is the personnel from these outlets would take even longer (six to eight months) to fully ramp up as they are brand new to the company, and two is even the 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 employee
- Simplify processes or improve related training and documentation to reduce transition or onboarding time for folks new to an area
- 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 a majority 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 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 % 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 % 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, 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 there were several issues found with this. 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 PCB's 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 PCB's on higher-end models that could carry more margin.

9.4.6 MITIGATING STRATEGIES / SCRM CONTROLS

- Diversify suppliers not just by immediate location, but 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
- Employ more resources in countries or regions of key suppliers in hopes of receiving advanced Intel of new legislature that may negatively affect business

The National Risk Management Center (NRMC), Cybersecurity and Infrastructure Security Agency (CISA), is the planning, analysis, and collaboration center working in close coordination with the critical infrastructure community to Identify; Analyze; Prioritize; and Manage the most strategic risks to National Critical Functions. These are the functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating impact on security, national economic security, national public health or safety, or any combination thereof. NRMC products are visible to authorized users at HSIN-CI and Intelink. For more information, contact NRMC@hq.dhs.gov or visit https://www.cisa.gov/national-risk-management.

DHS POINT OF CONTACT

Cybersecurity and Infrastructure Security Agency
National Risk Management Center
U.S. Department of Homeland Security NRMC@hq.dhs.gov
For more information about NRMC, visit www.cisa.gov/national-risk-management

PDM20149

[1] U.S. Customs and Border Patrol, "Intellectual Property Rights Seizure Statistics Fiscal Year 2015," Last Modified 2016 https://www.cbp.gov/sites/default/ files/assets/documents/2016-Apr/FY%202015%20IPR%20Stats%20Presentation.pdf.
[2] Communications Security, Reliability, and Interoperability Council III | Federal Communications Commission, "Secure BGP Deployment Final Report" Last Modified March 2013
fcc.gov
[3] Robert Lemos, "How to keep USB thumb drive malware away from your PC" Last Modified May 18, 2016 https://www.pcworld.com/article/3070048/how-to-keep-usb-thumb-drive-malware-away-from-your-pc.html
[4] Ponemon Institute/ServiceNow, "State of Security Response," Last Modified 2018
[5] Tenable, "Vulnerability Intelligence Report" Last Modified November 2018 https://www.tenable.com/cyber-exposure/vulnerability-intelligence#download
[6] Tenable, "Tenable Research Discovers Vulnerability in Zoom that Could Lead to Conference Hijacking" Last Modified November 29, 2018 https://www.tenable.com/press-releases/tenable-research-discovers-vulnerability-in-zoom-that-could-lead-to-conference
[7] Tenable, "Multiple Zero-Days in PremiSys IDenticard Access Control System" Last Modified January 14, 2019 https://www.tenable.com/blog/multiple-zero-days-in-premisys-identicard-access-control-system
[8] Tenable, "Tenable Research Discovers "Peekaboo" Zero-Day Vulnerability in Global Video Surveillance Software" Last Modified September 17, 2019 https://www.tenable.com/press-releases/tenable-research-discovers-peekaboo-zero-day-vulnerability-in-global-video
[9] Intelligence and National Security Alliance, "A Preliminary Examination of Insider Threat programs in the U.S. Private Sector" Last Modified September 3, 2013 https://issuu.com/insalliance/docs/insa_wp_insiderthreat_pages_hires
[10] National Institute of Standards and Technology (NIST), "Preliminary Examination of Insider Threat Programs in the U.S.A. Private Sector" Last Modified September 2013 https://www.nist.gov/system/files/documents/2017/06/08/20131213_charles_alsup_insa_part4.pdf
[11] NIST, "Framework for Improving Critical Infrastructure Cybersecurity" Last Modified April 16, 2018 https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
[12] NIST, "Special Publication 800-53 (Rev. 4) Security and Privacy Controls for Federal Information Systems and Organizations" Last Modified January 22, 2015 https://nvd.nist.gov/800-53/Rev4/control/PM-12
[13] Craig Guillot, "Managing supply chain risk in an economic downturn" Last Modified November 18, 2019 https://www.supplychaindive.com/news/managing-supply-chain-risk-in-an-economic-downturn/567535/
[14] Paul Teague, "Supplier Financial Risk: Health Assessment Report" https://www.rapidratings.com/resources/whitepapers/supplier-financial-risk-assessment-whitepaper/
[15] Paul Teague, "Supplier Financial Risk: Health Assessment Report" https://www.rapidratings.com/resources/whitepapers/supplier-financial-risk-assessment-whitepaper/
[16] MetricStream, "Managing Vendor Risk : A Critical Step toward Compliance" https://www.metricstream.com/insights/5-best-practices-VRM.htm
[17] Simon Ellis, Stewart Bond, Matthew Marden, Harsh Singh, "Driving Strategic Value with IBM Sterling Supply Chain Business Network" Last Modified 2020 https://www.ibm.com/supply-chain/visibility?p1=Search&p4=43700050290103008&p5=b&cm_mmc=Search_Google-_-1S_1S-_-WW_NA-_-%2Bsupply%20%2Bchain%20%2Brisk%20%2Bmanagement_b&cm_mmca7=71700000060771755&cm_mmca8=kwd-296650934362&cm_mmca9=EAIaIQobChMI8LS9I8WQ6QIV3x-tBh1PTgsHEAAYAiAAEgLZkPD_BwE&cm_mmca10=432313318212&cm_mmca11=b&gclid=EAIaIQobChMI8LS9I8WQ6QIV3x-tBh1PTgsHEAAYAiAAEgLZkPD_BwE&gclsrc=aw.ds
[18] Victor Ng, "Mitigating against supply chain cyber risks" Last Modified October 23, 2019 https://www.cybersecasia.net/opinions/mitigating-against-supply-chain-cyber-risks
[19] Victor Ng, "Mitigating against supply chain cyber risks" Last Modified October 23, 2019 https://www.cybersecasia.net/opinions/mitigating-against-supply-chain-cyber-risks
[20] Tucker Bailey, Edward Barriball, Arnav Dey, and Ali Sankur, "A practical approach to supply-chain risk management" Last Modified March 8, 2019 https://www.mckinsey.com/business-functions/operations/our-insights/a-practical-approach-to-supply-chain-risk-management
[21] Simon Ellis, Stewart Bond, Matthew Marden, Harsh Singh, "Driving Strategic Value with IBM Sterling Supply Chain Business Network" Last Modified 2020 https://www.ibm.com/supply-chain/visibility?p1=Search&p4=43700050290103008&p5=b&cm_mmc=Search_Google-_-1S_1S-_-WW_NA-_-%2Bsupply%20%2Bchain%20%2Brisk%20%2Bmanagement_b&cm_mmca7=71700000060771755&cm_mmca8=kwd-296650934362&cm_mmca9=EAIaIQobChMI8LS9I8WQ6QIV3x-

