

Cybersecurity in the Hardware Supply Chain

by

Ahalya Sankararaman

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Master of Applied Science
in
Electrical and Computer Engineering

Waterloo, Ontario, Canada, 2024

© Ahalya Sankararaman 2024

Author's Declaration

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Abstract

Globalization in the hardware supply chain has increased sophisticated hardware security breaches. Once considered safe and secure in the early phases of the manufacturing life cycle, the semiconductor supply chain has become a convenient target for malicious attackers to take control of the hardware to execute cyber-attacks. Adopting a product integration model with multiple tiers of suppliers, contractors, and distributors spread across the globe optimizes cost and efficiency for original equipment manufacturers (OEM). Although economically beneficial, this model has increased hardware's exposure to supply chain vulnerabilities and challenges, such as counterfeiting, hardware trojan insertion, backdoors, intentional sabotage, and tampering attacks. After the manufacturing phase, the product is deployed in safety-critical industries such as automotive, military, healthcare, aerospace, and defense industries. These sectors' entire ecosystem greatly depends on a trust-based supply chain. They are largely unaware of the new cyber threats to hardware that might compromise the product's quality, security, and safety. Compromised hardware with substandard components or malicious modifications deployed in mission-critical sectors is prone to failures before its average life cycle, leading to loss/injury to life, disruption of infrastructure, financial losses, damage to the company's reputation and legal scrutiny.

The cycle of trust placed on suppliers and vendors within the supply chain can be disrupted by educating manufacturers about the risks posed by new threat actors, indicators of compromise and implementing the necessary preventive measures to avoid cyber attacks in the hardware supply chain. Several training programs have been widely adopted to raise awareness of cybersecurity risks. Gamification has proven effective in conveying complex security concepts using innovative and engaging in-game elements to deliver educational content.

This thesis aims to educate about the different types of cyberattacks in a hardware supply chain by suggesting a gamified tabletop exercise (TTX). This interactive approach is designed to educate about the risks of a trust-based supply chain in a way that actively involves the organizations exposed to such risks, allowing them to deploy necessary countermeasures well in advance to lower the impact of the attacks, ensure business continuity by evaluating and implementing the required policies.

Acknowledgments

I would like to thank my supervisor Dr. Sebastian Fischmeister for providing me with the opportunity to be a part of this research project and for his guidance and unwavering support during my master's program.

I would like to express my gratitude to Professor Dr. Hiren Patel and Professor Dr. Diogo Barradas for being my thesis readers.

Dedication

To my dad, mom, sister, and all my friends who have been a great pillar of strength at every milestone in my life.

Table of Contents

Author's Declaration	ii
Abstract	iii
Acknowledgments	iv
Dedication	v
List of Figures	xi
List of Tables	xiii
List of Abbreviations	xiv
1 Introduction	1
1.1 Motivation	1
1.2 Contributions	2
1.3 Objective and Importance	2
1.4 Organization of the Thesis	4
2 Background	5

2.1	Cybersecurity in Critical Infrastructure	6
2.2	What is a Table Top Exercise	6
2.3	Table Top Exercise in Cybersecurity	7
2.4	Types of Threats in Hardware Supply Chain	7
2.4.1	Counterfeiting	7
2.4.2	IP Piracy	10
2.4.3	Tampering	11
2.4.4	Insider Sabotage	11
3	Literature Survey of Game-based Learning Models	12
3.1	Pedagogical Learning Model	12
3.1.1	Bloom’s Taxonomy	13
3.1.2	Kirkpatrick Model	13
3.1.3	COFELET Framework	14
3.1.4	MOTENS Model	14
3.2	Serious Games in Cybersecurity	15
3.2.1	STRIDE	16
3.2.2	DREAD	16
3.2.3	Planning Poker	17
3.2.4	Protection Poker	17
3.2.5	Elevation of Privilege	18
3.2.6	Control Alt Hack	18
3.2.7	Play2Prepare	19
3.2.8	Decisions & Disruptions	19
3.2.9	LINDDUN GO	20
3.2.10	Cyberwar Gaming	20

3.2.11	Cyberceige	21
3.2.12	d0x3d	22
3.2.13	CIST	22
3.2.14	Riskio	23
3.2.15	Backdoor and Breaches	23
3.3	Key Takeaways from Existing Games	24
3.4	Advantages of Gamification in Cybersecurity	25
4	Game Methodology	26
4.1	The Importance of TTX	26
4.2	Game Components	27
4.3	Participants	28
4.4	Blue Team Roles in a TTX	29
4.4.1	Business Head/CEO	29
4.4.2	Engineering Head /CTO	29
4.4.3	Operations/Procurement	29
4.4.4	Legal	30
4.4.5	Finance	30
4.4.6	PR Head	30
4.4.7	HR/Communications	30
4.5	Setting the Stage for TTX	30
4.6	Character Prompts	31
4.7	Scenario Development	33
4.7.1	Scenario 1: Counterfeiting	34
4.7.2	Scenario 2: Intellectual Property (IP) Piracy	37
4.7.3	Scenario 3: Insider Sabotage	38

4.7.4	Scenario 4: Ransomware/Tampering	40
4.8	Incident Response Plan	41
4.9	Learning Outcomes of TTX	45
4.10	Evaluation of the TTX	45
4.11	Lessons Learnt from TTX	46
4.12	Limitations of TTX	47
5	Hardware Countermeasures	48
5.1	Legislation	49
5.2	Standards	49
5.2.1	SAE AS5553	50
5.2.2	SAE AS6171	50
5.2.3	IDEA Standard	52
5.2.4	Other Initiatives	52
5.3	Countermeasures for Counterfeiting	53
5.4	Countermeasures for IP Piracy	54
5.5	Countermeasures for Tampering	54
5.6	Countermeasures for Insider Sabotage	55
5.7	CIA Triad for Hardware Cybersecurity	55
5.8	Zero-trust Architecture	56
5.9	Tenets of Zero-trust Architecture	56
5.9.1	Zero-trust Framework for Hardware Supply Chain Security	58
6	Conclusion	59
6.1	Future Scope	60
	References	61

APPENDICES	69
A Game Elements of Tabletop Exercise	70
A.1 Game Property	70

List of Figures

1.1	Parts reported to ERAI vs semiconductor sales [3]	3
2.1	Types of components reported to ERAI [3]	8
2.2	Taxonomy of counterfeit components	9
2.3	Types of IP piracy	10
3.1	Bloom’s revised taxonomy [77]	13
3.2	The Kirkpatrick Model	14
3.3	MOTENS model [34]	15
4.1	Tabletop Exercise: Game Flow	27
4.2	Inject suggestions for Red Team	36
4.3	Reveal for Blue Team	37
4.4	Incident response template	42
4.5	Phases of incident response [66]	43
5.1	NIST tenets of a ZTA [52]	57
A.1	Game element: Letter from supplier Auto Inc.	71
A.2	Game element: Letter from NHTSA	71
A.3	Game element: Delayed cooperation.	72

A.4	Game element: Parts crisis	72
A.5	Game element: Unusual activity triggered by SIEM tool	73
A.6	Game element: Government intervention.	73
A.7	Game element: Denial of service attack.	74

List of Tables

4.1	Roles and character prompts for tabletop exercise	32
4.2	Adversary goals for different scenarios	35
5.1	Summary of AS6171 test methods	52
A.1	Severity scale for security threats	74
A.2	Likelihood of security breach in supply chain phases	75
A.3	Detectability of threats in the supply chain	75

List of Abbreviations

ADAS Advanced Driver Assistance Systems [8](#)

APMA Automotive Parts Manufacturer Association [2](#)

BSI Blue Solutions Inc. [28](#), [31](#), [34](#), [37–40](#)

CAD Computer-Aided Design [2](#)

CAPEC Common Attack Pattern Enumeration and Classification [14](#)

CKC Cyber Kill Chain [14](#)

DOD Department of Defense [2](#), [49](#)

ECU Electronic Control Unit [39](#)

ERAI Electronic Resellers Association International [3](#), [8](#)

GIDEP Government-Industry Data Exchange Program [3](#), [49](#)

IC Integrated Circuit [2](#), [7](#), [8](#), [22](#), [53](#), [54](#), [56](#)

ICS Industrial Control System [6](#)

IP Intellectual Property [viii](#), [ix](#), [1](#), [2](#), [10](#), [11](#), [22](#), [33](#), [37](#), [38](#), [48](#), [54](#)

IVI In Vehicle Infotainment [31](#), [34](#)

NCWF National Cybersecurity Workforce Framework [14](#)

NIST National Institute of Standards and Technology [26](#), [56](#)

OEM Original Equipment Manufacturer [5](#), [9–11](#), [26](#), [31](#), [39](#), [40](#), [52](#), [53](#)

OT Operational Technology [6](#)

PUF Physically Unclonable Functions [53](#)

RSI Red Solutions Inc. [28](#), [31](#), [34](#), [37–40](#)

TPM Threat Priority Metric [41](#)

TTX Table top Exercise [6](#), [7](#), [11](#)

VPN Virtual Private Network [21](#)

Chapter 1

Introduction

The term “Hardware Security” is a multifaceted domain associated with the secure design of the hardware, access control, securing the cryptographic keys, firmware authenticity and supply chain security. The security and authenticity of the supply chain is a growing concern as the industries are mostly not ready to acknowledge the cybersecurity risks of a hardware component in the supply chain. The concept of trusting the vendors and suppliers is deeply rooted in the functioning of the industries. This cycle of trust has become an epidemic in the defense and aerospace industries as there have been multiple incident reports of components of lower quality in the supply chain. There have been reported cases where an unrecognized alloy magnet in the F-35 fighter jets has caused a huge disruption in their day-to-day function due to insufficient security practices in the supply chain [51].

1.1 Motivation

The product manufacturing phases typically include Intellectual Property [IP](#) design, fabrication, assembly, testing and packaging, and lastly, the recycling phase. Each phase in the manufacturing life cycle needs to be meticulously monitored and traceable to avoid tampering with product designs. It is paramount that these electronic devices are certified to be reliable and devoid of any safety hazards or security threats along their overall life cycle. With the horizontal supply chain model where multiple entities apart from the design owner are involved in manufacturing the product, it has become increasingly difficult to maintain accountability for the components that go into the final hardware design. Without a robust security system, a rogue player within the process—such as an

IP provider, an Integrated Circuit [Integrated Circuit \(IC\)](#) design house, a Computer-Aided Design [Computer-Aided Design \(CAD\)](#) company, a foundry, a distributor, or a system integrator can easily steal IP or tamper with the IP design. Additionally, there is a risk that an external adversary might steal or alter the IP to extract data or perform other malicious operations [50].

Despite the widespread discussions on software and hardware security, supply chain security in hardware is often overlooked. Yet, it is crucial to ensure the integrity and reliability of devices from production to deployment. A survey conducted amongst the hardware part manufacturing leaders in the local Automotive Parts Manufacturer Conference [Automotive Parts Manufacturer Association \(APMA\)](#) has shown that security in the supply chain needs to be more widely acknowledged. Many industries do not recognize the threats to hardware in the supply chain and strongly believe in their vendors and suppliers to provide the requested components. The Department of Defense [Department of Defense \(DOD\)](#) began to realize the importance of securing hardware early in the manufacturing life cycle due to rising cases of reported counterfeits in mission-critical electronics.

1.2 Contributions

Several failures in mission-critical operations due to components like capacitors, resistors and microcontrollers have recently been brought to the attention [40]. These failures are triggered due to the lack of hardware supply chain integrity checks and stringent supplier verification practices. This thesis makes significant contributions to the field of cybersecurity within the hardware supply chain in the following ways:

- This thesis contributes to raising awareness on the supply chain cybersecurity by collating work in gamification of cyber training and summarizing supply chain cyber incidents.
- The thesis proposes using tabletop exercises to educate the risks of a trust-based supply chain.
- It also provides an incident response framework to quantify the impact caused by vulnerabilities identified in tabletop exercise and address them by adopting the appropriate countermeasures.

1.3 Objective and Importance

A survey conducted by the Department of Commerce’s Bureau of Industry and Security revealed that the defense supply chain had witnessed double the number of reported

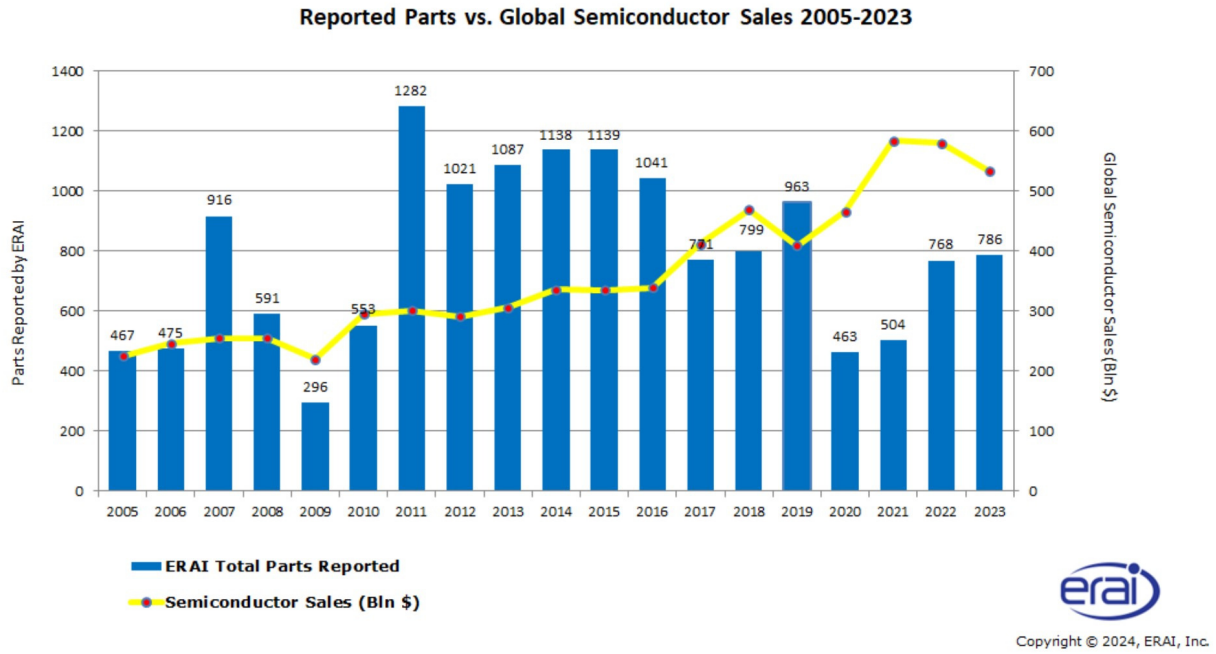


Figure 1.1: Parts reported to ERAI vs semiconductor sales [3]

counterfeit components incidents in 2008 [18]. The semiconductor industry has witnessed a spike in reported cases of counterfeit and substandard parts that infiltrate the supply chain and end up being deployed in electronics used in mission-critical sectors. The failure of one tiny component could pose significant safety and national security risks and lead to additional financial burdens due to product downtime and restorative operations. To address this problem, several organizations like Electronic Resellers Association International [Electronic Resellers Association International \(ERAI\)](#) and Government-Industry Data Exchange Program [Government-Industry Data Exchange Program \(GIDEP\)](#) have taken initiatives to curb the proliferation of fake, unreliable components from entering the supply chain by creating a database of hardware components that have been reported as a counterfeit component. Figure 1.1 shows the number of parts reported to the [ERAI](#) database versus the revenue recorded in the semiconductor market from 2005 to 2023. It is crucial to highlight the vulnerabilities in the hardware supply chain to safeguard the hardware from early life cycle failures.

1.4 Organization of the Thesis

The rest of the thesis has been organized into six chapters. **Chapter 2** provides background information on each type of attack in the hardware supply chain. **Chapter 3** provides a literature review of existing game-based learning methods to teach cybersecurity concepts and skills engagingly and effectively. **Chapter 4** describes the game mechanics and the components of a tabletop cyber security exercise for hardware supply chain. **Chapter 5** presents an overview of hardware countermeasures to build a robust supply chain and **Chapter 6** presents the conclusion and future scope of the study.

Chapter 2

Background

The root cause of security threats in the hardware supply chain was the fundamental concept of trust built over years of trade and partnership. The problem began when some suppliers took advantage of this trust and started sourcing components of lower quality (old, reused), referred to as counterfeit components, and selling them as newly manufactured components. These components are incorporated along with thousands of other electronic parts in a printed circuit board, which are later deployed in mission-critical industries where the product's lifetime's safety and reliability are of utmost importance. A part that needs to be incorporated into military, defense and aerospace industries generally undergo rigorous testing, and the temperatures for military-grade parts are higher than that of a commercial electronic part. Another common practice of fraudulent suppliers is to sell commercial-grade components as military-grade components where the components pass the initial testing phase in the [Original Equipment Manufacturer \(OEM\)](#) testing facility and trigger failure much before their expected lifetime. The U.S. Senate Armed Services Committee reports that around 1800 cases of suspected counterfeit parts went into more than 1 million individual products.

Furthermore, obsolescence also contributes to the increased counterfeit parts in supply chain. Obsolescence is the process of a product or technology becoming outdated and no longer used, often because newer, more efficient versions have replaced it. Generally, when an electronic part reaches the end of the production life cycle, the original component manufacturer announces the availability of the last batch of the component. The prime and subcontractors in the relevant industry bid to purchase the previous batch of the electronic part to ensure the continuous availability of component requirements/replacement post their obsolescence. A commercial electronic part lasts 6 to 10 years. In contrast, an electronic part used in fighter jets and other defense aircraft is expected to have a greater

life expectancy, as military-grade jets have a life expectancy of around 30 to 90 years. It is of profound importance that when one component is replaced due to obsolescence, the replacement meets the reliability criteria, as failure due to one of the low-quality components shall cause serious repercussions.

2.1 Cybersecurity in Critical Infrastructure

The critical infrastructure consists of many physical, non-physical, and cyber resources or services essential for a society's and its economy's basic operation [78]. Cyberattacks in the critical infrastructure like the Ukraine power grid [87], Colonial pipeline [41], and the Solarwinds supply chain attack [67] are some of the popular cases of raising concerns among industries. Compromising the security of the mentioned sectors through cyberattacks could cause breach of trust, crippling financial impacts and economic disruption. A common entry point for malicious entities is taking advantage of the less secure supply chain, where there is a greater chance of oversight due to inbuilt trust between suppliers, vendors, contractors, and foundries to launch an attack on the company.

