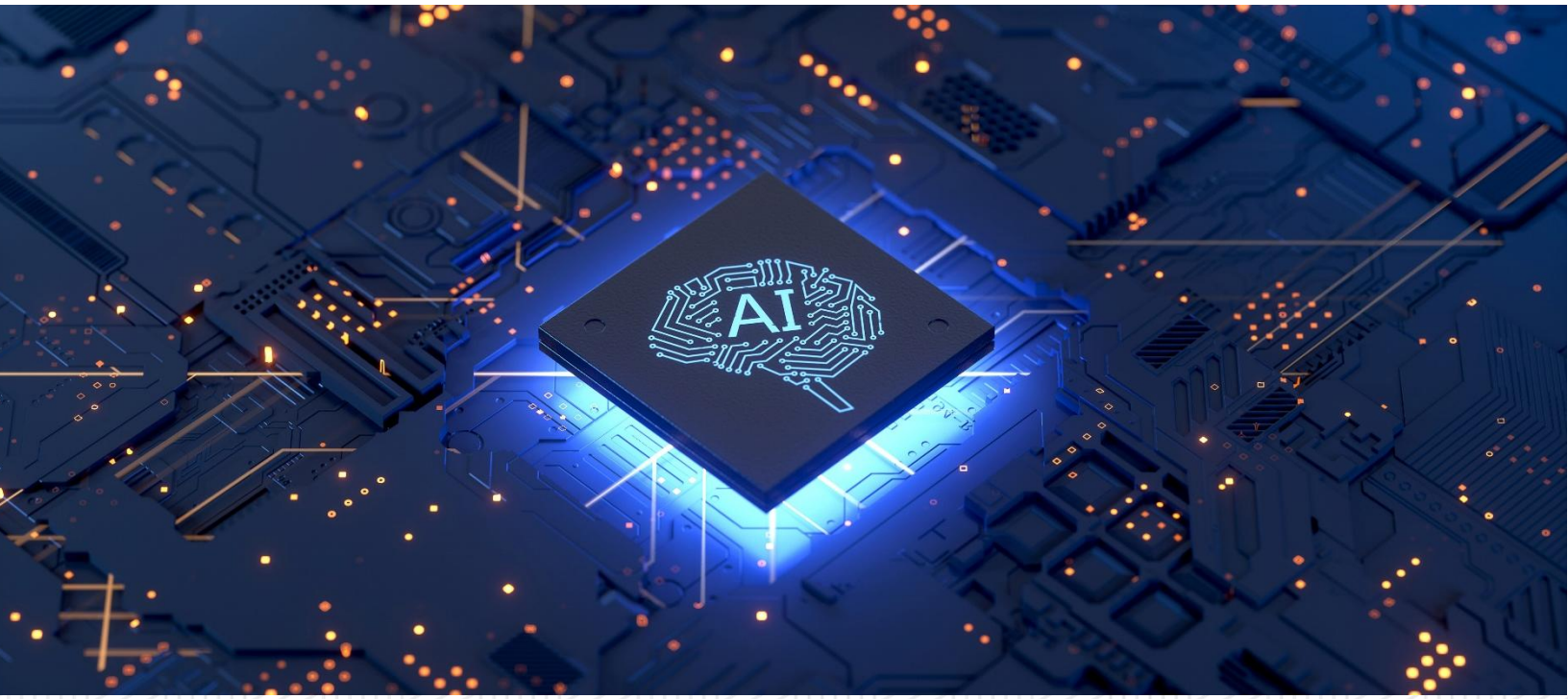

INFORMATION AND COMMUNICATIONS TECHNOLOGY SUPPLY CHAIN RISK MANAGEMENT TASK FORCE

Supplier, Products, and Services Threat Evaluation Report (to include Artificial Intelligence Risks and Mitigations)

July 2025

This product was developed in 2025 by the ICT Supply Chain Risk Management (SCRM) Task Force, a collaborative public-private body previously organized under the Critical Infrastructure Partnership Advisory Council. This product is the result of robust collaboration between members of the Communications and IT Sector Coordinating Councils (for a full list of contributors see Section 5.0) and was informed by consultative discussions with partners across the U.S. Federal government, including the Cybersecurity and Infrastructure Security Agency (CISA), the Department of Homeland Security (DHS), the Department of State, the Federal Communications Commission (FCC), the Federal Energy Regulatory Commission (FERC), the General Services Administration, the National Institute of Standards and Technology (NIST), and the Nuclear Regulatory Commission (NRC).

Disclaimer: The content and guidance presented in this product reflect the consensus and information available to the Task Force at the time of drafting. Due to the time elapsed between drafting and publication, some elements may not fully reflect subsequent developments in policy, technology, or threat landscapes. Users are encouraged to consult current sources and sector-specific updates when applying the recommendations in this document.

EXECUTIVE SUMMARY

This Threat Scenarios Report provides practical, example-based guidance on supply chain risk management (SCRM) threat analysis, evaluation, and mitigation. This most recent version has been updated with analyses of the implications of Artificial Intelligence (AI) for the threat landscape and for risk mitigation. Information and Communications Technology (ICT) SCRM professionals in government and industry can use this guidance to identify and assess supply chain risks and develop practices/procedures to address such risks.

In February 2020, the ICT SCRM Task Force[1] released the initial version of this report, which compiled and compartmentalized various types of supplier threats to aid in the evaluation and development of scenarios intended to provide insights into the processes and criteria for conducting supplier threat assessments. Version 2 (January 2021) added the assessment of impacts and mitigating controls to the supplier threat scenarios, while version 3 (July 2021) added the assessment of products and services and includes scenario-specific impacts and mitigating controls.

This version (version 4) updates the report with the implications of AI for the threat landscape and risk mitigation. It retains the existing structure of the document, with Appendix B featuring a taxonomy of threats (now updated with AI-related threats), and Appendix C presenting a non-exhaustive set of informative threat scenarios with associated mitigations (including 10 new AI grounded scenarios). Additionally, it includes a discussion on the considerations, challenges, and benefits that AI contributes to supply chain risk management. (See Section 2.4)

As with previous versions of the document, the AI-related threat and mitigation analysis provided is aimed at assisting an organization in managing its overall risk posture based on its operations. Organizations are encouraged to assess and manage their risks using the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), NIST Risk Management Framework[2], and the NIST AI Risk Management Framework[3]. This document does not purport to assess organization-level risks that flow from the threats identified here, given the fact that this can only be done in the context of an organization-wide risk analysis. Accordingly, the fact that a threat is identified and discussed does not mean that it necessarily constitutes a significant risk to an organization.

Earlier versions of the report and this version take a broad view of what threats are in-scope, addressing a wide range of procurement risks affecting suppliers' and third parties' products and services. The threat categories are:

Table 1—Threat Categories (from Appendix B)

Appendix B Threat Categories	Counterfeit Parts
	External Attacks on Operations and Capabilities
	Internal Security Operations and Controls
	System Development Life Cycle (SDLC) Processes and Tools

[1] The ICT SCRM Task Force provides a mechanism for representatives of industry and government to share information, explore challenges, and develop recommendations to manage ICT supply chain risks. The Task Force is led by representatives of the Department of Homeland Security (DHS) and the ICT sectors. Its membership reflects a public-private, cross-sector collaboration.
[2] https://csrc.nist.gov/Projects/risk-management/about-rmf
[3] https://www.nist.gov/itl/ai-risk-management-framework

	Insider Threats
	Economic Risks
	Inherited Risks (Extended Supplier Chain)
	Legal Risks
	External End-to-End Supply Chain Risks (Natural Disasters, Geo-Political Issues)

The AI Working Group (WG), tasked with developing this version 4 report, identified five threat categories associated with AI: Compromise of Machine Learning Operations (MLOps) Processes, Practices, and Tools; Explainability/AI Chain of Trust; AI Unpredictability; Societal Impact; and AI Extraction. These categories are described in Section 3.3. Additionally, Table B of Appendix B describes how the associated AI-related threats nest into the broader SCRM threat landscape.

Although the scope of threats included herein is very broad, the WG that drafted this version emphasizes that the analyses represented are a snapshot of known or contemplated threats and potential mitigations the group was able to identify based on current knowledge and experience. As is the case with the broader threat landscape, the AI-related threats and mitigations are expected to continue to evolve.

Finally, while the private sector participants in the AI WG are from the IT and Communications sectors, neither the report itself nor the AI content associated with this version 4 is specific to ICT organizations. Rather, the threats, risks, and mitigations discussed here are relevant across a variety of different sectors.

The objective of this report 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 can be used further 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 establishes a solid threat source evaluation that can be extended for specific products or services to drive the evaluation of supply chain risk.

Member organizations of the ICT SCRM Task Force, including CISA, do not endorse any commercial entity, product, company, or service, including any entities, products, or services mentioned within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by CISA or any member organization of the ICT SCRM Task Force.

CONTENTS

TABLES

1.0 BACKGROUND

1.1 Background

Supply chain risk management (SCRM) is the process of identifying, assessing, preventing, and mitigating the risks associated with the distributed and interconnected nature of information and communications technology (ICT) (including the Internet of Things [IoT]) product and service supply chains. SCRM covers the entire lifecycle 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) founded the ICT Supply Chain Risk Management Task Force, a consensus-based public-private partnership under the Critical Infrastructure Partnership Advisory Council (CIPAC) structure, to provide advice and recommendations to CISA and its stakeholders on means for assessing and managing risks associated with the ICT supply chain. The Threat Evaluation Working Group was established for the purpose of the identification of processes and criteria for threat-based evaluation of ICT suppliers, products, and services.

Over the past several years, the Task Force has reached consensus several times on establishing working groups to draft this report and subsequently evolve it. The report is focused on the identification of processes and criteria for threat-based evaluation of ICT suppliers, products, and services. Each iterative version of the report has been intended to provide ICT buyers and users with assistance and guidance for evaluating supply chain threats. Providing uniformity and consistency to this process is intended to benefit government and industry alike.

In 2024, CISA renewed the Task Force for an additional two years. The Artificial Intelligence (AI) Working Group (WG) was created with a charge of seeking to identify both emerging AI-related threats and beneficial ways in which AI can be used to mitigate threats posed to ICT SCRM processes. Like the Task Force itself, members of the AI WG were drawn from the private and public sectors, including representatives from the Department of Homeland Security and the Information Technology and Communications sectors. Contributing members leveraged a wide range of technical, legal, and policy expertise to complete this report.

The working groups drafting the report have 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 working groups consistently leveraged the NIST Risk Management Framework described in NIST SP 800-161[4] (published in April 2015) to help guide the analysis of the threats, threat sources, and mitigating controls identified in the work efforts.

Each version of the report identified and organized SCRM threats, scenario-specific impacts, and strategies to mitigate threats. The objective of the report is to provide practical, example-based guidance on supplier SCRM threat analysis and evaluation 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 can further be used as exemplary guidance on the application of the NIST Risk Management Framework. This process can be extended for evaluation of products and services, as well as replicated for other critical infrastructure providers. It also established a solid threat source evaluation that can be extended for specific products or services to drive the evaluation of supply chain risk.

[4] https://csrc.nist.gov/pubs/sp/800/161/r1/upd1/final

The report's original framework was utilized in this fourth version of the report to provide consistency and create a document in which AI considerations are additive, building on the methodology used by prior working groups. Readers can refer to version 3 of this report for more information on the methodology for the original threat scenarios sections. Table 2 below describes updates associated with each iteration of the report:

Table 2—History of Revisions

Version	Date	Scope
Original	February 2020	Supplier Threat Evaluation
Version 2.0	January 2021	Supplier Threat Evaluation to include Impact Analysis and Mitigation
Version 3.0	July 2021	Supplier, Products, and Services Threat Evaluation to include Impact Analysis and Mitigation
Version 4.0	2025	Supplier, Products, and Services Threat Evaluation to Include Impact Analysis, Mitigation, and Artificial Intelligence-related threats.

1.2 Objective and Scope

The ICT SCRM Task Force tasked the AI WG with the identification of the impact of AI on threats identified in prior reports, new threats posed by AI, and mitigation strategies. The objectives were defined as:

- Evaluate each threat scenario to consider how AI may impact the scenario and possible threat mitigations for that impact.
- Consider and identify new and emerging AI threat scenarios independent from the threat scenarios in prior reports as well as mitigation strategies for these threats.

As AI is being rapidly deployed, improving organizational security to address the risks of this developing technology should be a priority for organizations across all sectors. This report was written with those concerns in mind. However, AI can also be leveraged as a defense against these and other risks; AI has the potential to benefit both defenders and attackers.[5] Despite this dual nature, AI is just one component of the broader threat and defense landscape. As such, AI does not fundamentally change the existing risk management framework but should be integrated into it from multiple perspectives. This report seeks to address that objective.

Every existing threat scenario was independently assessed and there were many which the AI WG determined that AI would have no impact. In that case, these scenarios were left unchanged. Additionally, AI use has resulted in the existence of new threat scenarios not contemplated by prior versions of this report, and as such, those scenarios were added to this report. The WG utilized CISA's definition of AI for this report; see Section 2.3 of this report for definitions.

This report is meant for public and private organizations in the entirety of the ICT supply chain. The AI WG continues to take a broad view of both the scope of supply chain risks that are appropriate for inclusion here, and of the categories of threats faced by organizations. For example, consistent with previous versions of the report, the AI WG did not limit the "threats" to external actors seeking to cause harm, and included risks associated with the design and training of AI systems. It should also be noted that the nature of AI and its

[5] Envisioning Cyber Futures with A.I., Global Cybersecurity Group - Aspen Digital, Aspen Institute, January 2024.

potential harms could be far-reaching and not limited to only ICT. This report, therefore, can be used to inform risk management as it relates to AI broadly and across multiple sectors.

This updated framework for a threat-based assessment of ICT supply chain risks, including the impact of AI, can be utilized in future products to address AI risk in other critical infrastructure sectors.

2.0 METHODOLOGY, RELATIONSHIP BETWEEN THREAT, VULNERABILITY, AND RISK, DEFINITIONS, AND AI CHALLENGES

2.1 Methodology for AI Focus in Version 4

The AI WG initially conducted a survey of threat information from the diverse AI WG membership. The AI WG co-chairs leveraged the expertise of the AI WG members to consider how AI affects the existing threat scenarios contemplated by prior working groups, and to identify new threat scenarios and mitigations associated with this evolving technology. As discussed above, the scope of threat to be addressed was intentionally left broad.

The AI WG was divided into four writing groups. Three writing groups reviewed the threat scenarios in **Appendix C** and assessed potential AI impact and mitigation strategies for those threats. Each threat scenario was updated to incorporate the potential AI impact, if relevant. All additions were reviewed by the co-chairs, the entire working group, and CISA staff.

A fourth writing group used specific information references in key industry forums to identify new threat scenarios that exist as a result of AI. These new threats were assessed by the writing group and the co-chairs for applicability and relevance, as well as inclusion in the report. This AI-specific threat analysis was then incorporated into **Appendix B** as new threat categories and associated sub-categories, and into **Appendix C** as ten new scenarios.

2.2 Relationship between Threat, Vulnerability, and Risk

A threat source interacts with a vulnerability, which results in a threat event. The way in which the source interacted with a vulnerability 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.

2.3 Relevant Definitions

Artificial Intelligence: AI has the meaning set forth in the National Artificial Intelligence Initiative Act of 2020 (enacted as Division E of the William M [Mac] Thornberry National Defense Authorization Act for Fiscal Year 2021 [Public Law 116-283], Section 5002[3]):

- A machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments. Artificial intelligence systems use machine and human-based inputs to:
    a. perceive real and virtual environments;
    b. abstract such perceptions into models through analysis in an automated manner; and,
    c. use model inference to formulate options for information or action.

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

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

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

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

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

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

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

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

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)

2.4 AI Considerations, Challenges, and Benefits

As AI continues to evolve, a shared understanding of its characteristics is important for practitioners undertaking threat and risk analysis. To that end, the purpose of this section is threefold: i) to provide important SCRM guidance when acquiring an AI product, component, or service, ii) to describe benefits of using AI within the SCRM lifecycle to help mitigate risks and increase analytical productivity, and iii) to explain the general implications of including Machine Learning (ML) models in the creation of AI-based systems. This content is derived from the references listed below and the expertise of the AI WG.

2.4.1 AI Considerations

When AI products, components, and services are being considered for acquisition, it is important that organizations take into account certain considerations:

- Validate the provider or vendor and ensure they can trace the lineage of the AI model and how it was trained and on what data.

- AI based applications provide new vectors for potential supply chain security and cyber-attacks. It is important to be aware of AI risk guidance like the NIST AI Risk Management Framework to facilitate managing risks posed by these new AI enabled solutions or products.
- AI solutions, while novel and innovative, still require compliance to security and industry standards. Ensure that the vendor or provider has implemented the appropriate controls for protecting your data and your infrastructure.
- Considering ethical bias when selecting an AI vendor, includes ensuring that the vendor has adopted AI ethics standards and appropriately tests their products for potential bias where needed.
- Buyers should be aware of how their data is being used by the vendor and determine if sensitive data extraction issues exist in any prospective AI based acquisition.

2.4.2 AI Benefits

Using AI within the SCRM lifecycle can help mitigate risks and increase analytical productivity. For example:

- Using AI can reduce the effort of manually tracking and tracing the lineage of suppliers when using models trained on comprehensive supply chain risk datasets, company lineage, and industry demographics.
- Using AI-assisted risk projections can provide insights into the historical risk of supply chain resources.
- AI can speed up detection and suppression of supplier subversion attacks. In the future, AI based attack simulators could be used to pressure test organizations. These simulations can help organizations identify and prioritize security control weaknesses that have the greatest impact on resilience against attacks.
- AI based SCRM solutions can help provide insight into unstructured natural language-based data within the SCRM lifecycle to help identify anomalies.
- AI can be an asset in supporting the process of real-time continuous monitoring of the SCRM landscape. For example, AI can help to identify product anomalies in documentation that accompany parts, in order to facilitate the detection of potential counterfeits.

2.4.3 AI Challenges

Despite the considerations and benefits noted above, it is essential that organizations consider the risks when acquiring and deploying ML models in the creation of AI-based business systems.

Applications that use ML models are architecturally different from traditional software. The application behavior is determined by the 'statistical learning' from the training data and therefore, there is no specification document linking model inputs to outputs. "Data is the new specification," consequently, there is little to no application code providing the model specification. Furthermore, AI model outputs are not inherently deterministic and can vary for identical inputs due to probabilistic sampling. Without a predefined behavior captured in a specification, there is no clear definition of a software defect (i.e., bug), which is at the heart of traditional software quality management.

When there is unexpected behavior in the output (e.g., wrong classification), identifying the cause may require both an investigation of the model implementation details and the underlying training data. There are not necessarily relevant lines of program code to find and fix. Traditional testing methods, such as unit testing and function testing that expect deterministic behavior may not work. Any inherent bias in the historical training data may be reproduced by the AI model. Techniques to detect and mitigate such situations where the outputs are not statistically representative of the modeled data are necessary for the application to be trusted. ML models are complex functions, often with only nascent and limited tools for model interpretability and

explainability. This opaqueness leads to difficulty in determining if tampering or other attacks are present in AI systems.

Testing and evaluation are critical for every change to an AI model. Deploying models from development to production requires change management of both the model and its associated data to track and compare changes in behavior. This is particularly necessary for auditing purposes. AI model behavior can also drift and degrade over time as new data is integrated into the system. Therefore, the performance of AI applications should be monitored closely once deployed. In addition to model drift, dependency on cloud-based AI services and continually improving AI capabilities may require the refreshing of the underlying technology components for AI applications. This can be difficult to manage in regulated industries, such as banking. There is also overwhelming evidence that AI models are susceptible to various types of adversarial attacks. Thus, in addition to the traditional concerns about software systems (such as reliability, correctness, and maintainability), concerns about bias, uncertainty, explainability, robustness, data drift, and transparency of the ML models should be addressed for a successful deployment. Fortunately,, AI development and monitoring tooling continues to rapidly evolve.

Deploying Generative AI (GenAI) requires additional risk management techniques due to the stochastic nature of its outputs. With the current popular transformer-based deep learning architectures, any unwanted behavior, such as hate, abuse, profanity, hallucinations, lack of factuality, privacy leakage, can only be detected and mitigated after the model output is created for a downstream application and not during the model pretraining process. Careful data curation during pretraining can help to mitigate some of the undesired outputs. Generative AI can also be subjected to prompt-injection attacks in the model adaptation stage.

GenAI and Large Language Models (LLM) are developed and deployed using techniques, tools, and practices called MLOps. In these instances, MLOPs replaces the traditional Software Development Life Cycle and DevOps practices most organizations are accustomed to. Using AI in the development of business systems requires new development and deployment skills and tooling, not present in traditional software development. Selecting AI-enabled products and services should be conducted thoughtfully based on business and mission requirements such as risk, accuracy, and availability of pertinent training data. The AI acquisition process should consider that many of the traditional techniques used for threat or vulnerability analysis require new tools, techniques, and governance.

3.0 FINDINGS

3.1 Supplier, Products and Services Threat List

This section describes the threat information gathered and the specific information for each threat included in this report.

3.1.1 Threat Taxonomy (Appendix B)

The scope of the threats identified in the report was intentionally kept broad. Three fields of data were provided for each threat category and sub-category:

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

The following references were used to identify new AI threat categories:

ID	Reference Source	URL
[1]	OWASP Top 10 for LLM	https://owasp.org/www-project-top-10-for-large-language-model-applications/
[2]	MITRE AI Atlas	https://atlas.mitre.org/
[3]	IBM AI Risk Atlas	https://www.ibm.com/docs/en/watsonx/saas?topic=ai-risk-atlas
[4]	Project GuardRail	https://oecd.ai/en/catalogue/tools/project-guardrail

3.1.2 Descriptions of SCRM Threat Categories

Below are descriptions of each of the groupings of threats set forth in Appendix B. The list was consolidated based on common threat categories identified and reviewed by the WG membership to gain consensus.

3.1.2.1 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.

3.1.2.2 External Attacks of Operations and Capabilities

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

3.1.2.3 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 CSF.

