University of Zurich^UZH

MASTER THESIS – Communication Systems Group, Prof. Dr. Burkhard Stiller

Design and Implementation of a Business-driven Threat Quantification Framework

Muyao Dong
Zurich, Switzerland
Student ID: 21-740-196

Supervisor: Jan von der Assen, Chao Feng
Date of Submission: September 6, 2023

University of Zurich
Department of Informatics (IFI)
Binzmühlestrasse 14, CH-8050 Zürich, Switzerland

Master Thesis
Communication Systems Group (CSG)
Department of Informatics (IFI)
University of Zurich
Binzmühlestrasse 14, CH-8050 Zürich, Switzerland
URL: http://www.csg.uzh.ch/

Abstract

Heutzutage investieren Unternehmen und Organisationen zunehmend in Cybersicherheit, da sie mit digitalen Informationssystemen arbeiten. Das Cyber-Risikomanagement bietet einen klar definierten Weg zur Verwaltung kritischer Vermögenswerte, Bedrohungen und Gegenmaßnahmen. Innerhalb des Cyber-Risikomanagements ist die Bedrohungsmodellierung ein strukturierter Prozess zur Identifizierung potenzieller Bedrohungen, und in diesem Prozess ist es wichtig, jede Bedrohung zu bewerten und ihre potenziellen Auswirkungen abzuschätzen.

Jedoch konzentrieren sich die meisten Bedrohungsmodellierungsmethoden, obwohl sie tiefgreifend entwickelt wurden, hauptsächlich auf die Identifizierung von Bedrohungen in verschiedenen Kontexten, während die Quantifizierung ihrer Auswirkungen für weitere Untersuchungen weniger diskutiert wird. Diese Arbeit zielt darauf ab, eine Rahmenstruktur zu entwerfen, um diese Lücke zu schließen. Das Hauptergebnis dieser Arbeit ist eine Rahmenstruktur, die Benutzer dazu anleitet, Cyberbedrohungen in Geschäftskontexten zu bewerten und zu quantifizieren. Die Rahmenstruktur ist gut entwickelt, und der Prototyp wurde ordnungsgemäß bewertet. Es zeigt sich, dass die Rahmenstruktur den Designzweck gründlich präsentiert und die Benutzerfreundlichkeit des Prototyps zufriedenstellend ist.

Abstract

Nowadays, companies and organizations invest in cybersecurity more and more as they are operating with digital information systems. Cyber risk management presents a well-defined path toward the management of critical assets, threats, and countermeasures. Within cyber risk management, threat modeling is a structured process to identify potential threats, and in this process, it is significant to evaluate each threat and estimate its potential impacts.

Although threat modeling methodologies have been developed in depth, most of them focus on threat identification in different contexts, while how to quantify their impact for further inspection is less discussed. This thesis works on designing a framework to fill in this gap. The main outcome of this thesis is a framework that guides users to evaluate and quantify cyber threats in business contexts. The framework integrates applicable business impacts, calculates and visualizes the impacts of cyber threats, providing users with an intuitive picture of cyber threats analysis in the view of business. The prototype is well developed and properly evaluated, and the usability of the prototype is of satisfaction.

Acknowledgments

I'd like to express my heartfelt thanks to my supervisor Jan von der Assen. He has provided invaluable guidance and generous help during my completion of the thesis. His expertise and dedication have been instrumental in shaping this research.

I am also very grateful to Professor Stiller for the opportunity of this thesis. It is quite a pleasure to work on this thesis in the CSG group.

Declaration of Independence for Written Work

I hereby declare that I have composed this work independently and without the use of any aids other than those declared (including generative AI such as ChatGPT). I am aware that I take full responsibility for the scientific character of the submitted text myself, even if AI aids were used and declared (after written confirmation by the supervising professor). All passages taken verbatim or in sense from published or unpublished writings are identified as such. The work has not yet been submitted in the same or similar form or in excerpts as part of another examination.

Zürich,

Muyao Dong

Signature of student

Contents

Chapter 1

Introduction

Cybersecurity has become more and more critical to companies and corporations, as most organizations are becoming increasingly dependent on computer systems, and attacks on all aspects of computer system vulnerability are increasing. To address these problems and minimize potential losses, cyber risk management now is deployed by organizations. Cyber risk management presents a well-defined path toward the management of critical assets, threats, and countermeasures of an organization. The reason is that a well-defined risk model ensures that cybersecurity activities are tied to the business value of the assets they aim to protect [1].

1.1 Motivation

Threat modeling, serving as a critical step in cyber risk management, mainly identifies severe threats requiring more investigation in an organization or during the development of a system. During this stage, each threat should be evaluated to estimate its potential impacts, thus providing stakeholders with insights about how resources and funding should be allocated.

Nowadays, most threat modeling methodologies and tools deploy a qualitative approach like ranking the severity of the threat as low, medium, or high. A qualitative analysis sometimes cannot offer a clear and concise result to non-technical stakeholders, even though it may be sufficient in many situations (such as during a quick software implementation cycle). In contrast, a quantitative analysis would enable the translation of a threat model into the broader context of an enterprise's risk management program. For instance, while a straightforward qualitative threat assessment may be sufficient to support the need for a few hours of software engineering on a secure protocol, the adoption of an expensive security service (such as a managed firewall or DDoS (Distributed Denial of Service) filtering service) necessitates a more persuasive case for the business.

1.2 Description of Work

The main goal of this thesis is to design and implement a framework that is able to guide the user in business contexts, facilitating the threat quantification process with all required input parameters. Around this goal, existing threat evaluation methods are first surveyed and documented. Based on the literature research, the thesis proposes an architecture that facilitates the quantification of cyber threats with their business impacts. Furthermore, the thesis implements the prototype with the core mechanism perfectly realized, and the user interfaces properly designed. The prototype assists users in considering applicable business impacts and visualizing the possible losses of these impacts. Based on the visualization result, users can efficiently get insights into the quantification of each threat and prioritization of them.