A common misnomer in the industry is that cybersecurity in supply chain is the same as [Industrial Control System \(ICS\)](#)/[Operational Technology \(OT\)](#) security. The fundamental difference between [ICS](#)/[OT](#) security and supply chain security is that the former is focused on protecting the operational integrity and security of industrial control systems while the latter focuses on authenticity and safety of the physical hardware components from design, manufacturing to recycling phases. It addresses risks like counterfeit components, tampering, and unauthorized production modifications used across multiple critical infrastructure industries including the [ICS](#)/[OT](#) environments.

2.2 What is a Table Top Exercise

A [Table top Exercise \(TTX\)](#) is an informal discussion-based session conducted to test the responses of different stakeholders of an organization in the event of a crisis/disaster. The exercise helps review the roles, responsibilities, procedures, and policies needed to navigate the crisis. It is usually conducted in a board room setting where all the important executives of an organization sit through simulations of several crises deemed relevant to the company's business line. A facilitator usually conducts these sessions in a risk-free, calm environment with no serious outcomes if the players make wrong decisions during the exercise. [TTX](#) help brainstorming and identify gaps in the organisation's contingency and incident response plans to ensure the plan content is viable and implementable in case of an actual crisis.

2.3 Table Top Exercise in Cybersecurity

A Tabletop Exercise simulates any disaster or crisis and brainstorms the organization's incident response strategies. Multiple studies have shown promising learning outcomes of complex security concepts, which are discussed using TTX to raise awareness about specific disasters and crises. Wendelboe, Aaron M., et al. used the TTX to help organisations prepare for a health crisis [80]. Chi, Chih-Hsien, et al. used the TTX to train the medical technicians on disaster management practices [11]. High, Erika H., et al. proposed using TTX to help prepare for chemical disaster management [37].

Cybersecurity is a constantly evolving field, with new attacks discovered every day. In the context of cybersecurity, game-based learning approaches have shown positive outcomes in creating awareness about the current cybersecurity threats and the impact made by them. A TTX is a great way for the stakeholders of an organization to learn about the concepts of cybersecurity and the vulnerabilities in their organization to review their incident response protocols and implement changes required in sync with the executives of an organization when a similar event is encountered in the future.

2.4 Types of Threats in Hardware Supply Chain

In the early 1970s, a typical piece of hardware consisted of 2300 transistors, and as the computing complexity of hardware has increased, we can see billions of transistors in them. A typical NVIDIA GB200 Grace Blackwell, built on TSMC's 4 nm process, has recorded to have 203 billion transistors. In addition to transistors, hardware consists of micro controllers, microprocessors, logic devices, and memory components [54]. This astounding growth in the semiconductor industry has opened pathways to new attack surfaces for cyber criminals to exploit. Among multiple complex circuitry, finding a tiny piece of Trojan circuit or backdoor inserted to sabotage the operations or steal information is almost impossible. The following sections mentions in detail about types of hardware cyber attacks in a supply chain.

2.4.1 Counterfeiting

Counterfeiting is an illegal practice that involves the unauthorized copying of the original designs for monetary gains. Counterfeit ICs are usually characterized as having inconsistent performance and compromised quality. If counterfeit ICs are integrated into electronic devices, they could significantly compromise the device's quality, reliability, and performance. For example, using such counterfeit ICs in essential military operations could be deadly, possibly undermining the security and dependability of military electronic systems and negatively impacting a country's innovation and economic growth. For example, counterfeits

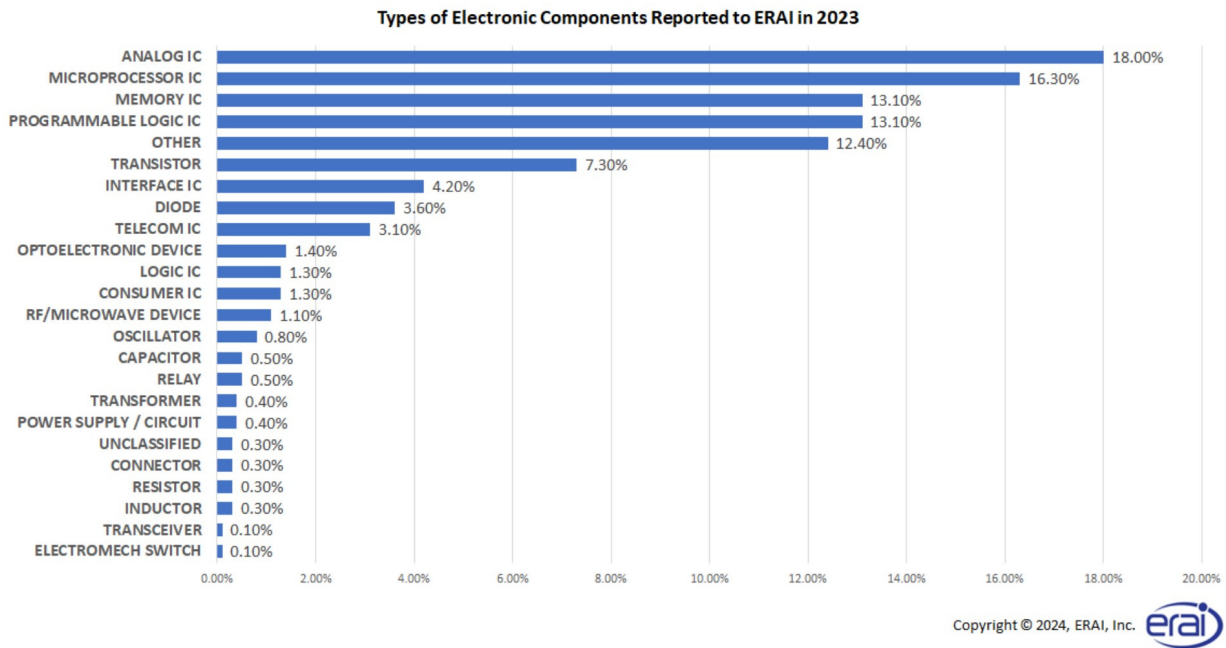


Figure 2.1: Types of components reported to ERAI [3]

in an [Advanced Driver Assistance Systems \(ADAS\)](#) electronic control unit, such as sensors, could seriously threaten human lives. Counterfeit in the country's defense sector (fighter jets and airplanes) could impact the safety and security of a country.

It is observed that the five most frequently counterfeited components, which include analog ICs, microprocessor ICs, memory ICs, programmable logic ICs, and transistors, pose a potential annual risk of 169 billion dollars to the global electronics supply chain, according to all counterfeit incidents reported in 2011 [27]. Figure 2.1 shows a report from the ERAI showing the different electronic components reported to the ERAI database as a suspected counterfeit part.

There are multiple ways to replace an original component with a counterfeit component in the hardware supply chain. Figure 2.2 shows a taxonomy of counterfeit components identified to date.

Recycled Components

Recycled components are those that have been previously used in other devices, removed from those devices, cleaned, possibly retested, packaged, and sold as new components [5]. The components of the old hardware are removed in a highly heated environment using

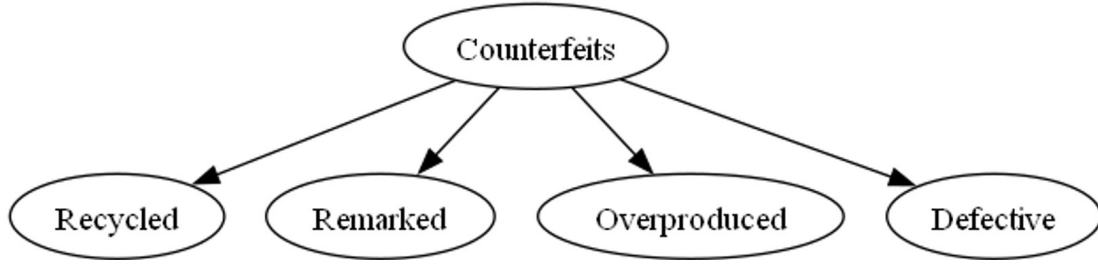


Figure 2.2: Taxonomy of counterfeit components

unconventional methods. These components often fail to meet the original manufacturing specifications due to missed quality assurance steps, leading to early failures in the field.

Remarked Components

Remarked components are lower specification or lower grade chips falsely labelled as a higher specification or higher grade part (e.g., commercial grade chips being sold as military-grade). This is typically done by altering or replacing the markings on the chip that indicate its grade and performance characteristics. The process includes sanding, painting, and grounding a lower-grade component to make it appear as good as new [30].

Overproduced Components

An untrusted foundry or assembly with access to a designer's intellectual property has unilateral control over the production and assembly of chips. These parts undergo the same manufacturing processes as the original components. If a consumer or supplier acquires these parts, they may not face any immediate risks, but integrating these counterfeit parts could be a liability to the OEM as they do not undergo the same quality assurance and verification procedures as a certified part, which could trigger unexpected failures in the hardware. Overproduced components do not meet the same stringent quality control standards and rigorous testing as the original parts, making it very challenging for the parts procurement team to detect these components [55].

Defective Components

Large batches of components undergo testing procedures to be certified for commercial and military-grade equipment use. When some components fail to meet these quality assurance standards due to functional defects, storing them until they are responsibly discarded properly is important. An oversight from the component manufacturer's end might lead

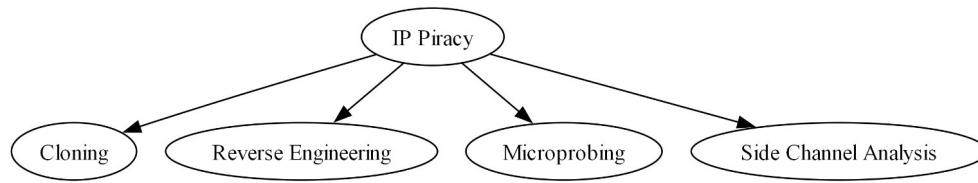


Figure 2.3: Types of IP piracy

to these rejected components finding a way back into the hardware supply chain. The malicious actors within the industry might potentially sell the components to unscrupulous entities without disclosure of their defects as original component, which in turn lowers the reliability of the product’s operational life cycle.

2.4.2 IP Piracy

IP piracy occurs when the rogue designer/ foundry has partial or complete access to the design files and gate-level net list to create a similar product [32]. The major types of IP piracy are cloning and reverse engineering. These unauthorized copies are created by copying the original component’s research and design efforts and reproducing them without the manufacturer’s authorization. Cloned components emulate similar design characteristics to a great extent and are sold at significantly lower rates, lowering the manufacturer’s market share and overall profits.

Reverse engineering of components could be achieved when a malicious foundry or rogue designer has access to partial forms of IP design files. They use the little information available to them to deduce the specifications of the original component. Other forms of IP Piracy include theft of data where sensitive information about the product is inferred by observing relevant patterns in the encryption keys, private data, and user credentials. Micro-probing and side-channel analysis are well-documented examples of data theft in a product [32]. Micro-probing is another well-known type of IP piracy, which is achieved by inserting a microscopic needle into the internal wiring of the hardware, which gives out sensitive design information about the component. The side channel attack is achieved by exploiting the dependency created between the physical characteristics of the system and the secret information like timing, electromagnetic emission, power consumption [74]. Any form of design piracy heavily disrupts OEM operations and causes a financial impact in the long run.

2.4.3 Tampering

Tampering with hardware in the supply chain is adding additional circuitry to the original hardware [IP](#) that serves as a logic bomb or as a backdoor which could leak sensitive information [\[9\]](#) or be modified to perform malicious operations. The common possibility of tampering with hardware in the supply chain is the fault injection and trojan insertion. In a fault injection attack, the cryptographic algorithm is targeted, resulting in cryptographic algorithm computation errors. The attackers look for a pattern of hardware vulnerabilities to gauge it later to cause data breaches and security risks. Threat actors perform trojan insertion by modifying or inserting a backdoor capable of executing malicious attacks or exfiltrating data. A trojan could be activated from a remote location using sensors and antennas as discussed in [\[57\]](#), modifying operating conditions [\[48\]](#), [\[20\]](#). Generally, a trojan could stay dormant and undetected for a prolonged duration unless the right combination of logic is executed.

2.4.4 Insider Sabotage

In hardware supply chain security, insider sabotage is bound to occur when the [OEM](#)'s direct competitor, estranged employees or suppliers deliberately aim to damage the hardware to ruin their reputation. A sabotage attack is feasible in any phase of the hardware in the supply chain. A famous incident of sabotage attack, which is also discussed in one of the [TTX](#) scenarios of the thesis, is when a company ruins the maintenance operations of their competitor to win the contract held by them in the past [\[6\]](#). Another way to execute sabotage attacks is by creating hurdles in one of the hardware manufacturing phases, which could potentially increase the time to market, causing monetary loss [\[32\]](#).

Chapter 3

Literature Survey of Game-based Learning Models

In this chapter, we discuss gamification in cybersecurity and its advantages for learning about cybersecurity concepts in an interactive, engaging way. We further learn about the several existing pedagogical frameworks/models used to create a targeted game-based training method to maximize the learning outcome of exercises incorporated through serious games. This chapter also discusses the most relevant serious games used in literature to create awareness and training about crisis management and planning in cyber security.

Gamification

Gamification in cybersecurity is an approach which uses game design elements such as role-playing, and simulation of the threat scenario in a competitive environment to educate the professionals about cybersecurity principles and practices, thereby enhancing awareness, education and training of the latest threat tactics, techniques, and persistence of malicious actors. It leverages the ability to engage a wide audience to learn about the state-of-the-art security protocol implementation.

3.1 Pedagogical Learning Model

Serious games are used primarily for purposes beyond entertainment, such as education, training, and behavior change. They provide an interactive and engaging way to learn, practice, and understand complex concepts through simulation and game play mechanics. These

games enhance learning retention, motivate participants, and facilitate the development of practical skills in a risk-free environment. The literature contains several pedagogical theories and learning models that aid in increasing the learning outcome of a serious game which are discussed briefly in the following sections.

3.1.1 Bloom's Taxonomy

Bloom's Taxonomy is a model created to be used as a guide in developing, teaching and providing instructional content for a wide range of audiences. The revised taxonomy version promotes engagement while delivering instructional content efficiently [47]. The categories in this taxonomy briefly fall into a broader category of cognition, affective and psycho-motor skills to help designers curate games that effectively engage the participant.

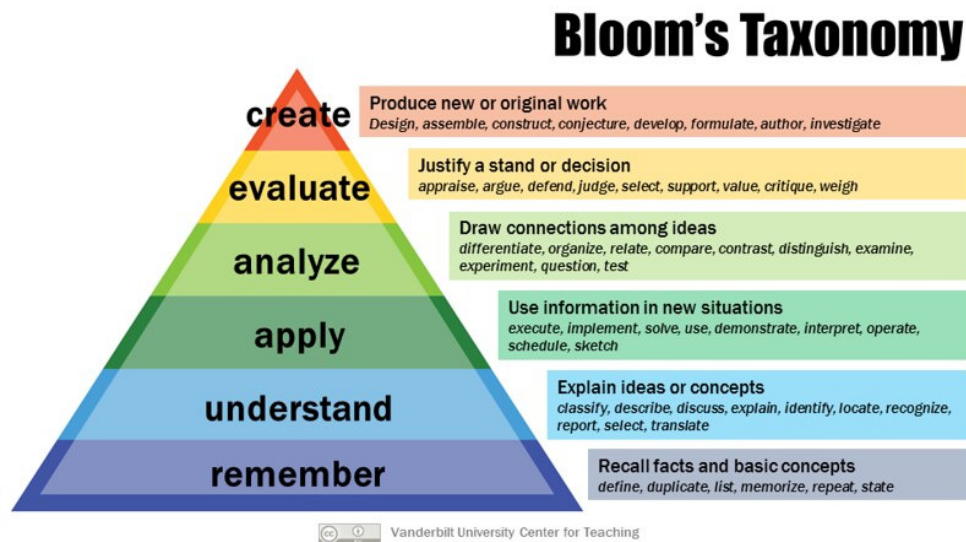


Figure 3.1: Bloom's revised taxonomy [77]

3.1.2 Kirkpatrick Model

The Kirkpatrick model is used to evaluate the learning outcomes of a training program by using four different parameters: reaction, learning, behaviour and results of the training program [44]. In the reaction (Level 1) phase, the participants record their responses to the training program through feedback surveys, followed by a learning phase, which measures the new skills/information gained through the program. The behaviour phase is used to

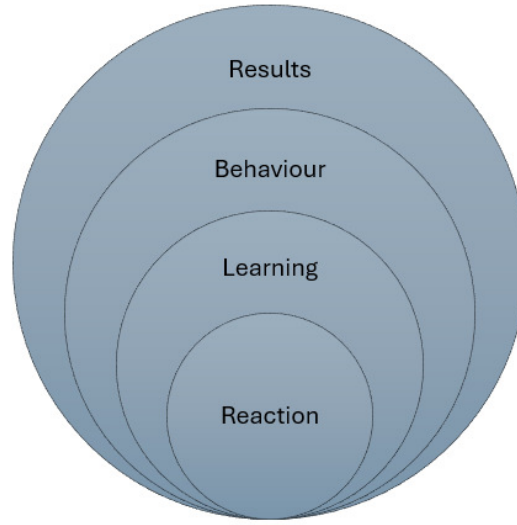


Figure 3.2: The Kirkpatrick Model

observe how the employees use these newly learnt skills. The results phase is measured in terms of the overall improvements brought by implementing the training program.

3.1.3 COFELET Framework

The Conceptual Framework for e-Learning and Training (COFELET) was created to improve the learning outcomes of a serious game [42]. The framework integrates elements from the Activity Theory Model for Serious Games (ATMSG), the [Common Attack Pattern Enumeration and Classification \(CAPEC\)](#), the [Cyber Kill Chain \(CKC\)](#), and the [National Cybersecurity Workforce Framework \(NCWF\)](#) to help develop a serious game that improves pedagogical effectiveness of cyber security training. It requires the participants to complete dedicated tasks stipulated by the game that carry a learning objective and educational content to accomplish the game goals.

3.1.4 MOTENS Model

The MOTENS is a pedagogical model developed based on the lessons learnt while designing the game “Riskio” to help evaluate the effectiveness of serious cyber games. The “Multiple Modes of Learning” allow players to explore different types of cyber-attacks and their defences [34]. It will enable players to take “Ownership” of their learning outcomes by customizing the game scenarios by backing the “Theory” that synchronizes with the original

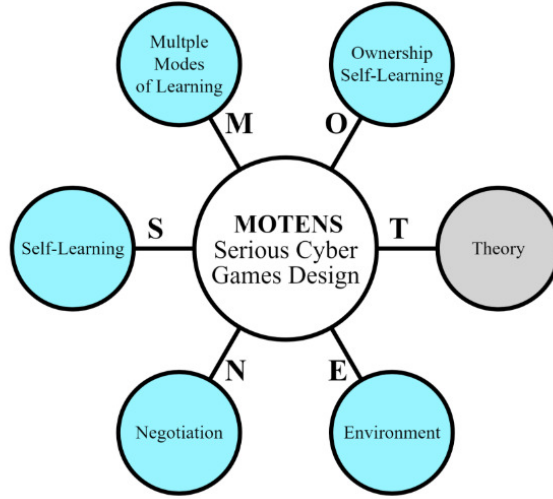


Figure 3.3: MOTENS model [34]

game design. The users play the designed game in their desired/preferred “Environment” to accelerate the learning outcome. The “Negotiable” aspect of the model allows the teacher to be a coach that transforms lecture-style teaching into a problem-based learning experience. Lastly, the model enables “self-learning,” as the games based on the MOTENS model can be played without a facilitator or a game master.