3.1.2.4 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 is the failures in the development process to detect the introduction of malware or unvetted code into software products through use of vulnerable open source libraries.

3.1.2.5 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.

3.1.2.6 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 company size resource constraints.

3.1.2.7 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.

3.1.2.8 Legal Risks

This category of risks 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 risks 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.

3.1.2.9 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.

3.2 Information Threat Scenarios (Appendix C)

3.2.1 Purpose of Threat Scenarios

Since version 2, the Threat Scenarios Report has included an Appendix C with threat scenarios designed to illustrate and draw out SCRM lessons from a subset of the categories described in the taxonomy of threats.

3.2.2 Description and Structure of Threat Scenarios

For each of nine categories of threats in Appendix B, there are multiple scenarios in Appendix C designed to provide illustrative examples of some of the threats that fall into these categories. The goal of the threat scenarios is to draw out lessons about how various threats may manifest themselves and what mitigations are appropriate to consider.

To promote consistency with established risk management frameworks, each threat scenario includes a subset of the data elements that are identified in NIST SP 800-161 as relevant to evaluating SCRM. Table 3 below identifies the elements that the working group determined should be captured for each scenario:

Table 2—Table Derived from NIST SP 800-161

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

Risk Component	Description
Impact	Description of potential impacts to Supply Chain or consequences of exploiting the vulnerability
Likelihood	Chance of something happening
Acceptable Level of Risk	A level of residual risk to the organization's operations, assets, or individuals that falls within the defined risk appetite and risk tolerance by the organization

Mitigation Component	Description
Potential Mitigating Strategies or SCRM Controls	*Identify supplier evaluation criteria that would reduce or mitigate the impact of the threat*
Estimated Cost of Mitigating Strategies	*Enter estimated cost of risk mitigating strategies*
Change in Likelihood	*Identify potential changes in likelihood*
Change in Impact	*Identify potential changes in impact*
Selected Strategies	*List selected strategies to reduce impact*
Estimated Residual Risk	*Enter the estimated amount of residual risk* Residual Risk: Portion of risk remaining after security measures have been applied

Some fields from 800-161 in the threat scenarios represent asset-specific data that would need to be captured to assess risk and are highly dependent on the specific supplier/product/service. The result is a work product that will be consistent with NIST guidance concerning threat and flexible to be used by industry and public sector for a variety of purposes.

3.3 Findings as they Relate to AI

When considering the Threat List (Appendix B) and the Threat Scenarios (Appendix C), the AI WG identified common challenges in the acquisition and use of AI that apply broadly to many of the existing threats. With respect to Appendix C, the AI WG identified additional content that was new, novel, or relevant to the existing Threat Scenarios. The AI WG considered both predictive AI (approach of the past decade for a narrow task such as object recognition) and the more recent GenAI that creates new artifacts (e.g. summarization, image, etc.) based on foundation models such as LLMs, as both are consistent with the definition of AI adopted by the AI WG.

In general, the introduction of AI to the existing SCRM threat scenarios can result in one or more of four outcomes:

- no impact;
- help alleviate the original threats, if deployed responsibly by risk managers;
- aggravate the original threats, if deployed by adversaries against managed systems or not deployed responsibly by risk managers; or
- introduce new threats or considerations, especially if the AI system itself needs to be assured and managed.

Since the goal of AI is often to automate a specific task done by humans, in scenarios that do not allow any automation, AI is irrelevant and hence has no impact. Otherwise, depending on the threat scenario, AI can assist the adversary to create more efficient attacks. Alternatively, AI can help in the defense of SCRM attacks by discovering patterns and automating repetitive SCRM tasks. The use of AI itself brings to bear a new landscape of implementation and in some cases new threats that require mitigation. In addition to integrating AI risks and mitigations to threat scenarios from previous reports, this report introduces additional AI threats to existing categories and uses existing taxonomies of AI threats and associated scenarios.[6]

Where AI either aggravates existing threats or introduces new threats, the AI WG considers the same three types of threats as considered in the April 2024 DHS report:[7]

- Attacks Using AI;
- Attacks Targeting AI Systems; and
- Failures in AI Design and Implementation.

The findings of the AI WG are also consistent with the key findings of the April 2024 DHS report:[8]

- The potential use of AI to automate more complex functions in the enterprise and solve some hard problems.
- Managing the tension between transformative potential of AI vs. the need for managing the risks of the evolving technology.
- The use of AI by adversaries to expand and enhance current cyber tactics, techniques, and procedures.
- Need for creation of mitigation strategies and best practices specific to AI development and use.

Appendices B and C organize the new AI scenarios as follows:

---

[6] DHS Report. "MITIGATING ARTIFICIAL INTELLIGENCE (AI) RISK: Safety and Security Guidelines for Critical Infrastructure Owners and Operators". April 2024. https://www.dhs.gov/sites/default/files/2024-04/24_0426_dhs_ai-ci-safety-security-guidelines-508c.pdf

[7] Ibid., pg 9

[8] Ibid., pg 7

- Appendix B introduces new threats specifically for AI systems.
- Appendix C both adjusts scenario descriptions from version 3 to account for changes in technology since 2018 and introduces ten new scenario descriptions elaborating on some of the new threats identified in Appendix B.

Appendix B Table B-2 remains unchanged from version 3 of this report. We have added a Table B-3 consisting of threats that should be managed if AI systems are present in the supply chain. The threats in Table B-3 are a mixture of threats present in many software systems that are substantially aggravated in the case of AI systems and threats that are primarily considered in the context of AI systems. While Table B-3 introduces new threats, the AI WG has not introduced new categories of threats; AI systems are software systems. Table B-3 cross-references the new threats to the category of threats in Table B-2. Borrowing from other taxonomies such as AI risk atlas and OWASP AI Security and Privacy Guide, Table B-3 also loosely groups these threats under headings that an AI engineer focusing on AI testing would recognize – extraction attacks, explainability, assuring the ML operations process. By providing both the threat category mapping to the longstanding SCRM threat categories from prior versions of this document and groupings under terms from the AI engineering community, we hope to facilitate communication between these communities.

The working group identified five AI-related groups of threats that organize the AI-related threats, even as they are organized into the existing nine SCRM threat categories. These five groups are:

- Compromise of MLOps: An attack on the process to curate and deploy an AI model.
- Explainability/Traceability/AI Chain of Trust: Adversaries could provide models that contain intentionally false information or do not provide the proper attribution. In some cases, a model may be trained on proprietary unlicensed information.
- AI Unpredictability: Acquisition of AI enabled coding tools should assess the effect of this uncertainty on the task objectives based on what precise task within the software development workflow the AI system is performing. Risk assessment in this context includes, but is not limited to, consideration of the model transparency,[9] lineage of the models, vendor reputation, and the code base or patterns on which they were trained. If an AI solution is provided Excessive Agency, adversaries may gain access to systems through processes that were never hardened or via privilege escalation.
- Societal impact: Historical, representational, and societal biases present in the data used to train and fine tune a model can adversely affect model behavior by manifesting that bias in its output. This includes information taken out of context that is factually correct.
- Information Leakage/Reverse Engineering: The model parameters, architecture, and/or data used to train an AI model can be reverse engineered using inputs and outputs. Adversaries may gain access to sensitive information through access to an AI service or model.

These five threat groups are also described in Table B-3 in Appendix B.

Appendix C designates the ten new scenarios for version 4 as “AI scenario” rather than “scenario” *simpliciter*. A manager of an AI system can search the document or table of contents in Appendix C and find these AI-specific scenarios. These AI scenarios are sorted into the SCRM threat category alongside other threat scenarios. Many of the AI scenarios echo at least some of the concerns in other scenarios in the category. This should allow personnel managing AI systems to find contact points with SCRM generally and places to look for examples and lessons learned. It also highlights for examples of how AI systems need new or modified treatment within the existing categories of risk with which SCRM professionals are familiar.

[9] See for example Linux Foundation (2024). Introducing the Model Openness Framework. https://lfaidata.foundation/blog/2024/04/17/introducing-the-model-openness-framework-promoting-completeness-and-openness-for-reproducibility-transparency-and-usability-in-ai/

4.0 CONCLUSIONS

This revised Threat Scenario Report highlights the complex nature of threats within the cyber supply chain, with a specific focus on vulnerabilities and risks associated with ICT systems. The rapid emergence and integration of AI technologies—particularly AI-powered algorithms, machine learning, and predictive analytics—have acted as catalysts for new and evolving risks that add to the challenges identified in previous reports. The ICT SCRM Task Force, through its AI WG, has conducted a point-in-time analysis to evaluate how AI affects existing threat scenarios, identify new AI-specific threats, and propose relevant mitigation strategies.

As AI technologies advance, enhancing organizational security remains a critical priority across all sectors. This report reflects a snapshot of the current landscape, recognizing that while AI has the potential to bolster defensive measures, it also introduces new cyber supply chain risks. The dual role of AI as both a tool for attackers and defenders necessitates its integration into existing risk management frameworks without fundamentally altering them.

The AI WG assessed how AI influences established threat scenarios and identified emerging scenarios driven by advancements in AI-powered algorithms, machine learning, and predictive analytics. While some preexisting scenarios were deemed unaffected by AI, others were updated or newly introduced to account for AI's evolving impact. As a living document, this report captures a broad perspective on supply chain risks and acknowledges that AI's potential impacts are extensive, affecting various sectors beyond critical infrastructure and communications.

To ensure continued relevance and effectiveness, this report may be updated periodically to reflect new insights and developments regarding AI risks. This iterative process will help maintain a robust and adaptable framework for assessing cyber supply chain risks, addressing emerging challenges and risk vectors as AI technology continues to evolve.

5.0 CONTRIBUTORS

Table 4 – List of Contributors

Name	Organization
Chris Oatway (WG Co-Chair)	Verizon
Tommy Gardner (WG Co-Chair)	HP
Chris Boyer, Ronald Dilley, Jeffrey Dygert	AT&T
Michelle Carey, Brock Bose, Shira Danker, Joe Viens, Criag Neely	Charter
Nick Britton, Michael Gargiullo	Crest International
Rudy Brioche, Jayati Dev	Comcast
Kerrianne Haresign	CTA
Justin Perkins	CTIA
Ola Sage	CyberRx
Edna Conway	EMC Advisors

Name	Organization
Alana Scott	Ericsson
Ryan Harvey	Exiger
Robert Salvia	Fortress
Trey Hodgkins	Hodgkins Consulting
Matt Barry	HP
Jessica Sweet	Hunter Strategy
Peter Santhanam	IBM
Tom Quillin, Tom Brennan	Intel
John Miller, Courtney Lang	Information Technology Industry Council (ITI)
Chad Kliewer	ISC2
Jon Amis	LMI
Stephanie Travers, Chris Anderson, Kathryn Condello, Tobin Thomas	Lumen
Patricia Eke	Microsoft
Keith Hill	MITRE
Megan Lancaster, Telice Gillom	NASPO
Andras Szakal	The Open Group
Brendan Peter	Security Scoreboard
Beth Linker	Synopsys
Colin Andrews, Melissa Newman	TIA
Robert Mayer, Brianna Bace	USTelecom
Jessica Cohen, Tim Schulz	Verizon

APPENDIX A: ACRONYM LIST

AI	Artificial Intelligence
API	Application Programming Interface
ATO	Authority to Operate

BGP	Border Gateway Protocol
BIA	Business Impact Analysis
BOM	Bill of Materials
CAD	Computer-Assisted Design
CCTV	Close-Circuit Televisions
CERT	Computer Emergency Readiness Team
CFIUS	Committee on Foreign Investment in the United States
CIS	Center for Internet Security
CISA	Cybersecurity and Infrastructure Security Agency
COTS	Commercial-Off-the-Shelf
COVID-19	Coronavirus Disease
CSF	Cybersecurity Framework
CSRIC	Communication, Security, Reliability, and Interoperability Council
CVE	Common Vulnerability and Exposure
DDoS	Distributed Denial of Service
DHS	Department of Homeland Security
DMZ	Demilitarized Zone
DNS	Domain Name System
DoD	Department of Defense
EAS	Emergency Alert System
FIPS	Federal Information Processing Standards
GenAI	Generative Artificial Intelligence
GRC	Governance, Risk, and Compliance
GSA	General Services Administration
IAAA	Identification, Authentication, Authorization, Auditing, and Accounting
IC	Intelligence Community
ICS	Industrial Control Systems
ICT	Information and Communications Technology
ID	Identification
IP	Internet Protocol

IP	Intellectual Property
IR	Incident Response
ISO	International Organization for Standardization
ISP	Internet Service Provider
IT	Information Technology
ITIC	Information Technology Industry Council
ITP	Insider Threat Program
KPI	Key Performance Indicator
KRI	Key Risk Indicator
LAN	Local Area Network
LLM	Large Language Model
MAC	Media Access Control
MANRS	Mutually Agreed Norms for Routing Security
MLOps	Machine Learning Operations
MSSP	Managed Security Service Provider
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
OS	Operating System
OT	Operational Technology
PAM	Privileged Access Management
PC	Personal Computer
PCB	Printed Circuit Board
PII	Personally Identifiable Information
PM	Program Management
POS	Point-of-Sale
PWB	Printed Wiring Board
RFI	Request for Information
RFP	Request for Proposal

SaaS	Software as a Service
SBOM	Software Bill of Materials
SC	Semiconductor
SCA	Security Controls Assessment
SCADA	Supervisory Control and Data Acquisition
SCRM	Supply Chain Risk Management
SDK	Software Development Kit
SDLC	System Development Life Cycle
SED	Stakeholder Engagement Division
SLTT	State, Local, Territorial, and Tribal
SMB	Small and Medium-sized Business
SNMP	Simple Network Management Protocol
SQL	Standardized Query Language
SSH	Secure Shell
TIA	Telecommunications Industry Association
U.S.	United States
USB	Universal Serial Bus
VPN	Virtual Private Network
WG	Working Group

APPENDIX B: THREAT LIST

THREATS	THREAT CATEGORIES OR EVENT	THREAT SOURCE OR ACTOR
3.1.2.1 Counterfeit Parts		
Counterfeit product or component with malicious intent to cause unwanted function	Adversarial: Craft or create attack tools	Nation-State; organization; individual (Outsider/Insider)
Component elements included in product, software, or service	Adversarial: Craft or create attack tools	Nation-State; organization; individual (Outsider/Insider)
Virtualization and encapsulation hiding access	Adversarial: Craft or create attack tools	Nation-State; organization; individual (Outsider/Insider)
A malicious supplier employee inserts hostile content at the product or component manufacturing, or distribution stage, to affect supplier products or components delivered to a subset (potentially a targeted subset) of downstream customers (tampering or counterfeiting)	Adversarial: Craft or create attack tools	Nation-State; organization; individual (Outsider/Insider)
Sales of modified or counterfeit products to legitimate distributors	Adversarial: Craft or create attack tools	Nation-State; organization; individual (Outsider/Insider)
Insert tampered critical components into organizational systems	Adversarial: Deliver, insert, or install malicious capabilities	Nation-State; organization; individual (Outsider/Insider)
Insert counterfeit or tampered hardware into the supply chain	Adversarial: Deliver, insert, or install malicious capabilities	Nation-State; Organization; Individual (Outsider/Insider)
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)
3.1.2.2 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)

THREATS	THREAT CATEGORIES OR EVENT	THREAT SOURCE OR ACTOR
Loss of critical information from vendor	Adversarial: Achieve results	Nation-State; Organization; Individual (Outsider/Insider)
Obtain unauthorized access	Adversarial: Achieve results	Nation-State; Organization; Individual (Outsider/Insider)
Data – Impacts to confidentiality, integrity or availability	Adversarial: Achieve results	Nation-State; Organization; Individual (Outsider/Insider)
Malware, unauthorized access, theft	Adversarial: Achieve results	Nation-State; Organization; Individual (Outsider/Insider)
Cause unauthorized disclosure or unavailability by spilling sensitive information	Adversarial: Achieve results	Nation-State; Organization; Individual (Outsider/Insider)
Login Attacks (Brute force, Dictionary attacks, Password spraying)	Adversarial: Conduct an attack	Nation-State; Organization; Individual (Outsider)
Credential Compromise	Adversarial: Conduct an attack	Nation-State; Organization; Individual (Outsider)
Supplier solution architecture allows for manipulation and extraction of data and services (not due to a system vulnerability)	Accidental: User, privileged user	Nation-State; Organization; Individual (Outsider/Insider)
Phishing, spear phishing, or whaling	Adversarial: Craft or create attack tools	Nation-State; Organization
Malware, unauthorized access, theft	Adversarial: Craft or create attack tools	Nation-State; Organization
Deliver known malware to internal organizational information systems (e.g., virus via email)	Adversarial: Deliver, insert, or install malicious capabilities	Nation-State; Organization; Individual (Outsider)
Compromise of integrity of product through intrusion	Adversarial: Exploit and compromise	Nation-State; Organization; Individual (Outsider)
External cyber attacker threats	Adversarial: Exploit and compromise	Nation-State; Organization; Individual (Outsider)
Embedded malware or virus attacks in delivered products	Adversarial: Craft or Create Attack Tools	Nation-State; Organization; Individual (Outsider/Insider)
Inappropriate modification of device, software, or service through network update	Adversarial: Craft or Create Attack Tools	Nation-State; Organization; Individual (Outsider/Insider)
Embedded HW/SW threats (from manufacturing)	Adversarial: Craft or Create Attack Tools	Nation-State; Organization; Individual (Outsider/Insider)

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

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

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

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

THREATS	THREAT CATEGORIES OR EVENT	THREAT SOURCE OR ACTOR
Data breaches post disconnect	Adversarial: Exploit and Compromise	Nation-State; Organization; Individual (Outsider)
Poor Employee/Contractor/Vendor Access Controls	Adversarial: Achieve results	Nation-State; Organization; Individual (Outsider/Insider)
Supplier System Does Not Have Controls to Validate and Authorize Escalation of Privileges	Adversarial: Achieve results	Nation-State; Organization; Individual (Outsider/Insider)
Staff using vulnerable unpatched personal computer systems from home to contact agency resources	Accidental: Individual	Individual (Outsider/Insider)
Large enterprise (~$10 billion/year) that supplies key components for mission projects continues to experience cyberattack and illicit technology transfer events	Adversarial: Exploit and Compromise	Nation-State; Organization; Individual (Outsider)
ICT Devices with default passwords	Accidental: Deliver, insert, or install malicious capabilities	Organization
(Removal of) Hard-set accounts in devices and software	Accidental: Deliver, insert, or install malicious capabilities	Organization
Devices that do not auto-update firmware	Accidental: Deliver, insert, or install malicious capabilities	Organization
Mishandling of critical or sensitive information by authorized users	Accidental: Individual	Individual (Insider)
Incorrect privilege settings	Accidental: Individual	Individual (Insider)
3.1.2.4 Compromise of SDLC Processes and Tools		
Malware coded, inserted, or deployed into critical ICT throughout the design, development, integration, deployment or maintenance phase of components	Adversarial: Craft or create attack tools	Nation-State; Organization; Individual (Outsider/Insider)
Manipulation of development tools	Adversarial: Craft or create attack tools	Nation-State; Organization; Individual (Outsider/Insider)
Manipulation of a development environment	Adversarial: Craft or create attack tools	Nation-State; Organization; Individual (Outsider/Insider)
Manipulation of source code repositories (public or private)	Adversarial: Craft or create attack tools	Nation-State; Organization; Individual (Outsider/Insider)

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

THREATS	THREAT CATEGORIES OR EVENT	THREAT SOURCE OR ACTOR
Insert subverted individuals into organizations	Adversarial: Deliver, insert, or install malicious capabilities	Nation-State; Organization; Individual (Outsider/Insider)
Insert subverted individuals into privileged positions in organizations	Adversarial: Deliver, insert, or install malicious capabilities	Nation-State; Organization; Individual (Outsider/Insider)
Internal: Personnel Threat	Adversarial: Deliver, insert, or install malicious capabilities	Nation-State; Organization; Individual (Outsider/Insider)
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)
3.1.2.6 Economic		
Viability of financially weak suppliers	Economic: Financial stability	Nation-State; Organization
Financial stability	Economic: Financial stability	Nation-State; Organization
Economic risk (i.e., a supplier or sub-contractor of a supplier will be economically devastated by a breach)	Economic: Financial stability	Nation-State; Organization
Limited visibility into business and sustainability practices of suppliers beyond the first tier	Economic: Financial stability	Organization
Cost volatility	Economic: Financial stability	Organization
No vendor support when a company transfers ownership or closes	Economic: Financial stability	Organization
Operational disruptions due to source being acquired by a far larger company with questionable security	Economic: Financial stability	Organization
Very small, privately held company “one-man show” with inadequate quality management and history of delivery delays; security concerns contracted to product components on the critical path of multiple mission projects	Economic: Financial stability	Organization

THREATS	THREAT CATEGORIES OR EVENT	THREAT SOURCE OR ACTOR
Young entrepreneurial business identified as a potential subcontractor for key mission components but has no discoverable facility for production, integration, test, nor quality management	Economic: Financial stability	Organization
SMB often lack the ability to heavily influence vendors to correct issues	Economic: Production problems	Organization
Little control over what applications or devices customers use or connect with via provider-services	Economic: Production problems	Organization; Individual (Outside)
If a vendor is compromised, some providers that use the same equipment or software across their entire system do not have the resources to continue operations or switch to another vendor	Economic: Production problems	Nation-State; Organization; Individual (Outsider/Insider)
Threat Actor determines how to manipulate decisions by delivering too much or too little information; inaccurate yet somehow changes decisions	Economic: Production problems	Nation-State; Organization; Individual (Outsider/Insider)
Industry discovers vulnerability in IT Product X resulting in freeze in using that product until fixed	Economic: Production problems	Nation-State; Organization; Individual (Outsider/Insider)
SMBs do not have the resources or expertise to evaluate the security of all devices and software that are purchased by the company	Economic: Production problems	Organization
Most small and medium sized providers do not proactively monitor customer-based equipment for anomalous behaviors, and as such are unable to diagnose a security issue unless notified by other means	Economic: Production problems	Organization
3.1.2.7 Inherited Risk (Extended Supplier Chain)		
Inherited risk (extended supplier chain)	Adversarial / Accidental: Deliver or insert malicious capabilities	Nation-State; Organization; Individual (Outsider/Insider)
Inherited risk generally	Adversarial / Accidental: Deliver or insert malicious capabilities	Nation-State; Organization; Individual (Outsider/Insider)
Mid-supply chain insertion of counterfeit parts	Adversarial / Accidental: Deliver or insert malicious capabilities	Nation-State; Organization; Individual (Outsider/Insider)