tBh1PTgsHEAAYAiAAEgLZkPD_BwE&cm_mmca10=432313318212&cm_mmca11=b&gclid=EAIaIQobChMI8LS9I8WQ6QIV3x-tBh1PTgsHEAAYAiAAEgLZkPD_BwE&gclsrc=aw.ds

[22] Tucker Bailey, Edward Barriball, Arnav Dey, and Ali Sankur, "A practical approach to supply-chain risk management" Last Modified March 8, 2019 https://www.mckinsey.com/business-functions/operations/our-insights/a-practical-approach-to-supply-chain-risk-management

[23] European Union Agency For Cybersecurity, "Hardware Threat Landscape and Good Practice Guide" Last Modified February 8, 2017 https://www.enisa.europa.eu/publications/hardware-threat-landscape

[24] NIST, "Best Practices in Cyber Supply Chain Risk Management" https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-Supply-Chain-Best-Practices.pdf

[25] NIST, "Best Practices in Cyber Supply Chain Risk Management" https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-Supply-Chain-Best-Practices.pdf

[26] Christine Leong, Tal Viskin, Robyn Stewart, "Tracing the Supply Chain" Last Modified 2018 https://www.accenture.com/_acnmedia/pdf-93/accenture-tracing-supply-chain-blockchain-study-pov.pdf

[27] Louis Columbus, "Why Manufacturing Supply Chains Need Zero Trust" Last Modified August 29, 2019 https://www.forbes.com/sites/louiscolumbus/2019/08/29/why-manufacturing-supply-chains-need-zero-trust/#50e8f007a730

[28] Centrify, "WHAT IS ZERO TRUST PRIVILEGE?" https://www.centrify.com/education/what-is-zero-trust-privilege/