3.2 Serious Games in Cybersecurity

Serious games in cybersecurity are educational tools designed to simulate real-world cyber threats and scenarios. These interactive games engage participants in learning about cybersecurity practices, enhancing their skills and knowledge through practical application. Serious games are created to incorporate the game elements into non-game contexts. These serious game-based learning and training programs have proven to be an effective way of testing an organization’s incident response plan to analyze the current plan of action and discuss the areas of improvement at the end of the session to be better prepared at the time of an actual crisis [4]. The following sections provide a brief overview of the existing serious games used in cybersecurity.

3.2.1 STRIDE

STRIDE is a threat model designed to teach participants about the different categories of security threats. STRIDE is an acronym that stands for Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege. The learning outcome of STRIDE is to educate players on identifying and categorizing potential security threats in software applications and systems using the STRIDE methodology [69]. STRIDE consists of game cards that describe a component, user action, or system process that could be vulnerable. It comes with a game board and scenario cards that depict and define various components of an IT system, where players can place threat cards. It also comes with role cards that assign the player as moderator, attacker, or defender.

Game Play

The board is set up and the respective game cards are distributed which define their roles and responsibilities. The players discuss the vulnerabilities that are identified in the IT systems and classify the threats using the STRIDE threat taxonomy. Furthermore, discussions are facilitated to learn how these threats can be mitigated and improve the system's security.

3.2.2 DREAD

DREAD is a risk assessment methodology by Microsoft that detects and prioritizes threats to mitigate serious threats. The name is based on the different attack categories for Damage Potential, Reproducibility, Exploitability, Affected Users, and Discoverability. Each threat actor's damage potential is scaled from 1 -10, and every threat's overall risk factor is calculated. After assigning each category to a numerical value, the sum of the values calculated shows the risk value to the organization if an attack occurs [38].

Game Play

The DREAD method is a threat classification and assessment method. It is a quantitative assessment method which enables the security analyst to rate and compare the evaluated risks, further helping them to prioritize the threats based on their severity rating. Risks with a higher severity rating shall be addressed first, followed by others in order of criticality. The overall threat rating is categorized as Critical (40-50), High (25-39), Medium (11-24) and Low (1-10).

3.2.3 Planning Poker

Planning poker is a consensus-based technique used to estimate the effort or complexity of project tasks in software development for agile work development. It involves all development team members to collect and give realistic estimates of work [26].

Game Play

In planning poker, each participant is given a set of cards numbered as a fibonacci sequence (0, 1, 2, 3, 5, 8, 13, 21, etc.). The facilitator presents a task or user story and asks each team member to estimate the time needed to complete the task, which is decided based on time, complexity and size. When asked by the facilitator, the team members reveal their private estimates, and a discussion is encouraged to allow each member to present their thought process, which gives an estimate. The final estimate is fixed after every team member agrees to the final decision. Even though this game is not directly relevant to the tabletop exercise, the key takeaways of team collaboration, allocation of resources required for completing a task, scenario development, and participants' engagement through gamification help create a customized tabletop exercise.

3.2.4 Protection Poker

Protection poker is derived from planning poker. It differs from the latter, focusing on security risk assessment rather than estimating effort. The game aims to increase the team's awareness of several security vulnerabilities in software through a detailed threat analysis and risk assessment. It is performed in iterations, and at the end of each iteration, the participants review the verification and validation effort needed to mitigate those risks [81].

Game Play

The facilitator or product manager gives out a new requirement to members of a development team to understand its scope and implications. The team then investigates the security aspects of the requirement. A wide range of scenarios are discussed regarding what happens in the event of data deletion, data theft, corruption, and the possibility of an insider exploiting the new functionality. After identifying the security vulnerabilities, the team votes on the security risk components. It is generally evaluated as follows:

$$Risk = (\text{probability of loss}) * (\text{impact of loss}) \quad (3.1)$$

Protection poker determines the risk of a flaw using the improved formula as stated below.

$$(\text{Security risk}) = (\text{ease of attack}) * (\text{asset value}) \quad (3.2)$$

The ease of attack and the asset’s value are determined through an anonymous voting process where members use a predefined scale of numbers (1, 2, 3, 5, 8, 13, 20, 40, 100). Votes are revealed, and a consensus is reached after a discussion and several iterations of voting. The final risk score is calculated by calculating the product of the agreed-upon values for ease of attack and asset value. This game-based learning method sets a great example for fostering a discussion-based learning environment to evaluate the security flaws in a product.

3.2.5 Elevation of Privilege

Elevation of privilege is one of the earliest models of threat modelling techniques proposed by Shostack et al. It is designed to be played during the design phase of software development and aids the team in identifying and mitigating vulnerabilities. The game comes with a deck of cards of different categories of threats based on the STRIDE threat model. The categories are Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege [70].

Game Play

The game is typically played with 3 to 6 players and could last for 30 minutes to an hour. Each player takes turns to draw a card from the deck. The players go around the table describing a threat in their system that matches the description in the drawn card. The team further discusses the impact and likelihood of the occurrence of the security risk. The major goal is to finish the entire deck to ensure a comprehensive discussion of the threat to understand their system’s security needs. The game’s benefit is that it simplifies the understanding of threat assessment for non-security professionals. Multiple game versions were created based on the elevation of privilege such as OWASP Cornucopia, Elevation of Privacy, OWASP Cumulus and Elevation of MLsec.

3.2.6 Control Alt Hack

Control Alt Hack is a tabletop card game designed to create awareness of computer security challenges and the risks of not having proper security defense mechanisms. The game provides a fictitious company called “Hackers, Inc” with a motto where players assume the role of a white hat hacker motto of “You pay us to hack you”. It’s a fun, collaborative, game-based learning method for learning about computer security [17].

Game Play

In Control Alt Hack, each player assumes a role with unique abilities that influence the overall turn of events in the game. The deck includes character cards, mission cards, tool cards and scenario cards. They are given tools and other resources like software tools, hardware devices and social engineering tactics to accomplish missions, such as solving a puzzle, cracking a password or securing a network. The game ends, followed by a discussion to brainstorm the scenarios, threats encountered and their implications in the real world.

3.2.7 Play2Prepare

Play2Prepare is a board game designed to create awareness of IT security incidents for industrial control systems. The game has several scenarios and threats simulated through a large-scale attack on the electric power grid. The learning outcome of this game is to help organizations improve their incident response plan strategy [23].

Game Play

The game consists of a board that depicts a network where the players move their pawns around the game board to prevent attacks that spread with each round. It shall be played amongst 3-4 players, and each player has unique skills to mitigate the attacks. It consists of role cards, attack cards, attack propagation and fact cards. The game simulates IT security incidents throughout the game that the players must mitigate using their roles and other information given to them. It's an ideal example of educating an industry on the relevant cyber attacks.

3.2.8 Decisions & Disruptions

Decisions & Disruptions is a tabletop game designed to create awareness about industrial control systems [21]. The players are challenged to manage the operations of a utility company, where they make management-related decisions to ensure the smooth functioning of their infrastructure. The game is designed to create awareness of cybersecurity threats to which a company's asset may be prone. It fosters a culture of team collaboration, strategic decision making and risk management.

Game Play

The game shall be played with a team of 5 to 7 players along with a game master who shall give the narrative of the game and guide the players into making the appropriate decisions.

The game also allocates a budget to the company that allows the players to decide on the initiatives that would suit their company’s financial state while ensuring protection from the several cybersecurity threats discovered while playing the game.

The game consists of a physical game board with the company’s network and physical infrastructure, including the workstations and servers. Players take on roles in an organization, such as the CEO, CFO, CTO, and security manager, who provide their perspective from the perspective of the roles assigned to them. It consists of threat cards which depict cyberattacks like data breaches, ransomware, and insider threats. The impact of the threat is evaluated based on the budget allocated for each cyber attack.

3.2.9 LINDDUN GO

LINDDUN GO is a threat modelling tool designed to identify and manage cybersecurity and privacy risks in a software system. It was originally adapted from the LINDDUN framework into a card-based game format to reduce complexity and foster systematic analysis of security risks in a system. It is designed for beginners who need to gain a technical background in security to understand threat modelling [82]. The learning outcome of this game is to simplify the concepts of privacy, encourage the designers to implement privacy-related features in the early stages of software development and improve communication among team stakeholders.

Game Play

The LINDDUN framework stands for Linkability, Identifiability, Non-repudiation, Detectability, Disclosure of Information, Unawareness, and Non-compliance. The game helps classify the threat encountered in their software into one of the above threat categories. It starts by using a data flow diagram to model the software system, drawing the threat cards, and checking whether they apply to the modelled system. Later, the game focuses on developing mitigation strategies to mitigate the identified threat. This game is played in a collaborative discussion-styled manner to elucidate the cyber threats of a software system.

3.2.10 Cyberwar Gaming

Cyberwar gaming is an innovative gamification approach to increase awareness of cyber security threats by projecting threats in a war gaming environment and analyzing their effectiveness in an educational setting. The players discuss risk assessment and strategic decision-making to prevent organizational threats. The learning outcome of the game is

to get a deeper understanding of cybersecurity threats, strategic decision-making under pressure, and improved incident response strategies [31].

Game Play

Cyberwar gaming consists of realistic cyber threat scenarios discussed among organizational stakeholders. The game begins by assigning executive roles to players in an organization, such as network administrator, security analyst, incident responder, or strategic decision maker. Players are given details about the scenario of a specific cyber attack and are required to discuss their strategies to contain the severity of the attack and implement preventive measures. Examples of scenarios could be a data breach or a cyber attack on national infrastructure. The preventive measures mentioned in the game literature are deploying a firewall, forensic analysis, and coordinating with police and legal enforcement. Cyberwar gaming is another innovative implementation of a tabletop exercise.

3.2.11 Cyberceige

Cyberceige is designed to teach principles of information assurance using a video game interface. The players spend virtual game money to operate and defend networks and learn about the consequences of the decisions through a virtual game setting in the cyberceige game [39]. It largely covers topics of computer and network security and defense. The learning outcome of the game is to learn about cybersecurity principles and implementing defense measures within a budget while managing the organization's productivity.

Game Play

Cyberceige game is a real-time simulation of an organization in a virtual game setting with packages that allow players to buy and configure workstations, operating systems, servers, applications, and network devices. Furthermore, it enables in-game configuring of firewalls and [Virtual Private Network \(VPN\)](#), linking encryptors and implementing access control mechanisms. The attack type comprises insider attacks, trojan horses, trap doors, denial of service attacks, and exploiting weak configurations in existing system infrastructure. The attacker's motive varies in each game scenario depending on the asset under attack. The game is organized to constantly evaluate the trade-offs between the implemented security measure and how it affects business continuity. It also allows facilitators/educators to create custom scenarios applicable to their organization.

3.2.12 d0x3d

d0X3d is a board game-styled tabletop exercise designed to teach the concepts of computer network security and create interest in pursuing a career in cybersecurity. Players take the role of white hat hackers who work together to protect digital assets from a network controlled by adversaries [22]. Players learn the importance of data protection and the dynamics behind securing an asset and think strategically in collaboration with top stakeholders in the event of a cybersecurity breach.

Game Play

d0X3d game consists of digital assets like Personally Identifiable Information (PII), financial data, authentication credentials, and IP. The game's goal is to infiltrate a network, navigate along the gameplay to recover the stolen assets and escape the game without being detected by the network administrators who play the role of adversary. The game intends to teach security definitions like zero-day, intrusion detection, compromise, patch and forensics in the gameplay. The game components include digital loot cards that give information about system vulnerabilities or the data associated with a particular asset category.

3.2.13 CIST

The CIST game is a serious game designed for learning about cybersecurity risks in hardware supply chain [35]. The primary learning outcome of the CIST game is to enhance players' awareness and understanding of cybersecurity attacks and defense mechanisms within the IC hardware supply chain. Players learn to identify and categorize potential security threats using the CIST threat model and apply appropriate countermeasures. The game is a single-player web-based learning model that incorporates various components, including a threat model specifically designed for hardware threats, gameplay scenarios that cover different stages of the IC supply chain, and interactive elements in which players analyze attacks, identify the type of threat, and select countermeasures.

Game Play

Players engage in the game by going through scenarios that present different types of security threats at various stages of the IC supply chain. They must analyze each scenario, determine the appropriate threat category using the CIST model, identify potential attackers, and choose suitable countermeasures from a set provided. The game aims to simulate real-world decision-making and problem-solving within the context of IC hardware security.

3.2.14 Riskio

Riskio is a board game designed to enhance cybersecurity awareness among individuals without a technical background employed in an organization. The game creates a dynamic learning atmosphere by allowing players to actively engage and accumulate knowledge about cyber threats and protective measures [36]. The game components include a fictitious organization setup, attack and defense cards covering a wide range of potential cybersecurity threats and countermeasures, and role cards allowing players to assume specific responsibilities within the game.

Game Play

The players within the organization assume the roles of attacker and defender. Each turn, a player draws from the attack deck and formulates a potential threat based on the card, and then other players use defense cards to propose countermeasures. The game fosters a dynamic learning environment for playing the offence and defense roles. This process helps players understand the complexity of cybersecurity and develop strategic thinking about real-world cyber defense.

3.2.15 Backdoor and Breaches

The game Backdoor and Breaches is designed as a tabletop exercise to help students and professionals practice incident response during a cybersecurity breach. The primary objective of backdoor and breaches is to improve participants' skills in cybersecurity incident response. It teaches players how to effectively analyze and respond to various cyber attack scenarios using real-world tools and techniques [86]. The game has an incident master who facilitates it, presents the scenario, challenges players, and records their responses. It has game cards divided into several categories, such as Initial Compromise, Pivot and Escalate, Persistence, C2 and Exfil, Procedure, and Inject. A dice introduces randomness in the game's outcome by simulating the unpredictability of a real-world incident response.

Game Play

The incident master draws attack cards from various categories, creating a unique security incident without revealing specific details to the defenders. Defenders are given a set of procedure cards to address the incident. Gameplay involves strategically selecting procedure cards and rolling a 20-sided die to determine the success of chosen responses. Points are added from the cards and dice rolls to decide if the defenders' actions successfully mitigate parts of the attack. Inject cards may be used by the incident master to introduce additional

challenges or changes in the scenario, complicating the defenders' tasks. The goal for defenders is to uncover and mitigate all attack cards within a limited number of turns. The game encourages teamwork, problem-solving, and strategic thinking in high-pressure environments typical of cyber incident responses.

3.3 Key Takeaways from Existing Games

Serious games are targeted at a specific game audience to educate the concepts of cybersecurity. These games are designed to improve the learning outcome through experiential learning [4]. It has been shown to improve the retention of complex concepts when combined with game elements like character role-play, scorecards, and discussion. The key takeaways from the games discussed in the previous sections are as follows:

- The games, designed as a framework, focus on discovering new threats, categorizing them, and learning to prioritize the most vulnerable threats.
- The literature review covers many vulnerability identification methods in software, hardware, and industrial control systems.
- The above games enable the participants to provide their perspectives on each threat and suggest solutions for each threat, which fosters effective collaboration, which is crucial in an organization in the event of a cybersecurity breach.
- Most serious games have a facilitator or moderator who controls the game's flow to maximize the learning outcomes according to the specific organization's business requirements.
- Each game discussed in the literature review proposes unique ways for an organization to learn about cybersecurity concepts, like single-player online games, war gaming, scrum discussions, board games, video games and tabletop exercises.

Every game discussed in this chapter serves as a reference, which greatly helped design a customized serious game for conveying the cybersecurity risks in the hardware supply chain. The CIST game greatly inspired the game design for the TTX. We created the TTX design so that it could be played in a boardroom setting amongst a group of different stakeholders. The game components, such as the inject and reveal, are inspired by serious games like Backdoor and Breaches, d0X3d. The TTX, like the game Decisions and Disruptions, also contain players or participants who assume the role of different stakeholders. Adopting a fictitious company to deliver the security concepts was based on games like Control Alt Hack and Riskio. The key components of the TTX and other details are discussed in depth in Chapter 4.

However, there are few components from the games discussed in this chapter that was not considered while designing the table top exercise. The games discussed in this chapter are meant to be played as an actual board game with fixed outcomes that limits the potential of expanding new security threats unless the creators decide to release a latest version. However, the TTX is easy to adapt on the go and the facilitators can seamlessly introduce new security concepts into the game.

3.4 Advantages of Gamification in Cybersecurity

The advantages of adopting game-based learning in the cybersecurity landscape are as follows:

- **Enhanced Engagement:** The elements in a game, like the points, levels, attack and defence method, make the overall process of learning cybersecurity more enjoyable. It helps gain more participation and interest amongst employees of an organization.
- **Realistic Scenarios:** The gamified learning method usually refers to real-life cyber threats in a safe and controlled environment, which allows the users to learn about the threats without actual risks, which in turn helps them be better equipped to handle such crises in the future.
- **Behavioral Change:** Game-based learning influences the behaviour of the game character by rewarding actions that are considered desirable. For instance, rewarding the characters for implementing a strong password policy in the organization to act more responsibly in real-world scenarios.
- **Fosters Collaboration:** Simulating game-based learning practices improve coordination and communication among players/teammates. The game fosters community, crucial in responding to real-world cybersecurity incidents.
- **Game Metrics:** Gamification often includes tools to track performance and progress. The data is useful for identifying the weak points in their current strategies and targeting improvements more effectively.
- **Scalability and Accessibility:** Online gamification training solutions such as the CIST game [35] could be accessed by many users from different locations to train many employees in different geographic locations. The scalability also helps create a standard format adopted across large organizations.

Chapter 4

Game Methodology

The hardware supply chain has shifted its manufacturing model, with OEM's now opting to reduce costs by outsourcing various stages of production to third-party vendors, suppliers, and design foundries. This has contributed to the growth of malicious attackers profiting off this horizontal integration by introducing hardware products of unknown provenance to make more profit in shorter time span. Several cases of low-quality microchips and transistors have been reported, leading to compromise in the product's functionality causing serious threat to human life [13]. It is important to raise awareness of this problem so that organizations can implement the necessary policies to curb the proliferation of low-quality hardware products.