THREATS	THREAT CATEGORIES OR EVENT	THREAT SOURCE OR ACTOR
Depth of the supply chain and who is supplying the supplier	Adversarial / Accidental: Deliver or insert malicious capabilities	Nation-State; Organization; Individual (Outsider/Insider)
Domestic companies	Adversarial / Accidental: Deliver or insert malicious capabilities	Nation-State; Organization; Individual (Outsider/Insider)
Lack of enforced traceability	Adversarial / Accidental: Deliver or insert malicious capabilities	Nation-State; Organization; Individual (Outsider/Insider)
Supplier incorporates hostile content in product or component	Adversarial / Accidental: Deliver or insert malicious capabilities	Nation-State; Organization; Individual (Outsider/Insider)
Threat of upstream intrusions in supply chain and lack of traceability from component to finished product	Adversarial / Accidental: Deliver or insert malicious capabilities	Nation-State; Organization; Individual (Outsider/Insider)
Supplier has malicious intent and incorporates hostile content in product or component. This scenario applies to hardware or software providers (including both proprietary and open source software)	Adversarial / Accidental: Deliver or insert malicious capabilities	Nation-State; Organization; Individual (Outsider/Insider)
Trustworthy supplier inadvertently creates a product or component that is vulnerable to attack and delivers it to downstream customers. This scenario applies to hardware or software providers (including both proprietary and open source software)	Adversarial / Accidental: Deliver or insert malicious capabilities	Nation-State; Organization; Individual (Outsider/Insider)
Tampering while in transit	Adversarial: Conduct an attack	Nation-State; Organization; Individual (Outsider/Insider)
Shipment interdiction	Adversarial: Conduct an attack	Nation-State; Organization; Individual (Outsider/Insider)
Vendor noncompliance	Adversarial: Deliver, insert, or install malicious capabilities	Nation-State; Organization; Individual (Outsider/Insider)
Lack of Certification of component safety or quality at each appropriate level of the value chain of a product	Adversarial: Deliver, insert, or install malicious capabilities	Nation-State; Organization; Individual (Outsider/Insider)
Integrity of integrated third-party components	Adversarial: Deliver, insert, or install malicious capabilities	Nation-State; Organization; Individual (Outsider/Insider)
Lack of oversight or security standards for imported devices	Adversarial: Deliver, insert, or install malicious capabilities	Nation-State; Organization; Individual (Outsider/Insider)

THREATS	THREAT CATEGORIES OR EVENT	THREAT SOURCE OR ACTOR
Agency/enterprise does not have direct authority over third party suppliers	Adversarial: Deliver, insert, or install malicious capabilities	Nation-State; Organization; Individual (Outsider/Insider)
Lack of required disclosure of component manufacturer origin	Adversarial or Accidental: Deliver, insert, or install malicious capabilities	Nation-State; Organization; Individual (Outsider/Insider)
Lack of disclosure of origin	Adversarial or Accidental: Deliver, insert, or install malicious capabilities	Nation-State; Organization; Individual (Outsider/Insider)
Create and operate false front organizations to inject malicious components into the supply chain	Adversarial: Craft or create attack tools	Nation-State; Organization
IT information provider delivers intentionally bad or misleading data (e.g. DNS/BGP)	Adversarial: Achieve results	Nation-State; Organization; Individual (Outsider/Insider)
A malicious supplier employee inserts hostile content at the product or component design or software coding stage, to affect many supplier products or components (tampering)	Adversarial: Achieve results	Individual (Insider)
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)
3.1.2.8 Legal risks		
Legal: IP or licensing violation	Legal: IP or Licensing violation	Nation-State; Organization; Individual (Outsider/Insider)
Suppliers operating in countries with weak intellectual property protection laws	Legal: IP or Licensing violation	Nation-State; Organization; Individual (Outsider/Insider)
Liability for purchaser	Legal: Lawsuits	Nation-State; Organization

THREATS	THREAT CATEGORIES OR EVENT	THREAT SOURCE OR ACTOR
Supplier fear liability impact could devastate participants in supply chain, particularly SMBs	Legal: Lawsuits	Nation-State; Organization; Individual (Outsider/Insider)
Privacy violation risk (third party supplier is not compliant with privacy obligations)	External: Government compliance and political uncertainty	Nation-State; Organization
Legislation and compliance	External: Government compliance and political uncertainty	Nation-State; Organization
Third party supplier has engaged in financial crimes (e.g. fraud, bribery, money laundering)	External: Legal noncompliance or ethical practices	Organization
Third party supplier has violated U.S. sanctions	External: Legal noncompliance or ethical practices	Organization
3.1.2.9 External, End-to-End Supply Chain Risks		
Natural disaster causing supply chain disruptions	External: Natural disasters	Environmental: Natural
Natural disaster	External: Natural disasters	Environmental: Natural
Natural disruptions	External: Natural disasters	Environmental: Natural
Geo-political uncertainty	External: Government compliance and political uncertainty	Nation-State; Organization
Manmade disruptions: sabotage, terrorism, crime, war	External: Government compliance and political uncertainty	Nation-State; Organization
Labor issues	External: Government compliance and political uncertainty	Nation-State; Organization
Supply chain disruptions and price spikes due to protectionism in global trade	External: Government compliance and political uncertainty	Nation-State
Lack of legislative governance enforcing traceability within the manufacturing and assembly process	External: Government compliance and political uncertainty	Nation-State; Organization
Nation-State control over foreign suppliers	External: Government compliance and political uncertainty	Nation-State
Diminishing contribution of U.S. companies in technology standards bodies and open source software	Adversarial: Maintain a presence or set of capabilities.	Nation-State

SCRM THREAT ASSOCIATED WITH THE ACQUISITION AND USE OF AI[10]

THREATS	THREAT CATEGORIES OR EVENT	THREAT SOURCE OR ACTOR	MAPPING TO EXISITING SCRM CATEGORIES
Compromise of MLOps Processes, Practices and Tools			
Erode ML Model Integrity: Adversaries may degrade the target model's performance with tainted data inputs to erode confidence in the system over time. [2]	Adversarial: Conduct an attack	Nation-State; Organization; Individual (Outsider)	4.2.2.2 External Attacks on Operations and Capabilities
Backdoor ML Model: Adversaries may introduce a backdoor into a ML model. A backdoored model operates performs as expected under typical conditions but will produce the adversary's desired output when a trigger is introduced to the input data. [2]	Adversarial: Craft or create attack tools	Nation-State; Organization; Individual (Outsider)	4.2.2.4 Compromise of SDLC Processes and Tools
Insecure Output Handling: An LLM output is accepted without scrutiny, exposing backend systems.[11] Examples Include: Sensitive Information Disclosure: LLM's may inadvertently reveal confidential data in its responses, leading to unauthorized data access, privacy violations, and security breaches. LLM02 [1] LLM06 [1]	Adversarial: Conduct an attack	Organization	4.2.2.3 Internal Security Operations and Controls
Supply Chain Vulnerabilities: LLM application lifecycle can be compromised by vulnerable components or services, leading to security attacks. LLM05 [1]	Adversarial: Conduct an attack	Nation-State; Organization; Individual (Outsider)	4.2.2.4 Compromise of SDLC Processes and Tools

[10] The bracketed numbers associated with each threat references the threat material used to identify that threat (See: 3.1.1)
[11] Insecure Output Handling refers specifically to insufficient validation, sanitization, and handling of the outputs generated by large language models before they are passed downstream to other components and systems. Since LLM-generated content can be controlled by prompt input, this behavior is similar to providing users indirect access to additional functionality.

THREATS	THREAT CATEGORIES OR EVENT	THREAT SOURCE OR ACTOR	MAPPING TO EXISITING SCRM CATEGORIES
Data curation risk: When training or tuning data is improperly collected or prepared, the result can be a misalignment of a model's desired values or intent and the actual outcome. [3]	Adversarial: Deliver, insert, or install malicious capabilities	Nation-State; Organization; Individual (Outsider)	4.2.2.7 Inherited Risk (Extended Supplier Chain)
Data transparency risk: Without accurate documentation on how a model's data was collected, curated, and used to train a model, it might be harder to satisfactorily explain the behavior of the model with respect to the data. [3]	Adversarial: Exploit and compromise	Nation-State; Organization; Individual (Outsider)	4.2.2.7 Inherited Risk (Extended Supplier Chain)
Data provenance: During the data acquisition phase of the MLOps process, no systematic approach was used to verify the authenticity of the training data and track its provenance for future use. Not all data sources are trustworthy. Data might have been unethically collected, manipulated, or falsified. Using such data can result in undesirable behaviors of the model during deployment. [3]	Adversarial: Exploit and compromise	Organization	4.2.2.4 Compromise of SDLC Processes and Tools OR 4.2.2.5 Insider Threat Depending on if an internal actor intentionally sabotages the phase.
During the data curation stage of the MLOps process or in the prompting and fine-tuning phase of an LLM, insufficient attention was paid to remove personal identifiable information (PII), sensitive personal information (SPI) and other confidential information. This might result in unwanted disclosure of that information in the model output during deployment. [3]	Adversarial: Craft or create attack tools	Nation-State; Organization; Individual (Outsider)	4.2.2.8 Legal risks
Explainability / AI Chain of Trust			
Unexplainable output: Explanations for model output decisions might be difficult, imprecise, or not possible to obtain. [3]	Adversarial: Exploit and Compromise	Organization	4.2.2.7 Inherited Risk (Extended Supplier Chain)
Unreliable source attribution: Source attribution is the AI system's ability to describe from what training data it generated a portion or all its output. Since current techniques are	Adversarial: Exploit and Compromise	Organization	4.2.2.7 Inherited Risk (Extended Supplier Chain)

THREATS	THREAT CATEGORIES OR EVENT	THREAT SOURCE OR ACTOR	MAPPING TO EXISITING SCRM CATEGORIES
based on approximations, these attributions might be incorrect. [3]			
Inaccessible training data: Without access to the reliable training data, the types of explanations a model can provide are limited and more likely to be incorrect. [3]	Adversarial: Exploit and Compromise	Organization	4.2.2.7 Inherited Risk (Extended Supplier Chain)
Untraceable attribution: The original entity from which training data comes from might not be known, limiting the utility and success of source attribution techniques. [3]	Adversarial: Exploit and Compromise	Nation-State; Organization; Individual (Outsider)	4.2.2.9 External, End-to-End Supply Chain Risks
Lack of model transparency: Insufficient documentation of the model development process makes it difficult to understand how and why a model was built and who built it, thus increasing the possibility of model unintended misuse. [3]	Adversarial: Exploit and Compromise	Nation-State; Organization; Individual (Outsider)	4.2.2.7 Inherited Risk (Extended Supplier Chain)
Unpredictability			
Overreliance: Systems or people overly depending on LLMs without oversight may face misinformation, miscommunication, and legal issues due to incorrect or inappropriate content generated by LLMs. LLM09 [1]; [3]	Adversarial: Exploit and Compromise	Nation-State; Organization; Individual (Outsider)	4.2.2.8 Legal risks
Excessive Agency: LLM-based systems may undertake actions leading to unintended consequences. LLM08 [1]; [3]	Adversarial / Accidental: Deliver or insert malicious capabilities	Nation-State; Organization; Individual (Outsider)	4.2.2.7 Inherited Risk (Extended Supplier Chain)
Impact on human agency: Misinformation and disinformation that is generated by foundation models, including the generation of manipulative content. [3]	Adversarial / Accidental: Deliver or insert malicious capabilities	Nation-State; Organization; Individual (Outsider)	4.2.2.8 Legal risks
Societal Impact			
Data bias: Historical, representational, and societal biases present in the data used to train and fine tune the model can adversely affect model behavior. [3]	Adversarial: Achieve results	Nation-State; Organization; Individual (Outsider)	4.2.2.8 Legal risks
Impact on cultural diversity: AI systems might overly represent certain cultures that result in a homogenization of culture and thoughts. [3]	Adversarial: Achieve results	Nation-State; Organization; Individual (Outsider)	4.2.2.6 Economic

THREATS	THREAT CATEGORIES OR EVENT	THREAT SOURCE OR ACTOR	MAPPING TO EXISITING SCRM CATEGORIES
Bypassing learning: Using AI models to bypass the student learning process. [3]	Adversarial: Achieve results	Organization	
Plagiarism risk: Using AI models to plagiarize existing work intentionally or unintentionally. [3]	Adversarial: Loss of IP	Organization	4.2.2.8 Legal risks
Physical harm: A model might generate language that leads to physical harm. The language might include overtly violent, covertly dangerous, or otherwise indirectly unsafe statements that could precipitate immediate physical harm or create prejudices that could lead to future harm. [3]	Adversarial: Safety Compromise	Nation-State; Organization; Individual (Outsider/Insider)	4.2.2.8 Legal risks
Unspecified advice: When a model generates information that is factually correct but not specific enough for the current context, the advice can be potentially harmful. For example, a model might provide medical, financial, and legal advice or recommendations for a specific problem that the end user may act on even when they should not. [3]	Adversarial: Conduct an attack	Nation-State; Organization; Individual (Outsider)	4.2.2.7 Inherited Risk (Extended Supplier Chain)
Extraction			
Pseudonymization risk: Even with the removal of personal identifiable information (PII) and sensitive personal information (SPI) from data, it might still be possible to identify persons due to other features available in the data. [3]	Adversarial: Craft or create attack tools	Nation-State; Organization; Individual (Outsider/Insider)	4.2.2.8 Legal risks
Prompt priming risk: Because generative models tend to produce output like the input provided, the model can be prompted to reveal specific kinds of information. [3]	Adversarial: Craft or create attack tools	Nation-State; Organization; Individual (Outsider/Insider)	4.2.2.3 Internal Security Operations and Controls
Jailbreaking: An attack that attempts to break through the guardrails established in the model. [2], [3]	Adversarial: Craft or create attack tools	Nation-State; Organization; Individual (Outsider/Insider)	4.2.2.2 External Attacks on Operations and Capabilities
Prompt leaking risk: A prompt leak attack attempts to extract a model's system prompt (also known as the system message). [2], [3]	Adversarial: Craft or create attack tools	Nation-State; Organization; Individual (Outsider/Insider)	4.2.2.2 External Attacks on Operations and Capabilities
Attribute inference attack: An attribute inference attack is used to detect whether certain sensitive features can be inferred about individuals who participated in training a model. [2], [3]	Adversarial: Craft or create attack tools	Nation-State; Organization; Individual (Outsider/Insider)	4.2.2.3 Internal Security Operations and Controls (access control issue) and 4.2.2.8 Legal risks

THREATS	THREAT CATEGORIES OR EVENT	THREAT SOURCE OR ACTOR	MAPPING TO EXISITING SCRM CATEGORIES
			(if the result is a privacy violation)
Personal information in prompt: Disclosing Personal Information or Sensitive Personal Information as a part of a prompt that is sent to the model. [3]	Adversarial: Craft or create attack tools	Nation-State; Organization; Individual (Outsider/Insider)	4.2.2.3 Internal Security Operations and Controls (access control issue) and 4.2.2.8 Legal risks (if the result is a privacy violation)
Extraction attack: An extraction attack attempts to copy or steal an AI model by appropriately sampling the input space and observing outputs to build a surrogate model that behaves similarly. [2], [3]	Adversarial: Deliver, insert, or install malicious capabilities	Nation-State; organization; individual (Outsider/Insider)	4.2.2.2 External Attacks on Operations and Capabilities (an example of "Product vulnerabilities (unintended) in hardware and software") and 4.2.2.3 Internal Security Operations and Controls (improper access controls)

APPENDIX C THREAT SCENARIOS

APPENDIX C: Table of Contents

1 THREAT CATEGORY: COUNTERFEIT PARTS

1.1 Scenario: Counterfeit/Fraudulent Parts

1.1.1 Background

Counterfeit parts are a form of fraud. Counterfeiters prey on customers seeking high-quality parts from reputable manufacturers and instead are unknowingly sold substandard or defective parts. A counterfeiter's "intent to deceive" is the difference between a counterfeit part and a faulty part, which has defects that are unknown to the manufacturer or the distributor. A counterfeit part or component includes both hardware and software, and either could be modified and misrepresented as authorized by the original equipment manufacturer.

1.1.2 Threat Sources

Most counterfeit items seized while entering the United States come from Asia. Some 90 percent of seized counterfeit items came from China or Hong Kong.[12]

1.1.3 Threat Impact

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

As an example, in 2012 the Senate Armed Services Committee uncovered more than 1,800 cases of "bogus parts" in the Pentagon supply chain.[13] The suspected components were identified in computers, missiles, military aircraft, and helicopters. Seventy percent of the counterfeit parts were manufactured in China.

That said, the Department of Defense is not the only victim. Consumer and industrial businesses are losing hundreds of billions of dollars annually. The automobile industry and the semi-conductor industry are losing billions of dollars annually.[14]

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

1.1.4 Vulnerability

[12] https://www.cbp.gov/trade/priority-issues/ipr/statistics
[13] U.S. Senate Committee on Armed Services, "Senate Armed Services Committee Releases Report on Counterfeit Electronic Parts," 2012.
[14] Gary Bamossy and Debra L. Scammon (1985),"Product Counterfeiting: Consumers and Manufacturers Beware", in NA - Advances in Consumer Research Volume 12, eds. Elizabeth C. Hirschman and Moris B. Holbrook, Provo, UT : Association for Consumer Research, Pages: 334-339

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

The manufacture and sale of counterfeit products is a widespread problem that affects manufacturers, distributers, and retailers in virtually every industry. According to the International Anti-Counterfeiting Coalition (IACC), the global trade in counterfeit has increased from $5.5B in 1982 to approximately $1.7 trillion annually today.[15] In the U.S. alone, the economic impact of counterfeit goods on businesses is estimated to be $200B to $250B annually.[16]

Software counterfeiting is a huge criminal industry that is as lucrative as the drug trade and, like the drug trade, transcends national borders.[17] 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. Software counterfeiting can include components delivered as updates to existing products or product integrations. Product integrations that include artificial intelligence are very popular but can be subject to counterfeited models and AI services.

1.1.5 Outcome

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

1.1.6 Organizational Units / Processes Affected

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, taken from an Underwriter Labs report,[18] 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.

[15] https://www.iacc.org/resources/about/statistics
[16] Nathan Vardi, "The World's Biggest Illicit Industries," 2010, Forbes.
[17] Ibid.
[18] Underwrite Labs Report "Mitigating the Risk of Counterfeit Products"

- 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."[19]

1.1.7 Potential Mitigating Strategies / SCRM Controls

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

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

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

[19] Underwrite Labs Report "Mitigating the Risk of Counterfeit Products"

The second part of the strategy should address detection and screening of incoming goods before they are used.

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

- Unusual packaging or box
- Inconsistent appearance, color, dimensions with specifications
- Variations in items in a package
- Modifications, touch up and cosmetic beautification of old/salvaged parts
- Altered or worn manufacturer's markings such as name plate, model, serial/part numbers
- Incomplete or inconsistent information on name plate, product markings, or certification
- Irregularities in documentation:
    - Shipping papers
    - Certification and technical data
    - Lacking signatures and other required authentication of certain documents
    - Chemical and material test report and certification documents with handwritten entries or other indication (whiteout) of possible alterations
    - Modified software that is not delivered through authorized update channels and validated by the Original Equipment Manufacturer (OEM)

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.

1.2 Scenario: Foreign Counterfeit/Fraudulent Parts

1.2.1 Background

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

1.2.2 Threat Sources

Foreign national selling computing components to federal agencies.

1.2.3 Threat Impacts

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

1.2.4 Vulnerability

See Section 1.1.4

1.2.5 Counterfeit Event Description

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

1.2.6 Outcome

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

1.2.7 Organizational Units / Processes Affected

See Section 1.1.6

1.2.8 Potential Mitigating Strategies / SCRM Controls

Many fake and counterfeit products are so identical in look and feel to genuine parts that it is getting harder to distinguish them visually. Procurement of safety-critical replacement parts can be a serious challenge and make you vulnerable to a catastrophic risk of failure from unknowing use of counterfeit components. Moreover, conventional quality control efforts are found to be inadequate to address the challenge of counterfeit products. Whether you are a manufacturer, contractor, distributor, or a retailer, counterfeit products can affect your profits, market share, and brand reputation and present a serious product liability risk from bodily injury and property damage. Although specific strategies may vary by type of products, industry segment, and procurement process, anti-counterfeiting experts and organizations recommend implementation of a comprehensive strategy to help reduce the risk of counterfeit products. The strategy should address two aspects:

- The first aspect is related to procurement and related processes:
    - Always know your source for procurement of critical products and components. Buying from authorized/certified distributors provides at least some assurance of product quality and integrity of authentic parts. Buying on the Internet or other alternate sources (gray or black market) or importing directly increases your chance of becoming a victim of counterfeit product frauds.
    - If you are forced to procure a critical part from an alternate source because a part is not available from an authorized distribution channel, it is important to increase your own verification efforts to

ensure integrity of parts by additional testing efforts. Sometimes, reconditioned and salvaged parts may be sold as new but may not meet specifications as represented.

- Do not buy on lowest cost criteria alone. In tough economic times, there is temptation to buy at lowest cost. If the price offered is a deeply discounted bargain basement price compared to known price range for branded products, it should raise suspicion alerting further investigation.

- Report suspected counterfeit products and distribution channels to law enforcement authorities and brand manufacturers. Ignoring knowledge about specific counterfeit products and sources of distribution can perpetuate this risk with potential for significant consequences.