1.3 Thesis Outline

The whole thesis is structured in the following way: First, the first chapter has already illustrated the motivation and description of this work. Second, Chapter 2 introduces related background knowledge of this work, including cyber threats and Business Impact Analysis (BIA). Chapter 3 presents literature research on existing threat modeling methodologies and discusses their threat prioritization work. Chapter 4 introduces the design of the framework, with each step and design purpose, and Chapter 5 further elaborates on the implementation details of the framework and data transmission among different modules. Chapter 6 evaluates the usability and effectiveness of this framework through two methods: a usage scenario and a focus group discussion. Finally, Chapter 7 summarizes the whole thesis work and concludes future work.

Chapter 2

Background

Cyber threats are constantly evolving and changing. To develop a threat modeling method that can assess business impacts, it is crucial to understand the current state of cyber threats to accurately evaluate the risks and vulnerabilities an organization may face. In this chapter, common cyber threats and crimes are discussed in detail. What's more, threat modeling and business impact analysis is also briefly introduced for a preview of the thesis.

2.1 Cyber Threats and Attacks

Based on operations of implementing threats and attacks, cyber threats are categorized into three classes. technical threats, which mainly rely on computer and Internet operations, non-technical threats, which involve more physical conditions and human factors, and hybrid threats, which consist of both technical and non-technical processes. This categorization is defined by this thesis for a more comprehensive research of cyber threats and attacks, since both the technical and non-technical cyber threats become increasingly complicated as technologies evolve.

2.1.1 Technical Threats

DDoS and DoS Attacks DDoS (Distributed Denial of Service) and DoS (Denial of Service) attacks are the kind of attack in which an attacker intentionally consumes resources to prevent hosts from using the targeted service. focusing on specific applications to manipulate their memory structure, authentication protocols, or specific algorithms for host-based methods. Through the depletion of resources, such attacks can disrupt numerous services and lead to a downgrade in network performance [2].

Zero-day Attack A zero-day attack refers to a type of cyber attack that takes advantage of a vulnerability in the system that has not yet been made public. Cybercriminals can use unpatched flaws in widely-used programs, such as Microsoft Office and Adobe Flash, to attack targets like large corporations and millions of individual PCs worldwide [3]. The most concerning aspect of this type of attack is that, due to the lack of available data until the attack has been identified, very little is known about zero-day attacks [3].

Botnet Botnets are networks of hijacked computer devices used to carry out fraudulent activities and cyber assaults. They are often assembled as part of a multi-layer scheme, with the bots serving as a tool to automate mass attacks, such as data theft, server crashing, and malware distribution. The greatest danger lies in cheap and easy-to-propagate botnet operations, which are lucrative to controllers to conduct attacks [4].

Web-based Attack As Internet users exchange private data via websites and web applications a lot nowadays, the vulnerability of web-based data transmission has been exploited awfully. The web-based attack usually takes four steps: exploring the target, accessing the target system, performing malicious activities, and obfuscating victims by spoofing and log cleaners [5]. Common web-based attack techniques include SQL injection, Local File Inclusions, and Cross Site Scripting (XSS).

Malware As mentioned above, malware is one of the frequently used tools to perform malicious activities. It is a kind of software that performs malicious tasks on a digital device or network, such as corrupting data or taking over a system. To launch a malware attack, the software must first be installed on the targeted device, therefore malware is usually a step of other cyber attacks or crimes. Common types of malware include Spyware, Keylogger, Trojan Horse, Virus, Worm, Adware, Ransomware, and Rootkit [6]. Ransomware is widely considered the most dangerous type of malware, as it can impose a high financial burden on organizations. Attackers who launch ransomware attacks use various techniques to hijack users' or organizations' files and resources, demanding a ransom in exchange for freeing the encrypted or captured data or resources [7].

Man-in-the-Middle Attack The Man-in-the-Middle(MitM) attack is an attack that an unauthorized third party enters communication between two users while not being detected by the two participants. Attackers often use malware to access, read, and modify encrypted data between the two users [8]. For example, when two users communicate through a TCP protocol, it may be intercepted by an attacker acting as the information transfer station to falsify the data. By stealing or altering classified or secret defense sector information, this threat may have an impact on a nation's economy and contribute to international unrest [8].

Eavesdropping Similarly, the eavesdropping attack also thefts data in the process of information transfer. This attack is also known as sniffing or spoofing, and is usually performed to hack data being transmitted between unsecured network communications [9]. Eavesdropping can be categorized as active eavesdropping and passive eavesdropping. For passive ones, with the use of a sniffer tool, the attacker can use a computer to receive all data packets flowing through the local computer, thus enabling the theft of sensitive information. As the sniffer is well concealed and only passively receives data without sending it outwards, it is difficult to detect that someone is listening during the transmission of data [9]. For active eavesdropping attacks, the attacker disguises himself as harmless websites and sends transmitter inquiries to obtain information [9].

2.1.2 Non-technical Threats

For non-technical threats, technologies are used as a weapon to exploit people and carry out attacks. Attackers manipulate human behavior for a specific purpose, like stealing money or accessing sensitive data. Non-technical cyber threats can be just as dangerous as technical threats and can lead to serious security breaches, financial losses, and reputational damage for individuals and organizations. Therefore, it is necessary to investigate them.