The main contribution of this thesis is modelling a tabletop exercise based on the existing game-based learning methods discussed in the literature survey chapter. This exercise aims to educate the executives of an organization about the cybersecurity risks involved in the hardware supply chain. It simulates scenarios based on real-world incidents that enable a discussion-based environment to summarize their state of art defense strategies, incident response plans and measures to upgrade the company's policies to ensure business continuity. The [National Institute of Standards and Technology \(NIST\)](#) has provided a framework that helps facilitators create a customized tabletop exercise for disaster and crisis management [24].

4.1 The Importance of TTX

There are many game-based learning categories discussed in Chapter 3. We chose the tabletop exercise as a way to convey the cybersecurity risks in a hardware supply chain. The design goals considered for developing a tabletop exercise are as follows:

- **Educate:** The tabletop exercise intends to educate and create awareness among the executives of an organization about the cyber threats and vulnerabilities in the hardware supply chain. The impacts of a cyber security breach and the post-incident management/recovery plans are to ensure business continuity, test their current policies and procedures, and modify them according to the changing threat landscape and business requirements.
- **Collaborative:** To enhance effective communication and engagement among top executives in different business verticals. Identify the roles and responsibilities of each individual during a cybersecurity breach and protocols to report the incident to the respective authorities and effectively convey it to the rest of the employees.
- **Adaptable:** Every organization and product supply chain is unique. The TTX is designed to customize the scenarios and threat medium unique to the specific organization by conducting an exploratory meeting to understand their assets and supplier interactions.
- **Enjoyable:** Information about cybersecurity risks is often conveyed through informative knowledge transfer sessions in a board room. This method might make the learning experience less fun. A tabletop exercise involves multiple stakeholders gathering and participating in a hands-on training session where active learning occurs. The scenarios are designed with an element of fun and surprise that could help in the long-term retention of cybersecurity concepts.

4.2 Game Components

The TTX game has initial information, character prompts, injects, and reveals throughout the discussion that decide the flow of the game. The summary of the TTX flow of events is summarized in Figure 4.1 below.

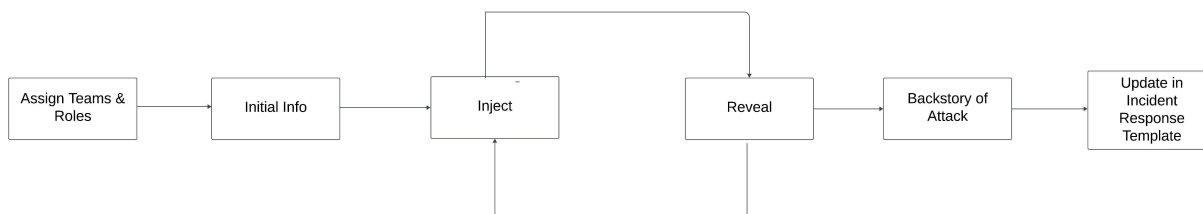


Figure 4.1: Tabletop Exercise: Game Flow

- **Initial Information** It gives details about [Red Solutions Inc. \(RSI\)](#) and [Blue Solutions Inc. \(BSI\)](#) to the respective team. It sets the stage for the participants to learn about the fictitious company information created by facilitators.
- **Character Prompts** These are information sheets given to the blue team that help them react to cyber threats by their respective organizational roles. Table 4.1 shows the sample character prompts created for the tabletop exercise. 0
- **Injects** These are planned interruptions or information given to the red team during the exercise to introduce new developments or emerging details about the scenario. Injects challenge the participants, force them to adapt their strategies, and test their ability to respond to changing conditions. For example, an inject might include sudden information about a cybersecurity breach or a new regulatory requirement that impacts the ongoing scenario.
- **Reveal** These are disclosures of information previously unknown to the participants but pivotal to the scenario's context. Reveals are given to the blue team. Reveals can help simulate real-world situations where critical information may not be available from the start, requiring participants to revise their strategies as more details become available. They test the participants' flexibility and adaptability to new information.

4.3 Participants

The TTX requires a minimum of five participants. The participants are divided into red team/ adversaries and blue team/responder that take on the roles of different verticals of an organization.

Red Team/Adversaries. In the TTX, the red team is responsible for planning a cyber attack in the hardware supply chain of the organization under the name of [RSI](#). They assume the role of bad actors in different ways, like the malicious supplier, disgruntled employee, malicious design foundry and finally, a ransom caller. They infiltrate various levels of hardware manufacturing phases (design, integration, fabrication, assembly, packaging, product usage and recycling) and find different ways to profit from the blue team's intellectual property. The attacker's motive varies in each game scenario depending on the asset under attack.

Blue Team/Defenders. The blue team is assigned to be a part of a fictitious company called [BSI](#) and is given several organizational roles. Each player receives an information sheet or character prompt that outlines their role in the organization, as summarized in Table 4.1.

Furthermore, each story is organized as an initial brief for the red and blue teams. In this case, the red team is given information about the business line of the blue team and details of their product line that help the participants in the red team better understand how they could attack the blue team's supply chain.

4.4 Blue Team Roles in a TTX

The participants of a TTX are usually the stakeholders within an organization. The TTX for the hardware supply chain has roles as stated in the sections below. The trial runs of TTX were run with players from an academic background who had to learn about the responsibilities of executives in an organization. The character cards are given to the players to help them understand their role in the TTX and make decisions that align with their assigned roles.

4.4.1 Business Head/CEO

The business head or the CEO focuses on the overall impact of the security breach and makes executive decisions to ensure business continuity. They prioritize long-term business viability and are answerable to the board of directors and company investors.

4.4.2 Engineering Head /CTO

The engineering team analyzes the technical details of the cybersecurity breach, working to identify the attack's source and nature and developing technical fixes. They collaborate closely with the security team to patch vulnerabilities and oversee the technical recovery plan.

4.4.3 Operations/Procurement

The operations/procurement team is responsible for maintaining business continuity in terms of day-to-day manufacturing operations. They often look into the effects of the incident on plant operational continuity and report to the business and engineering heads. They are responsible for sourcing valid electronic components. They strategize on rerouting resources in a crisis, possibly adjusting production lines or supply chain processes, and ensuring that operational impacts are minimized.

4.4.4 Legal

The legal head is responsible for the legal implications of security breaches and works closely to check compliance with laws related to data protection and contractual obligations with partners and customers. They suggest immediate and long-term legal action plans, assess the need for disclosures, and manage potential legal fallout, advising on communication from a legal standpoint.

4.4.5 Finance

The finance head is responsible for evaluating the financial impact of the breach, including potential fines, loss of business, and the cost of remedial actions. They work on adjusting financial forecasts and ensuring adequate liquidity to handle crisis-related expenses. They also interface with insurance providers for possible claims in the event of losses due to cybersecurity breaches.

4.4.6 PR Head

The PR head is responsible for managing the external communication strategy to control damage to the company's public image. They craft clear, transparent messages to stakeholders and the public, coordinate press releases, and manage media responses to maintain trust and manage public perception effectively.

4.4.7 HR/Communications

The HR/Communications department is responsible for ensuring internal communications and morale within an organization. They ensure that all employees are informed, aligned, and reassured in their roles in the event of a crisis. They develop communication strategies to prevent internal panic, ensure staff know their roles in mitigating the breach, and maintain organizational integrity.

4.5 Setting the Stage for TTX

The TTX was created to create awareness on hardware cyber security attacks in the supply chain of a fictitious automotive ECU manufacturing company. The participants are divided into the red team and the blue team. Once they are assigned roles within an organization, as discussed in the previous section, we divulge information about the fictitious company created to test out the TTX. Generally, when the TTX is conducted among researchers and

students who are not from an industrial background, it is necessary to make them a part of a made-up company. [RSI](#) and [BSI](#) are the two fictitious company entities created for the TTX. The participants are also given character prompt sheets to help them understand their role in the TTX. Details about the character prompts are provided in the following sections of this chapter. The information about the two companies is summarised as follows:

Red Solutions Inc: The [RSI](#) is a supplier to [BSI](#). Your ultimate goal is to make more monetary gains by finding unsolicited ways to profit from the vulnerabilities in [BSI](#)'s poor hardware supply chain practices. The [RSI](#) would take on different roles within the entire TTX, and for each cyber attack, they would have a unique reason for attacking the blue team. Additionally, the red team would be given all details about the [BSI](#) business model and supply chain practices as any adversary would have a deep understanding of how their victim organization operates on a day-to-day basis by studying them for a prolonged period to figure out different ways to launch an attack in their systems.

Blue Solutions Inc: [BSI](#) is a publicly traded, global company that is a well-known player in manufacturing ECUs in the automotive, medical, aerospace, and defense industry. [BSI](#) operates globally, with manufacturing, research and development facilities in the United States, Europe, and Asia. An international team of engineers and specialists collaborates across borders to drive innovation and serve a growing list of clients worldwide. [BSI](#) manufactures [In Vehicle Infotainment \(IVI\)](#) for the automotive industry. The ECUs have high-mix, low-volume; thus, [BSI](#) has positioned itself with a large supplier network. [BSI](#)'s customers often have change requests on short notice, and [BSI](#) implemented agile processes to react to them quickly with decentralized purchasing and control. Auto Inc. is an [OEM](#) and is one of [BSI](#)'s most valuable customers.

4.6 Character Prompts

The TTX session was originally meant to be conducted in an organization that usually comes with stakeholders in leadership roles responsible for making important decisions. While the TTX for cybersecurity in the hardware supply chain was in the initial stages of development, we had trial runs of the game with students from different academic background. To improve the element of realism and engagement in the game, the later versions of the TTX included character prompt sheets given to the players before starting the session. A summary of the character prompts is stated in the [Table 4.1](#).

Table 4.1: Roles and character prompts for tabletop exercise

Role	Character Prompt
Business Head	• Investigate incident, analyse impact on business. • Initiate internal investigation. • Address the falling stock prices. • Report to the police, cyber crime division. • Confirm with other business regarding similar incidents.
Engineering Head	• Root cause analysis of product. • Robust encryption, identity access management, redesign systems. • Rigorous testing/simulation. • SIEM Tools integration. • Order testing of the affected products in a certified lab.
Operation and Procurement	• Work closely with vendors and supply chain partners. • Check the affected batches. • Ask more budget for quality assurance, safety and reliability testing. • Change suppliers, get approvals. • Postpone/halt operations. • Find replacement part for obsolete components.
Legal	• Sue the bad actors. • Send out legal notice. • Reply to legal notice received.
Finance	• Check company's free cash flow. • Analyse loss due to security breach. • Increase cash flow/raise money to fix problems. • Prioritize expenditures critical to recovery.

Table 4.1: Roles and character prompts for tabletop exercise (continued)

Role	Character Prompt
PR Head	• React to media allegations. • Social media management to boost positive PR. • Engage with all key stakeholders like customers, partners, investors, and regulators. • Develop predefined response templates for various scenarios. • Train the company spokespersons, executives for smooth media engagements.
HR/Communications	• Training programs on cybersecurity awareness. • Communicate with employees. • Review and update HR policies for cyber compliance. • Manage contract hires to control rare security breaches.

4.7 Scenario Development

The TTX, divided into scenarios representing each category of cyber attack in the hardware supply chain, is a practical tool for industry stakeholders to understand the vulnerabilities in the organization’s supply chain. It ensures that they are well-prepared to handle several documented types of cyber attack witnessed in the supply chain. The TTX is designed to simulate four different categories of cyber attacks recorded in the real world in the hardware supply chain. These scenarios, each lasting for 20 minutes, provide a brief idea about the supply chain vulnerabilities. The initial version of the TTX was scheduled to be presented at the International Symposium on Hardware Oriented Security and Trust (HOST) with a time constraint of 150 minutes. An actual tabletop exercise conducted with professionals of an organization can last up to 3 hours, demonstrating its thoroughness. We have narrowed down to four major categories of attacks in the supply chain. They are counterfeiting, IP piracy, sabotage/malicious insiders, tampering and ransomware cyberattacks.

The TTX is a collaborative effort meant to test the plan of action of stakeholders/participants in the event of a cyber security breach. Each participant, representing different roles, plays

a crucial part in the crisis response. Their responses, written down on the game sheet, are a valuable contribution to getting their understanding of the game scenario. As the plot of the game scenarios is revealed in phases, the facilitator responds to the participant's responses, fostering a sense of shared responsibility and learning. This feedback loop ensures that the participants' responses are coherent with the corrective actions that must be in place to curb the intensity of a real-world crisis.

4.7.1 Scenario 1: Counterfeiting

Information to Red Team: The Facilitator starts the TTX session by giving the attack goal for the scenario mentioned in Table 4.2. The red team gets an overall idea of ways to monetize the blue team's supply chain vulnerabilities. This scenario outlines a term called "pump and dump strategy", a malicious practice involving the artificial inflation of the price of a company stock through false and misleading positive statements, in order to sell the cheaply purchased stock at a higher price. The scheme operators dump their overvalued shares, and the price typically falls, and investors lose their money. Typically, pump and dump schemes are more common with small-cap stocks that are less liquid and easier to manipulate. Once the RSI initiates the cyber attack on BSI, they are given injects to decide how they want to continue with the attack scenario. Here, we give them the choice of injects to ensure that the red team/attacker is actively engaged in the TTX.

Inject Suggestions: The facilitator suggests relevant game injects which decide the course of the TTX. The red team could choose any creative inject other than the facilitator's suggested inject. A summary of injects created to help the red team select the course of TTX is shown in Figure 4.2. A TTX can have about 2 to 3 injects in one scenario as and when needed by the facilitator and red team. If multiple vulnerabilities need to be explored by the executive team within the organisation, the TTX shall have the corresponding number of injects to analyze and understand these vulnerabilities.

Information to Blue Team: After the red team initiates the attack, the facilitator informs the group about the failing IVI units using game elements, such as an email or letter from BSI's client, who reported the product failures, as depicted in Figure A.1. The different stakeholders in the blue team are asked to write down their response to the crisis.

Meanwhile, the red team decides on an inject, and the facilitator informs the blue team about the change in events through this inject. Later, a reveal is used as a game element in the TTX to inform the blue team about the technical details of the cyber attack (counterfeit components in this scenario), providing evidence from the initial investigations conducted by the blue team.

A reveal (Figure 4.3) helps the blue team understand critical information about the attack

Table 4.2: Adversary goals for different scenarios

Scenario	Purpose of attack	Details
Counterfeiting	Monetary gains	• RSI is a hardware broker selling electronic parts. • Company is under severe financial hardships and needs to make more money to ensure business continuity. • You get to know about stock pump and dump schemes through a colleague. • You get access to old, aged parts from discarded ECUs and resell them as new parts. • After selling fake parts, you decide to manipulate the stock price of BSI.
IP Piracy	Monetary gains	• RSI is a contract manufacturer. • Access to full SMT manufacturing lines and associated tools. • RSI is a supplier to BSI and manufactures sub-assembly boards for them. • You execute IP theft and plant a malicious insider.
Insider Sabotage	Sabotage competitor	• You manufacture model X vehicles used as public transit. • You also manage the service and restoration for the vehicles. • A competitor outbids you and wins the service contracts causing monetary loss. • You decide to sabotage their operations and win back the lost contracts.
Ransomware/Tampering	Create chaos	• You tamper with the last 12 months' batch of battery management ECU. • RF-controllable implant in the charging circuit that can overcharge the batteries, potentially causing fire. • Ransom call to BSI.

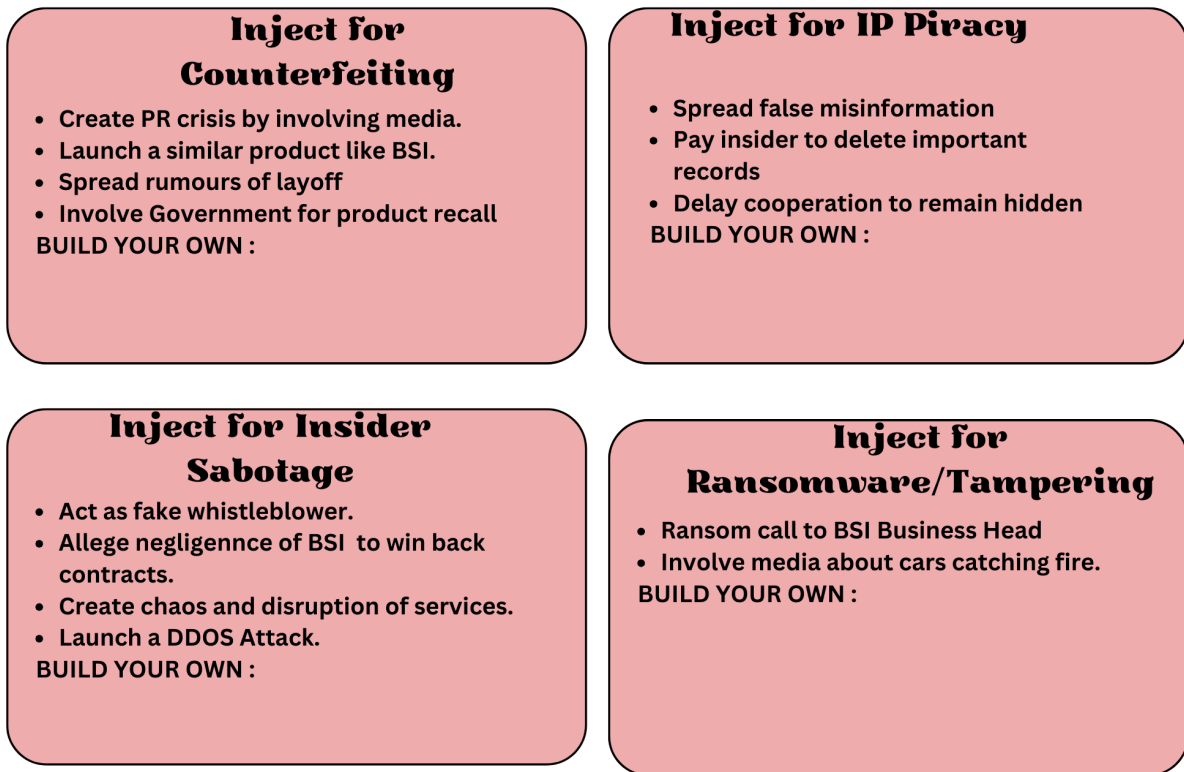


Figure 4.2: Inject suggestions for Red Team

location and goal of the adversary and helps them decide on policies and guidelines in place and the changes that need to be implemented to prevent such encounters in the future ensuring that their business is resilient to such attacks.