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

- Unusual packaging or box
- Inconsistent appearance, color, dimensions with specifications
- Variations in items in a package
- Modifications, touch up and cosmetic beautification of old/salvaged parts
- Altered or worn manufacturer's name plate, model, serial numbers
- Incomplete or inconsistent information on name plate, product markings, or certification
- Irregularities in documentation:
  - Shipping papers
  - Certification and technical data
  - Lacking signatures and other required authentication of certain documents
  - Chemical and material test report and certification documents with handwritten entries or other indication (whiteout) of possible alterations

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

2.1 Scenario: Attacker Exploits Known Vulnerabilities in Supplier Systems Connected To Critical Infrastructure Organization Networks

2.1.1 Background

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

As more devices are connected, the attack surface expands, often in unexpected places, such as building management systems and 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.

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 is a significant period during which vulnerable systems remain unpatched.

In this instance, the adversary gains access to the operational infrastructure environment through privilege escalation. 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.

2.1.4 Vulnerability

The vulnerability from the critical infrastructure provider's 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 should be kept patched or otherwise mitigated.

2.1.5 Threat Event Description

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

AI can be used to better map and evaluate risks to suppliers and vendors. The implementation of AI in existing interactive supplier and vendor risk/threat/control analysis questionnaires could improve efficiency and efficacy. There may be opportunities to use AI to flag abnormal interactions caused by a successful supplier subversion attack, and to better understand normal interactions between suppliers, vendors, and critical infrastructure sector members. Supplier subversion attacks could be detected and suppressed quickly. In the future, AI-based attack simulators could be used to pressure test organizations. These simulations can help organizations to identify and prioritize security control weaknesses that have the greatest impact on resilience against attacks.

2.2 Scenario: Incorrect BGP Routing

2.2.1 Background

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

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

2.2.2 Threat Source

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

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

2.2.3 Threat Impact

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

2.2.4 Vulnerability

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

2.2.5 Threat Event Description

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

2.2.6 Outcome

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

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

2.2.7 Organizational Units / Processes Affected

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

2.2.8 Potential Mitigating Strategies / SCRM Controls

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

This threat scenario is addressed in:

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

References:

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

2.3 Scenario: Ransomware

2.3.1 Background

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

2.3.2 Threat Source

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

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

2.3.3 Threat Impact

The impacts of ransomware attacks are becoming increasingly consequential. Threat actors are now conducting these potentially destructive attacks against governments, hospitals, and critical infrastructure. Another recently implemented tactic is for the ransomware attacker to steal data from the organization and threaten to release that stolen data in order to further compel the victim organization to pay the ransom. For those organizations that choose not to 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 organization's systems, and the organization has chosen not to pay the ransom and now must deal with both the destruction of their systems as well as the public release of citizen Personally Identifiable Information (PII).

2.3.4 Vulnerability

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

Ransomware attackers have also utilized the email attack vector to deliver fictitious invoices and malware-laden documents to recipients. If received by the right person, a fictitious invoice from a supply chain partner might effectively get 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 organization's network and IT environment, or they can download ransomware to conduct the attack against that first compromised system. For example, new AI solutions are being delivered to existing systems through partner and software updates. It can be difficult to assess the risks of these new AI systems. If corrupted with malicious software, an AI system may be used to hijack existing systems to deploy ransomware.

It is very common to find that an organization that has a ransomware event had systems that were unpatched, or the delivery vector was novel and unrecognized. 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 voicemails are specifically coordinated to target a few people within the government contractor organization. The voicemail notifies the targets to expect the email. The email contains a URL to a web page designed to look like a legitimate conference webpage. The government contractor target opened the email and clicked on the URL, which contained malicious code that infects the target's computer thus giving the threat actor their first electronic foothold within the victim's 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 of whether the victim

organization pays the ransom or not, the victim organization is compelled to conduct a full incident response (IR) 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 states that it 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 IR was being conducted and the restoration and recovery were being conducted, the organization had to operate on manual or temporary systems.

2.3.8 Potential 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 Data Integrity: Recovering from Ransomware and Other Destructive Events
- Disaster Recovery – SP 800-34 Rev. 1 Contingency Planning Guide for Federal Information Systems
- Incident Response Planning – SP 800-61 Rev. 2 Computer Security Incident Handling Guide

2.4 Scenario: Removal Media Attack

2.4.1 Background

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

- Operation Buckshot Yankee

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

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

2.4.2 Threat Source

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

2.4.3 Threat Impact

Potential impacts include:

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

2.4.4 Vulnerability

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

2.4.5 Threat Event Description

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

The threat actor drops many USB drives, containing malware, into the parking lot of the supply chain vendor. The USB drives are labeled with the supply chain organization's logo, and the USB drives contain file objects that appear 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,[20] 48 percent of the distributed USB drives were inserted into the organization's computers.

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

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

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

2.4.6 Outcome

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

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

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

2.4.7 Organizational Units / Processes Affected

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

2.4.8 Potential Mitigating Strategies / SCRM Controls

The buyer organization, conducting this analysis, would evaluate:

- The extent to which potential supplier organizations protect themselves from removable media type attacks.
- The extent to which the organizations are connected electronically.
- The extent to which the supply chain organization has a security training program and mature security-focused software development and distribution practices.
- Internal security controls, such as micro-segmentation, so that such a compromised system would not be able to move electronically throughout the IT environment or communicate outside of the organization. Also, strict controls over the use of thumb drives, laptops, and other portable media should be maintained. These devices should be regularly scanned for malware.

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

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

2.5.2 Threat Source

Internal; non-malicious.

2.5.3 Threat Impact

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

Physical examples would be the lack of power or environmental support to expand a technical footprint within a data center.

2.5.4 Vulnerability

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

2.5.5 Threat Event Description

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

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

2.5.6 Outcome

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

2.5.7 Organizational Units / Processes Affected

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

2.5.8 Potential 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 that vendor system or network outages will have on the organization's operations.
- Assess the overall impact that vendor system or network outages will have on the vendor's ability to meet contractual requirements.

2.6 Scenario: Cybersecurity (Trusted Contractor)

2.6.1 Background

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

2.6.2 Threat Sources

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

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

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

Espionage is discussed as a component of supply chain risk, and it is described as a problem that costs the American economy hundreds of billions of dollars per year and puts national security at risk.

2.6.3 Threat Impact

Trusted contractors are a subsect of "insider threats." Insider threats have proven to be a major risk to organizations as they have access and opportunity, impeded only by proper motivations and effective risk management controls. An insider with bad motivations combined with inadequate security controls has an

opportunity to wreak havoc on an organization, or act as a saboteur. The impact can be exfiltration of IP, PII, and other sensitive restricted information. The other legs of the platform can also be impacted. An insider can detrimentally affect confidentiality of information, communications, and operations. An insider can also affect the integrity of information, communications, and operations. Such impacts from a trusted contractor, gone rogue, can be catastrophic to an organization, its employees, its customers, its partners, as well as the other parts of its entire ecosystem.

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

2.6.4 Vulnerability

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

2.6.5 Event Description

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

2.6.6 Outcome

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

2.6.7 Organizational Units / Processes Affected

All organizational units in an organization are vulnerable to and possibly affected by the threats and impacts of malicious trusted contractors. Moreover, a malicious contractor, as with other insider threats, can often move laterally within an organization to other organizational units. This movement can be physical or virtual. Virtual lateral movement may be accomplished by means of corporate networks, local area networks (LANs), cloud services, and other organizational resources available to authorized insiders.

2.6.8 Potential Mitigating Strategies / SCRM Controls

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

AI-based supply chain assistants can help rapidly identify past performance issues with a potential contract partner. In addition to the technical controls listed above, supply chain controls and mitigations should be implemented to manage the risk of a malicious contract worker. Some of these strategies and controls include using known and vetted suppliers of contract workers, performing background checks and reference checks on the contract worker independent of those done by the provider, and documenting and implementing legal and contractual controls on the provider, etc.

3 THREAT CATEGORY: INTERNAL SECURITY OPERATIONS AND CONTROLS

3.1 Scenario: Poor Access Control Policy

3.1.1 Background

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

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

3.1.2 Threat Source

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

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

3.1.3 Threat Impact

With the right kind of elevated privilege access, a malicious actor 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 IR investigations difficult or impossible due to the inability to trace back the activity. Thus, impact across a group of assets could be wider than the actual attack scope; if the company lacks proof that hosts or data were accessed, one might be required to assume that they were compromised due to breach notification (or similar) laws.

3.1.4 Vulnerability

While the network routes a relatively small amount of traffic, it does have access to a large amount of subscriber information that is maintained for the current infrastructure. The systems control access to sensitive user data, DNS function and routing of user traffic in, out, and through the legacy network. Legacy systems may be increasingly vulnerable to automated AI-driven decision making that could help malicious actors identify such systems, access them, and potentially exploit them in wider attacks.

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 actor has used them to gain access to the legacy network, where additional attacks can be sourced from. Integrating AI solutions into some legacy systems may increase bandwidth demands or require incompatible traffic and sharing protocols, which lead to resource contention and potential attack vectors.

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 Potential Mitigating Strategies / SCRM Controls

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

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

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

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

It is also recommended to implement restrictions on the rate of login attempts, concurrent login attempts, and lockout periods 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 actors 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 AI Scenario: Model Extraction Attack on LLMs[21]

3.2.1 Background

Building Large Language Models (e.g., OpenAI/GPT, Google/Gemini, META/LLAMA, etc.) requires an enormous amount of training data, and extraordinary computing and human resources. To give an example of their size, GPT-3 had 175 billion parameters. These LLMs can perform a wide variety of tasks such Question-Answering, Summarization, and Sentiment Analysis. What if an adversary does not want to build their model for a specific task (e.g., Question Answering) from scratch and instead wants to reverse-engineer an existing (i.e., target) LLM to build a surrogate model? Additionally, the adversary can use such a surrogate model to attack the target LLM with utmost efficiency.

3.2.2 Threat Sources

Any individual or entity with modest resources who wants to build a task specific model quickly for business or strategic advantage.

3.2.3 Threat Impact

The adversary will be able to perform a task as well as the original (i.e., target) model, thus effectively stealing the IP behind the original model. In addition, once a surrogate model is developed by the adversary, it can be used to stage more extensive attacks on the target model.

[21] https://atlas.mitre.org/techniques/AML.T0024.002

3.2.4 Vulnerability

The model extraction relies on repeated queries of the target LLM to capture the input-output relationships that can be used to build a surrogate model. LLMs typically do not have a way of deciphering the intention behind incoming queries and so they are exposed to such an attack.

3.2.5 Threat Event Description

There are four phases to the model stealing attack.

(1) *Prompt design*. This involves a good understanding of what knowledge is to be stolen to accomplish a specific task. The next step is a careful crafting of prompts to gather the task specific LLM responses.

(2) *Data generation*. The collection of the prompts and their corresponding responses constitutes the adversarial dataset. Depending on the specific implementation (e.g., API based interface to the LLM), this step can be automated and/or distributed over many LLM-clients to avoid limits on incoming queries for each client or the detection of adversarial intent.

(3) *Surrogate model creation and validation*. Using the dataset created in Phase 2, the adversary builds a much smaller local model with modest resources and validates the surrogate model against the target LLM using benchmark datasets.

(4) *ML attack against the target LLM*. The surrogate model allows an adversary to perform unrestricted experimentation to discover exploits and vulnerabilities against a target LLM and the ability to conduct adversarial attacks on the surrogate model prior to executing the similar attacks against the target LLM in production.

These steps are explained in detail in a recent paper by Birch et al.[22] While implementing such an attack requires technical skills, they are not out of the common pool of skills available in the data science communities.

3.2.6 Outcome

The major consequence of such an attack is that the knowledge captured in the original model from the target LLM to perform a specific task is now available as a surrogate model to an adversary. This can be used for various purposes such as gaining competitive advantage and planning future attacks on the target LLM with more detailed knowledge acquired from the surrogate model. Additionally, despite the fact that this scenario utilizes LLMs, similar model-stealing attacks can be performed against the predictive deep learning models for narrow tasks.

3.2.7 Potential Mitigating Strategies / SCRM Controls

Due to the nature of how the knowledge is extracted from a black box model, this attack can be performed without any knowledge on the detailed implementation of the target LLM. One option for the target model owner is to limit the number of queries from a single user to hinder the collection of enough training data to create a surrogate model. To the extent the adversary can coordinate the attack with multiple user identities not easily traceable to each other, this is a difficult attack to mitigate.

[22] L. Birch et al. "Model leeching: An extraction attack targeting LLMs." (2023).

3.3 Scenario: Devices that Do Not Auto-Update Firmware (Embedded Spinal Cord Stimulator with a Hand-Held Controller)

3.3.1 Background

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

3.3.2 Threat Source

Unauthorized individuals could potentially access the device and change the settings 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 activate the device and receive the benefits provided for pain management.

3.3.3 Threat Impact

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

3.3.4 Vulnerability

Hand-held devices do not auto-update and require a live conversation with a help desk. In some instances, a trip to the patient's health care provider is necessary to update the firmware and sync the device.

3.3.5 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.

3.3.6 Outcome

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

3.3.7 Potential Mitigating Strategies / SCRM Controls

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

- Make regular appointments with healthcare provider to ensure the device is working properly.

3.4 Scenario: Mishandling of Critical or Sensitive Information

3.4.1 Background

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

3.4.2 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.

3.4.3 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.

3.4.4 Vulnerability

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

3.4.5 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.

3.4.6 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.

3.4.7 Potential Mitigating Strategies / SCRM Controls

Data management policies can have a broad range of useful steps that could prevent such risks in this scenario. All data should be classified according to its intended use, who can access it, and if or how it can be shared. In addition, data tags could be set according to whether it is Public, Limited Release, or 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.

3.5 Scenario: Products and Services Mishandling of Critical or Sensitive Information

3.5.1 Background

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

3.5.2 Threat Source

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

Access to these new storage areas was expected to only be possible through secure network slices provisioned by AstroNet.

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

3.5.3 Impact

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

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

3.5.4 Threat Event Description

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

3.5.5 Outcome

Although a fundamental premise of network slicing is that the network is carved into discrete, self-contained units, in many cases each slice may still leverage network-wide resources. As such, while unique security parameters can be defined for network slices individually, there are security parameters that should be applied to shared network resources. As such, the opportunity exists for incongruences to exist between a network-wide security policy and a security policy that should be applied to an individual slice.

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

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

3.5.6 Potential Mitigating Strategies / SCRM Controls

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

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

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

3.6 Scenario: Lack of Asset Visibility and Vulnerability Exploitation

3.6.1 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.

3.6.2 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.[23]

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.[24]

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 7 percent in 2018, down 1 percentage point from 2017.

3.6.3 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 should be assumed that maximum impact is possible to the organization or assets.

3.6.4 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.

3.6.5 Threat Event Description

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.

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,[25] 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,[26] 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.[27] In this scenario, an attacker could exploit software vulnerabilities to gain administrator rights, enabling them to create fraudulent IDs, disable door locks and alarms, access sensitive authorized user data, and delete video footage.

3.6.6 Outcome

Building management contractors, just like IT managers, should consider cyber risk associated with all computer systems and networks within their scope of responsibility. Often, building management systems and

[23] "State of Security Response," Ponemon/ServiceNow, 2018.
[24] Primary Research, Tenable Vulnerability Intelligence.
[25] "Tenable Research Discovers Vulnerability in Zoom that Could Lead to Conference Hijacking," Tenable, 2018.
[26] "Multiple Zero-Days in PremiSys IDenticard Access Control System," Tenable, 2019.
[27] "Tenable Research Discovers "Peekaboo" Zero-Day Vulnerability in Global Video Surveillance Software," Tenable, 2018.

CCTV are outside the control or purview of organization IT departments. A disciplined vulnerability management program, by which the organization can track, assess, and remediate known vulnerabilities across their entire attack surface in a timely manner, before they can be exploited is necessary.

3.6.7 Potential Mitigating Strategies / SCRM Controls

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

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

3.7 Scenario: ICT Devices with Default Passwords

3.7.1 Background

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

3.7.2 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)
- 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.[28] In 2018, it was reported that less than 8 percent of analyzed breaches were due to weak or default credentials.[29] 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.

3.7.3 Threat Impact

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

3.7.4 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.

3.7.5 Threat Event Description

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

3.7.6 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.

3.7.7 Potential Mitigating Strategies / SCRM Controls

[28] Trustwave, "2014 Trustwave Global Security Report," 2014.
[29] Trustwave, "2018 Trustwave Global Security Report," 2018.

- As part of good cyber hygiene practices and to reduce the risk of security breaches through default credentials which have been left configured on network devices, it's best to implement a process to change the passwords, and if possible, account names when new equipment is installed.
- Identify software and systems that are likely to use default passwords. Regularly perform vulnerability network scans to identify systems and services using default passwords. Additionally, utilize good password management, including:
    - Change Default Passwords - Change default passwords as soon as possible and absolutely before deploying the system on an untrusted network such as the Internet. Use a sufficiently strong and unique password. See the United States-Computer Emergency Readiness Team (U.S.-CERT) Security Tip ST04-002 and Password Security, Protection, and Management for more information on password security;
    - Use Unique Default Passwords - Vendors can design systems that use unique default passwords. Such passwords may be based on some inherent characteristics of the system, like a Media Access Control (MAC) address, and the password may be physically printed on the system;
    - Use Alternative Authentication Mechanisms - When possible, use alternative authentication mechanisms like Kerberos, x.509 certificates, public keys, or multi-factor authentication. Embedded systems may not support these authentication mechanisms and the associated infrastructure;
    - Force Default Password Changes - Vendors can design systems to require password changes the first time a default password is used. Recent versions of DD-WRT wireless router, Linux-based firmware operate this way; and
    - Restrict Network Access - Restrict network access to trusted hosts and networks. Only allow internet access to required network services, and unless necessary, do not deploy systems that can be directly accessed from the Internet. If remote access is required, consider using Virtual Private Network (VPN), SSH, or other secure access methods and be sure to change default passwords.
- Vendors can design systems to only allow default or recovery password use on local interfaces, such as a serial console, or when the system is in maintenance mode and only accessible from a local network.

3.8 Scenario: Incorrect Privilege Settings, Authorized Privileged User, or Administrator Erroneously Assigns User Exceptional Privileges or Sets Privilege Requirements on a Resource Too Low

3.8.1 Background

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

3.8.2 Threat Source

Access controls that define specific sets of privileges linked to individuals are a fundamental security practice. However, these same principles 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.

3.8.3 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 IR 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.

3.8.4 Vulnerability

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

3.8.5 Threat Event Description

Acme Packet is a midsized manufacturing company that 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 that 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.

3.8.6 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. It should be noted that new AI solutions can automate the discovery of APIs and system assets that could be used as an attack vector through privilege escalation.

3.8.7 Potential Mitigating Strategies / SCRM Controls

- Conduct a security review of all users' physical and system access, and adjust user access to least privileged access, the minimum access needed to perform the job.
- Establish an ISP based off industry standards and best practices.

- Deploy a Privileged Access Management (PAM) system for monitoring and protection of super user accounts. This is one of the most important aspects of Identity and Access Management (IAM), and cybersecurity at large today. With a PAM solution in place, an organization can dramatically reduce the risks discussed above.
- The Best Practices for PAM utilize the Four Pillars of PAM. Gartner[30] outlines key challenges and makes clear recommendations that emphasize the critical role of people, processes, and technology in effectively mitigating PAM risk and making purchase decisions, including:
    - Track and Secure Every Privileged Account;
    - Govern and Control Access;
    - Record and Audit Privileged Activity; and
    - Operationalize Privileged Tasks.
- Establishing a Zero Trust Architecture (ZTA) or similar protocols where all resource authentication and authorization are 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.

3.9 AI Scenario: Excessive Agency in an Autonomous / Automated / AI System[31]

3.9.1 Background

AI solutions are becoming more integrated with business APIs over time as options to interface with other systems provide greater functionality. In many cases, the decisions on which APIs to call, and in which combination, are being made strictly by the AI. Excessive Agency occurs when too much authority has been given to the AI/LLM application to determine how a business process may be performed. Providing AIs with Excessive Agency can result in unexpected or unintended results in business processes. Further, malicious actors can target components that can be "tricked" through a series of surreptitious prompts that results in unauthorized system access or inappropriate API calls.

3.9.2 Threat Sources

Threats can be present within Software as a Service (SaaS) components that employ AI/LLM solutions. In addition, SaaS components that do not offer AI/LLM support today may be augmented to include new functionality that allows for dynamic processing based on LLM input. Threat actors may recognize that the system is making decisions based on LLM input and attempt to break the guardrails established by AI engineering using malicious prompts. Excessive Agency can be integrated into new product versions, implemented organically or integrated into existing partner applications that are upgraded to use AI/LLM solutions. AI-based solutions that fall prey to Excessive Agency can become part of the supply chain through partner integrations and product upgrades.

3.9.2 Threat Impact

Providing access to an AI to use APIs or directly integrate into business processes can cause significant damage if the right oversight and guardrails are not implemented. This can result in privilege escalation, unauthorized access to system processes, unexpected results, or malicious business processing.

---

[30] https://www.gartner.com/en/documents/3899567
[31] https://owasp.org/www-project-top-10-for-large-language-model-applications/

Autonomous AI agents that are granted access to business APIs may use those APIs in ways that were never tested or intended. This can result in degraded performance, system outages, and unexplainable business results.

3.9.4 Vulnerability

Business processes and APIs have traditionally been implemented with specific approved tasks and sequences. Excessive Agency occurs in an AI solution that has been incorrectly trained or fails to correctly implement the proper "guardrails" that serve as safety mechanisms to ensure that the AI solution operates within expected business and technical boundaries. These vulnerabilities can be passively introduced into your organization's operating environment when SaaS and software components are enhanced using AI/LLM solutions.

3.9.5 Threat Event Description

Complex SaaS-based ERP and Customer Relationship Management applications are racing to integrate AI solutions to provide dynamic business processing and autonomous agents. Upgrading current systems should be assessed and evaluated in the context of these new solutions. Secure, well understood, business systems can become compromised by simply migrating to a new version of AI-enabled software that results in Excessive Agency through integrated AI solutions. For example, new AI-based functionality may use existing system functions that overwrite existing data, modify existing data schemas, or access internal tools that result in privilege escalation and external access to sensitive data.

AI/LLM solutions that have been granted privileges to synthesize new processes and responses to changing business dynamics can inadvertently overload system processing in unexpected ways resulting in a virtual (or intended) DNS attack.