Social Engineering As [10] elaborated, social engineering *"is a type of attack wherein the attacker exploits human vulnerability through social interaction to breach cyberspace security"*. Since it preys upon natural social mores, institutions, and patterns of behavior, it is parasitic upon these features of human society [11]. The result is correspondingly hard to estimate, from negative social impacts to financial loss. [12] proposed several social engineering attack scenarios, like pretexting attacks fabricate convincing scenarios to acquire a victim's personal data, baiting attacks luring individuals with complimentary services and request sensitive information in return, and dumpster diving attacks, which collect sensitive documents from company's trash or discarded equipment.

Physical Attack Physical attack is a subset of social engineering to some extent. As the name implies, a physical attack refers to performing the attack by accessing critical machines, servers, or computers in person. The physical attack includes physical manipulation, damage, theft, loss, etc [13]. For example, RFID (radio-frequency identification) card attacks can access forbidden spaces for malicious intentions. An attacker pretends to forget his RFID card and asks a victim to hold the door open, then performs the attack.

Disinformation Apart from these common attacks, some new attacks that emerge with technology development are also proposed by researchers. Disinformation is proposed by [14], which refers to the deliberate spread of misleading or false information. [14] suggests formally recognizing disinformation as a cybersecurity threat for its prospective future categorization, as disinformation delivers negative emotions on online social environments and profoundly reduces the financial value of organizations through reputation damages.

Insider Threat Unlike attacks discussed above, insider threat define a kind of threat from the attacker's perspective. [15] defined that an "insider" is someone who has been permitted to utilize one or more authentication mechanisms, like plain text password, Public Key Infrastructure (PKI), biometric or smart card token, in order to get access to one or more components of the IT system. This insider acts as an entry point, requiring less time and effort to gain additional privileges compared to an external attacker. As a consequence, not only the IT infrastructure weaknesses will be exploited more easily, but also the insider is less likely to be discovered by security measures as he enjoys a high level of trust [15].

2.2 Hybrid Threats

As technology evolves, cyber threats have become more sophisticated. An increasing number of threats are difficult to be simply dichotomized as technical or non-technical, as they may result from different causes or motivations and be accomplished by a combination of technical and non-technical cyberattacks. In this context, they are defined as hybrid threats.

Data Breaches A data breach, or data leakage, is when sensitive information is unintentionally or negligently made available to unauthorized parties [16]. Based on attackers, it can be caused by insider threats (e.g. data theft), or intruders (e.g. sabotage). In terms of motivation, data breaches may be conducted on purpose or inadvertently. Sensitive data leakage can have a negative impact on an organization's long-term stability as well as cause severe reputational and financial damage [16]. For instance, healthcare data is so sensitive that any falsification will lead to improper treatment and irreversible damage to patients.

Cyber Fraud Like data breach, cyber fraud is also a cyber threat that focuses on stealing sensitive information for different goals. It is a broad concept of fraudulent activities committed via the Internet, including crypto-ransomware [17], stock fraud, telemarketing fraud, dating scams, job scams, online auctions, credit card fraud, false advertising schemes, false damage claims, insider trading, Ponzi/pyramid schemes [18]. It usually aims at stealing money from Internet users, and leads to a great financial loss for individuals or organizations.

Phishing Phishing is actually a social engineering technique. It can be performed with different mediums, like the Internet, to a wide range of vectors, such as Email, social networks, websites, WiFi, and so on. For instance, spear phishing [19] is one non-technical approach of phishing that pretends to be emails from the people victims know and tricks them into doing whatever it is the sender desires [20]. Whaling, on the other hand, is a kind of technical phishing that targets senior-level executives who command sensitive information, and induces victims to install malware [20].

2.3 Cybercrime

In the context of information security, cybercrime is also taken into consideration here to get a comprehensive overview of cyber threats. Cybercrime comprises offenses and misdemeanors that use computers or communication devices as targets, commission tools, or are connected to the widespread use of computer technology [21]. Cybercrime often consists of many kinds of cyber threats and attacks, and usually results in huge social or economic losses, even serious national security issues.

Cyberstalking Cyberstalking is a crime that involves using digital devices, such as the internet or other communication tools, to follow and harass another individual or group by sending words and images, so that victims get significant emotional distress [22]. It is often motivated by feelings of vengeance, hatred, envy, or just no valid purpose [22].

Cyber terrorism Cyberstalking is a crime aiming at individuals, while cyber terrorism targets at a wide range of netizens. It usually has a political, racial, or ideological motivation. Terrorists utilize the Internet for propaganda dissemination, individual recruitment, public opinion implication, and corrupting national infrastructure such as transportation, dams, traffic lights, and energy facilities [21]. This type of crime can incite fear, anxiety, and violence among people or result in damage to properties such as computers and networks. For instance, the Ukrainian attack on a power grid in December 2015, which began with a phishing email, is an example of cyber terrorism [21].

Cracking Cracking is the breach of computer security that typically occurs on a network to access another person's computing system, pass passwords or licenses through software, or engage in other illegal activities. A cracker might do it intentionally for financial gain, or for a variety of charitable causes [23]. For example, WI-FI Networks that utilize WPA2-PSK (Pre-shared Keys) are often used within homes and small businesses. A single passphrase is shared between many users and is configured within the wireless access point. The passphrases set on these networks are often too simple and are susceptible to brute force or dictionary attacks [24].

Email spoofing is some kind of cybercrime that is similar to phishing, while it focuses on email-related operations. It usually happens when the recipient gets an email that has been manipulated and dispatched from an unauthorized source. The primary goal of email spoofing is to persuade the recipient to interact with the message, whether it's by opening, responding to, or clicking on it. For example, a spoofed email could pretend to be from a popular shopping website and ask for personal information, like a password or credit card number. Alternatively, a forged email could contain a link that, if clicked, installs malware on the recipient's device [22].