At the end of scenario 1, the facilitator shall conclude the simulation of the cyber attack by discussing the backstory of the attack, what went right, what went wrong, review and update the incident response template accordingly. The team's responses are recorded throughout the game to make sure they can be used as a reference to revise their incident response strategies to be prepared for cyber attacks in the future. A brief overview of an incident response template is shown in Figure 4.4.

Summary of Blue Team Responses: The blue team responded to the crisis with the business head discussing with the finance team to evaluate the losses due to failed display units and decided to lay off their entire quality assurance team and hire more competent

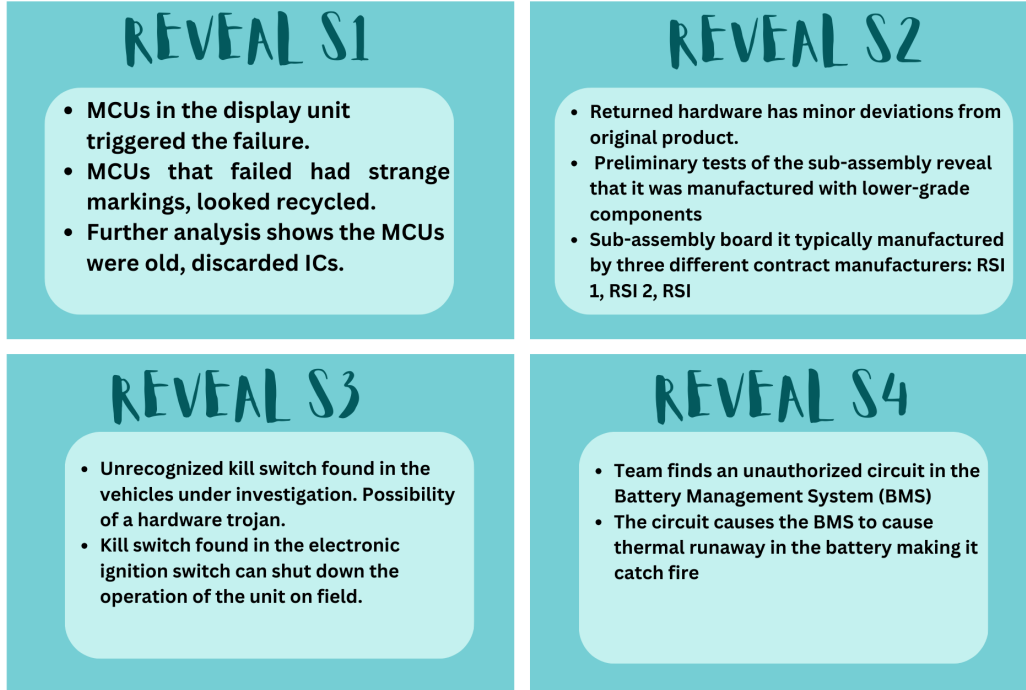


Figure 4.3: Reveal for Blue Team

engineers who can navigate the crisis and making sure the necessary quality and reliability checks are in place. The operations team decided to halt the production until further notice from the engineering team about why the microcontroller unit failed. The legal team chose to sue the identified supplier for providing unreliable components.

4.7.2 Scenario 2: IP Piracy

Information to Red Team: The Facilitator starts the TTX session by giving the attack goal for scenario 2, which is about IP piracy as mentioned in Table 4.2. Once the RSI initiates the cyber attack on BSI, we move to the injects to decide the red team's next move in the IP piracy attack scenario. Figure 4.2 shows the choice of injects for IP piracy.

Information to Blue Team: Once the red team launches the attack, the facilitator provides the following information to the blue team.

- There is an unusual increase in the influx of service requests for products.

- Multiple customers have returned their product and demanded a replacement.
- Closer examination of the returned product reveals that the Serial number of the returned product is not found in the manufacturing database.

The blue team shall record their plan of action based on the information presented to them by the facilitator. Meanwhile, the red team decides the inject and the facilitator informs the blue team regarding the change in events through the introduction of inject. Later, the reveal for scenario two (IP piracy) shall be given to the blue team. In this case, the reveal scenario two is outlined in Figure 4.3.

At the end of scenario 2, the facilitator shall conclude the cyber attack simulation by discussing the backstory of the attack, what went right, what went wrong, reviewing and updating the incident response template accordingly.

Summary of Blue Team Responses: The business head took the required action to trace the supplier that delivered the defective/cloned product and consulted with the engineering team to address the root cause of the vulnerability. The PR team requested that the customers not approach the media by assuring them of the appropriate actions to prevent such incidents in the future and preparing the other stakeholders to respond to the crisis effectively. The finance team promptly looked into the losses due to the defect in the product and adjusted the organization's expenditure to accommodate the defense countermeasures, finding more money to fund the quality assurance team to prevent product cloning and IP piracy. The operations team actively traced the source of the defective product, confirmed that it was cloned from its original product, and investigated the suppliers involved in the entire product life cycle. The legal team looked into the contracts with suspected suppliers to send them a formal notice to investigate their role in the security breach.

4.7.3 Scenario 3: Insider Sabotage

Information to Red Team: The Facilitator starts the TTX session by giving the attack goal for scenario 3, which is about the practice of sabotaging (attacking the reputation) competitors for monetary gains as mentioned in Table 4.2. Once the RSI initiates the cyber attack on BSI, we give them the injects that the red team wants to continue with for the Insider sabotage attack scenario. Figure 4.2 outlines the choice of injects for scenario three.

Information to Blue Team: Scenario 3 of the TTX begins for a blue team with the facilitator providing an updated business portfolio of BSI. In this scenario, the blue team's corporate overview is as follows:

- BSI is an in-service support (ISS) company.

- BSI operates globally with a team of engineers and specialists collaborating across borders.
- BSI is responsible for spare parts supply, repairs, and operations of a fleet of super car taxi vehicles.
- The government decided that the ISS contract for its fleet of public transit vehicles, previously manufactured and maintained by RSI, should be up for public tender.
- You recently won the super car taxi ISS contract.
- RSI's the OEM of the vehicles in the maintenance contracts.

Once the red team launches the attack, the facilitator provides the following information to the blue team as mentioned below.

- You recently won the ISS contract for a fleet of government supercar taxis
- Taxis are facing sporadic failures in the field. Overwhelming requests for maintenance of vehicles.
- You receive replacement parts from RSI (the original manufacturer).
- You need to work with RSI to identify the issue. Seems like the Electronic Control Unit (ECU) is the culprit, but you're not sure.
- Sporadic failures cause disruption to public transport and require timely action to restore proper service

The blue team shall record their plan of action based on the information presented to them by the facilitator. Meanwhile, the red team decides the inject and the facilitator informs the blue team regarding the change in events through the introduction of inject. Later, the reveal for scenario 3 (insider sabotage) shall be given to the blue team. The reveal for this scenario is shown in Figure 4.3.

At the end of scenario 3, the facilitator shall conclude the cyber attack simulation by discussing the backstory of the attack, what went right, what went wrong, reviewing and updating the incident response template accordingly.

Summary of Blue Team Responses: The Blue team responded to the scenario with the head of business replying to the letter sent by the transit governance head and calling in the OEM who supplies the vehicles to discuss the failures in the field. The operations team initiated an examination of the cars that failed in the field and tried to find a technical expert who could help support the ongoing issues, as BSI representatives were not reachable. The legal team wanted to pause on the government's idea of taking back the business contract till their investigations were completed and sue RSI for defamation as they went

public and alleged misconduct of [BSI](#). The PR team was handling the media accusations by holding a press conference.

4.7.4 Scenario 4: Ransomware/Tampering

Information to Red Team: The facilitator starts the TTX session by giving the attack goal for the final scenario, which discusses tampering of hardware in the supply chain and ransomware cyber attacks as mentioned in Table 4.2. Once the [RSI](#) initiates the cyber attack on [BSI](#), we move to the injects to decide the flow of the scenario. The choice of injects for Ransomware attack/tampering is outlined in Figure 4.2.

Information to Blue Team: Scenario 4 of the TTX begins for the blue team with the facilitator providing an updated business portfolio of [BSI](#). In this scenario, the blue team's corporate overview is as follows:

- [BSI](#) is an electric vehicle [OEM](#).
- [BSI](#) operates globally with engineers and specialists collaborating across borders.
- [BSI](#) manufactures and sells electric vehicles and has a large supplier network.

Once the red team launches the attack, the facilitator provides the following information to the blue team.

- Four cars caught on fire on parking lots.
- The owner was not near them.
- No loss of human life.

The blue team shall record their plan of action based on the information presented to them by the facilitator. Meanwhile, the red team decides the inject and the facilitator informs the blue team regarding the change in events through the introduction of inject. Later, the reveal for scenario 4 (Ransomware/Tampering) shall be given to the blue team. The reveal for this scenario is shown in Figure 4.3.

At the end of scenario 4, the facilitator shall conclude the cyber attack simulation by discussing the backstory of the attack, what went right, what went wrong, reviewing and updating the incident response template accordingly.

Summary of Blue Team Responses: The blue team reacted to this scenario with the business head asking for a report on financial setbacks by issuing a call back of the cars that caught fire. The finance team responded with the report of losses incurred due to the incident of tampered battery management units. The PR team decided to act and release a statement to the public about the active investigation and effort [BSI](#) took to mitigate the

crisis. Later, they decided to issue a recall of cars to control the situation. The engineering team deployed the forensic analysis team to find out why a specific batch of vehicles caught on fire. The operation team launched an investigation to trace the product lifecycle and find the root cause of the hardware trojan that triggered the fire.

4.8 Incident Response Plan

An incident response plan is an established strategy that an organization uses to address cyberattacks. This plan should consist of a record of incident response team members, detailing their roles and responsibilities and the tools and technologies they will use. It should also outline the steps to detect and identify cyberattacks, measures to contain and mitigate damage (including harm to reputation), and procedures for incident recovery.

The facilitator of the TTX, along with help from the cybersecurity incident response team, shall go through the assets of the organization, current policies in place which are relevant to cyber attacks, and their current incident response plan in the event of a cyber security breach. After the initial discussion with the organization, the facilitator shall narrow down the various cybersecurity threats and revise the attack scenarios according to the organization's requirements. The goal of the TTX is to educate every major stakeholder of the organization about the threats and vulnerabilities in their hardware supply chain and the necessary, safe practices to minimize the impact of a security breach by having robust business contingency plans.

To record the vulnerabilities in an orderly, accountable way, we propose adopting an incident response template as shown in Figure 4.4, which helps quantify the rationale of a supply chain security breach and prioritize to control the threat with maximum potential to disrupt the organization's business continuity.

Threat Priority Metric: There are several research in the Failure Mode and Effects Analysis (FMEA), which help prioritize the risk with maximum hazard impact using the calculation of Risk Priority Number (RPN). Similarly, in this study, we suggest analyzing the impact of each threat or vulnerability identified during the TTX session by calculating the **Threat Priority Metric (TPM)**. At the end of the session, the IT security team shall work with the facilitator to quantify the potential of disruption caused by every supply chain vulnerability, which helps the organization to understand the supply chain breach with the most impact and compare the effectiveness of their current countermeasures and policies for a timely threat mitigation. The **TPM** could be calculated as follows:

$$\text{TPM} = S \times L \times D \quad (4.1)$$

where:

- S = Severity of the threat,
- L = Likelihood of the threat occurring,
- D = Detectability of the threat.

Severity It is a measure in the threat priority metric which gives the potential impact caused by the security breach in the supply chain. It is measured on a scale of 1 to 10, with 1 representing negligible impact and 10 representing catastrophic impact. To determine the severity of supply chain threat refer to Table A.1.

Likelihood It is a measure that represents the probability of the threat category to occur in any phase of the supply chain where one shows it is less likely for this vulnerability to happen and ten shows that there is a high chance of this threat to occur in the particular phase of the hardware supply chain. To determine the likelihood of a supply chain threat, refer to Table A.2

Detectability It is a measure of the mechanisms deployed by the organization to detect the type of threat under consideration. It is also represented on a scale of 1 (easily detected) to 10 (Extremely difficult to detect). To determine the detectability of a supply chain threat, refer to Table A.3.



Figure 4.5: Phases of incident response [66]

The incident response plan is suggested to record the vulnerabilities identified during the

TTX. This template helps the organization keep track of threats identified in their organization's assets during the TTX. After the TTX, the organization shall work on deploying the suggested countermeasures and policies to better equip itself for a real-time cybersecurity breach. This template could be used in addition to the official crisis management playbook to help proactively secure the organization's supply chain. Conducting at least one follow-up session after the initial TTX session is necessary to assess the organization's cybersecurity posture after identifying certain vulnerabilities. The facilitator shall schedule a follow-up session with the organization to evaluate the efficiency of the countermeasures and policies.

According to SANS institute's handbook of incident response [46], the incident handler shall follow a six step strategy to mitigate any cyber security incident within a organisation. Figure 4.5 shows the different phases of incident response mentioned in their handbook . Each phase outlined in the standard and how its used to create a customisable TTX is mentioned below:

- **Prepare:** Preparation is crucial for an effective and timely response to incidents, minimizing organizational impact and legal vulnerabilities. This phase enable the incident handling team to traverse through a wide attack scenario applicable to each organisation and check their current strategies to handle the incidents. The key elements in this phase is to establish clear policies, creating a incident response plan, implementing a communication strategy, thorough documentation, establishing roles of team members, ensuring access control, equipping the team with necessary tools, and conducting regular training sessions like the TTX.
- **Identify:** This phase involves accessing the scope of incidents of deviation from the normal operation observed through log files, error messages, intrusion detection systems and firewalls. A TTX helps identify the different type of vulnerabilities within the scope of your organisation well in advance.
- **Contain:** The purpose of this phase to limit the extent of breach by isolating the affected asset or network segment and avoiding further escalation. It also involves creating forensic images of the affected asset which could be referred in the future for investigation. In TTX, the entire threat scenarios are simulated in a harmless, risk free environment to ensure that the organisation is trained to respond right when similar incidents occur in the future.
- **Eradicate:** This phase ensures that the affected systems are diligently restored or removed. The vulnerabilities identified in the TTX could be periodically audited to ensure that all malicious content is thoroughly removed to enhance system defenses against future attacks.
- **Recover:** This phase aims to reintegrate affected systems into the production

environment, ensuring that they are not reinfected or compromised. Key decisions include determining the time and date to restore operations, testing and verifying that systems are clean and functional, setting the duration for monitoring abnormal behaviors, and selecting appropriate tools for testing and validation.

- **Lessons learnt :** The phase involves completing and expanding on incident documentation by writing a detailed report answering the Who, What, Where, Why, and How of the incident. The goal is to improve the team's future performance and create reference materials for similar incidents. Documentation can also serve as training for new team members and benchmarks for future crises. In a TTX, most of the threats and vulnerabilities are simulations of real world threats but the lessons learnt at the end of a TTX plays a crucial role in reviewing and upgrading the state of art defence countermeasures.

4.9 Learning Outcomes of TTX

The purpose of the TTX for hardware supply chain are as follows:

- **Understanding the Dynamics of Supply Chain :** The players learn about the complexities involved in the hardware supply chain, phases involved in the product manufacturing life cycle, vendors, and suppliers involved in the supply chain.
- **Risk Assessment and Management:** The exercise helps identify vulnerabilities/cyber risks along the supply chain and discuss mitigation strategies.
- **Crisis Communication and Coordination:** The participants exercise crisis management and decision making skills while effectively communicating to the appropriate teams enabling them to handle such crisis's when encountered in the future.
- **Compliance to Regulations and Standards:** The TTX allows organizations to review their current policies to review their compliance to the manufacturing regulations and also implement newer risk mitigation strategies.

4.10 Evaluation of the TTX

Adopting TTX for hardware security in the supply chain is rather new and needs to be constantly evaluated and upgraded by collecting the participants feedback. We created a customised survey to understand the overall learning impact among the participants by implementing feedback meticulously at the end of each TTX simulation. Some of the key feedback received at the end of TTX sessions are as follows:

- The red and blue team participants suggested that swapping roles at the end of one attack simulation could help engage the participants.
- A pre-lecture session to learn about the security landscape in the hardware supply chain could help participants get a better idea to respond effectively in the TTX session.
- Implementing more security-related injects and reveals to make the cyber attacks more realistic.
- Few participants suggested that the scenarios could be longer to help strategize better, and others suggested using a timer for players to summarize their responses within stipulated game time.
- In the initial TTX versions, we included several legal injects for the red team. Still, after post-TTX discussions, we chose to remove legal injects as they did not provide any immediate actions to be taken by the blue team.

4.11 Lessons Learnt from TTX

The TTX, conducted over multiple iterations within the academic setup, provided invaluable insights. The final iteration was conducted amongst hardware security experts, and the lessons learned from these iterations are summarized below.

- The **first iteration** of TTX conducted amongst the students helped streamline the time efficiency of the TTX. The session was designed for four different attack scenarios, and we found that some scenarios required more than 20 minutes for the Blue team to discuss amongst their team members and come up with their respective responses to the supply chain attacks. Most participants in the first iteration were from the same research group, greatly contributing to effective collaboration and communication.
- The **second iteration** consisted of participants representing diverse skills and perspectives. This diversity, however, highlighted a challenge: participants felt that certain roles were less important than others. This observation underscores the importance of inclusivity and the need for all roles, including PR, communications, and legal, to be valued in a cybersecurity breach scenario. On the contrary, when a TTX is conducted in a real industrial setting with all stakeholders, it is important to note that every role, including PR, communications, and legal, plays a pivotal role in case of a cybersecurity breach.
- The **third iteration** of the TTX was conducted similarly to the previous session, with students selected randomly from different educational backgrounds. The responses of

the blue team were significantly better as we introduced character prompts, which helped players from non-industrial backgrounds understand their roles and respond better.

- The **last iteration** of TTX was conducted amongst the hardware security experts at the HOST conference. The experts in the red team enjoyed playing the role of an adversary by exploiting the vulnerabilities in the hardware supply chain. The responses of every participant in the blue team also greatly matched the expectations of an actual organizational stakeholder. At the end of the TTX, we provided a lecture-style summary of hardware countermeasures, as discussed in Chapter 5. The session sparked insightful discussions amongst the security experts on the state-of-the-art hardware countermeasures to secure the hardware supply chain.