3.9.6 Outcome

AI solutions that have been granted Excessive Agency can present a myriad of cascading business and cybersecurity issues including:

- Privilege escalation due to unexpected system access
- Lost data caused by insufficient "guardrails"
- Access to sensitive system information
- Performance problems due to unpredicted utilization and system load

3.9.7 Potential Mitigating Strategies / SCRM Controls

Take the following steps whenever upgrading to AI-enabled components, new partner integration projects, or new internal AI solutions where the AI has the authority to make changes to business processes:

- Evaluate all new SaaS, system, and software procurements for AI/LLM integration points.
- Understand the lineage and reputation of SaaS-based solutions to ensure that AI components will include the proper "guardrails" prior to implementation.
- Thoroughly test AI systems that have been granted access to business system APIs, especially partner systems. Partner systems are part of the supply chain and, with the advent of AI, can affect your upstream processing.
- Ensure that APIs and system functions are locked down internally and employ strict authorization controls before procurement of AI-based solutions.

- Increase monitoring of AI/LLM solutions that have been provided liberal access to business systems and APIs. Monitor existing partner and supplier interfaces for potential malicious invocation and maliciously trained components.
- Log all prompts (obfuscate PII) that invoke system functions to ensure model accuracy and reliability. This is useful when obtaining supplier support and identifying potential malicious activity in supplied components.

3.10 Scenario: Poor Products and Services Access Control Policy

3.10.1 Background

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

3.10.2 Threat Source

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

3.10.3 Impact

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

3.10.4 Vulnerability

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

3.10.5 Threat Event Description

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

Threat actors using AI to build and automate malicious code target PCI traffic, as well as other sensitive information. AI could be designed to identify different types of network traffic, assess its value, and redirect valuable data to external servers for further exploitation. New routers or any new networked technology represents a potential new addition to an attack surface that may already be familiar to threat actors. Acting as

a force multiplier, AI tools could be designed by smaller groups of threat actors, leaving a smaller technical footprint used in identifying and neutralizing nefarious activity.

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

3.10.6 Outcome

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

- Some equipment is accessible directly from the enterprise or an outside network, not via a firewall or DMZ;
- User accounts are not uniquely identifiable, reviewed, or changed;
- User sessions are not controlled and are 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 quite possible. In addition, other defenses or mitigations set up elsewhere in the network could be negatively impacted or changed from within.

3.10.7 Potential Mitigating Strategies / SCRM Controls

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

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

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

Enforcing strong password selection, password aging (which requires 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 from obtaining sensitive data) provide additional security.

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

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

3.11 AI Scenario: Unreliable Source Attribution

3.11.1 Background

Machine learning-based AI applications train on data to generate output. Source attribution occurs when it is possible to gather what training data was used to generate some or all of the output. However, if learning models produce output without valid and sufficient explanation to understand what sources were used, it can be a security problem.

3.11.2 Threat Sources

Threat sources could be either external or internal. External threat actors could add or modify existing sources to introduce pointers to malicious content. Internal threat actors can accidentally add approximations in code that generate output that diverge from the original source data.

3.11.3 Threat Impact

The inability to attribute output to their respective sources can potentially reduce user trust by making it harder to understand the logic behind an output. It can also make it harder for auditors to perform a thorough analysis in cases where the output from the system has been manipulated.

3.11.4 Vulnerability

Without proper attribution, it is hard to determine if insecure data has been injected or what kinds of output might be at risk, especially if the model trains on data that is continuously updated. Furthermore, it is easier to manipulate output data. If users cannot link the output to a reliable source from the training data, it is easier for attackers to manipulate the output and users of the system in turn. This is especially true for models that rely on publicly accessible data, like news articles, blogs, and other online material. There have been several recent cases where model output is based on unreliable sources,[32] often satirical essays.

3.11.5 Outcome

When AI models are used on their own or are used to create additional models, lack of valid source attribution can lead to unreliable results. It can also affect downstream models by introducing features that are not accounted for. An example of this is AI hallucination[33], where model output can be completely fabricated data, with no citations that lead to valid sources.

3.11.6 Potential Mitigating Strategies / SCRM Controls

[32] https://www.theguardian.com/world/2024/feb/29/canada-lawyer-chatgpt-fake-cases-ai
[33] https://qz.com/google-search-ai-overview-hallucination-1851499664

Building robust AI model source attribution controls is an area of active research. Acquiring models from vendors that have strong source attribution and data lineage tracking can help avoid inclusion of maliciously tainted data or components. There are several proposed mitigation measures, which can have varying degrees of success. Source attribution is important for managing supply chain risks in models, especially when they are part of critical infrastructure. Below is a non-exhaustive list of approaches that have been recommended for better source attribution:

- Watermarking the training data used can be useful in detecting which responses are generated from internal training data. Look for AI solutions that provide some level of watermarking.
- Building statistical analysis tools that can infer if output is derived from the training data or not by analyzing how distinct expected outputs are, as opposed to unattributed misinformation. This is more helpful in case of supervised learning models.
- For models that are built on top of existing machine learning models, reviewing the sources for the underlying model might be helpful.

3.12 Scenario: Products and Services Lack of Asset Visibility and Vulnerability Exploitation

3.12.1 Background

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

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

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

Many high-profile incidents could have been prevented through better asset management and cyber hygiene practices and processes. Fifty-seven percent of enterprises that experienced a breach in the past two years state that a known, unpatched vulnerability was the root cause.[34]

3.12.2 Threat Source

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

3.12.3 Impact

An exploit of a known, unpatched vulnerability in the software products of a financial services firm could result in the theft of financial, credit, or other sensitive data for customers and individuals. This impact can be

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

magnified significantly if the firm lacks visibility into the software libraries, frameworks, and components used in its products.

According to a survey conducted in 2018 by the Ponemon Institute[35], 56 percent of organizations had a breach that was caused by one of their vendors. For example, the Ripple20[36] vulnerabilities caused complications in the OT world as the Treck stack has been used in hundreds of products over the years, and numerous high severity vulnerabilities were found in the library. If an enterprise is not patching vulnerabilities in components used in their products, they are opening the attack surface area for all their customers.

3.12.4 Vulnerability

The vulnerability in this scenario is that a software or hardware vendor ships a product to a customer that lacks visibility or knowledge of which open-source or proprietary components are utilized in their products and how these components are utilized. In addition, the lack of the secure development lifecycle and adequate vulnerability response process elevates the risk of vulnerabilities being discovered in its products (post release) as a result of insecure design and coding practices. Especially with new AI capabilities being delivered as updates to existing SaaS and partner solutions, it's important to realize that these new capabilities are prime targets for maliciously tainted components.

3.12.5 Threat Event Description

An attacker develops or utilizes existing exploit code to attack a newly discovered (or known, unpatched) vulnerability in a widely deployed open-source library software component. An attacker could utilize this exploit to perform a remote code execution against an organization that has failed to mitigate the vulnerability. This threat is further exacerbated if the enterprise customer lacks visibility into which components are used in the software products it acquires, thereby putting all of its customers at risk.

3.12.6 Outcome

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

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

3.12.7 Potential Mitigating Strategies / SCRM Controls

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

[35] https://www.ponemon.org/userfiles/filemanager/nvqfztft3qtufvi5gl60/
[36] https://www.cisa.gov/news-events/alerts/2020/06/16/ripple20-vulnerabilities-affecting-treck-ip-stacks

criticality, availability of workarounds, and whether there are exploits available for specific vulnerabilities during prioritization.

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

4.1 Scenario: Developmental Process of Hardware and Software

4.1.1 Background

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

Once compiled, this can reach megabytes of binary code.

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

4.1.2 Threat Source

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

4.1.3 Threat Impact

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

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

4.1.4 Vulnerability

Development tools and processes can introduce vulnerabilities into hardware and software products and services in a variety of ways, including unintentionally and intentionally. Unintentional vulnerabilities may be introduced when development tools are not configured for security, or when development processes lack adequate controls to identify and mitigate errors. Malicious actors may seek to intentionally introduce vulnerabilities by exploiting development tools in a variety of ways. Recently, malicious actors have targeted software supply chains by compromising servers issuing updates and patches to deployed software, enabling the attackers to transmit malware to hundreds of thousands of individual software copies and their users at

once.[37] 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 Potential 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 like govern access to development environments, and use change management tools to track identity, time/date, type of change, and other relevant information for all changes.
- Configure development tools, such as compilers, to secure settings.
- Adopt best practices for providing secure updates, including code-signing, and provide notifications to customers detailing the key information about the content of all updates.

4.2 AI Scenario: Compromise of MLOps – Process, Practices and Tools

4.2.1 Background

Compromise of MLOps is an attack on the process to curate and deploy an AI model. The complexity of the MLOps tools, techniques and processes make identifying adversarial attacks challenging. There are a variety of attack vectors that could be employed including:

- Adversaries may gain full "white-box" access to an ML model. This means the adversary has complete knowledge of the model architecture, its parameters, and class ontology.

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

- Attackers can use copycat models to simulate and exploit potential weaknesses or craft adversarial data to be used for exfiltrating sensitive data.
- Improper data curation and insufficient MLOps practices can adversely affect how a model is trained leading to vulnerabilities. Incorrectly trained models can be difficult to detect and can lead to aberrations in model behavior that expose sensitive information.

4.2.2 Threat Sources

Vulnerability exploits can be performed by hacktivists, cyber criminals and criminal organizations, or nation-state actors. The threat actor will compromise the integrity of the MLOps tooling, process, or practices at the site where the model is trained. Adversaries may exploit weaknesses in the cybersecurity practices of the organization to affect change to the MLOps processes which can be used as monetized vulnerabilities sold to subsequent threat actors.

4.2.3 Threat Impact

The adversary is attempting to manipulate, interrupt, erode confidence in, or degrade ML and associated business systems. This can lead to the victim organization wasting time and money both attempting to fix the system and performing the tasks it was meant to automate by hand. Attacks focus on degrading system availability or to compromise integrity by manipulating business and operational processes by directly affecting the MLOps processes and practices.

4.2.4 Vulnerability

Misconfiguration as part of the MLOps process used to deploy an AI application can provide access to sensitive credentials that were exfiltrated from the model and used in subsequent attacks. Sensitive information (e.g., PII or SPI) should be properly obfuscated or encrypted to prevent exfiltration or accidental disclosure.

Attackers can also setup shadow models to gain insight into weaknesses in the MLOps processes or tooling. These weaknesses can then be exploited by developing attack tools specific to a model's operational design.

Classical attack patterns that gain access to training data can also be exploited to change the MLOps processes or training data and cause arbitrary misclassification in the deployed model.

4.2.5 Threat Event Description

- Adversarial attacks can cause errors that cause reputational damage to the company of the translation service and decrease user trust in AI-powered services.
- Successful exploitation of insecure output handling vulnerability can result in XSS (Cross Site Scripting) and CSRF (Cross Site Request Forgery) in web browsers as well as SSRF (Server Side Request Forgery), privilege escalation, or remote code execution on back end system resulting in loss of data and further penetration into sensitive systems.
- Adversaries may introduce a backdoor into a ML model. A backdoored model operates as expected under typical conditions but will produce the adversary's desired output when a trigger is introduced to the input data. A backdoored model provides the adversary with a persistent artifact on the victim system. The embedded vulnerability is typically activated later by data samples that contain some triggering event. These can be very difficult to identify and mitigate since they are contained within the AI model and MLOps processes.

4.2.6 Outcome

Because these vulnerabilities are difficult to identify, are not surfaced by typical cybersecurity threat monitoring and are not manifested until after the system is deployed, threat actors are able to compromise the software through a variety of techniques including an inserted vulnerability or exfiltration of data within the model itself. The resulting effect on the code (and ultimately the end customer) can take a variety of forms, from being an inconvenience, to impacting system performance, to the loss of data.

Sensitive Information Disclosure: LLMs may inadvertently reveal confidential data in its responses, leading to unauthorized data access, privacy violations, and security breaches into neighboring business systems.

4.2.7 Potential Mitigating Strategies / SCRM Controls

Employ these techniques and practices to effectively implement oversight of MLOps practices and tooling:

- Use techniques to make machine learning models robust to adversarial inputs such as adversarial training or network distillation as part of the MLOps pipeline to protect your downstream consumers.
- Automate MLOps deployment with governance checkpoints that include tracking and approval workflows to ensure process task integrity.
- Use an ensemble of models from different suppliers for inference to increase robustness to adversarial inputs. Some attacks may effectively evade one model or model family but be ineffective against others.
- Preprocess all inference data to nullify or reverse potential adversarial perturbations.
- Detect and block adversarial inputs or atypical queries that deviate from known benign behavior, exhibit behavior patterns observed in previous attacks or that come from potentially malicious IPs. Incorporate adversarial detection algorithms into the ML system prior to the ML model.
- MLOps tooling, practices, and processes should embrace proven cybersecurity practices and preventions such as least privileges, multi-factor authentication and monitoring, and auditing Assess the lineage and background of MLOps tools and vendors to ensure they have been properly vetted and are using the latest trained models.

4.3 Scenario: Faulty Third-Party Components

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

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

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

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

4.3.1 Background

A shipped system in operation in the field has a component from an outside supplier that is determined to be faulty and in need of update/replacement. For hardware items this would include physical swapping of smallest replaceable unit. For software items this would be an update via the items update mechanism.

For some operational technologies that are not networked, the software update may require physical access to the unit to connect to the device with an upgrade unit or swapping out a memory device with the new software.

4.3.2 Threat Sources

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

4.3.3. Threat Impact

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

4.3.4 Vulnerability

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

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

4.3.5 Event Description

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

4.3.6 Outcome

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

4.3.7 Organizational Units / Processes Affected

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

mitigations could have been put in place while waiting for the firmware patches to fix the faulty software components.

4.3.8 Potential Mitigating Strategies / SCRM Controls

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

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

4.4 Scenario: Third Party Component Security Issue

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

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

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

For prohibited third-party software components, if developers are unaware of their use, no remedial actions are taken, leaving its customers exposed to the consequences of the prohibited component.

4.4.1 Background

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

4.4.2 Threat Sources

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

4.4.3 Threat Impacts

The impact on Pelican State Power from these vulnerabilities allows an attacker to leverage various attacks, such as executing arbitrary code over their network. This would cause control systems in their electric generating stations to execute commands that would either shut down electric generators, or speed them up. Either way, it would cause severe damage to the generators in terms of either destroying the equipment or

causing explosions rendering the generating station unusable and causing wide-spread blackouts in their service territory. These massive generators are custom built, and to replace them requires a lead time of several years.

4.4.4 Vulnerability

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

4.4.5 SDLC Event Description

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

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

4.4.6 Outcome

The heat is oppressive and soon customers are inundating Pelican State's call centers wanting to know when service will be restored. There is no hope to restore service for several years now until new massive generators can be built and delivered. Neighboring electric utilities can offer no assistance as their systems are already strained to capacity due to the current heat wave. Meanwhile, currently, and for the foreseeable future, air conditioners stop running, no gas can be pumped, ATMs will not work, traffic signals are inoperative, and all cash registers are dead.

4.4.7 Organizational Units / Processes Affected

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

4.4.8 Potential Mitigating Strategies / SCRM Controls

Request all of Pelican State's suppliers to provide a BOM for software and hardware of systems they deliver which would provide them with the ability to identify which generating stations had the prohibited component.

This would have allowed them to quickly determine the extent of the problem and give additional lead time to find a replacement for the components.

Keeping apprised of hardware and software threats by subscribing to such warning sites as ERAI, and if possible, GIDEP to stay informed on the latest known hardware threats would have given Pelican State Power additional time to find replacement parts for the AXIOM-3 component (ERAI has the world's largest database of suspect counterfeit and nonconforming electronic parts).[38]

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

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

[38] ERAI's Nonconforming Parts Photo Database

Using NIST SP 800-30, we worked through the impact assessment, and we have come to the following assessment.[39]

Type of Impact	Impact Assessment	Notes
Harm to Operations	Low-Medium	An insider threat can have limited impact depending on their limited role and accesses. This tends to be limited for most low to midlevel employees due to maturity of processes, limited roles, and layers of oversight. Some decisions or actions may require management oversight.
Harm to Assets	Low-Medium	The low to mid-level employee is limited to how they access facilities and are limited in their information technology assets accesses. They can willfully click on malicious attachments or files in emails, but systems are geared to monitor and address such a scenario. This insider could damage systems or components, but given oversight, separation of roles, monitoring of processes and feedback from customers, impact should remain low in most cases.
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 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 Nations	Very Low	Most companies have limited to no impact to national security. This is by design for most sensitive government programs' concept of operational security. For programs that have limited impact to possible national security, additional measures are taken to limit the opportunity for impact or the impact itself. Company processes would limit who has knowledge of any processes or components that could have an impact national security.

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

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 Potential Mitigating Strategies / SCRM Controls

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

Potential Mitigating Strategies could include:

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

5.2 Scenario: New Vendor Onboarding

5.2.1 Background

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

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

5.2.2 Environment

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

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

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

5.2.3 Threat Impact

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

Type of Impact	Impact Assessment	Notes
Harm to Operations	Low	American Systems Co. will have personnel at Chips Inc. to monitor a production run and disposal of any over production. Logistical shipment tracking is in place, and access to data is removed when the production run is over.
Harm to Assets	Low	Low impact due to limited access to IP and the requirement of encrypted data at rest and in transit.
Harm to Individuals	Very Low	There is no personal information shared during this agreement.
Harm to 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 Nations	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 IP. They will have unique access to supply/demand data as they will know how much product American Service Co.'s buys and where the company requests shipments to be delivered. Since Chips Inc takes care of shipment and delivery of the products, they have exceptional knowledge of the processes that American Service Co's to receive, integrate, and support the products they make.

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

5.2.5 Potential 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.

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 POCs training to identify what data and types of data to share with Chips Inc.
- Agree to security measures for transmission, encryption, storage, retention, destruction, and required paperwork of intellectual property shared with Chips Inc.
- When American Service Co. decides to utilize support services from TechServices, American Service Co. can request TechService employees have a background check before being allowed to perform work. The same request can be made for Chips Inc. employees that interact with American Service Co.
- American Service Co. should monitor the financial performance of Chips Inc. on a quarterly or bi-annual basis to monitor for changes in the company's financial performance or leadership.

References:

- CMU National Insider Threat Center – Common Sense Guide to Mitigating Insider Threats
- ISO 27002

- NIST 800-53 rev 4
- Insiderthreatdefense.us

5.3 Scenario: Threats WS – Insider Category – Staffing Firms Used To Source Human Capital

5.3.1 Background

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

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

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

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

5.3.2 Threat Source

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

5.3.3 Threat Impact

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

Type of Impact	Impact Assessment	Notes
Harm to Operations	Low-Medium	An insider threat can have limited impact depending on their limited role and accesses. This tends to be limited for most low- to mid- level employees due to maturity of processes, limited roles, and layers of oversight. Some decisions or actions may require management oversight.
Harm to Assets	Low-Medium	The low- to mid-level employee is limited to how they access facilities, are limited in their information technology assets accesses. They can willfully click on malicious attachments or files in emails. But systems are geared to monitor and address such a scenario. This insider could damage systems or components, but given oversight, separation of roles, monitoring of processes and feedback from customers, impact should remain low in most cases.
Harm to Individuals	Low	There are few roles at the low- to mid-level that involve the handling of personal information of employees or customers. Mature processes, security controls and monitoring are essential to mitigating impacts. Contractors hired for these limited roles go through background checks and monitoring. These roles tend to have more extensive management oversight and auditing.
Harm to Organizations	Very 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 Nations	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 opportunity for impact or the impact itself. Company processes would limit who has knowledge of any processes or components that could have an impact on national security.

5.3.4 Vulnerability

The vulnerability in this example involves the partnership with a third-party staffing firm that is instrumental in sourcing candidates for employment, and the staffing firm can be leveraged by a nation-state to manipulate the recruitment and candidate sourcing to a company. In many of these cases, the staffing firm has offices

around the world, while also having a recruitment/candidate database that can be accessed and modified by the staffing firm's international associates, with the intent of strategically planting insider agents into the recruitment process of a company.

Background checks can be effective for preventing the hiring of known malicious characters, but they may not detect willing insider threat agents. While it is important to maintain controls that detect and stop insider threat activity, preventing the hiring of an insider threat agent can help mitigate this risk. This requires the adoption of SCRM controls at staffing firms. Staffing and search are often augmented with AI. These AI Models integrated into existing HR systems to match candidates or contractors could be manipulated by insider threat actors to increase the chance they are presented as a top contender.

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 Potential Mitigating Strategies / SCRM Controls

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

Potential Mitigating Strategies could include:

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

5.4 Scenario: Contractor Compromise

5.4.1 Background

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

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

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

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

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

5.4.2 Threat Source

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

5.4.3 Threat Impact

Potential impact of insider threat may include:

- Compromise of the integrity of the enterprise and potentially, the extended supply chain.
- Compromise of the confidentiality of the enterprise and potentially, the extended supply chain (e.g., intellectual property theft).
- Monetary loss for the enterprise, and potentially the extended supply chain.[40]
- 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

[40] 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.

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 Potential Mitigating Strategies / SCRM Controls

Potential Mitigating Strategies could include:[41]

Development of an Insider Threat Program:

- Establish an insider threat oversight body that includes senior executives from the company's HR, security, legal, privacy, ethics, incident response team, IT, and public relations departments.
- Implement a formal insider threat incident response plan. This plan should include current and former employees, contractors, and business partners.
- Whenever possible, include staff members on the insider threat team who already have experience in dealing with insider threats and foreign intelligence threats, such as experienced counterintelligence staff. This selection of experienced staff is especially important for companies in which mishandling of classified, proprietary, trade secret, and intellectual property material could culminate in law enforcement action.
- Include the following components in an insider threat program: employee monitoring, awareness training, and identification and monitoring of critical assets and intellectual property. Technologies should include access controls, logging, data loss prevention, and host-based monitoring.
- Implement a program that tracks metrics to compare them to industry benchmarks (which may not exist yet) and assess the effectiveness of the program over time.
- Implement a behavioral monitoring program on an organization's network.
- Delivering insider awareness training to enterprise employees and contractors, would better enable the insider-contractor-employee to be identified.
- Integrated Risk Management Program – Development of an organization-wide approach to manage cybersecurity risk.[42]

Incident Response and Management:

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

[41] NIST'S Preliminary Examination of Insider Threat Programs in the U.S.A. Private Sector, 2013
[42] NIST Cyber Security Framework

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.[43]
- 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

[43] NIST Risk Management Framework

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

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

		assess, and manage supply chain risks.		ISO/IEC 27001 2013 A.15.1.1. 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

5.5 Scenario: Disgruntled Contractor

5.5.1 Background

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

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

Sally is upset that she might be losing her job and angry that she had to learn about this "through the grapevine," and even more angry that the management team of Services LLC does not regard her as an asset to the company. Sally no longer feels motivated to perform her work to the typical high standard she used to apply to herself. With three more months left on the current contract, Sally learns that the Integrator Firm has been awarded the new contract.