Cyber warfare is a large cybercrime that may result in the most serious consequence among these cybercrimes. It can be conducted by organizations or groups of hackers without government permission and can cause political tensions between countries. For instance, in 2008, Russia and Georgia were involved in a cyberwar that saw the Georgian government websites targeted through SQL injection, DDoS, and cross-site scripting (XSS) attacks [25]. Cyber espionage is also a sort of cyber warfare which refers to the act of using spies to steal sensitive information from rival companies or foreign governments by using computers to carry out these missions [25].

Children Pornography is a kind of new cybercrime phenomenon that occurs on the Internet nowadays. It refers to illegal online pornography involving children in sexual activities. Some illegal online activities include exploiting children through pornographic productions, sex exhibitions, cybersex, prostitution, sex slavery, and the distribution of images and videos. It also includes online communication aimed at sexually stimulating children [18].

Cryptocurrency-related crimes Like child pornography, cryptocurrency-related crimes are also a kind of emerging cybercrime. Cryptocurrencies are prevalent all around the world, and gaining traction as an alternative online currency. Consequently, more attention should be paid to addressing this threat. Cryptocurrencies can be used either as a tool or target in the facilitation of cybercrimes, including blatant theft, illegal trading, money laundering, extortion, and ransomware [26]. For instance, fraudulent traders without valid licenses induce customers to trade or invest digital money which actually does not exist [27].

2.4 Threat Modeling Method

In order to combat these increasingly complex and varying levels of cyber threats, the system should be designed and implemented as resiliently as possible. According to the National Institute of Standards and Technology (NIST) [28], threat modeling is "*A form of risk assessment that models aspects of the attack and defense sides of a logical entity, such as a piece of data, an application, a host, a system, or an environment*". Threat modeling methodologies are created to analyze the system, so that weaknesses in it can be detected and effective measures or modifications can be taken to lower the risk and reduce operation or business loss.

Threat modeling usually takes place in the early stage of development cycle, and it should be noted that threat modeling is a cyclic activity, which requires repeated analysis and actions [29]. In addition, threat modeling is a task that needs a certain amount of specialized knowledge and asks for concerted effort, therefore the involvement of a wide range of stakeholders may contribute to a better modeling result.

Many threat modeling methodologies have been created and put into practice, while not all of them are comprehensive enough to deal with all situations. Some emphasize abstraction, while others are more focused on the needs of individuals. Some methods also concentrate solely on risk or privacy. Combining threat modeling techniques can produce a more complete and accurate picture of prospective threats [30]. As the design of the threat modeling method is the core work of this thesis, detailed research, and discussion about current threat modelings will be put in the next chapter.

2.5 Business Impact Analysis

According to the document ISO/TS 22317 [31], the BIA process "analyses the effects of a disruption on the organization". The process produces critical information about the impact of resource disruption on business [32], and provides statements about business continuity priorities and requirements.

Business impacts can be classified as tangible or intangible based on whether they can be quantified [33]. Tangible impacts are often evaluated by the business loss and repairing cost when an attack succeeds, such as penalties caused by a data breach, or loss of sales due to machine downtime, etc. Intangible ones may not be quantified into specific units, but they can be compared by some qualitative metrics like low, medium, and high.

NIST [34] provides three necessary steps to perform a BIA process: (1) identify critical IT resources, (2) identify disruption impacts and allowable outage times, and (3) develop recovery priorities. [35] illustrates step 2 more specifically, that critical functions like Maximum Tolerable Period of Disruption (MTPD) should be measured and taken into consideration. [36] designs an additional step between step 2 and 3 to prioritize the recovering business functions and data in the event of an outage. Overall, the rough framework of the BIA process has been defined, while details of each step may vary a lot to adopt different management requirements.

Business Continuity Management (BCM), as mentioned above, is a broader concept that includes BIA as a substep. The ISO 22301:2012 document [37] describes it as *"a holistic management process that identifies the potential threats to an organization and the impacts to business operations that those threats, if realized, might cause, providing a framework for building organizational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand, and value-creating activities."* BCM doesn't just consist of one or several general recommendations about how to keep business 'as usual', instead, it should be designed based on the specific situation of each organization. In addition, the BCM should also be dynamic to continuously adapt to business and cybersecurity environment changes [33].

The BIA process is a kind of strategic analysis that allows organizations to have a more clear picture of where to invest critical assets in terms of cybersecurity, in which priority, and to what extent [38]. However, there is still a missing bridge between cybersecurity mitigation and business impact analysis in practical use. As [39] indicates, although some organizations and companies have cyber security incidence responses, they focus more on mitigating those attacks than keeping business continuity. More attention should be paid to further develop corresponding preparations for mitigating more and more complicated cyber threats and attacks.

Chapter 3

Related Work

Within cyber risk management, threat modeling is a crucial activity to understand specific threats that need further attention during the system's design process. Essentially, threat modeling is a systematic approach that identifies potential threat sources and the associated events that may occur in an information system. In this chapter, 23 papers in total are studied with a focus on three dimensions: what they focus on, how they work, and if they involve threat assessment work. The included literature is retrieved mainly from IEEE and Elsevier, with the keywords ”cyber threat modeling” and ”cyber security threat modeling”. Since a wealth of research has been amassed in threat modeling methodologies, two kinds of papers are mainly considered to avoid repetition and investigate as thoroughly as possible: methodology literature review focusing on general threats and methodologies designed for a specific scenario or system.

It should be noted that although threat assessment and risk assessment usually do similar tasks in practice, there is a slight difference between them. While threat analysis concentrates on identified threats, risk analysis encompasses the entire system as its analysis objective. Furthermore, threat assessment is reactive and only takes place in real-time, while risk assessment is more proactive and continuously occurs alongside the system. In this thesis, threat evaluation is emphasized.