4.12 Limitations of TTX

The TTX was designed to be tested out amongst the stakeholders of the critical infrastructure organization. The data collected to date are from participants from academic backgrounds, which largely restricted the ability to calculate the game’s empirical effectiveness due to the game’s qualitative nature. The game needs to be tested with real-time organizations in the critical infrastructure to evaluate a measurable learning outcome of the TTX. The game is designed to simulate a cybersecurity attack on the hardware supply chain. Still, the realism could be simulated only to some extent as the participants know the session is happening in a risk-free, controlled environment. It is largely dependent on the participants to maximize the learning outcomes of the TTX. Furthermore, unlike a few other games discussed in the literature survey, the TTX is not designed to evaluate any one winner. It is meant to be conducted as an effective alternative to practicing team skills and effective communication, along with learning about cybersecurity in the hardware supply chain or any other topic of interest.

Chapter 5

Hardware Countermeasures

The previous chapters detailed the vulnerabilities in the hardware supply chain and the importance of having a secure product supply chain ecosystem. It is important to ensure that the components and systems remain safe and secure from the point of manufacture to delivery and operation. The analysis must inherently consider potential vulnerabilities and address them with necessary countermeasures at the hardware level, as exploiting these can render all defences established at the software level null and void [63]. Several cases of counterfeit parts penetrating the defense industries have come to manufacturers' attention, where 70 percent of the problems are traced back to one geographic location [8]. An IP theft or piracy of designs while being transported could lead to losses in billions of dollars for the IP owner. Similarly, tampered hardware in critical infrastructure could allow attackers extended access to sensitive data or systems. An disgruntled insider paid off by the competition could perform a wide range of malicious operations from within the company and go undetected for a long time. These incidents emphasize why strict and reliable countermeasures are needed to protect the hardware prone to compromise in the supply chain.

In the effort to address these supply chain cyber-attacks, robust hardware security measures need to be put in place, which envisage addressing security threats in the manufacturing process, handling, transportation, and integration phases of the hardware life cycle. Effective strategies must account for combining practices from cybersecurity, logistics, quality assurance, and risk management.

Hardware Counterfeit Prevention Standards

In theory, it is difficult to completely eliminate the proliferation of counterfeit parts entering the supply chain, but the government has taken some collective approaches to curb the occurrence of defective or counterfeit components in mission-critical hardware devices deployed in the military, defense, and aerospace sectors.

5.1 Legislation

Legislation to curb the occurrence of counterfeit components is as follows:

- **National Defense Authorization Act for Fiscal Year 2012 (NDAA 2012):** This rule mandates the Department of Defense ([DOD](#)) to take stringent measures to curb counterfeit components from entering the supply chain. It distinguishes an original from a counterfeit part. It instructs the suppliers and contractors of the [DOD](#) to establish themselves as a vetted resource and establish traceability of parts supplied to ensure that they get business contacts from the government.
- **Defense Federal Acquisition Regulation Supplement (DFARS):** This rule mandates the defense contractors to define and follow necessary protocols to help detect and avoid counterfeit electronic parts and suspected fake parts that ensure parts integrity in the defense and military systems.
- **Federal Acquisition Regulations (FAR):** The federal regulations were created as the government realized the counterfeit market had taken root in the electronics supply chain and expanded with significant market share and profits for the malicious entities. The regulation also introduced the creation of standards like the SAE AS9100 and SAE AS5553 to avoid counterfeit components. It has also mandated reporting of non-conforming items to entities like the [GIDEP](#) to ensure that the reported parts are eliminated from further being put to use by other companies.

5.2 Standards

Although the government passes multiple laws to prevent further breaches of counterfeit parts in the supply chain, it isn't easy to implement them quickly to wipe them out of the supply chain. The legislation is limited to government participation. Hence, we have multiple SAE standards for counterfeit electronic parts. A special G-19 committee was formed to draft the first SAE standards to curb counterfeit electronic parts. The table [5.1](#) provides a summary of standards working on the counterfeit component problem.

5.2.1 SAE AS5553

The SAE AS5553, titled “Counterfeit Electrical, Electronic, and Electromechanical (EEE) Parts; Avoidance, Detection, Mitigation, and Disposition,” was created to control the problem of counterfeit EEE parts in safety-critical industries. It is intended to be used along with other quality standards like the higher-level quality standards like the AS9120, AS9003, , ISO-9001, ANSI/ASQC E4, AS/EN/JISQ9100 [59]. The standard was introduced to ensure system reliability, safety, and integrity by preventing counterfeit parts from entering the hardware supply chain and being integrated into products. It helps organizations adhere to product compliance and regulations to safeguard themselves against the financial and reputational damages associated with counterfeit incidents. The key contributions of the standard are summarized below.

- **Detect and Avoid Counterfeit Parts** The standard provides an overview to the industries to prevent procurement and integration of substandard counterfeit parts and further guides them to improve their supplier management practices.
- **Mitigating the Impact of Counterfeit Parts** The standards shall guide the users with necessary practices to mitigate the impact of parts that have already been integrated into safety-critical hardware. It states the containment procedures, reporting the suspected part and corrective plan of action to reduce the consequences of their impact.
- **Disposal of Counterfeit Parts** AS5553D provides guidelines and instructions to dispose of the detected counterfeit parts properly, ensuring they do not re-enter the hardware supply chain.
- **Traceability** AS5553D suggests stringent documentation and traceability to ensure the quality and authenticity of the product from the manufacturer to the end-user.
- **Training** It encourages industries to train the employees involved in the procurement and management of EEE parts, which includes an awareness initiative about what is a counterfeit part and the common ways how they infiltrate the supply chain.

5.2.2 SAE AS6171

There are multiple techniques and approaches to test and detect counterfeit components, and the SAE AS6171 standards provide methods to evaluate the effectiveness of the existing test plans. The tests mentioned in the standards are the Counterfeit Defect Coverage (CDC), Counterfeit Type Coverage (CTC), Not-Covered Defects (NCDs) and Under-Covered Defects (UCDs) [59].

Counterfeit Defect Coverage: It is the ratio of possible detectable defects to the total number of known counterfeit related. It gives an overall assessment of multiple test methods based on their capacity to detect defects and provides overall confidence after performing a sequence of tests. It is represented as follows :

$$CDC = \frac{\text{Possible Detectable Defects}}{\text{Total Defects}} \times 100\% \quad (5.1)$$

Counterfeit Type Coverage : The capacity to detect the type of counterfeit based on defects present given the test methods performed to check them. It is expressed as:

$$CTC = DI \times \frac{\text{Possible Detectable Defects for a CT}}{\text{Total Defects for a CT}} \times 100\% \quad (5.2)$$

Here, CT is the counterfeit type and DI is the decision index.

The CTC test shall be used to determine the effectiveness of a counterfeit detection test plan. It is mathematically represented by the following equation:

$$CTC_k = DI_k + \frac{\sum (x_{Rj} \cdot w_{jk})}{\sum w_{jk}} \times 100 \quad (5.3)$$

where:

- CTC_k = Counterfeit type coverage for counterfeit type k
- DI_k = Decision index for counterfeit type k
- x_{Rj} = Resultant confidence
- w_{jk} = Weighting for defect j for counterfeit type k

Not-Covered Defects and Under-Covered Defects These are metrics that identify defects that are not detected or is partially detected (i.e., below the desired confidence level) by the chosen test methods.

The above metrics provides a structured approach to evaluating test plans that ensures a rigorous, data-driven strategy to detect counterfeit parts, crucial for maintaining the integrity and safety of aerospace and defense components.

Few other standards from SAE to refer while considering techniques to prevent counterfeit EEE parts are summarised in the Table 5.1.

Table 5.1: Summary of AS6171 test methods

Standard	Detail
AS6171-1	Suspect/Counterfeit Test Evaluation Method
AS6171-2	Visual Inspection, Remarking and Resurfacing, and Surface Texture Analysis Using SEM Test Methods.
AS6171-3	X-Ray Fluorescence Test Methods.
AS6171-4	Delid/Decapsulation Physical Analysis Test Methods.
AS6171-5	Radiological Test Methods.
AS6171-6	Acoustic Microscopy (AM) Test Methods.
AS6171-7	Electrical Test Methods.
AS6171-8	Raman Spectroscopy Test Methods.
AS6171-9	Fourier Transform Infrared Spectroscopy (FTIR) Test Methods.
AS6171-10	Thermogravimetric Analysis (TGA) Test Methods.
AS6171-11	Design Recovery Test Methods.

5.2.3 IDEA Standard

Independent Distributors of Electronics Association (IDEA) has developed a standard on counterfeit mitigation and training titled IDEA-STD-1010 which discusses the electronic components distributed in the open market [72]. This standard outlines the checklists and guidelines to handle products, details about storage, packaging, the inspection of workstation equipment and tools, test and test house relationship management, inspection techniques to be followed by the OEM's, electronics manufacturing service providers (EMSs), contract manufacturers (CMs), and both authorized and open market component distributors. It also provides training and awareness sessions on its standards multiple times a year to help exercise the guidelines mentioned in the standard by implementing them in the training sessions.

5.2.4 Other Initiatives

The CCAP 101 is a certification program to avoid the risk of a counterfeit part entering the supply chain by establishing standard procedures to procure electronic parts from independent distributors for commercial and military purposes. It outlines methods similar

to inspection procedures, testing methods, audit, and approval practices to be implemented by an organization [1]. Security experts created the MITRE ATT&CK framework to provide the adversary tactics and techniques used by adversaries during various stages of a cyber attack. Similarly, the research collaboration between MITRE and the defense for systems engineering came up with a catalogue of supply chain attack patterns to create awareness of the vulnerabilities in the supply chain that could compromise the reliability of the mission-critical components [64].

5.3 Countermeasures for Counterfeiting

In the previous sections, we discussed the four major categories of hardware cyberattacks in the supply chain. This section briefly summarizes the hardware security threat mitigation techniques identified to control their provenance and detect hardware tampering in the supply chain.

Several detection techniques are identified in the literature to help differentiate between an original and counterfeit IC. Physical inspection is the most common method to look for damages or scratch marks in the components that have been recycled from an old discarded unit. Side channel parameters like power, electromagnetic noise and timing patterns are observed with the help of a golden IC to differentiate anomaly [28], [68]. Attaching a unique identifier to every component like DNA marking that utilises the botanical DNA sequences [73] is another common way to prevent counterfeits from entering the supply chain. Physically Unclonable Functions (PUF) are also a notable way to create a digital identity that is unique to each IC to ensure that any evidence of damage to the PUF would lead to different challenge-response pairs and alert the manufacturer of any supply chain breach [33]. Digital fingerprinting creates a digital identity to differentiate between components [19]. When there is a reported case of counterfeiting, this method retrieves the watermark of the element, and using the fingerprinting process, it identifies the suspected vendor who aided in creating counterfeit components. The adoption of non destructive techniques for detecting counterfeit components is the silgeo technique that uses high-frequency, analog-domain signaling to interact with unpowered electronic devices [56].

While there are effective methods to detect a counterfeit component, there are few notable methods to prevent the occurrence of counterfeits in the supply chain. IC metering is used to prevent or monitor the overproduction of components by a malicious foundry without the necessary approval from OEM [15]. Anti fuse technology is an active chip lock which disables selected IC pins that prevents unauthorised usage of the hardware [7]. Other notable methods are smart contract technology and blockchain, where PUF is used for unique component identification [85]. These methods, when implemented, provide a strong

barrier against counterfeit components, ensuring the integrity and security of the supply chain.

5.4 Countermeasures for IP Piracy

An untrusted foundry generally has complete access to the IP's design and layout files, which is a major vulnerability in the supply chain that leads to attacks like cloning and reverse engineering attacks. Split manufacturing divides the layout information given to the design foundries into Front End of Line (FEOL) and Back End of Line (BEOL), making it harder for the untrusted foundries to copy the designs [83].

Hardware obfuscation hides the IC design, which hinders malicious attackers from stealing the design information. Logic locking is one of the widely renowned methods for obfuscation where functional design specification is slightly altered by adding dark states (sequential logic locking) or XOR/XNOR gates (combinational logic locking), which is active only when the right key combination is provided [49], [32]. IC camouflaging, used to prevent reverse engineering supply chain attack, is adopted at a layout of the design file by adding dummy contact or filler cells. The research in [16] stipulates the use of trapped charges at the gate oxide of the hidden gate, which can assume multiple logic functionalities. This means that the same physical gate can perform different logical operations based on the trapped charges, making it challenging to deduce the logic circuit from physical inspection.

5.5 Countermeasures for Tampering

The tampering attacks discussed in this study that are relevant to the supply chain are trojan insertion and fault injection attacks. Attackers often substitute the filler cells with a malicious circuit. The tampering attacks can be prevented by using a digital signature that detects malicious circuitry's addition [84]. Hardware property checking and hardware wrappers have shown promising results in runtime detection of trojans in hardware with greater efficiency[58], [62]. Research developments to prevent fault injection attacks include restricting physical device access by using tamper-proof enclosures or locks. The research mentioned in [25] depicts the usage of nichrome wires and wire meshes to detect any signs of physical tampering.

5.6 Countermeasures for Insider Sabotage

The insider sabotage attack is a broader spectrum attack that could use the adoption of any malicious activity that could lead to financial losses and damage to the organization's reputation. General anomaly detection mechanisms like regular firewall updates, monitoring SIEM tool activity for intruder alerts, restricted or segmented access to a network where users are provided controlled access to selected assets, and adopting multi-factor authentication to allow access to critical infrastructure help control the severity of a security breach.

5.7 CIA Triad for Hardware Cybersecurity

The CIA triad is a widely adopted model to ensure security in information systems. They are used to identify vulnerabilities and guide the creation of policies and methods to secure information systems. The CIA triad comprises confidentiality, integrity and availability, and several researchers have studied the application of CIA triad to the hardware supply chain [76]. This CIA triad could also be applied to ensure security in hardware assets along the supply chain as follows.

Confidentiality: The design specification, manufacturing process and logistics details of the asset are considered to be sensitive information and shall be protected by adopting measures as follows:

- Conduct background checks and implement strict access controls for personnel involved in the supply chain.
- The data stored and communication shall be encrypted within the hardware supply chain.
- The shipping methods are adopted to eradicate interception and tampering by malicious actors.

Integrity: The hardware shall not be tampered with or altered by a malicious actor in any phase of the supply chain. It plays a critical role in ensuring that an asset is not exposed to the insertion of a backdoor or any other vulnerability that could divulge sensitive information. The integrity of hardware is ensured by

- Implementing tamper-preventing packaging or seals.
- Conduct regular audits and inspections of the manufacturing process and look for signs of interference.

Availability: The disruption in supply chains due to natural calamity, political conflict or attacks shall not affect the availability of hardware components. This shall be ensured by

- Diversifying the supply source to multiple geographic locations means there is plenty of alternate parts when one resource is shut off.
- Creating a database of alternate reliable parts such that when one is obsolete, there is a quality replacement for the original component.
- Reviewing and updating contingency plans through TTX to counteract the supply chain disruptions.

5.8 Zero-trust Architecture

Zero-trust architecture operates on the fundamental principle of “never trust, always verify”. It focuses on implementing the model of zero trust to control data breaches in an organization, reducing chances of lateral movement of threat actors to other systems [71]. The architectures advocate verification of identity, least privilege access, and robust security controls across an organization’s network, irrespective of the interactions, whether they are internal or external. The NIST has released a standard that explains the zero-trust model and its importance in safeguarding critical infrastructure and systems from cyber-attacks.

Ahmed et al. mention how we can implement a zero-trust model in hardware to secure chip-to-chip communication. The semiconductor supply chain faces various security threats, including the insertion of hardware trojans, theft of intellectual property, and overproduction. The Zero-trust model presents a valuable strategy for enhancing the security of ICs [2].

5.9 Tenets of Zero-trust Architecture

The Figure 5.1 briefly summarizes the tenets of zero-trust architecture and the key takeaways from the zero trust architecture are mentioned below:

- **Verify Explicitly:** This involves confirming the user’s identity, geographic location, device health, the service or workload they are accessing, the classification of the data involved, and any anomalies detected.
- **Use Least Privilege Access:** Limit user access with just-in-time and just-enough access (JIT / JeA) and implement adaptive policies based on the risk exposure and protection of data to minimize the impact of breaches.
- **Assume Breach:** Control the impact of a breach by preventing lateral movement. This is achieved by adopting network segmentation of the user. Ensuring end-to-end encryption and using advanced analytics to effectively understand visibility, threat detection, and improve defences.

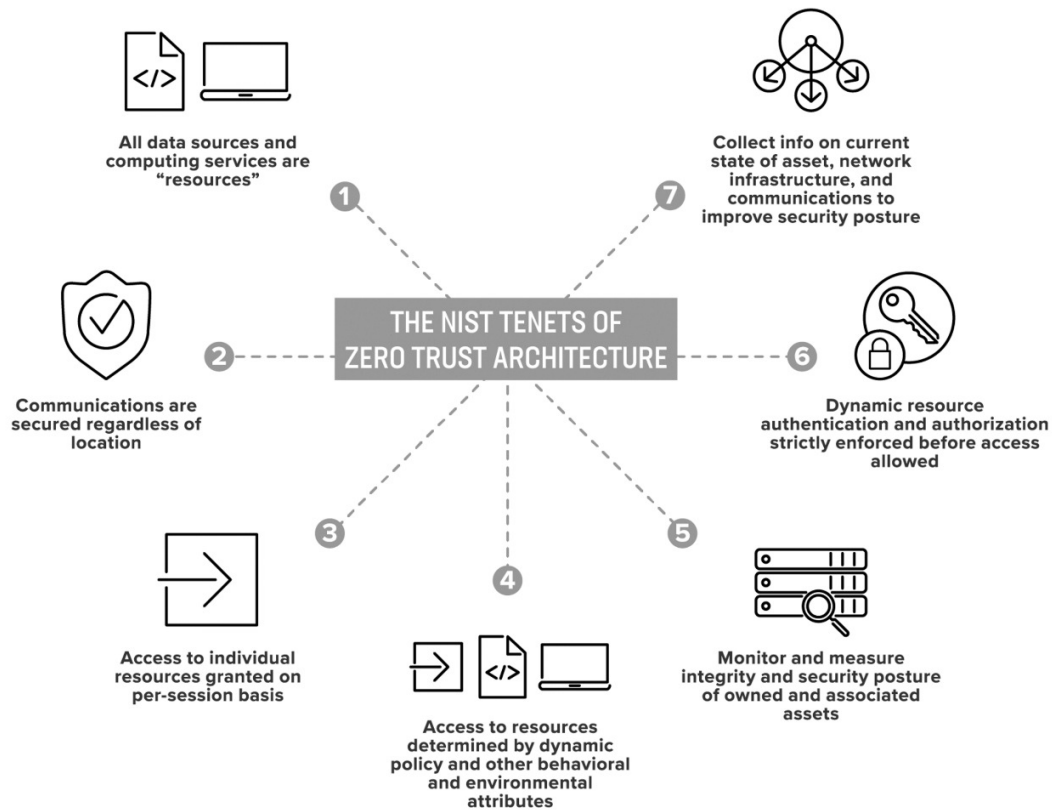


Figure 5.1: NIST tenets of a ZTA [52]

- **Micro Segmentation:** The process of creating secure zones in data centers and cloud environments to isolate workstations, workloads, and secure sensitive data.
- **Multi-factor Authentication (MFA):** Use multiple layers of verification to confirm the legitimacy of the transaction or access request.
- **Security Posture Check:** Ensure that all hardware and software are in a known and expected state before granting access. Check for vulnerabilities and outdated firmware/software.