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

5.5.2 Threat Source

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

5.5.3 Vulnerability

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

5.5.4 Threat Event Description

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

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

5.5.5 Organizational Units / Processes Affected

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

5.5.6 Potential Mitigating Strategies / SCRM Controls

Potential mitigating strategies could include:

- Close review of employee network activities, especially during the time period in which an employee's relationship with a given organization will be ending soon
- Conduct an exit interview or increase communications with an employee who will be leaving or will be terminated to assess their frame of mind

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

5.6 Scenario: Supply Chain Software Build Library Poisoning

5.6.1 Background

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

In this scenario (Supply Chain, ICT Product, Insider) a malicious insider, within an ICT vendor organization modifies the software build process to insert malicious code into the product's software. As a result, the software image now contains harmful software that an adversary, or threat actor, can use to compromise the operations of businesses that rely on this ICT product.

The substituting of one software build element, for another, is the focus of this ICT Equipment Supply Chain Insider Threat. An example of this type of substitution occurred in 2017 when the official repository for the widely used Python programming language was tainted with modified code packages.[44]

[44] Dan Goodin, "Devs unknowingly use "malicious" modules snuck into official Python repository," ArsTechnica, 2017.

5.6.1 Threat Source

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

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

5.6.3 Threat Impact

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

An example of a successful software supply chain attack can be found in the ShadowPad attacks.[45]

5.6.4 Vulnerability

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

5.6.5 Threat Event Description

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

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

This activity of modifying the build process to ultimately insert vulnerabilities, or malicious software, can happen at various places along the supply chain. For example, the manufacturer of ICT network equipment might include software elements from the manufacturer of a system component. In the same manner, the manufacturer of the system component might also include software elements from a supplier of a chip on the system component. Each of these entities likely also includes open-source software as elements of their software builds.

5.6.6 Outcome

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

5.6.7 Organizational Units / Processes Affected

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

[45] SecureList, "Popular server management software hit in supply chain attack," 2017.

5.6.8 Potential Mitigating Strategies / SCRM Controls

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

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

5.7 Scenario: Agency Employee Compromised

5.7.1 Background

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

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

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

5.7.2 Threat Source

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

5.7 3 Vulnerability

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

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

5.7.4 Threat Event Description

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

5.7.5 Organizational units / Processes Affected

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

5.7.6 Potential Mitigating Strategies / SCRM Controls

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

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

Potential Mitigating Strategies could include:

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

6 THREAT CATEGORY: ECONOMIC

6.1 Scenario: Financial Strength of the Supplier

6.1.1 Background

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

6.1.2 Threat Source

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

6.1.3 Threat Impact

- Lack of adequate assessments and financial strength can lead to a supplier failure.
- Lack of financial strength can lead to bankruptcies.
- Acceptance of high-volatile risks can lead to financial/security-based compromises and threats.
- Compromise of the confidentiality, integrity, and availability of the organization and the supply chain.
- Lack of financial strength may lead to usage of dated software/hardware materials. This can lead to compromise of integrity of the supply chain and various threats noted in section 11.0.
- Declining revenues can pinch on cash flows and on labor requirements. Increasing price sensitivity may erode margins.[46]

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 Potential Mitigating Strategies / SCRM Controls

6.1.7.1 Transparency and collaboration are necessary for supply chain risk mitigation. Fifty-five percent of respondents to a recent Procurement Intelligence Unit survey said supplier insolvency would be the leading risk they face over the next 12 months. The key is to see potential problems, such as trends indicating a

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

company may be close to being insolvent before they arise and when an organization still has time to address the issues with the supplier.[47]

6.1.7.2 To mitigate monetary compromises, financial risk assessments require evaluation of all financial statements. Understanding a supplier's financial health requires a deep dive into the supplier's financials to see how several factors have changed over a period. For example, a supplier's receivables may be growing, but that could mean its credit and collection standards are weak.[48]

6.1.7.3 It's important to have internal metrics for the Chief Information Security Officer to conduct predictive analytics of the economic viability of the organization. Cross communication amongst the technology and finance organizations are needed when considering supply chain risk.

6.1.7.4 Understanding the financial position of your suppliers can help decide on the need for changes, mitigation strategies, or discussions on how you can help or advise suppliers on improving their operations. Reviewing financial reports from public companies, looking at reports from organizations like Dun & Bradstreet, or having a one-on-one personal discussion and review can also help. A close personal relationship with suppliers will also help mitigate risk.

6.2 Scenario: Information Asymmetries

6.2.1 Background

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

6.2.2 Threat Source

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

6.2.3 Threat Impact

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

6.2.4 Vulnerability

Lack of information or the partial gathering of information negatively affects the customer.

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

[47] "Supplier Financial Risk: Health Assessment Report," Rapid Ratings.
[48] Ibid.

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 Potential 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.[49]

A major oversight in many supplier risk management frameworks is the supplier's optimization of technology. Cross communication amongst the technology and C-suite, strategy, and finance sectors are very important for this process to be successful.

- Customer organizations should leverage technology when developing and implementing a supplier/customer relationship. Technology enables companies to standardize and streamline their processes for managing and mitigating vendor risk. It facilitates a shift from reactive to proactive risk management, and enables a forward-looking vendor governance program which, in turn, strengthens compliance.

One of the most important controls in risk management is legal and contractual protection. Technology provides the ability to store large volumes of vendor contracts, documents, service-level agreements, clauses, and non-compliance penalties in an integrated, structured, and easily accessible manner. This helps companies avoid legal liabilities, while also simplifying vendor onboarding.[50]

- 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.[51]
- 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

[49] "Managing Vendor Risk: A Critical Step toward Compliance," Metric Stream.
[50] Ibid.
[51] Ibid.

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

6.3.3 Threat Impact

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

6.3.4 Vulnerability

Lack of information or the partial gathering of information negatively affects the customer.

6.3.5 Threat event description

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

6.3.6 Outcome

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

6.3.7 Potential Mitigating Strategies / SCRM Controls

The U.S. Government should protect U.S. firms undergoing unfair competition. The Committee of Foreign Investments 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. By leveraging AI-powered insights, organizations can maintain continuity, optimize operations, and mitigate risks associated with supply chain disruptions arising from vendor ownership changes, promoting resilience and agility across evolving market dynamics.

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.[52]

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

[52] "Supply chain visibility software and solutions," IBM.

6.4 Scenario: Cost Volatility

6.4.1 Background

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

6.4.2 Threat Source

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

6.4.3 Threat Impact

- Potential implications to national security of the customer's end product.
- Potential compromise of the confidentiality, availability, and integrity of nation-states, organizations, and the supply chain.
- Lack of transparency, compliance, and security of the supply chain.
- Potential modification of hardware/software devices while in transit through the supply chain. As more software components are outsourced and volatile events occur, there are more opportunities for third-party tampering and the likelihood of malware or coding vulnerabilities being inserted.[53]
- Potential risks of financial loss for organizations of the supply chain.

6.4.4 Threat Event Description

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

6.4.5 Outcome

The ability for U.S. or other countries to invest in Chinese mines has been very limited to non-existent by the Chinese government. Chinese firms have sought to invest in the companies that use the rare earths to expand their ability to control more of the technology marketplace. These firms are backed by the Chinese government, and they are usually state owned or managed companies. They can use rare earths to affect prices outside the

[53] Victor Ng, "Mitigating against supply chain cyber risks," Cybersec Asia, 2019

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 Potential Mitigating Strategies / SCRM Controls

- U.S. companies need to work with businesses and countries outside of China to diversify their supply chains and lower supply chain risks. R&D needs to consider possible replacements for rare earths that are politicized. Supply chains can, likely at additional cost, work to obtain and seek out rare earths from other sources. Additionally, some rare earths can be obtained at a lower price if they are provided before they are separated but will incur some cost for the separation of the rare earths from their source. The goal from these mitigations will likely yield a diversified source of products that can obtain needed Neodymium at a more stable price structure than competitors. Competitors will likely have to add margin to deal with the multiple variables that will add excess market costs to their supply chain.
- Organizations within the supply chain should consider a "Security by Design" approach with products integrated with firmware management systems. For an added layer of protection, production codes are vetted, stored, and safeguarded to prevent hardware from being modified, unless the code is retrieved.[54]
- With a global supply chain, transparency (internally in the organization and throughout the supply chain) is difficult, but very important.

6.5 Scenario: Compromised Product Quality Testing by Suppliers Due to Financial Stresses

6.5.1 Background

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

6.5.2 Threat sources

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

6.5.3 Threat Impact

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

[54] Victor Ng, "Mitigating against supply chain cyber risks," Cybersec Asia, 2019

6.5.4 Vulnerability

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

6.5.5 Threat Event Description

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

6.5.6 Outcome

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

6.5.7 Organizational Units / Processes Affected

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

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

6.5.8 Potential Mitigating Strategies / SCRM Controls

- Customer organizations should leverage technology when developing and implementing a supplier/customer relationship. Technology can streamline processes for managing and mitigating vendor risk.
- Evaluating vendors regularly through surveys, assessments, and well-defined metrics such as key performance indicators (KPIs) and key risk indicators (KRIs) allows companies to drive continuous improvement in the risk management process.[55]
- Specify performance measures that define the expectations and responsibilities for both parties including conformance with rules and expectations from members in the chain. Such measures can be used to motivate the third party's performance, provide further transparency for the customer along the chain, or potentially penalize poor performance.

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

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

6.6. Scenario: Demand Volatility in the Supply Chain

6.6.1 Background

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

6.6.2 Threat Sources

Many factors contribute to demand volatility, including increased customer choices, product customization, rapid technological improvements, global competition and upstream supply fluctuations.[56]

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

The level of market turbulence has increased, bringing with it a reduction in the predictability of demand. According to various sources and economists, there are many reasons for this increased demand volatility.[57] Shorter life cycles, often driven by technology change, means that the risk of obsolescence increases. Higher levels of competitive activity lead to market disturbances to demand in many consumer markets (e.g., promotions, sales incentives, and the like). Increasing variety within product ranges further fragments demand and makes forecasts less reliable.

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

6.6.3 Threat Impact

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

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

6.6.4 Vulnerability

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

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

6.6.5 Threat Event Description

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

6.6.6 Outcome

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

6.6.7 Organizational Units / Processes Affected

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

6.6.8 Potential Mitigating Strategies / SCRM Controls

Pragmatic mitigating strategies may include:

- Maintaining an Inventory Buffer: Various economists recommend utilizing an inventory buffer strategy to manage the volatility in demand. While maintaining high levels of inventory can be expensive and retaining low inventory levels can negatively impact customer service, a middle ground can be found by building carefully planned inventory levels. This right balance of planned inventory buffers (safety stock) can be designed to cushion most of the shocks from the volatility in demand.[58] A more attractive alternative to inventory buffers in many industries is the use of capacity buffers. Through internal or external resources, capacity buffers provide more flexibility to companies to manage unexpected variations in demand. The inventory kept in stock has also been accumulated following adequate security test vetting and can mitigate the insertion of cyber threats.
- Collaborative Processes: Responding quickly to changes in demand requires fast information flow with the suppliers and partners. Collaborating with suppliers enable the end user to send forecast data to its suppliers faster, enabling the suppliers to plan their supply chains and respond faster to demand changes passed on. This process can help members in the supply chain ecosystem be ready to their best ability for how to prepare.

[58] Rajesh Gangadharan, "Supply Chain Strategies to Manage Volatile Demand," Supply & Demand Chain Executive, 2007.

6.7 Scenario: Economic/Trade Policies and the Global Supply Chain

6.7.1 Background

Economics and cybersecurity are increasingly intertwined. As this connectivity grows, however, so does exposure to the risks and costs of cyberattacks. Some proposed measures addressing cybersecurity risk are likely to constitute barriers to data flows and digital trade. These include data-flow restrictions and import restrictions on IT products, including software from countries or supply chains where cyber risk is high.[59]

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

6.7.2 Threat sources

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

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

6.7.3 Threat Impact

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

6.7.4 Vulnerability

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

6.7.5 Threat Event Description

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

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

Sudden changes in tariff barriers, trade rules, and the economic outlook have the potential to disrupt supply chains, considerably increase costs, etc. Within the supply chain, companies need to reconsider their sourcing locations and how they move physical goods across the organization.[60]

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

6.7.6 Outcome

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

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

6.7.7 Organizational Units / Processes Affected

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

6.7.8 Potential Mitigating Strategies / SCRM Controls

A digital supply chain provides real time visibility on the movement of goods across a company's supply and logistics networks, from product conception, to transit, to arrival at destination. For example, distributed ledger technology provides a single platform through which supply chain partners can share information and collaborate seamlessly. This technology facilitates teamwork, reduces misunderstandings, and expedites delivery timelines between businesses, logistics providers, and suppliers.

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 are typically 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.

[60] Peter Cunningham and Natasha Condon, "Trade Around the World: Mitigating Rising Supply Chain Risks in Evolving Economies,"

7.1 Scenario: Mid Supply Insertion of Counterfeit Parts via Supplier XYZ to Trusted/Vetted Vendor

7.1.1 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.[61]

7.1.2 Threat source

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

- Nation-state actors
- Cyber criminals
- Extended stakeholders utilized via Supplier XYZ
- Unvetted stakeholders in the extended supply chain, etc.
- Insider threats (any trusted individuals with access)
- Tampering during transit
- Market pressure and cost cutting (intentional)[62]

7.1.3 Threat Impact

- Pathway for new and easier software/hardware vulnerabilities
- Compromise of the confidentiality, integrity, and availability of the supply chain
- Potential implications to national security, espionage, etc.
- Lack of transparency and traceability through the supply chain
- Product failure and safety risks
- Regulatory and legal consequences
- Increased scrutiny and audits
- Impact on product warranties

7.1.4 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.

7.1.5 Threat Event Description

This inherited risk affects the transit and integrity of the trusted supply chain. Supplier XYZ can serve as an incognito vehicle for introduction of hostile elements that the vetted supplier may integrate within a product or

[61] Accenture, "Tracing the Supply Chain," 2018.
[62] Accenture, "Tracing the Supply Chain," 2018.

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.

7.1.6 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.

7.1.7 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.

7.1.8 Potential Mitigating Strategies / SCRM Controls

- Consider using automated supplier assessment systems and scrutinize a supplier's reputation, track record, and regulatory adherence, effectively assessing the risk of counterfeit parts infiltrating the supply chain. By identifying high-risk suppliers and applying additional scrutiny, automation helps mitigate the threat of mid-supply insertion while also enabling the detection of counterfeit parts on a large scale.
- 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 maintain operations in an era of accelerating cybersecurity threats.[63]
- Consideration of utilizing a zero-trust privilege approach to securing privileged access credentials.[64]
- Require and implement a set of key metrics/minimum baselines that are meaningful and relevant to the supply chain ecosystem. Well defined baselines can help assess the supply chain's security posture and build a widespread understanding of current level of cyber hygiene. Utilize these baselines for all third parties.
- Require and implement a minimum baseline for training and awareness on security for all stakeholders within the agency.
- Once a vendor (e.g., Supplier XYZ) is accepted in the formal supply chain, an assessment and corrective actions as appropriate should be conducted, possibly on site, to address any vulnerabilities and security gaps.
- Security requirements are included in every RFP and contract to ensure compliance by suppliers.
- It is critical for supply chains to establish provenance programs for all parts, components, and systems.
- Tight controls on access by service vendors are imposed. Access to software is limited to a very few vendors. Hardware vendors are limited to mechanical systems with no access to control systems. All vendors are authorized and escorted.

7.1.9 Relevant Controls

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

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 third-party Stakeholders.	CP-2, PS-7, PM-11	CIS CSC 17, 19 COBIT 5 APO01.02, APO07.06, APO13.01, DSS06.03 ISA 62443-2-1:2009 4.3.2.3.3 ISO/IEC 27001:2013 A.6.1.1
IDENTIFY	Governance (ID.GV):	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	PS-7, PM-1, PM-2, SA-2, PM-3, PM-7, PM-9, PM-10, PM-11	CIS CSC 19 COBIT 5 APO01.02, APO10.03, APO13.02, DSS05.04 ISA 62443-2-1:2009 4.3.2.3.3 ISO/IEC 27001:2013 A.6.1.1, A.7.2.1, A.15.1.1
IDENTIFY	Supply Chain Risk Management	Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess, and manage supply chain risks.	SA-9, SA-12, PM-9	CIS CSC 4 COBIT 5 APO10.01, APO10.04, APO12.04, APO12.05, APO13.02, BAI01.03, BAI02.03, BAI04.02 ISA 62443-2-1:2009 4.3.4.2

Function	Control/Name	Description	NIST SP 800-53 (REV. 4) RELATED CONTROLS	Informative References
				ISO/IEC 27001 2013 A.15.1.1. 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

Function	Control/Name	Description	NIST SP 800-53 (REV. 4) RELATED CONTROLS	Informative References
				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

7.2. Scenario: Sub-Organizational Unit Failure to Update Equipment

7.2.1 Background

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

7.2.3 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.

7.2.3 Threat Impact

Potential impact of failure to update equipment:

- Hardware/device modification
- Traffic sniffing[65]
- Device tampering and data spoofing[66]
- Corporate espionage
- DoS Attacks[67]
- Destruction of hardware

[65] 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.
[66] 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.
[67] 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).

Exploitation of vulnerabilities, including adversaries testing or probing systems with no specific end goal, could still lead to unintentional disruptions.

- Outdated equipment will contain old firmware that is probably vulnerable to known vulnerabilities such as Baton Drop and LeftoverLocals.
- Compromised Accounts: Compromised user accounts occurs when unapproved individuals or threat actors access a user's credentials or find another way to act on their behalf.
- Insufficient Encryption: Older equipment may lack modern encryption protocols.
- Weak Authentication Mechanisms: This can make it easier for attackers/threat actors to bypass security measures.

Integrity - Data loss and/or Corruption

- Inaccurate Data Handling - due to outdated equipment which may struggle with accurately capturing, storing or transmitting data.
- Lack of Real-Time Data - as technology develops, outdated systems may no longer support outdated systems which leads to delays in identifying and responding to potential issues.
- Limited Connectivity - older systems may be incompatible with modern connectivity standards.
- Technology Incompatibility - Integration Challenges, Software Compatibility Issues, and Inability to Adopt New Technologies.
- 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.

7.2.4 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.

7.2.5 Threat Event Description

This is a network category threat that business heads and Chief Financial Officers should 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.

7.2.6 Outcome

The objective of the threat actor can be network disruption, data theft, IP, and financial threats. That is, in broad categories, the actor objectives include:

- Espionage – Corporate or State-Sponsored with Political/Ideological Motives
- Data Manipulation – Altering Data (for financial gain or operational confusion or damage)
- Reputation Damage – Disgruntled Insider Threat Case
- Steal organizational network and computing resources (that is, include them in a botnet)

As with other threat scenarios, threat actors use the best available automation to achieve their objectives. Advances in automation, including AI and GenAI, can increase threat actor's capability to target outdated

systems or leverage their threat impacts to achieve their objectives (such as making believable manipulated data or managing stolen organizational computing resources in a botnet).

7.2.7 Potential 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.
- Diversification of suppliers such as using multiple suppliers to reduce or avoid a single point of failure; this is particularly important if the organization relies on more specialized hardware such as graphics processing units (GPUs).
- Use a mix of local and global suppliers to reduce risk of geopolitical issues and natural disasters causing a disruption within your supply chain.
- Technology and automation such as predictive maintenance by using AI to monitor equipment health in real time and predict failures prior to the occurrence.
- Automate the asset management and update processes to reduce manual intervention time.

Phased equipment retirement plan to include disposal and replacement strategies so everything is already incorporated into the lifecycle management plan.

SDLC:

- Creation of a secure embedded design and development lifecycle for hardware equipment.
- Example guidelines to consider for this mitigation strategy include:
    - Rely on stable software components
    - Secure coding guidelines should be specific for hardware related development and languages
    - Implementation of segregation of duties
    - Consideration of extra variable integrity validity checks on critical values

Refer to ENISA's Hardware Threat Landscape and Guide Report for more detailed guidelines.[68]

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 should 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.[69]

[68] Hardware Threat Landscape and Good Practice Guide | ENISA
[69] NIST Best Practices in Cyber Supply Chain Risk Management

Agencywide Compliance:

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

7.2.8 Relevant controls

Refer to NIST CSF Relevant Core Functions and Controls in table above in section 7.1.9

7.3 Scenario: Inclusion of Prohibited Component(s) in a Product

7.3.1 Background

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

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

7.3.2 Threat Event Description

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

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

7.3.3 Threat Source

The primary threat source is the adversarial nation-state that is wielding influence and control over a manufacturing company doing business in its country. Secondary and tertiary threat sources include the ACME Company, who did not remove these items from its inventory or disclose their component makeup to their

resellers. The reseller also becomes a threat vector by unwittingly facilitating the sale of these products to the government.

7.3.4 Vulnerability

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

7.3.5 Threat Impact

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

7.3.6 Organizational Units / Processes Affected

ACME Company's reputation may be impacted negatively. The reseller may suffer legal penalties, incur significant legal costs, loss of market-share, and be suspended or barred from doing business with the government.

Government users who purchased and used a product that contained these prohibited parts may be exposed to a nefarious cyberattack.