Most of these methodologies are designed for general situations like STRIDE modeling methodology [40], and some are tailored to suit particular scenarios, like the Isabelle/HOL framework [41] is developed particularly for insider threats. In the following part they are discussed in detail. Besides, several tables are made to precisely summarize these methodologies, which provides a more explicit comparison and emphasis on them.

STRIDE modeling methodology is a risk-centric methodology deployed by Microsoft. It represents six threat types that usually appear in software. First, Spoofing attacks cover the behaviors that masquerade as legitimate users, processes, or system elements. Second, Tampering attacks that modify or edit legitimate information. Third, Repudiation attacks which deny or disown a certain action executed in the system. Fourth, the information disclosure includes Data breach or unauthorized access to confidential information. Fifth, the DoS attack that leads to disruption of service for legitimate users, and last, the Elevation of privilege getting higher privilege access to a system element by a user with restricted authority [40]. Analysts first model the system with DFD diagrams, and then identify threats in each process with the threat library. The result turns out to be a threat list of the system, while how to deal with these attacks is not included.

Similarly, PASTA (Process for Attack Simulation and Threat Analysis) method is also a risk-centric methodology. It is designed to combine business objectives and technical requirements together and brings the threat modeling process to a strategic level. Therefore, decision-makers from different aspects are required to be involved. The laborious process has a perfect document to guide users to perform seven steps and output an asset-centric result with threat itemization and evaluation. Notably in the last step of PASTA, the business impact is qualified or quantified, but how this substep is done depends.

The TARA (Threat Assessment and Remediation Analysis) method resembles PASTA in the process of threat identification. However, as its name indicates, focuses on not only threat analysis, but also mitigation generation [42]. It focuses on improving the cyber security and resilience of systems early in the acquisition process. It mainly consists of cyber threat susceptibility assessment, which outputs a matrix with a quantitative risk score for each attack vector and attack target, and risk remediation analysis, which provides a solution table. It is worth noting that TARA does include threat prioritization work by giving a risk score, but how the number is calculated is not clearly illustrated in its official report.

Trike [43] is also a risk-centric threat modeling method that manages threats from a defensive perspective. It aims at providing a clear assessment of threats. Analysts first decompose the system into an actor-asset-action matrix, and in each cell of the matrix, there are four parts: creating, reading, updating, and deleting. For each part three values may be assigned: allowed action, disallowed action, or action with rules. To evaluate the attacks, each actor in the matrix is qualitatively defined as always, sometimes, or never for the possibility of performing actions on each asset. Unfortunately, there is no document about the mechanism of Trike, which leaves the scale system vague.

The Common Vulnerability Scoring System (CVSS) [30] was developed by NIST, which aims at providing users with quantitative results of possible vulnerabilities. It provides a unified scoring system, which consists of three metric groups (Base, Temporal, and Environmental), for common cyber or physical systems. The scores provide users with an intuitive view of how severe the threat is. Analysts manually assign scores to each metric, but regrettably, the formulations are not clearly documented.

Attack Trees also focuses on identifying threats by depicting attacks to a system in the tree form [30]. The tree root is the goal for the attack, and the leaves are ways to achieve that goal. Experts decompose the component into several steps and connect them with logical operations AND or OR, and then assign weight or value, like probability, to each node for deeper analysis. The tree helps to identify if the system is vulnerable and what attacks it may encounter. The tree is easy to understand, but as it assumes that users have professional knowledge, risk and threat evaluation is not provided.

Security card focuses on identifying unusual or complex threats [30]. It covers four dimensions, including human impact, adversary's motivation, adversary's resources, adversary's methods, and a total of 42 kinds of threats to help experts to discover potential attacks. Each card has a type of attack and a brief introduction to it. This method is usually integrated into a more complicated framework or serves as a supplement for other methodologies.

Persona non Grata [44] is a threat modeling method based on the idea of figuring out the motivations and skills of attackers. It depicts a persona of potential attackers to experts so that experts can have a picture of the system's vulnerabilities and points of compromise from the other side. This method works similarly to Security Cards, as they both focus on identifying a certain group of threats.

The Operationally Critical Threat, Asset, and Vulnerability Evaluation method, abbreviated as OCTAVE, is also a risk-centric one that especially targets organization activities instead of a continuous process, and focuses on strategic, practice-related issues [45]. This method requires a small group of people from different departments like the operation and IT of the organization and perform the following three steps: identify threats based on assets from the organizational level, identify information infrastructure vulnerability from the technical level, and develop mitigation strategies.

Visual, Agile, and Simple Threat (VAST) modeling method is developed based on an automatic platform named Threat Modeler [30]. This method is designed for the software development process. Most abovementioned threats are labor-intensive and time-consuming, while VAST modeling tends to be light and scalable in large organizations. It guides users to build a DFD diagram to model the operational threats in the view of attackers, and a process flow diagram in an architectural view. These two diagrams recognize the difference between development and infrastructure teams, which can be performed in DevOps lifecycles.

Linkability, Identifiability, Non-Repudiation, Detectability, Disclosure of Information, Unawareness, Non-Compliance (LINDDUN) threat modeling methodology pays attention to privacy during the software development lifecycle [46]. Similar to STRIDE, LINDDUN also builds up a privacy-related threats library. It consists of six steps, for the first three steps it defines DFDs, maps privacy threats to DFD elements, and identifies real threat scenarios. This phase is called problem space. For the last three steps, which are designed for solutions, LINDDUN provides guidance to prioritize threats and elicit countermeasures. It is worth noting that LINDDUN defines the risk as probability times impact to prioritize threats, but if it is quantitatively or qualitatively calculated is not mentioned.