5.9.1 Zero-trust Framework for Hardware Supply Chain Security

The hardware supply chain vulnerabilities discussed in the previous chapters could be addressed by breaking the hierarchy of in-built trust and implementing a zero-trust model in assets prone to cyberattacks. The concept of zero trust framework, when applied to the hardware supply chain, the focus needs to shift to ensuring that hardware components are secure from manufacturing to deployment in the field [14].

- **Supplier Verification:** It is mandatory to verify the suppliers' credentials and security practices.
- **Secure Manufacturing Practices:** Use secure and verified processes to protect against the insertion of malicious hardware by exploiting the loopholes in the supply chain. An end-to-end encryption and access control must be in place throughout the life cycle stages of hardware.
- **Tamper Detection:** Deploy mechanisms to detect/prevent tampering attempts during manufacturing and shipping.
- **Regular Audit:** Conduct regular audits of different stages of hardware in the supply chain.
- **Secure Integration:** Adherence to the strict access controls and monitoring dictated by Zero-trust principles to ensure that when new hardware is integrated into existing systems, they are devoid of any security risks.
- **Continuous Monitoring and Management:** Implement real-time threat detection and response strategies, monitoring all hardware components continuously for unusual behaviour that could indicate a security breach.

Chapter 6

Conclusion

It is paramount that the hardware is secure in the supply chain to ensure that advanced security mechanisms deployed at the software and hardware level are carried out effectively. A hardware breach at its early manufacturing phases can cause disruption and financial losses of greater magnitude as the severity of such breaches is harder to detect and mitigate in time. The tabletop exercise discussed in this study provides a method to engage the stakeholders of an organization about the hardware cybersecurity risks, overview of key vulnerabilities and response strategies, offering valuable insights into the practical challenges and operational dynamics during a cybersecurity breach. The incident response template developed as part of this research serves as a starting point to streamline crisis management, ensuring that organizations are better equipped to respond effectively to security incidents at the end of the simulated tabletop exercise sessions.

Moreover, the survey of hardware countermeasures for relevant supply chain vulnerabilities provides a thorough understanding of current technologies and practices, highlighting the strengths of adopting state-of-the-art hardware technology.

From this study, it becomes clear that enhancing hardware supply chain security is not a task for a single entity, but requires a collaborative and layered approach. This approach combines robust technological solutions with well-defined response protocols and continuous stakeholder engagement. By offering this multifaceted solution, this research contributes to the academic discourse on hardware security. It provides actionable recommendations to industry practitioners, paving the way for a more secure and resilient supply chain ecosystem.

6.1 Future Scope

The insights gained in this study, while based on preliminary sessions conducted amongst students and hardware academic research experts, hold significant potential for real-world application. The initial responses and actions taken by stakeholders during the tabletop exercise, while not in a corporate setting, provided a valuable learning experience. However, their lack of industrial context made it challenging for them to fully grasp the relevance of cybersecurity concerns in the hardware supply chain. The future potential of this study lies in conducting the TTX in industries involved in critical infrastructure, such as the electric power grid, hydroelectric industry, automotive, military, and aerospace companies. This would encourage these industries to deploy a hardware supply chain that is resilient to cyber-attacks and develop better incident response strategies in the face of an actual crisis. Moreover, after conducting the TTX in multiple industrial settings, this thesis could serve as a reference point to develop a framework, as mentioned in [65], to measure the quantitative effectiveness of a tabletop exercise.

References

- [1] CCAP-101 Standard. <https://www.cti-us.com/pdf/CCAP101Certification.pdf>, 2013.
- [2] Ashfaq Ahmed, Abdulhadi Shoufan, and Kais Belwafi. Light-Weight Security Protocol and Data Model for Chip-to-Chip Zero-Trust. *IEEE Access*, 11:60335–60348, 2023.
- [3] Damir Akhoundov. Reported parts vs. global semiconductor sales. https://www.era1.com/era1_blog/3183/2023_annual_report, 2024.
- [4] Gideon N Angafor, Iryna Yevseyeva, and Ying He. Game-based learning: A review of tabletop exercises for cybersecurity incident response training. *Security and privacy*, 3(6):e126, 2020.
- [5] Md Tanvir Arafin, Andrew Stanley, and Praveen Sharma. Hardware-Based Anti-Counterfeiting Techniques for Safeguarding Supply Chain Integrity. In *2017 IEEE International Symposium on Circuits and Systems (ISCAS)*, pages 1–4. IEEE, 2017.
- [6] Badcyber. Polish trains competitor sabotage attack. <https://badcyber.com/dieselgate-but-for-trains-some-heavyweight-hardware-hacking/>.
- [7] Abhishek Basak, Yu Zheng, and Swarup Bhunia. Active Defense against Counterfeiting Attacks through Robust Antifuse-based On-Chip Locks. In *2014 IEEE 32nd VLSI Test Symposium (VTS)*, pages 1–6, 2014.
- [8] BBC. China fake parts 'used in us military equipment'. <https://www.bbc.com/news/world-us-canada-18155293>, 2013.
- [9] Mark Beaumont, Bradley Hopkins, and Tristan Newby. Hardware Trojans-Prevention, Detection, Countermeasures (A Literature Review). 2011.
- [10] Pauline Bowen, Joan Hash, and Mark Wilson. NIST SP 800-100: Information Security Handbook: A Guide for Managers, 2006.

- [11] Chih-Hsien Chi, Wen-Hsin Chao, Chia-Chang Chuang, Ming-Che Tsai, and Liang-Miin Tsai. Emergency Medical Technicians’ Disaster Training by Tabletop Exercise. *The American journal of emergency medicine*, 19(5):433–436, 2001.
- [12] Nabin Chowdhury and Vasileios Gkioulos. A Framework for Developing Tabletop Cybersecurity Exercises. In *European Symposium on Research in Computer Security*, pages 116–133. Springer, 2022.
- [13] Rachel S. Cohen. An F-16 Pilot Died Due to Failure in Ejection Seat. <https://www.airforcetimes.com/news/your-air-force/2022/09/13/an-f-16-pilot-died-when-his-ejection-seat-failed-was-it-counterfeit/>, 2022.
- [14] Zachary A Collier and Joseph Sarkis. The zero trust supply chain: Managing supply chain risk in the absence of trust. *International Journal of Production Research*, 59(11):3430–3445, 2021.
- [15] Aijiao Cui, Yan Yang, Gang Qu, and Huawei Li. A Secure and Low-overhead Active IC Metering Scheme. In *2019 IEEE 37th VLSI Test Symposium (VTS)*, pages 1–6. IEEE, 2019.
- [16] Asmit De, Anirudh Iyengar, Mohammad Nasim I Khan, Sung-Hao Lin, Sandeep Thirumala, Swaroop Ghosh, and Sumeet Gupta. CTCG: Charge-Trip Based Camouflaged Gates for Reverse Engineering Prevention. In *2018 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pages 103–110. IEEE, 2018.
- [17] Tamara Denning, Adam Lerner, Adam Shostack, and Tadayoshi Kohno. Control-Alt-Hack: The Design and Evaluation of a Card Game for Computer Security Awareness and Education. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, pages 915–928, 2013.
- [18] DSIAC. Combating Counterfeit Components in the DoD Supply Chain. <https://dsiac.org/articles/combating-counterfeit-components-in-the-dod-supply-chain>, February 2019.
- [19] Carson Dunbar and Gang Qu. A Practical Circuit Fingerprinting Method Utilizing Observability Don’t Care Conditions. In *Proceedings of the 52nd Annual Design Automation Conference*, pages 1–6, 2015.
- [20] Maik Ender, Samaneh Ghandali, Amir Moradi, and Christof Paar. The First Thorough Side-Channel Hardware Trojan. In *Advances in Cryptology–ASIACRYPT 2017: 23rd International Conference on the Theory and Applications of Cryptology and Information*

Security, Hong Kong, China, December 3-7, 2017, Proceedings, Part I 23, pages 755–780. Springer, 2017.

- [21] Sylvain Frey, Awais Rashid, Pauline Anthonysamy, Maria Pinto-Albuquerque, and Syed Asad Naqvi. The Good, the Bad and the Ugly: A Study of Security Decisions in a Cyber-Physical Systems Game. *IEEE Transactions on Software Engineering*, 45(5):521–536, 2017.
- [22] Mark Gondree and Zachary N.J. Peterson. Valuing Security by Getting [d0x3d!]: Experiences with a Network Security Board Game. In *6th Workshop on Cyber Security Experimentation and Test (CSET 13)*, Washington, D.C., August 2013. USENIX Association.
- [23] Ingrid Graffer, Maria Bartnes, and Karin Bernsmed. Play2prepare: A Board Game Supporting it Security Preparedness Exercises for Industrial Control Organizations. 2015.
- [24] Timothy Grance, Tamara Nolan, Kristin Burke, Rich Dudley, Gregory White, and Travis Good. Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities. 2006.
- [25] Joe Grand. Practical Secure Hardware Design for Embedded Systems. In *Proceedings of the 2004 Embedded Systems Conference, San Francisco, California*, 2004.
- [26] James Grenning. Planning Poker or How to avoid analysis paralysis while release planning. *Hawthorn Woods: Renaissance Software Consulting*, 3:22–23, 2002.
- [27] Ujjwal Guin. Efficient Strategies for Detection and Avoidance of Counterfeit ICs. In *IEEE North Atlantic Test Workshop (NATW)*, 2017.
- [28] Ujjwal Guin, Domenic Forte, and Mark Tehranipoor. Design of Accurate Low-Cost On-Chip Structures for Protecting Integrated Circuits Against Recycling. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 24(4):1233–1246, 2015.
- [29] Ujjwal Guin, Xuehui Zhang, Domenic Forte, and Mohammad Tehranipoor. Low-cost On-chip Structures for Combating Die and IC recycling. In *Proceedings of the 51st annual design automation conference*, pages 1–6, 2014.
- [30] Zimu Guo, Xiaolin Xu, Mark M Tehranipoor, and Domenic Forte. FFD: A Framework for Fake Flash Detection. In *Proceedings of the 54th Annual Design Automation Conference 2017*, pages 1–6, 2017.
- [31] Andreas Haggman. Cyber Wargaming: Finding, Designing, and Playing Wargames for Cyber Security Education. 2019.

- [32] Basel Halak. *Hardware Supply Chain Security: Threat modelling, Emerging Attacks and Countermeasures*. Springer Nature, 2021.
- [33] Basel Halak and Basel Halak. Security Attacks on Physically Unclonable Functions and Possible Countermeasures. *Physically Unclonable Functions: From Basic Design Principles to Advanced Hardware Security Applications*, pages 131–182, 2018.
- [34] Stephen Hart, Basel Halak, and Vladimiro Sassone. MOTENS: A Pedagogical Design Model for Serious Cyber Games. *arXiv preprint arXiv:2110.11765*, 2021.
- [35] Stephen Hart, Basel Halak, and Vladimiro Sassone. CIST: A Serious Game for Hardware Supply Chain. *Computers & Security*, 122:102912, 2022.
- [36] Stephen Hart, Andrea Margheri, Federica Paci, and Vladimiro Sassone. Riskio: A Serious Game for Cyber Security Awareness and Education. *Computers & Security*, 95:101827, 2020.
- [37] Erika H High, Kay A Lovelace, Bruce M Gansneder, Robert W Strack, Barbara Callahan, and Phillip Benson. Promoting Community Preparedness: Lessons Learned From the Implementation of a Chemical Disaster Tabletop Exercise. *Health promotion practice*, 11(3):310–319, 2010.
- [38] Threat Intelligence. DREAD Threat Modeling: An Introduction to Qualitative Risk Analysis. <https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/dread-threat-modeling-intro/>, 2022.
- [39] C.E. Irvine, M.F. Thompson, and K. Allen. CyberCIEGE: Gaming for Information Assurance. *IEEE Security & Privacy*, 3(3):61–64, 2005.
- [40] Michael Riley Jordan Robertson. The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies. <https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies>, 2018.
- [41] William Turton Jordan Robertson. Colonial Hackers Stole Data Thursday Ahead of Shutdown. <https://www.bloomberg.com/news/articles/2021-05-09/colonial-hackers-stole-data-thursday-ahead-of-pipeline-shutdown>, 2021.
- [42] N Menelaos Katsantonis, Isavella Kotini, Panayotis Fouliras, and Ioannis Mavridis. Conceptual Framework for Developing Cyber Security Serious Games. In *2019 IEEE global engineering education conference (EDUCON)*, pages 872–881. IEEE, 2019.
- [43] N. Menelaos Katsantonis, Isavella Kotini, Panayotis Fouliras, and Ioannis Mavridis. Conceptual framework for developing cyber security serious games. In *2019 IEEE Global Engineering Education Conference (EDUCON)*, pages 872–881, 2019.

- [44] James D Kirkpatrick and Wendy Kayser Kirkpatrick. *Kirkpatrick's Four Levels of Training Evaluation*. Association for Talent Development, 2016.
- [45] Kirsten M Koepsel. *Counterfeit Parts and Their Impact on the Supply Chain*. SAE International, 2018.
- [46] Patrick Kral. *The Incident Handlers Handbook*. Sans Institute, 2011.
- [47] David R Krathwohl. A Revision of Bloom's Taxonomy: An Overview. *Theory into practice*, 41(4):212–218, 2002.
- [48] Raghavan Kumar, Philipp Jovanovic, Wayne Burleson, and Ilia Polian. Parametric Trojans for Fault-injection Attacks on Cryptographic Hardware. In *2014 Workshop on Fault Diagnosis and Tolerance in Cryptography*, pages 18–28. IEEE, 2014.
- [49] Leon Li, Shuyi Ni, and Alex Orailoglu. JANUS: Boosting Logic Obfuscation Scope Through Reconfigurable FSM Synthesis. In *2021 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pages 292–303. IEEE, 2021.
- [50] Bao Liu and Gang Qu. VLSI supply chain security risks and mitigation techniques: A survey. *Integration*, 55:438–448, 2016.
- [51] Stephen Losey. Pentagon Suspends F-35 Deliveries Over Chinese Alloy in Magnet. <https://www.defensenews.com/air/2022/09/07/pentagon-suspends-f-35-deliveries-over-chinese-alloy-in-magnet/>, 2023.
- [52] Sander Vinberg Malcolm Heath. What Is Zero Trust Architecture ? <https://www.f5.com/labs/learning-center/what-is-zero-trust-architecture-zta>, 2022.
- [53] Tiffany M McClaskey. *Tabletop Exercises: Gamification in Cybersecurity*. PhD thesis, Utica University, 2022.
- [54] Oskar Mencer, Dennis Allison, Elad Blatt, Mark Cummings, Michael J Flynn, Jerry Harris, Carl Hewitt, Quinn Jacobson, Maysam Lavasani, Mohsen Moazami, et al. The History, Status, and Future of FPGAs: Hitting a Nerve with Field-programmable Gate Arrays. *Queue*, 18(3):71–82, 2020.
- [55] Microsemi. Overview of Design Security Using Microsemi FPGAs and SoC FPGAs. https://ww1.microchip.com/downloads/aemdocuments/documents/fpga/productdocuments/supportingcollateral/overview_design_sec_ms_and_soc_fpgas.pdf, 2013.
- [56] Carlos Moreno, Philippe Vibien, Srijan Pabbi, Lukas Schmidt, Goksen Guler, and Sebastian Fischmeister. Microcircuit Defect and Counterfeit Detection via Silicon Geometry. In *2023 34th Annual SEMI Advanced Semiconductor Manufacturing Conference (ASMC)*, pages 1–6, 2023.

- [57] Xuan Thuy Ng, Zakaria Naj, Shivam Bhasin, Debapriya Basu Roy, Jean-Luc Danger, and Sylvain Guilley. Integrated Sensor: A Backdoor for Hardware Trojan Insertions? In *2015 Euromicro conference on digital system design*, pages 415–422. IEEE, 2015.
- [58] Xuan Thuy Ngo, Jean-Luc Danger, Sylvain Guilley, Zakaria Najm, and Olivier Emery. Hardware Property Checker for Run-time Hardware Trojan Detection. In *2015 European Conference on Circuit Theory and Design (ECCTD)*, pages 1–4. IEEE, 2015.
- [59] SAE organisation. Standards to Prevent Counterfeit Parts. <https://www.sae.org/>.
- [60] Enahoro Oriero and Syed Rafay Hasan. Survey on recent counterfeit ic detection techniques and future research directions. *Integration*, 66:135–152, 2019.
- [61] Jean Lin Otto, Robert J Lipnick, Jose L Sanchez, Robert F DeFraitess, and Daniel J Barnett. Preparing Military Installations for Pandemic Influenza Through Tabletop Exercises. *Military medicine*, 175(1):7–13, 2010.
- [62] Juan Portillo and Eugene John. Using Static Hardware Wrappers to Thwart Hardware Trojans and Code Bugs at Runtime. In *2018 IEEE 61st International Midwest Symposium on Circuits and Systems (MWSCAS)*, pages 1034–1037. IEEE, 2018.
- [63] Paolo Prinetto, Gianluca Roascio, et al. Hardware Security, Vulnerabilities, and Attacks: A Comprehensive Taxonomy. In *ITASEC*, pages 177–189, 2020.
- [64] Melinda Reed, John F Miller, and Paul Popick. Supply Chain Attack Patterns: Framework and Catalog. *Office of the Deputy Assistant Secretary of Defense for Systems Engineering*.–2014.–88 p, 2014.
- [65] Ensieh Roud, Anne Haugen Gausdal, Ali Asgary, and Eric Carlström. Outcome of Collaborative Emergency Exercises: Differences between Full-scale and Tabletop Exercises. *Journal of Contingencies and Crisis Management*, 29(2):170–184, 2021.
- [66] SECUIINFRA. Phases in Incident Response. <https://www.secuinfra.com/en/incident-management/incident-response/>.
- [67] Rachel Sharp. Solar Winds Cyber Attack. <https://www.dailymail.co.uk/news/article-9202019/Massive-Russian-hack-went-FAR-SolarWinds-30-victims-NOT-installed.html>, 2021.
- [68] Satyajeet Shinde, Sasi Jothibas, Mohammad Tayeb Ghasr, and Reza Zoughi. Wide-band Microwave Reflectometry for Rapid Detection of Dissimilar and Aged ICs. *IEEE Transactions on Instrumentation and Measurement*, 66(8):2156–2165, 2017.
- [69] Adam Shostack. Experiences Threat Modeling at Microsoft. *MODSEC@ MoDELS*, 2008:35, 2008.