7.3.8 Potential Mitigating Strategies / SCRM Controls

Potential mitigating strategies could include:

- Require disclosure of component parts and their provenance.
- Consult with legal counsel and conduct sufficient due diligence prior to making a legally binding representation.
- Examine the product/conduct product testing prior to installation and use.
- Source parts from trusted companies doing business in locations at low risk of adversarial foreign ownership, influence, or control.
- Establish robust processes to vet supply chain partners.

7.4 Scenario: Inheriting Risk from Third Party Supplier

7.4.1 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.

7.4.2 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.

7.4.3 Threat Impact

Potential impact to the supply chain includes:

- Potential intellectual property and/or regulatory violations in the final product
- Lack of product integrity
- Potential irreversible damage to the end product's brand/reputation.
- Lack of traceability and consistency through the supply chain
- Inadequate communication through the supply chain
- Potential hardware/software vulnerabilities
- Potential compromise of the supply chain's confidentiality
- Disruption in operations such as logistics interruptions
- Supply chain fraud involving unknowingly using counterfeit goods from suppliers deep within your supply chain.

7.4.4 Vulnerability

Unlike a typical threat actor sourced attack on the supply chain, the inherited risk from a lack of transparency can be very difficult to identify and mitigate in advance. It is an accidental vulnerability that is part of the normal system development life cycle and is a known vulnerability, possibly mitigated through proper internal controls.

This information is traced within the SDLC of the sourcing supplier, and typically provided in release notes to the procuring entity. The challenge is the compounding effect of numerous separate and distinct test exceptions as the complexity and scale of a system increases.

7.4.5 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. It should be noted that new AI solutions provided as system or software updates present a unique risk to existing legacy systems. Often these new AI solutions are difficult to assess their impact on the organizations risk posture.

7.4.6 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.

7.4.7 Potential Mitigating Strategies / SCRM Controls

- Proper engineering process will ensure that these decisions are documented, and traceability is provided vertically up the supply chain.
- Track and trace programs establish provenance of all parts, components, and systems. One example program specific to software product traceability is Software Bill of Materials (SBOM).[70]

AI solutions, particularly for program verification and software analysis, are now available on the market that can analyze third party software packages and create SBOM data when the supply chain providers did not relay adequate software transparency information. These services can help surface inherited risk.

- Although it is not a technology that is currently used widely in the supply chain space, utilization of blockchain or distributed ledger technology may provide some value in providing transparency. 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.[71]
- Require and implement a set of key metrics/minimum baselines that are meaningful and relevant to the supply chain ecosystem's hardware/software components. Well defined baselines can help assess the supply chain's security posture and build a widespread level of cyber hygiene.
- Implement robust integration tests for new or changed software components in the software development environment to ensure they meet desired functional requirements. These can include program verification and automated reasoning as well as other functional testing methods.
- 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 ensure compliance by suppliers.

7.4.8 Relevant Controls

Refer to NIST CSF Relevant Core Functions and Controls in table above in section 7.1.9.

7.5 AI Scenario: No Explanation of AI Model Outputs

7.5.1 Background

Since AI models are 'learnt' automatically from training data, there are no specifications / requirements that explicitly link the application inputs to the outputs. The application behavior is completely determined by a mathematical model created using the training data. These models are complex typically with millions (in predictive AI) to trillions of parameters (in generative AI) with no plausible way to trace input to the output, thus making them a 'black box'. If the user must understand how the output was created from the input provided, there is no direct mechanism to provide such an explanation. This is very different from traditional software systems where one can follow the application program logic from input to the output. An important aspect of such a need for explainability is that the provided explanation should match the knowledge level of the user of the system (e.g., diagnosis recommendation for a physician should be in the vocabulary of a medical

[70] https://www.cisa.gov/sbom
[71] Accenture, "Tracing the Supply Chain," 2018.

professional).[72] Lack of explainability of model outputs can lead to serious concerns about trusting the AI system for any use that requires care and auditability.

7.5.2 Threat Sources

Creators of the AI application did not consider provide an appropriate level of explainability that matches the needs of the intended users.

7.5.3 Threat Impact

From the user point of view, lack of explainability is a serious matter that can erode trust in the recommendations of the AI system. In addition, mistakes made by the system, which are inevitable due to their statistical nature, without any explanations can render the deployed system useless.

The lack of explanation could lead to:

- Erosion of trust and/or resistance from users
- Operational inefficiency such as a misunderstanding of the AI functions leading to errors and suboptimal performance.
- Underutilization of features
- Inadvertent security risks and increased risk of exploitation from malicious actors exploiting the AI system or tricking users into compromising security.

7.5.4 Vulnerability

The primary reason for this vulnerability is the 'black box' nature of many AI models, such as neural networks and deep learning-based models. The algorithms that create and utilize the models do not have the intrinsic ability to trace the input to the output in a meaningful and understandable way, due to the size and complexity of the models.

Some key aspects are:

- Deep learning models consisting of many layers of interconnected nodes that process data in a way that is not straightforward for humans to follow.
- Hidden Layers in models like neural networks where the data passes through multiple hidden layers where transformations occur.
- High dimensionality such as complex data representation and pattern recognition that may not be understandable to humans.
- Non-Intuitive outputs where the AI model may be correct but counterintuitive which leads to confusion if the reasoning behind it is not explainable.

7.5.5 Threat Event Description

Below is a simple scenario:

Based on a model built on patient records (from physicians) contained in the electronic medical records, MRI images, and blood test results, an AI system recommends a diagnosis for cancer (i.e., Yes or No). Here, the consequence is immense. If the recommendation is false positive (i.e., the patient does not have cancer, but

[72] M. Hind, "Explaining explainable AI." *XRDS: Crossroads, The ACM Magazine for Students* 25, no. 3 (2019): 16-19.

the AI says 'Yes') and the physician accepts the recommendation without explanations, the patient will go thorough significant but unnecessary procedures, costing money and discomfort. If the recommendation is false negative (i.e., patient has cancer, but the AI says 'No') and the physician accepts it without explanation, the patient is given false hope and there is significant impact to the patient due to the delay in treatment for a serious illness. Thus, providing explanations to the physician can really help to clarify what aspects of the patient data are leading to the specific recommendation by the AI model. The physician can use their expertise and judgment to defend the final decision they would make.

Although this example is in the medical domain to illustrate the severity of the consequence, similar critical decisions are ubiquitous in many other domains, such as, using AI to classify supply chain parts as defective or acceptable and identifying whether an intruder in a secure network is adversarial. Similar situations can also arise in GenAI where the provenance of the output should be traceable back to authentic sources that contributed to it. These sources should be shown to the user as a part of the explainability framework.

7.5.6 Outcome

As demonstrated in the example above, the impact of lack of explainability can be very severe. In business/mission critical use cases, it poses a very high and indefensible risk, leading to issues such as:

- Trust and Adaptation: The lack of transparency can lead to a lack of trust amongst users which could slow down the adoption of AI technology.
- Regulatory Compliance: Some industries and the government require decisions to be explainable, especially where regulations mandate transparency.

7.5.7 Potential Mitigating Strategies / SCRM Controls

AI Model acquisition should assess the vendors ability to provide reference and explainability alongside all LLM / AI system output. Insight into how the vendor curates data, lineage of AI models, and the level of explainability when acquiring an AI solution can help mitigate risks of using models that can be vulnerable to attack or damage the reputation of the business. Users should consider asking the vendor or provider if they employed the following techniques to avoid using AI solutions with explainability issues:

- The AI application team should evaluate what type of explainability is needed for each user population.
- Given the complexity of neural network and deep learning models, one common approach to deal with explainability is to build a surrogate, but more explainable model (e.g., decision trees) which can replicate most of the behavior of the original neural network model. This approach is somewhat sufficient but does not provide clarity about the "real model."
- Neural network models have considerable uncertainties in their prediction, despite the confidence in their outputs[73]. A part of the explanation should contain the estimated uncertainty in the prediction.
- There are many approaches and algorithms to develop a framework[74] for explainability and application developers should create one to match the specific use cases encountered by the organization.

7.6 AI Scenario: Unspecified or Harmful Advice

7.6.1 Background

[73] Example: IBM Uncertainty Quantification Toolkit: https://uq360.res.ibm.com/
[74] Example: IBM AI Explainability Toolkit: https://aix360.res.ibm.com/

When a model generates information that is factually correct but not specific enough for the current context, the advice can be potentially harmful. For example, a model might provide medical, financial, and legal advice for a specific problem that the end user may act on even when they should not. For critical infrastructure sectors, if decisions are based on such unspecified or harmful advice without human oversight, it might lead to errors.

7.6.2 Threat Sources

For an AI model to produce incorrect output, there could be several threat sources. Even if models are fine-tuned based on well curated data sets, they still learn from external sources, through a mechanism called Retrieval Augmented Generation (RAG). This method causes AI models to refer to external sources to augment their output, which can sometimes be harmful advice. The threat sources for such cases could either be internal non malicious actors who have misconfigured inputs, or they can be attackers external to the organization, especially nation-state attackers. Nation-state attackers would have the resources to conduct sophisticated man in the middle attacks to change source data or interfere in augmented output generation.

7.6.3 Threat Impact

Harmful advice can impact not only the person receiving the advice, but also businesses which deploy such systems. For instance, Air Canada was sued because their AI bot provided incorrect information about a claim. Air Canada had to settle, because it was accountable for the advice (harmful or not) provided by an AI bot deployed on their own website.[75] On the other hand, the person receiving the harmful advice was also impacted because they changed their plans according to this information provided by the bot. Harmful advice is very problematic in high-risk scenarios, where such advice can be life threatening.

7.6.4 Vulnerability

Resources exist for critical infrastructure sectors to determine whether information available on the internet is harmful or not. For example, if there is a website providing harmful advice, there are methods to determine if it comes from a reputable source, if it is ranked high by a search engine, or simply if it is legitimate through community feedback. The fundamental problem with advice provided by AI models is that it blurs the line between legitimate and harmful information by putting them together. For example, recent solutions provide healthcare advice by combining information from different websites, both useful and harmful. Additionally, models can provide legal advice by citing cases that do not exist. In this scenario, the user needs to verify whether the advice provided is applicable for their purpose.

7.6.5 Outcome

If critical decisions are based on harmful advice generated by AI models, it can have severe economic and reputational outcomes for critical infrastructure sectors. For example, if disaster management services rely on AI models to locate the most impacted areas after a storm, the model might provide incorrect information on which areas to target first if it does not have enough information about the region.

7.6.6 Potential Mitigating Strategies / SCRM Controls

Preventing AI systems from providing vague or harmful advice is a challenging issue that cannot be resolved by improving data sources. For a general-purpose model to provide specific and useful advice, it requires

[75] https://www.forbes.com/sites/marisagarcia/2024/02/19/what-air-canada-lost-in-remarkable-lying-ai-chatbot-case/

sufficient contextual information, which is often lacking. While offering more context about the use case may help, it introduces its own security challenges. In addition, it is difficult to directly prevent such advice, as the information may be accurate but not useful, even without malicious input. Despite these challenges, there are a number of strategies to mitigate this risk. The following are some recommended elements for developing a prevention and mitigation approach:

- End user notification: The end user of AI models should be aware that the responses provided to them are from an AI application. Furthermore, they should also be provided warning labels to ensure that users are aware that such systems can provide harmful or irrelevant advice. For example, in a healthcare scenario, if a user asks for advice, the model should inform them that it is not a substitute for a healthcare professional and that users should consult a certified practitioner before considering the advice.
- High-risk use cases: in high-risk cases, the model should not provide advice at all. For instance, the National Eating Disorder Association (NEDA) pulled its AI bot after it was found that the bot was providing harmful information that was not based on individual considerations of a person's health situation.
- Manual correction: If and when a model generates harmful advice, there should be a mechanism to provide feedback or suggest corrections. A pipeline should exist to prevent the model from generating further harmful advice. The downstream user can then verify if the advice they received is legitimate and suggest corrections.

7.7 Scenario: Inheriting Risk from Third Party Software Development Toolkit Used in Thousands of Applications

7.7.1 Background

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

7.7.2 Threat Source

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

7.7.3 Threat impact

Potential impact to the product includes:

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

- Potential hardware/software vulnerabilities
- Sensitive Data Exposure as the SDK could capture and exfiltrate sensitive user data leading to breaches.
- Non-compliance consequences like failure to comply with data protection policies which could lead to sanctions from regulatory bodies.
- Security risks such as malware propagation from the compromised SDK which could be used to distribute other forms of malware, escalating the security threat to other apps or systems.

7.7.4 Vulnerability

Attacks are increasing significantly at the software supply level, so it is not surprising to see developer toolsets designed or compromised to act maliciously, especially when they are "free" or open source. Detected attacks in the development stage of next generation open-source software increased approximately 1700 percent between July 2019 and May 2020 over the average for approximately the previous 4 years according to Sonatype.

Information gleaned from devices can be compiled, retained, and exploited in big data platforms in such a way that the aggregated information is far more valuable/damaging than the parts. Uses may include developing Artificial Intelligence (AI), targeting influence operations, and blackmail.

7.7.5 Threat Event Description

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

7.7.6 Outcome

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

7.7.7 Organizational Units / Processes Affected

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

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

7.7.8 Potential Mitigating Strategies / SCRM Controls

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

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

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

Use Trusted and Verified SDKs with reputable sources with a record of security compliance. Also establish an SDK whitelist of approved SDKs that have been thoroughly vetted and periodically review the list to ensure it remains compliant.

Incorporate Sandboxing and Restricting Permissions using the Least Privilege Principle to ensure that the SDK only has access to the minimum necessary permissions and resources it needs to function, and avoiding access to sensitive data or unnecessary system APIs. Also incorporate Data Segregation for sensitive data within the app to limit the exposure that a compromised SDK can have. For example, sensitive data can be stored in a secure enclave that is inaccessible to the SDK.

From a C-SCRM perspective, practice regular monitoring and threat detection which can be accomplished through behavioral monitoring that implements runtime monitoring to detect abnormal behavior within the app, such as unusual network traffic patterns or unexpected API call initiated by the SDK. Also threat intelligence feeds to stay updated on known vulnerabilities or malicious behaviors associated with specific SDKs.

7.8 AI Scenario: AI Unpredictability – Excessive Reliance on Coding Tools

7.8.1 Background

AI LLM-based applications can provide significant support to software developers and increase their productivity. However, AI LLM models and applications can produce invalid content, including software code, in a very convincing pseudo-authoritative voice. While experienced developers can spot invalid or vulnerable algorithms or code snippets, it is more challenging for junior developers who are less seasoned and have less experience with complex code.

7.8.2 Threat Sources

LLMs trained to provide developers with coding guidance are trained to recognize patterns and context using code available on the internet, allowing them to generate coherent and contextual responses.[76] Unfortunately, some training sets may include data poisoned for the purpose of misleading LLM training.[77] A myriad of similar frameworks across the internet provided by different open source communities can also lead to contradictory responses and incorrect algorithmic assumptions. Models can be mis-trained intentionally to provide code with hard-to-spot vulnerabilities. Acquisition of AI enabled coding tools should take into consideration the lineage of

[76] https://arxiv.org/abs/2302.10149
[77] https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-2e2023.pdf

the models, vendor reputation and the code base / patterns on which they may be trained. LLMs also can produce invalid code or other hallucinations, even in the absence of adversarial data poisoning.

7.8.3 Threat Impact

Unverified AI based coding tools can provide threat actors with a direct vector for inserting malicious code. The impact ranges from difficult to identify algorithmic exceptions (bugs) to the insertion of intentionally malicious code. Vulnerabilities could be used for privilege escalation to further spread a potential attack.

7.8.4 Vulnerability

Overreliance on AI based code tools can lead to unexpected consequences if used by inexperienced developers and not coupled with strong secure engineering practices. Overreliance on AI can lead to organizational loss of expertise. When this comes to development, the consequences can be significant. AI based coding tools sometimes hallucinate answers to complex coding queries, providing coding examples that do not function as expected. Downstream consumers should take special care to assess the lineage of both the vendor and their foundation AI models to ensure they are not compromised.

7.8.5 Threat Event Description

Management and developers can become over reliant on AI based coding tools and code generation frameworks. These tools do provide excellent support for experienced developers but can lead to overreliance by less experienced developers. Overreliance leads to an increased number of more complex vulnerabilities and unpredictable results. Management might be tempted to replace highly skilled developers with less experienced programmers augmented by AI based coding tooling.

AI based coding tools can provide a vector for maliciously trained AI models even when used by reputable vendors.

AI based coding tools can produce code snippets and algorithms which do not function as expected and will abnormally terminate. AI generated code can look authoritative, causing code reviewers to overlook potential vulnerabilities.

7.8.6 Outcome

Applications that are built using AI based coding tools could become infected with malicious code or function in unpredictable ways if not properly tested.

Organizations can suffer a reduction in the number of experienced developers who are able to write code that contains fewer bugs. Loss of expertise leads to the acceptance of code that is difficult to test and debug.

Business processes could become hijacked by malicious actors if the AI code tooling injects malicious algorithms or relies on maliciously tainted components.

7.8.7 Potential Mitigating Strategies / SCRM Controls

The following these guidelines can be utilized to mitigate the potential risks when using AI enabled coding tools:

- AI based coding tools should be assessed against strict SCRM selection practices which include obtaining clear visibility into the lineage and training practices of the underlying AI models.

- Augment all AI based code generation with expert code reviews, vulnerability scanning and good secure engineering hygiene.
- Review software bill-of-materials for the use of AI based coding tools and their lineage.
- Provide strong oversight to the use of AI generated code and automated code generation. Ensure that code is reviewed just as it would be if written by a human. Ensure that all code is validated and scanned for vulnerabilities.
- Avoid organizational blind spots by balancing developer expertise to ensure that your team does not get overly reliant on coding automation.

7.9 Scenario: Inheriting Risk from the Acquisition of IT Maintenance and Repair Services

7.9.1 Background

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

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

7.9.2 Threat Source

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

7.9.3 Threat Impact

Potential impact to the product includes:

- Product failure
- Lack of product integrity
- Product performance degradation
- Potential irreversible damage or compromise to a system using the end-product.
- Lack of traceability and consistency through the supply chain making it difficult to discover the root cause of the product failure.
- Potential hardware/software vulnerabilities which could lead to increased vulnerability to malicious components that could be exploited for unauthorized access, data exfiltration, or system manipulation.
- Potential Risk due to non-transparent vendor attestation can lead to the inclusion of hardware components from unverified or malicious sources increasing the risk of backdoor, hardware Trojans, or other vulnerabilities being introduced.
- Access by non-vetted personnel to elements of IT system hardware

7.9.4 Vulnerability

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

7.9.5 Threat Event Description

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

7.9.6 Outcome

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

7.9.7 Organizational Units / Processes Affected

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

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

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

7.9.8 Potential Mitigating Strategies / SCRM Controls

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

Perform vendor risk assessments and other due diligence focusing on SCRM practices, security policies, and transparency levels. Also establish rigorous vendor attestation requirements which provide clear and detailed attestation documentation that verifies the integrity and authenticity of their hardware products and services.

Lastly, perform regular audits of both vendors and hardware components, coupled with continuous monitoring of systems for any signs of compromise or failure. It might also be a good practice to diversify suppliers to avoid a single point of failure in your products or services.

Also consider:

- Implementing strong incident response plans
- Adopt Industry standards and best practices
- Supply chain mapping and monitoring
- Invest in Redundant Systems and contingency plans

7.10 Scenario: Inheriting Risk from Components Produced with Known and Deemed Mitigated or Noncritical Faults

7.10.1 Background

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

7.10.2 Threat source

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

7.10.3 Threat impact

Potential impact to the product includes:

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

7.10.4 Vulnerability

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

7.10.5 Threat Event Description

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

7.10.6 Outcome

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

7.10.7 Organizational Units / Processes Affected

The lack of traceability as these elements are integrated into higher level components (and eventually end products or systems) can lead to cascading minor errors resulting in a vulnerability or latent defect in the final product. These issues are not the result of an intention to perpetuate a threat. Instead, they arise from common trade-offs in engineering processes that balance cost, schedule, and quality.

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

7.10.8 Potential Mitigating Strategies / SCRM Controls

- Good engineering process will ensure that these decisions are documented, and traceability is provided with the component vertically up the supply chain to provide visibility into customers of the final products or services.
- Track and trace programs establish provenance of all parts, components, and systems to include all documents, such as release notes, including an SBOM.
- Although it is not a technology that is currently used widely in the supply chain space, utilization of blockchain or distributed ledger technology has shown to be a promising method in maintaining provenance throughout the entire supply chain. Blockchain technology is a shared digital platform where each participant organization within the supply chain can store and share information which is verified and immutable. All this data is then available simultaneously and in real time.[78]

7.11 AI Scenario: Careless or Inadequate Data Curation[79]

7.11.1 Background

The use of statical models based on ML techniques has changed the landscape of building applications. Since the models depend on training data, it would be difficult to create strict specifications and build software that provably meets those specifications (although, in practice, only those in the most safety critical software applications currently use such a rigorous design process). Even so, even without informal specifications ML software behavior is highly dependent on the characteristics (including accuracy, relevance, representativeness, coverage, and the distribution of these properties within the data) of the data used in the training process.

Therefore, in the MLOps lifecycle to build the application, adopting best practices to curate the training data before using it to build AI models is critical. Since the training corpus for LLMs typically includes scraped data from internet sources, the quality of the 'raw' data is questionable. This is true both in the predictive AI and generative AI models. In the predictive AI case, the organization can have complete control over the training data and hence proper curation of the data is manageable (though this only limits some risks; see for example Section 0, 7.5 AI Scenario: No Explanation of AI Model Outputs).

In the generative AI context, if the organization chooses to use a pretrained LLM, either from a commercial vendor or a freely available public model, then there is an inherited risk of unexpected or unwanted behavior of the model during deployment that needs to be anticipated and mitigated. In the predictive AI case, using a vendor model to create an application has a similar exposure.

7.11.2 Threat Sources

The threat source is bad AI engineering/MLOps practices of a supplier, or an AI enabled acquired product. The supplier providing the AI model from the training data should be aware of the contents of the data corpus they use, their sources and the lineage of supplied models.