The quantitative Threat Modeling Method is proposed to address the problem in cyber-physical systems, which have complex and highly interdependent components [47]. It combines STRIDE, CVSS, and attack trees, focuses on dependencies among components, and gives a quantitative analysis result of each threat. It builds attack trees based on components with 6 categories of threats provided by STRIDE, then applies CVSS to assign scores for components.

Hybrid Threat-Modeling Method (hTMM) is also a methodology that consists of several general threat modeling methods, including SQUARE (Security Quality Requirements Engineering Method) [48], Security Cards, and PnG, to get a more comprehensive modeling result. The main goal of hTMM is to provide a cost-effective result without false positives and overlooked threats. It first [49] applies SQUARE to identify the system for assets, business and security goals, then uses Security Cards and PnG for brainstorming, which leads to a summary of threats, including its actor, purpose, result, target, and impact. The result then can be used for later risk assessment. Apparently, the impact analysis is also done manually by specialists.

Apart from formal modeling like [50], graphic modeling is also developed. For instance, [51] uses the risk graph to analyze threat scenarios with dependencies. This work pays more attention to the probability of each risk scenario caused by interdependence among components and events. [52] designs a weight distribution algorithm to evaluate all attack paths in a threat tree, which includes both the probability and damage to a threat. However, the paper focuses more on the design and validation of the algorithm, and probability and damage parameters are provided without illustration.

The methods discussed above are threat modeling methodologies applied to a wide range of situations. As mentioned previously, some methods and frameworks are proposed for a certain kind of attack or system. These methodologies involve more explicit operations and professional information, which helps deal with more practical-related issues in specific scenarios.

[41] pays attention to the insider threat. It applies social behavior theory, the Isabelle/HOL framework for a social explanation, to model insider threat behavior. The result is proof or validation to justify possible malicious attacks, which can be used to improve the infrastructure and policies, leading to an improved security architecture. This framework can be further applied to any cyber-human systems, as HOL can be used to convey human psychological propensities, regional and international policies, as well as network and physical characteristics of an organization's architecture [41].

Similarly, [15] also focuses on insider threat analysis. It starts with how to precisely document insider misuse by designing a language development methodology, thus helping experts efficiently deal with them. It classifies misuse cases and then abstracts the problem domain. This work is still under construction, but is also promising in building a library for certain kinds of threats.

[53] emphasizes the area of the supply chain. It suggests a social-technical framework from a systematic view. The framework consists of a dynamic system, which is made up of four subsystems interacting with each other to ensure the integrity of the whole modeled organization, and a static 7-layer model, which serves as a security consensus base. After using a signal diagram to simulate a process in the supply chain, users can use the 7-layer model to itemize threats from social to technical, and the dynamic system works to discover more possible related threats.

As illustrated in Section 2.3, cyber terrorism is a subset of cybercrime, and [54] proposes HMMs and Bayesian models to efficiently extract terrorist activities and predict threats from a large amount of data that represent any activities like travel or communication between people or item of suspicious origin. This work utilizes mathematical models to deal with threats caused by cyberterrorism.

[55] aims to improve the trustworthiness of software design by a unifying threat model. It is similar to the working principle of the Quantitative Threat Modeling Method. This model

uses a UML activity diagram to model system functions and then applies STRIDE threat categories to identify attacks. As the specific threat scenario is defined, the corresponding attack tree is also built. Each node in the tree is assigned a weight, which helps calculate the overall criticality of the threat. In this way, the unifying model can provide users with attack situations and critical degree analysis. However, how the weighted node is quantitatively defined is not discussed, as the point of this work is to implement the whole algorithm.

[50] builds an information security management system based on a scenario in the library. The system uses a business process model to identify and assess threats, and most analysis work is done manually by information security specialists. The risk analysis stage is included in the system, while it is just roughly defined without detailed implementation steps. [56] performs threat identification in smart grid systems. Although it does a comprehensive check to accumulate all possible threats that may occur in the smart grid system, it does not continue to evaluate identified threats.

Similarly, [57] proposes a social-technical framework to perform threat identification tasks in the supply chain industry. It involves sociology theory to construct the threat identification model. It can be concluded that most threat modeling methods with practical applications in industries remain aiming at recognizing all possible threats with different measures.

Based on the aforementioned methodologies, some conclusions can be drawn. First, some methodologies combine both manual and automatic modeling techniques, like VAST modeling, and some employ both graphical and formal modeling methods with various weight algorithms. This indicates that the form of threat modeling can be quite flexible and adjustable by deploying different methods.

Moreover, most threat modeling methodologies remain to be done manually by stakeholders, which can be pretty subjective and time-consuming. Consequently, there is a demand for a higher level of automation to model the system, which is one of the goals this thesis is going to achieve.

Last but not least, identifying threats is a focus. It can be seen that a certain number of methods still try to itemize as many as possible threats to systems, and then build up a threat library for further application. The drawback is obvious, as it is discussed in the previous cyber threats part, since new cyber attacks may appear rapidly with the development of technology. While some methods prioritize threat identification, few provide a systematic approach to deal with them. 8 of the 23 methods mentioned threat prior step, 3 of those 8 methods are in a quantitative way, and only Trike provides a clearly defined formula to prior. Therefore, there is a missing methodology that can automatically help organizations quantify and prioritize threat impacts from a business view, and this thesis is trying to address this gap.