- [70] Adam Shostack. Elevation of Privilege: Drawing Developers into Threat Modeling. In *2014 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 14)*, San Diego, CA, August 2014. USENIX Association.
- [71] VA Stafford. Zero Trust Architecture. *NIST Special Publication*, 800:207, 2020.
- [72] IDEA Standards. The Independent Distributors of Electronics Association IDEA-STD-1010 Inspection Standard. <https://idofea.org/idea-std-1010-inspection-standard/>.
- [73] Mark Tehranipoor, Ujjwal Guin, Domenic Forte, Mark Tehranipoor, Ujjwal Guin, and Domenic Forte. *Counterfeit integrated circuits*. Springer, 2015.
- [74] Randy Torrance and Dick James. The state-of-the-art in ic reverse engineering. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 363–381. Springer, 2009.
- [75] Tracelaboratories. Counterfeit Electronic Components: Understanding the Risk. <https://smtnet.com/library/files/upload/Counterfeit-Electronic-Components.pdf>.
- [76] Andrew M Tun. *Cybersecurity-Centric Analysis of Complex Integrated Circuit’s System Development Life Cycle Supply Chain*. PhD thesis, Capitol Technology University, 2022.
- [77] VanderbiltUniversity. Bloom’s Taxonomy. <https://cft.vanderbilt.edu/guides-sub-pages/blooms-taxonomy/>.
- [78] Eleonora Viganò, Michele Loi, and Emad Yaghmaei. Cybersecurity of Critical Infrastructure. *The Ethics of Cybersecurity*, pages 157–177, 2020.
- [79] Arya Voronova. Counterfeit Cisco Hardware Bypasses Security Checks With Modchips. <https://hackaday.com/2023/02/01/counterfeit-cisco-hardware-bypasses-security-checks-with-modchips/>, 2023.
- [80] Aaron M Wendelboe, Amanda Miller, Douglas Drevets, Linda Salinas, EJ Miller, Dalton Jackson, Ann Chou, Jill Raines, Public Health Working Group, et al. Tabletop Exercise to Prepare Institutions of Higher Education for an Outbreak of COVID-19. *Journal of emergency management*, 18(2):1–20, 2020.
- [81] Laurie Williams, Andrew Meneely, and Grant Shipley. Protection Poker: The New Software Security ”Game”. *IEEE Security & Privacy*, 8(3):14–20, 2010.
- [82] Kim Wuyts, Laurens Sion, and Wouter Joosen. Linddun go: A Lightweight Approach to Privacy Threat Modeling. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 302–309. IEEE, 2020.

- [83] Kan Xiao, Domenic Forte, and Mark Mohammed Tehranipoor. Efficient and Secure Split Manufacturing via Obfuscated Built-in Self-authentication. In *2015 IEEE International symposium on hardware oriented security and trust (HOST)*, pages 14–19. IEEE, 2015.
- [84] Kan Xiao, Domenic Forte, and Mohammed Tehranipoor. A Novel Built-in Self-authentication Technique to Prevent Inserting Hardware Trojans. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 33(12):1778–1791, 2014.
- [85] Xiaolin Xu, Fahim Rahman, Bicky Shakya, Apostol Vassilev, Domenic Forte, and Mark Tehranipoor. Electronics Supply Chain Integrity Enabled by Blockchain. *ACM Transactions on Design Automation of Electronic Systems (TODAES)*, 24(3):1–25, 2019.
- [86] Jacob Young and Sahar Farshadkhah. Teaching Cybersecurity Incident Response Using the Backdoors & Breaches Tabletop Exercise Game. *CYBERSECURITY PEDAGOGY & PRACTICE JOURNAL*, 2022.
- [87] Kim Zetter. Reported Parts vs. Global Semiconductor Sales. <https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/>, 2016.

APPENDICES

Appendix A

Game Elements of Tabletop Exercise

A.1 Game Property

The chapter 4 discusses in detail about the design methodology of the TTX. In order to make the game more exciting for the participants, there were many game properties used to simulate realism in the TTX. The figures below represent the different email and letter samples that the blue team shall receive during each game scenario. These elements make the simulation of a TTX more engaging and interactive for participants.

Table [A.1](#) outlines the metric to calculate the severity. It serves as a reference to assign the severity of the security breach in an organization's hardware supply chain. Table [A.2](#) provides a reference for the facilitator of the TTX to assign the likelihood of the security threat to occur in the organization's hardware supply chain. Lastly, Table [A.3](#) allows the facilitator to rate the hardware security threat's detectability by analyzing the existing preventive countermeasures used by the organization.

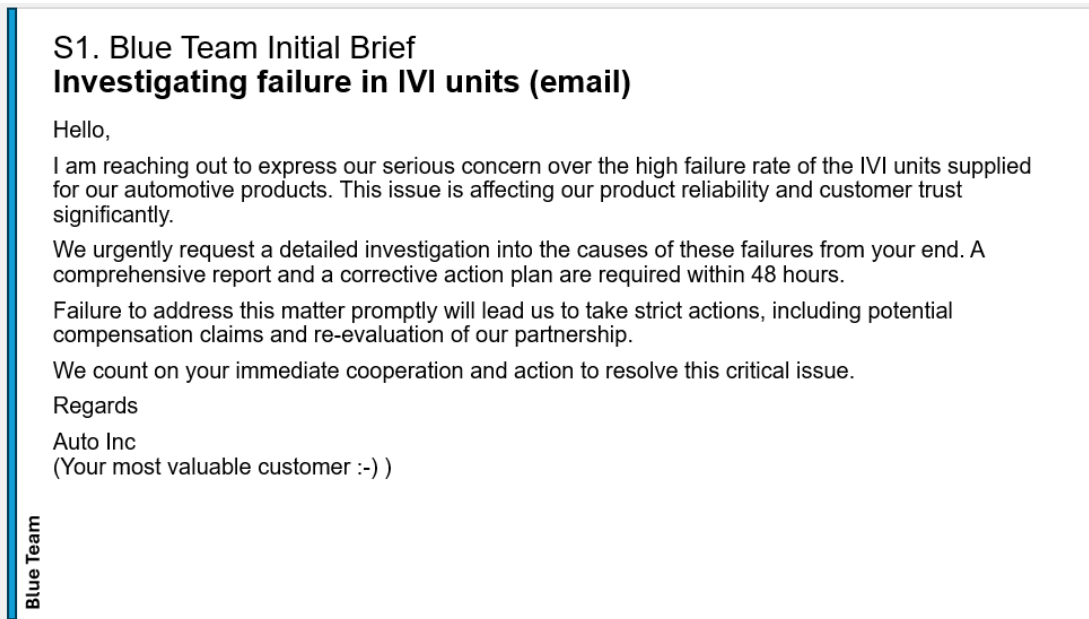


Figure A.1: Game element: Letter from supplier Auto Inc.

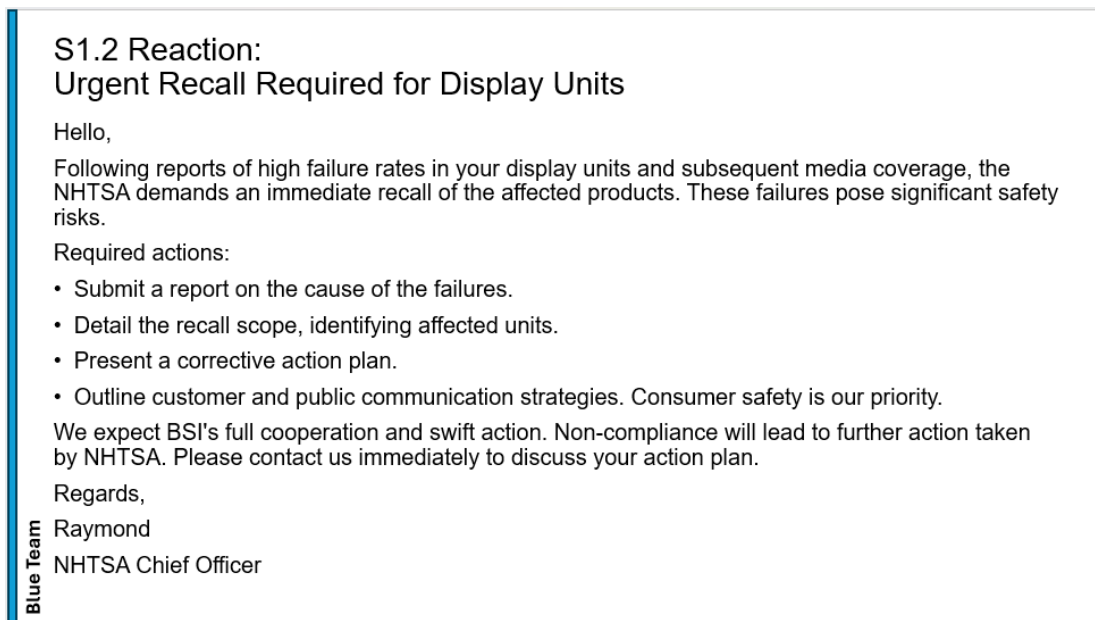


Figure A.2: Game element: Letter from NHTSA

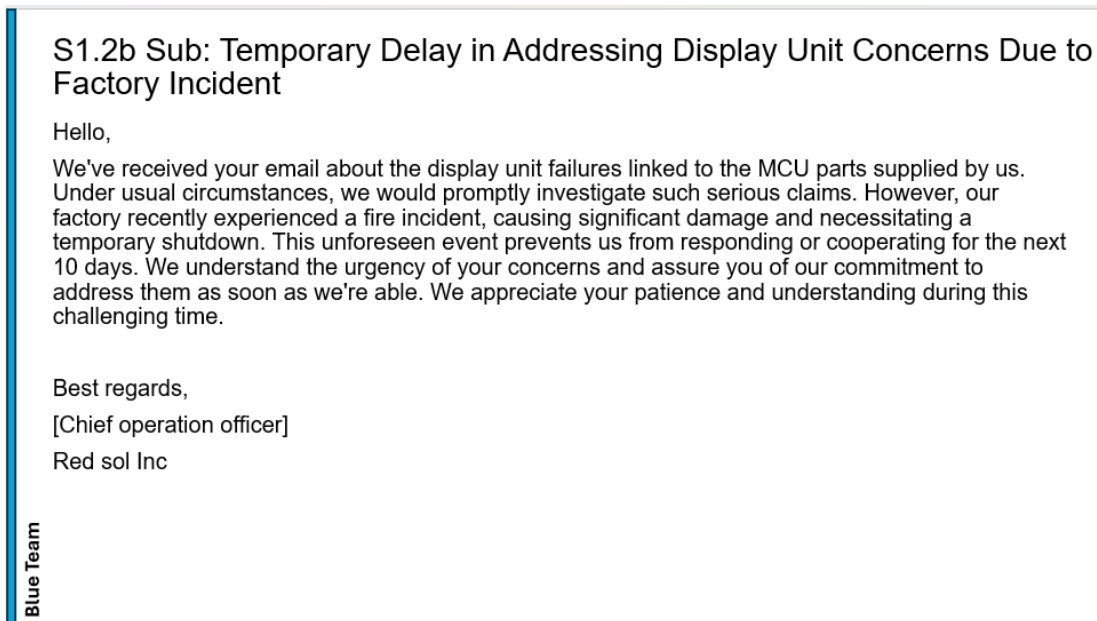


Figure A.3: Game element: Delayed cooperation.

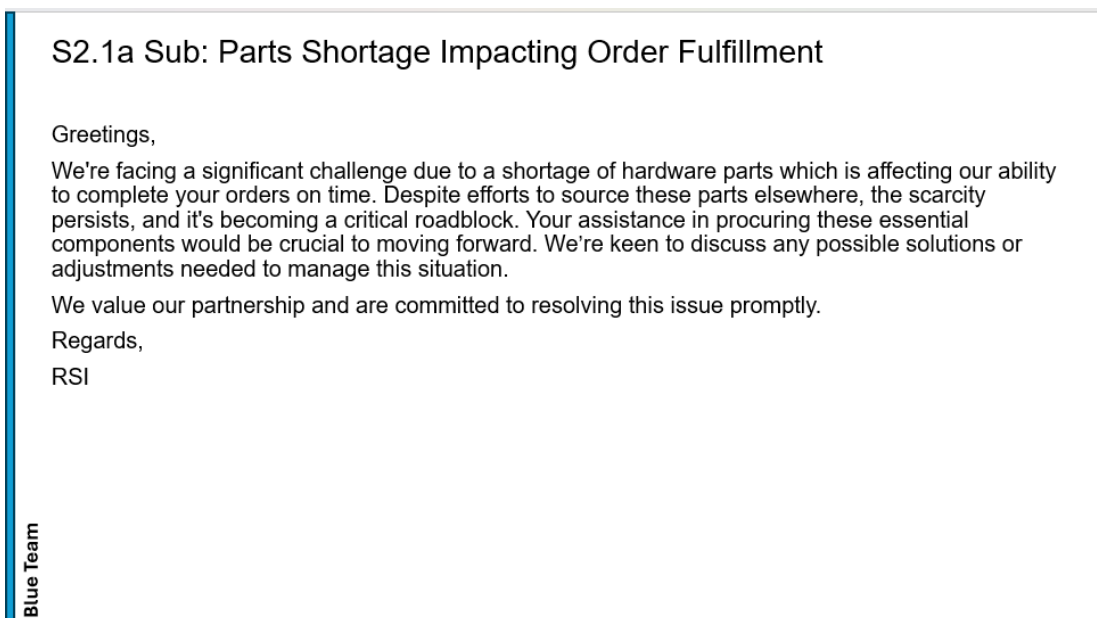


Figure A.4: Game element: Parts crisis

Blue Team

S2.2a Security Alert: Suspicious Activity Detected

Alert ID: 483920 ; Severity: High ; Date/Time: 2024-04-07, 02:15 AM EST Employee Name: John Doe ; Employee ID: 56789 Location: Data Center Access Point 3

Details:

Attempts: 5 unsuccessful attempts followed by 1 successful entry.

Access Time: Between 01:55 AM and 02:10 AM EST.

Resources Accessed: Main Server Room, Data Storage Unit D5.

Method: Employee access card and digital keypad entry.

Action Required:

Immediate Review: Please verify the legitimacy of these access attempts with the employee and their supervisor.

Physical Security Check: Inspect the accessed areas for any signs of tampering or unauthorized activities.

IT Security Measures: Review logs for any unusual data access or transfer during the time in question. Follow-Up: If the access is verified as unauthorized, initiate a detailed security investigation and consider revising access controls and security protocols.

Additional Information: This alert has been generated based on patterns and correlations identified by our SIEM tool, indicating potential security risks. The situation requires prompt attention to ensure the integrity and security of our facility resources.

Figure A.5: Game element: Unusual activity triggered by SIEM tool

Blue Team

S3.1a - Reaction

Subject: Immediate Compliance Required: Official Audit and Suspension Notice

Dear BSI,

We are issuing this formal communication to notify you of an immediate and mandatory audit of your maintenance operations pertaining to the public trans service contract awarded to your company. This directive follows post multiple reports of delay by your facility to complete restorative operations on public transport vehicle's that were reportedly subject to malfunction.

Given the critical nature of public transportation and the recent disruptions, it is imperative that these issues are addressed with utmost urgency.

Failure to comply promptly with the audit process and to initiate swift corrective measures may result in the termination of your current contract. We expect your full cooperation and an expedited response to resolve these critical issues. Please acknowledge receipt of this notice and provide your audit compliance plan within 48 hours. We have decided to suspend your eligibility on future contracts till further notice.

Sincerely,

Rob Stuart
Transit Governance Lead
Canada

Figure A.6: Game element: Government intervention.

Blue Team

S3.2b Subject Urgent: Immediate Attention Required - DDoS Attack Impact

Dear Team,

I hope this message finds you well. I must inform you that our company is currently experiencing a Distributed Denial of Service (DDoS) attack, which has resulted in significant downtime of our core servers. This incident is affecting our operations and services across multiple levels. We are treating this situation with the highest priority and urgency. Our IT security team is actively working to mitigate the attack and to restore services as quickly and securely as possible. We are also in the process of implementing additional security measures to safeguard our systems against future attacks.

In the meantime, I urgently request the following from all departments:

- **Minimize Non-Essential System Usage:** Please reduce the use of all non-essential internet-connected systems to help us manage the load and troubleshoot effectively.
- **Report Anomalies:** If you notice any unusual activity or performance issues, report them immediately to the IT helpdesk.
- **Stay Informed:** Please look out for further communications from the IT department. We will provide updates as more information becomes available and as we progress in resolving this issue.

Your cooperation and vigilance in this matter are crucial. If you have any immediate concerns or suggestions, please do not hesitate to contact me directly.

Sincerely,
IT operations

Figure A.7: Game element: Denial of service attack.

Table A.1: Severity scale for security threats

Scale	Severity Level	Description
1-3	Low Severity	Security threat causes minimal or no disruption to the operation or process;
4-6	Moderate Severity	Threat causes system performance degradation but does not halt overall operations; minor disruptions due to breach may be present.
7-8	High Severity	Threat significantly degrades system performance or causes temporary shutdowns.
9-10	Very High Severity	Threat results in system collapse, breach of security directly leading to severe injuries or fatalities, or violates legal compliance and results in significant financial losses.

Table A.2: Likelihood of security breach in supply chain phases

Scale	Likelihood Level	Description
1-3	Very Low Likelihood	The threat is theoretical, does not cause any supply chain disruptions.
4-5	Low Likelihood	The security breach is possible in one of the phases in manufacturing life cycle with minimal disruption in operations.
6-7	Moderate Likelihood	Security breach possible in two phases in manufacturing life cycle with significant disruption in operations.
8-10	High Likelihood	Well-documented, common occurrence possibility in three phases of manufacturing and heavily disrupts the operations.

Table A.3: Detectability of threats in the supply chain

Scale	Detectability Level	Description
1-3	Very Low Detectability	No effective countermeasures; threats are rarely detected as control systems are old and outdated.
4-6	Low Detectability	Basic countermeasures to detect few known security threats.
7-8	Moderate Detectability	Adequate countermeasures to detect significant number of threats.
9-10	High Detectability	State-of-the-art advanced countermeasures and systems to detect and prevent advanced threats .