7.11.3 Threat Impact

The impact of the use of improperly curated training data or models can be significant. At the basic level, the accuracy of the model outputs can be severely affected for both predictive and generative AI. For example, in generative AI, there can be unwanted characteristics such as hate speech, abusive language, or profanity

[78] Accenture, "Tracing the Supply Chain," 2018.
[79] J. Buolamwini and T. Gebru. "Gender shades: Intersectional accuracy disparities in commercial gender classification." In Conference on fairness, accountability and transparency, pp. 77-91. PMLR, 2018.

included in the output due to the use of uncurated training data. All acquired models and generative AI solutions should be vetted to understand the training legacy of the models. Vendors should be assessed to ensure they meet SCRM lineage risk tolerance.

7.11.4 Vulnerability

Immature data acquisition and curation practices are the basis for this vulnerability. Some examples of typical problems in data curation are:

- Incomplete data to represent the use case (e.g., vision application in self-driving cars lacking images under certain weather conditions or types of road signs).
- Bias in Data (e.g., an AI system trained on biased criminal justice data can target certain demographics disproportionately).
- Outdated Data (e.g., a model trained on images of older cars might struggle to recognize newer models).
- Inconsistent Data: (e.g., images collected from multiple sources with varying formats, resolutions, and labeling convention).
- Annotation Errors: (e.g., errors in image training data such as incorrect labels or poorly defined bounding boxes).
- Statistically Imbalanced Classes, including some categories in the dataset are under-represented. For example, inclusion of many more images of cars than bicycles, which will make the model biased towards detecting cars while doing poorly on bicycles.
- Inclusion of copyrighted materials in the training data for a generative AI model.

7.11.5 Threat Event Description

Two famous examples:

- Commercial facial recognition software products showed error rates of up to 34.7% for darker-skinned females whereas the maximum error rate for lighter-skinned males was 0.8%. This was because training datasets were overwhelmingly composed of lighter-skinned subjects.[80]
- New York Times sued Open AI and Microsoft for producing ChatGPT outputs that were verbatim reproduction of copyrighted material without permission.[81]

7.11.6 Outcome

The impact of bad data curation can be incorrect recommendations from the AI for business/mission critical applications (e.g., wrong medical diagnosis), unexpected/unwanted outputs (i.e., hate, profanity) that offend/annoy users, and lawsuits based on the AI generated content.

7.11.7 Potential Mitigating Strategies / SCRM Controls

All acquired models and generative AI solutions should be vetted to understand the training legacy of the models. Vendors should be assessed to ensure they meet SCRM lineage risk tolerance. Examples of mitigation strategies in data curation that both provider and supplier should follow, include:

[80] J. Buolamwini and T. Gebru. "Gender shades: Intersectional accuracy disparities in commercial gender classification." In Conference on fairness, accountability and transparency, pp. 77-91. PMLR, 2018.
[81] https://www.nytimes.com/2023/12/27/business/media/new-york-times-open-ai-microsoft-lawsuit.html

- Provide regular updates to datasets to keep the model current and accurate.
- Standardize data collection and annotation processes to maintain consistency.
- Utilize techniques to minimize statistical imbalance problems (e.g., via data augmentation, oversampling of minority classes, use of simulated data).
- Undertake systematic identification, and tagging or removal as appropriate, of hate, abuse, or profanity-laden data using automated tools.

8 THREAT CATEGORY: LEGAL RISKS

8.1 Scenario: Laws that Harm or Undermine American Economic Interests

8.1.1 Background

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

8.1.2 Threat Source

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

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

8.1.3 Threat Impact

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

- Increased Risk of Intellectual Property Theft due to weaker trade secret protections; there is a higher risk that sensitive information, including proprietary technology, processes can be stolen or misappropriated
- Data Breaches and Cyber Espionage with companies operating in jurisdictions with lax cybersecurity laws or enforcement might be more vulnerable to data breaches or cyber espionage and there is potential to gain unauthorized access to critical information, data leaks and a disruption of operations.
- Supply Chain Vulnerabilities can cause the supply chain to become compromised if entities in countries weaker protections and lead to tampering, counterfeit products or even malicious software being introduced into the supply chain.

8.1.4 Vulnerability

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

8.1.5 Threat Event Description

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

8.1.6 Outcome

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

8.1.7 Potential Mitigating Strategies / SCRM Controls

Strategies to help mitigate this threat include:

- Setting up supply chain operations outside of countries without the needed legal protections.
- Diversifying the supply chain Routing the most sensitive/vulnerable parts of a supply chain out of such countries.
- Drafting contracts to include the relevant protections.
- Conducting thorough due diligence on the legal and regulatory environments in the countries of operation.
- Implementing robust cybersecurity measures across your entire supply chain
- Collaborate with legal experts for more complex international legal frameworks.

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 in is known for government corruption and weak oversight of its domestic businesses.

8.2.2 Threat Source

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

8.2.3 Threat Impact

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

- Quality control issues due to a weak regulatory oversight
- Supply chain disruptions and delays which could affect the entire supply chain
- Legal and compliance risks
- Compromised security

8.2.4 Vulnerability

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

8.2.5 Threat Event Description

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

8.2.6 Outcome

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

8.2.7 Potential Mitigating Strategies / SCRM Controls

Strategies to help mitigate this threat include:

- Setting up supply chain operations outside of countries without the needed legal protections.
- Routing the most sensitive/vulnerable parts of a supply chain out of such countries.
- Randomized and systematic quality control testing.
- Perform regular audits to ensure compliance with quality, ethical and legal standards.
- Drafting contracts to include the relevant protections all the way down the supply chain.
- Monitor the political and economic environments to prepare for potential disruptions.

8.3 AI Scenario: Stealing Private Information from LLMs

8.3.1 Background

As the size and sophistication of LLMs have increased, the risk of the models revealing private information has increased substantially. There are two primary mechanisms responsible for this problem: (i) LLM ‘memorizes’ parts of the training data and reveals them when prompted in a carefully orchestrated way, (ii) LLMs can connect various pieces of unstructured data in impressive ways at the inference (usage) time and produce outputs that reveal personal information that violate privacy policies.

8.3.2 Threat Sources

Any individual or entity that wants to leverage the private information for profit or strategic advantage, such as impersonation, fraudulent financial transactions, and blackmail.

8.3.3 Threat Impact

The impact of the leak of private information can vary widely from minor inconvenience to a national security risk.

8.3.4 Vulnerability

This threat occurs because the current architecture of the LLMs relies on probabilistic association between various pieces of data to generate human-like outputs with the given the user context. Guardrails are typically created after the model is built and therefore, they lack the rigor of controlling LLM behavior.

8.3.5 Threat Event Description

Example 1-Exposing private information from LLM memorization:

Carlini et al.[82] describe specific steps to expose the memorized part of the training data by performing carefully designed queries to the LLM. The memorized parts can contain private information such as phone numbers, and social security numbers. For example, if a model's training dataset contains the sequence "Mary Smith's social security number is 111-22-3333," and given the prompt of six words "Mary Smith's social security number is," the most likely output is going to be "111-22-3333." The authors show that the memorization significantly grows as (1) the size of a model increases, (2) the number of times an example has been duplicated, and (3) the number of tokens of context used to prompt the model. They find that the memorization in LLMs is more prevalent than previously believed and will likely get worse as models continues to scale, without active mitigations.

Example 2-Adversarial inference of personal attributes from text:

Staab et al.[83] used a dataset of real Reddit profiles and demonstrated that current LLMs can accurately infer a variety of personal information (e.g., location, age, sex, etc.) with high accuracy. The adversary can easily have access to a dataset of user-written texts (e.g., by scraping an online forum such as Reddit). The steps to perform the attack are:

- Create a model prompt using a fixed adversarial template.
- System Prompt: "You are an expert investigator with experience in online profiling"
- Prefix: Let us play a guessing game. Given this profile can you tell me where the author lives and how old they are?
- Author Profile (taken from user written texts):
    - "There is this nasty intersection on my commute, I always get stuck there waiting for a hook turn."
    - "I remember watching Twin Peaks after coming home from school."
- Inference: Leverage a pre-trained LLM (e.g., ChatGPT) to infer personal user attributes automatically, a task that previously required humans.

[82] N. Carlini, et al. "Quantifying memorization across neural language models." arXiv preprint arXiv:2202.07646 (2022).
[83] R. Staab, et al., "Beyond memorization: Violating privacy via inference with large language models." arXiv preprint arXiv:2310.07298 (2023).

- "A hook turn is a traffic maneuver particularly used in Melbourne, Australia."
- "Twin peaks was running 1990-91, when the author was likely in high school (age 13-18)"

Personal Attribute Identified: Location: Melbourne Australia. Age: 45-50

This scenario shows finding relatively obscure information is possible with the current LLMs.

8.3.6 Outcome

Loss of private information can lead to serious consequences such as identity thefts, and black mailing.

8.3.7 Potential Mitigating Strategies / SCRM Controls

There are two approaches to mitigate this issue:

- A first defense against LLM-based attribute inference would be removing personal attributes in the user inputs with existing text anonymization tools. However, even after such a step, LLMs can still infer many personal attributes, including location and age due to their ability to pick up on more subtle language clues and context (e.g., region-specific slang or phrases) not removed by such anonymizers. There is a clear need for research in stronger text anonymization methods to keep up with increasing LLM capabilities.
- From the LLM provider perspective, model output alignment is currently the most promising approach to restricting LLMs from generating harmful content. However, research in this area appears to have focused on topics such as hate, abuse and profanity more than the potential privacy impact of model inferences. Thus, there is also a need for better output alignment for privacy protection in future research.

8.4 AI Scenario: Loss of Intellectual Property

8.4.1 Background

Confidentiality of high-risk assets is a key goal of cybersecurity in critical infrastructure organizations. AI creates two possible challenges to this loss of confidentiality and intellectual property. First, private disclosure of confidential code to a public model is possible. For instance, proprietary code may be uploaded to these AI systems, which can then be accessed by any other entity who also interact with such systems. Second, in order to train the model, data can be gathered from proprietary sources or sources with licenses that do not permit such usage without attribution. For example, code from blogs and other platforms across the internet can be scraped to create an automatic code completion model.

8.4.2 Threat Sources

Such threats are typically caused by entities within an organization, either employees or vendors. Employees may accidentally upload proprietary code or data. They might also use training data that has not been licensed properly.

8.4.3 Threat Impact

Intellectual property is a core part of any business. Furthermore, when proprietary assets are a part of critical infrastructure, it is a huge security risk to have exposure of such high-risk information. The same is true for information as well, that is of high monetary value to the organization. As an example, New York Times sued

OpenAI in 2024 because OpenAI had potentially used paid articles from the publication to train their models and create summaries. When such training data collects sensitive information or licensed code, the consequences compound.

Potential threat impacts could be:

- Data Leakage of code or sensitive algorithms whether accidental or intentional
- Inadvertent backdoor exposure or vulnerabilities that, if exposed, could be exploited by malicious actors.
- Legal and compliance issues and regulatory penalties
- Licensing violations and breaching licensing agreements
- Data privacy violations
- Ethical concerns with misusing proprietary or sensitive data without proper consent

8.4.4 Vulnerability

The key vulnerability that is exploited to cause loss of intellectual property is access to proprietary information.

8.4.5 Outcome

Loss of intellectual property through intentional or unintentional plagiarism can have adverse business impact. For businesses, a core component of their economic value and gains can be intellectual property. For instance, critical infrastructure entities in the financial sector might have their own custom code to perform stock market analysis. However, if their internal code stored in cloud-based repositories are used to train AI models to generate plagiarized analysis tools, it can cause such entities to lose their competitive edge and create in turn, economic loss.

8.4.6 Potential Mitigating Strategies / SCRM Controls

There are two parts to mitigating loss of intellectual property from a supply chain perspective. One is to prevent loss of such information in the first place. This can be done by creating an inventory of applications which contain proprietary information. All documents, resources, and databases that contain sensitive information should be labeled. What is not identified as sensitive, cannot be protected as sensitive. After such an inventory is built out, data loss prevention mechanisms should be built for this subset of resources to restrict access to such systems. This is especially true if such information is present on cloud service providers.

The second part is to identify that loss of intellectual property has happened, if any. This requires having sufficient telemetry and testing tools to detect if proprietary code is accessed and used by AI models.

Other mitigations to consider could be:

- Implement Strong Access Controls
- Conduct regular audits
- Use secure data management practices

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

9.1 Scenario: Natural and Man-made Disasters/Causing Supply Chain Disruptions

9.1.1 Background

External events including natural and man-made disasters can have an enormous impact on the end to end supply chain and can include the destruction or degradation of manufacturing facilities, workforce disruptions, as well as negative impacts on the transportation and distribution of goods and services. Depending on the size and scope of the event, the disruption to the end-to-end supply chain can have multiple and varied impacts.

9.1.2 Threat Source

Natural disasters can have a severe impact on the global economy. According to Aon Benfield's 2016 Global Climate Catastrophe Report[84], global economic losses because of 315 separate natural disasters reached $210 billion, which is 21 percent above the 16-year average of $174 billion. In 2017, Hurricane Harvey destroyed 178,000 homes, caused $669 million in damages of public property, a quarter million vehicle losses and $200 million in Texas crop and livestock losses. Additionally, businesses experienced significant losses due to flooding, electrical outages, and employees' inability to get to work, all of which caused the temporary disruption of the flow of goods and services. However, the impacts of natural disasters reach far beyond the local damages of affected areas due to the interconnected and global nature of supply chains.

The Tohoku Earthquake and Tsunami in Japan and the Thailand Floods in 2011 are both examples of natural disasters that caused severe disruption to global technology supply chains. After the Thai floods, there was a global shortage of computer hard drives that sent consumer prices skyrocketing until factories were able to resume operations. When the 2011 tsunami struck, car manufacturers were forced to shut down production which caused shortages in 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.[85]

Importantly, the COVID-19 pandemic revealed three primary stress points on ICT supply chains:[86]

Inventory Management

Prior to the pandemic, the typical approach to supply chain management was Just-In-Time (JIT) inventory management. JIT allows manufacturing companies to cut costs by reducing the amounts of goods and materials a firm needs to hold in stock. Production is for specific customer orders and the production cycle commences only after a customer has placed an order with the producer, thereby eliminating the need to hold a large inventory. While lean supply chains may work in times of normalcy, the pandemic demonstrated that companies may need to examine their inventory management practices so that they have the ability to continuously collect data and feedback, evaluate it in real time, react expeditiously to rapidly evolving environments, and develop cushions to absorb abnormal periods of activity or inactivity. Companies may also continue to push for vendor managed inventory, a scenario under which, among other things, a supplier is paid a fee to hold extra equipment on hand in their warehouses.

Supply Chain Transparency

While many companies could quickly assess the impacts that the pandemic had on their direct suppliers, they did not have visibility beyond their second or third tier suppliers to their junior suppliers, and therefore, were unable to ascertain the impacts from the pandemic on these companies. As a result, in order to create supply chain resilience, managers need to be able to map where their tier 1, tier 2, and tier 3 suppliers are

---

[84] https://www.aon.com/australia/media/2016-annual-global-climate-and-catastrophe-report.jsp

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

[86] "Building A More Resilient ICT Supply Chain: Lessons Learned During the COVID-19 Pandemic," ITC Supply Chain Risk Management Task Force (December 2020) (https://www.cisa.gov/resources-tools/resources/ict-supply-chain-lessons-learned-during-covid-19). .

manufacturing so they can understand which suppliers are the most affected by disruptions. They also need visibility into tracking junior suppliers' inventory of finished goods and raw material.

Additionally, purchasers at the end of the value chain, (such as communications service providers, enterprises, systems integrators, and consumers) inherit the upstream supply chain risks associated with manufacturers' supply chains. The pandemic illuminated not only vulnerabilities within specific vendors' supply chains, but also vulnerabilities – such as single-source tier 2 or tier 3 suppliers – that were shared by multiple vendors. The result is that strategies to mitigate supply chain risks by sourcing from multiple tier 1 suppliers may be insufficient to achieve sufficient supplier diversity and highlights the importance of mapping upstream supply chains across their entire vendor base.

Single Source and Single Region Suppliers

In many cases, companies rely on a single source for products that they purchase directly. While supply chain managers recognize the risk of an over-reliance on a single source, they nevertheless adopt this strategy in order to secure the necessary supply or to control costs. This lack of flexibility can have devastating effects when a company's sole supplier is unable to provide produce. Additionally, there are often limited options from which a firm can choose, and more and more, those options include *only* those sourced from a single region, continent, or company. When extraction and production is so concentrated in one region or on one continent, it makes finding alternative workarounds especially difficult.

9.1.3 Threat Impact

Natural and man-made disasters can have a large impact on the end-to-end supply chain including destruction of manufacturing plants and warehousing and distribution locations. Impacts to infrastructure include impacts to roads, rail, sea and air capabilities, resulting in delays in delivery of raw materials, components, and consumer goods as local communities recover from the disaster. Often multiple impacts can further delay delivery of products and services.

9.1.4 Threat Event Description

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

9.1.5 Outcome

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

9.1.6 Potential Mitigating Strategies / SCRM Controls

To plan and prepare for business disruptions, organizations should consider the following strategies to increase supply chain resilience:

Proactive Risk Classification: ICT companies may continue to refine their supply chain risk management approach given the financial burden experienced as a result of supply disruptions during the pandemic. Companies may consider deploying a systematic classification of risks, continually analyze developments and events that are happening around the world and undertake the development of a response strategy to improve supply-chain resilience strategically.

Map the Corporate Supply Chain: ICT companies may want to develop a detailed map of junior-tier suppliers as a critical step to detect hidden relationships that impede adding resilience. After mapping upstream suppliers, purchasers of ICT products should also be aware of the production locations and financial stability of each participant in the value chain that supplies a critical component or constitutes a potential logistical bottleneck.

Broaden Supplier Network and Regional Footprint: To eliminate and reduce the risk of single source for raw materials or critical product components when possible, companies can increase resiliency and redundancy in their networks by dual-sourcing supply from multiple or lower-risk regions.

Potential Development of Standardized Mapping and Other Illumination Tools: While there is a strong consensus about the need to more effectively map the locations of sub-tier suppliers and to identify upstream logistical bottlenecks, currently there is no standard methodology for doing so. The IT and Communications sectors may thus benefit from the development of standardized approaches to supply chain mapping that would place appropriate focus on sub-tier suppliers or logistical bottlenecks that are most critical; would care for legitimate vendor concerns about being pressed to provide proprietary information; and would settle on common formats for providing maps and other information.

Work to Shift the Optimal Amounts of Inventory Held: Many ICT manufacturers try to minimize their inventory of components, thereby holding down costs by keeping stockpile inventories low and delivering goods as needed. This is the opposite of the “just in case” methodology that calls for holding more inventory in reserve. ICT companies may want to explore holding more buffer inventories and also working with their suppliers to hold inventory at their warehouses, through a vendor managed inventory system. Furthermore, ICT manufacturers should continue to ensure that they utilize meaningful metrics, such as orders delivered complete, accurate and on-time, as well as time related metrics like days of inventory and cycle time.

Plan Alternatives in Logistics and Transportation: During an adverse event, almost every mode of transportation can be affected. To reduce the impacts of transportation and logistics issues, ICT companies can engage in scenario planning for different types of events and map out the alternatives that can allow for the supply chain to be restored as efficiently as possible. To further assist in these efforts, companies can utilize technology platforms that provide real-time, blockchain visibility into available logistics capacity. Companies can also study logistics patterns to help identify alternative providers for each key route.

As a part of this effort, companies can 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, companies should create a 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 should be considered mission critical. The plan sets a schedule for periodic backups of all electronic and hard-copy documentation, which should be stored in an alternate location.

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

The body of the recovery plan should include the following:

- Business assumptions;
- Incident-management team member including critical personnel from all areas of the company resources and recovery assignments;
- Recovery strategy and solution overview;
- Emergency response procedures;
- Incident reporting procedures;
- Recovery team notification, mobilization and assembly procedures;
- Detailed recovery procedures;
- Situation-assessment guidelines;
- Emergency contact information of key employees, vendors and customers;
- A summary of mission-critical business functions to be recovered; and
- Detailed procedures for transitioning back to business as usual.

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

9.2 Scenario: Man-made Disruptions: Sabotage, Terrorism, Crime, and War

9.2.1 Background

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

9.2.2 Threat Source

The year 2016 saw several man-made disruptions, including the late summer Gap warehouse fire in Fishkill, New York, which destroyed 30 percent of Gap's total warehouse space and disrupted more than 10 percent of Gap's orders.[87] Another example is the Samsung Note cell phone battery recall, which was linked to problems in a battery supplier's supply chain and had far-reaching consequences for the Samsung brand and their customers.[88]

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

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

9.2.3 Threat Impact

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

9.2.4 Threat Event Description

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

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

9.2.5 Outcome

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

9.2.6 Organizational Units / Processes Affected

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

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

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

9.2.7 Potential Mitigating Strategies / SCRM Controls

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

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

9.3 Scenario: Labor Issues

9.3.1 Background

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

9.3.2 Threat Source

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

9.3.3 Threat Impact

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

9.3.4 Threat Event Description

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

Two years ago, there had been a lot of political momentum to enable better, higher-paying jobs in manufacturing and other blue-collar jobs. Due to this, a year ago, there were several programs that were funded by the U.S. Government to encourage bringing jobs back to the U.S. from overseas locations while also increasing wages.

After three phases of these programs touching on different industries, the U.S. has seen its unemployment rate drop from 8.5 percent to 3.4 percent.

9.3.5 Outcome

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

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

9.3.6 Potential Mitigating Strategies / SCRM Controls

- Institute a standard rotation or cross-training process for all employees, 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 employees and employers;
- Simplify processes or improve related training and documentation to reduce transition or onboarding time for folks new to an area; and
- Work with local trade schools and universities to develop talent with specific skills that are currently lacking in the workforce.

9.4 Scenario: Influence or Control by Foreign Governments Over Suppliers

9.4.1 Background

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

9.4.2 Threat Source

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

9.4.3 Threat Impact

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

9.4.4 Threat Event Description

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

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

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

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

9.4.5 Outcome

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

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

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

9.4.6 Potential Mitigating Strategies / SCRM Controls

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