Table 3.1: General Threat Modeling Methods

Threat Modeling Method	***Focus***	***Process***	***Threat Prioritization***
STRIDE [40]	Risk-centric	DFDs+6 categories of threats	/
PASTA	Risk-centric	7 steps	Manually review in impact analysis step
TARA [42]	Mitigations	Associate mitigations to each identified vulnerability	/
Trike [43]	Risk-centric	/	Trike defines exposure as the value of asset times the action-specific risk
CVSS [30]	Severity of vulnerability	Build a matrix based on three metric groups	Metric value is predefined, qualitative but not transparent
Persona non Grata (PnG) [44]	Attacker-centric	“introduce” a technical expert to a potential attacker	/
Security Cards [30]	Unusual and complex attacks	Deck of 42 cards to facilitate threat discovery activities	/
hTMM [48]	Cost-effectiveness	Security Cards+PnG	/
Quantitative TMM [47]	Risk-centric	Attack Trees, STRIDE, and CVSS	Same as the CVSS
LINDDUN [46]	Privacy concerns	6 phases	/
OCTAVE [45]	Strategic, practice-related issues	Determine requirements-Identify vulnerability-Design strategies	/
VAST Modeling [30]	Scalability	Three pillars	/
Unified Threat Modeling [55]	Risk-centric	STRIDE+Attack Tree	How the impact is quantitatively defined is not discussed
Attack Tree [30]	Threat-identifying	Decompose the goal and identify nodes	/

Continued on next page

Table 3.1 – continued from previous page

Threat Modeling Method	***Focus***	***Process***	***Threat Prioritization***
Risk Graph [51]	Risk-centric	Dependency inference and probability and consequence value for calculus	Qualitative consequence value is assigned
Threat Tree [52]	Risk-centric	Iterative decompose the object	Manually provided by companies

Threat Modeling Method	***Focus***	***Process***	***Threat Prioritization***
Integrated smart grid systems security threat model [56]	For Smart Grid	/	/
Business process model [50]	For library	Analysis done by specialists	/
Socio-Technical Framework [53]	For supply chain	Static identifying model and dynamic system	/

Table 3.2: Threat Modeling Methods for Specific Industry

Threat Modeling Method	***Focus***	***Process***	***Threat Prioritization***
Isabelle/HOL framework [41]	Insider threat	A set of proof to validate possible insider threats	/
Insider threat Modeling [15]	Insider threat	Language development methodology	/
HMM&Bayesian networks [54]	Cyber tetorrism	Mathematical modeling	Mentioned but no detailed algorithm is provided

Table 3.3: Threat Modeling Methods for Specific Attacks

Chapter 4

Architecture

This chapter elaborates on the architecture of the business impact analysis for cyber threat prioritization proposed by this thesis. The framework assumes that the user has an explicit list of threat scenarios. A threat scenario involves not only the exact cyber threat, but also the context or the outcome the threat causes, like malware to a laptop leads to private information leakage. The goal of the framework is to provide both overall and detailed loss analysis for them, with business impact analysis. Overall, the framework consists of three key phrases. First, identify each threat scenario as one type of information compromise: confidentiality, integrity, and availability. Second, map possible business impacts based on different types of data loss. Finally, calculate the estimated lost revenue and visualize it by leveraging the BIA-related parameters provided by users. The result will be visualized and threats will be prioritized for users to gain insights about remedies. An example workflow of the framework is shown in Figure 4.1.

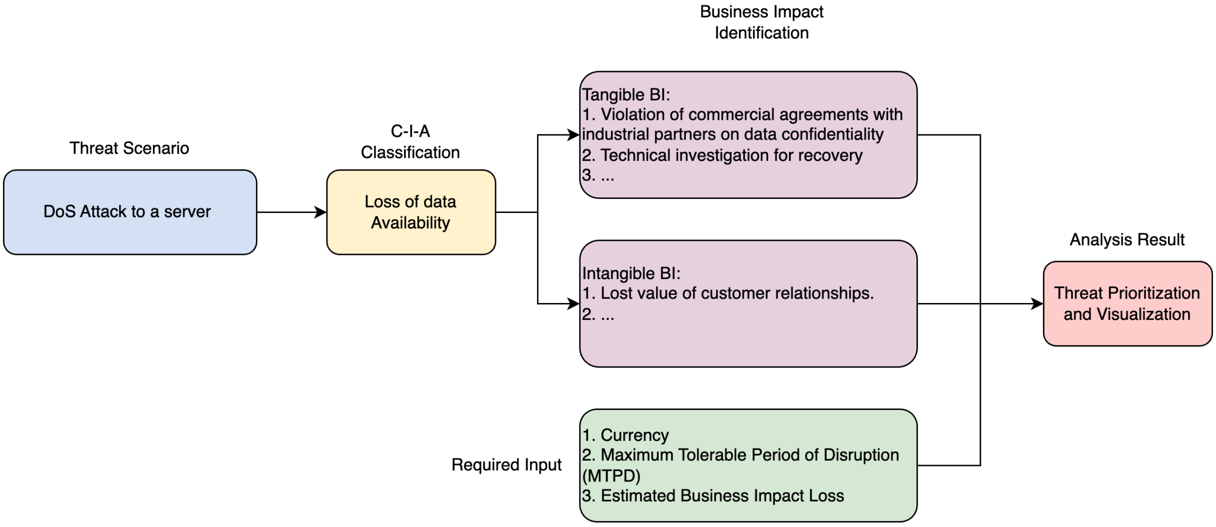

Business Impact Identification
Threat Scenario
DoS Attack to a server
C-I-A Classification
Loss of data Availability
Tangible BI:
1. Violation of commercial agreements with industrial partners on data confidentiality
2. Technical investigation for recovery
3. ...
Intangible BI:
1. Lost value of customer relationships.
2. ...
Required Input
1. Currency
2. Maximum Tolerable Period of Disruption (MTPD)
3. Estimated Business Impact Loss
Analysis Result
Threat Prioritization and Visualization

Figure 4.1: Example Workflow of the Framework

Type of data loss	***Threat***
Confidentiality	Zero-day attack, Malware, Ransomware, MitM attack, Web-based attack, Social engineering, Physical attack, Eavesdropping, Disinformation, Insider threat, Data breaches, Cyber fraud, Phishing
Integrity	Malware, Social engineering, Physical attack, Insider threat
Availability	DoS or DDoS attack, Botnet, Physical attack, Social engineering

Table 4.1: Threat Categorization

4.1 Threat Classification Mechanism

The first step to search for possible business impacts is to identify the threat as what kind of information compromise. The C-I-A (Confidentiality-Integrity-Availability) classification mechanism allows the narrowing of possible business impacts, as the research [33] has proved that different kinds of data loss may trigger different directions of business loss. This mechanism is populated as a result of the literature, the NIST guide, and ethnographic observations conducted in the industrial reference scenario.

As illustrated above, threat scenarios are known and provided by users. Then each threat is recognized by the framework. The C-I-A classification defines information loss from three perspectives: confidentiality ensures data is protected from unauthorized access and cannot be disclosed from unauthorized operations, integrity protects information from improper modification, and availability guarantees the data is accessible and usable on demand. For instance, one identified threat named the DoS attack on the main server should be categorized as the loss of data availability, since the DoS attack temporarily interrupts the service, rendering it inaccessible to its users.

Table 4.1 presents a mapping of general threats analyzed in chapter 2 and the C-I-A classification to provide a more intuitive picture of how this section works. The basis of the mapping is the most possible result that the cyber threat may cause. For example, the zero-day attack is a kind of attack that exploits the software vulnerability unaware of vendors. malicious actors then can utilize this vulnerability to steal data from the system, thus resulting in data confidentiality loss. Some cyber attacks can lead to different impacts according to different situations, like the proactive insider threat may lead to both data leakage and unauthorized modification, and these attacks are mapped to more than one type of information compromise.

4.2 Business Impact Factors Mapping

After determining what kind of data loss the threat will cause, the C-I-A to BI mapping is followed. To provide users with a clear picture of what business impacts may be caused due to different types of information compromise, a group of business impacts is collected from the multiple industry reports, such as [58] and [33]. These papers provide comprehensive lists of what business impacts one cyber threat may cause regarding confidentiality, integrity, or availability aspects, which are deployed and analyzed by this thesis. detailed discussion is illustrated in the following sections.

Business impacts can be further subdivided into tangible business impacts and intangible ones. Tangible business impacts are direct results caused by cyber threats, while intangible impacts are indirect ones, which may be easily ignored and have a more far-reaching impact. For instance, if the DoS attack on the server leads to the unavailability of data related to factory production, then the direct impacts will be product loss of revenue during the disruptive time, and possible penalty due to the violation of commercial agreements with customers on delivery time. Intangible impacts may include future lost contract revenue and customer relationships, as this factory cannot deliver products on time.

Furthermore, as the business impact analysis focuses on impacts over time after the attack, the timeliness of business impacts should also be taken into consideration. Some impacts, like the penalty of agreement violation, are one-time impacts and counted once when an attack happens, while some are persistent, like product loss during the disruptive time, which should be considered over the specific timeframe.

In the design of the architecture, 16 business impacts collected from [58], [33], and [58], are taken into consideration in the end. Users may choose what business impacts are applied in the current threat scenario. In the following sections, the discussion regarding categorization will be further elaborated regarding their tangibility and timeliness. Table 4.2 gives a summary of inspected business impacts, and the discussion of each threat about what it refers to and why it is categorized as that type of compromise is illustrated in the rest of this section.

4.2.1 Business Impacts of Integrity

Damage to information integrity usually leads to impacts on ongoing businesses, like sabotage of the entire critical infrastructure and components. First of all, the production or service will be directly influenced, which gives rise to resource waste and sale loss of the invalid product or service. The loss will grow as the disruptive time goes on, therefore both of them are identified as a persistent impact. For instance, one production line of a chip manufacturer is stalled as the parameters of the product are maliciously modified by a hacker. However, before the production line is stopped, one hundred defective chips have been produced, and the materials cost and the profit that would have been earned on this batch of defective products are all considered as business losses during the disruptive time.

Besides, for some industries, some unauthorized modification may damage critical components or infrastructure, thus resulting in additional recovery fees. This impact can be both one-time or persistent, and users may choose which type to apply in the scenario.

Correspondingly, agreements and contracts with customers cannot be fulfilled, and the penalty for the violation of product specifications should be involved. What's more, influenced business processes may also cause unexpected violations of industry guidelines

Category	***Type***	***Business Impacts***
Confidentiality	Tangible	1. Violation of commercial agreements with industrial partners on data confidentiality (penalty). 2. Customer breach notification. 3. Post-breach customer protection. 4. Attorney fees and litigation (theft of IP). 5. Public relations (and company reputation). 6. Violation of standards and regulations in privacy or data protection (regulatory compliance/penalty).
	Intangible	1. Increased cost to raise debt.
Integrity	Tangible	1. Damages to critical components (recovery fee). 2. Quality degradation of products (resource waste and sale loss of invalid products or services). 3. Violation of standards and regulations in safety and pollution (regulatory compliance/penalty). 4. Violation of commercial agreements with customers on product specifications (penalty).
Availability	Tangible	1. Product loss of revenue during disruptive time (lost sales). 2. Violation of commercial agreements with customers on delivery time (penalty). 3. Quality degradation of products (resource waste and sale loss of invalid products or services).
General	Tangible	1. Technical investigation. 2. Cybersecurity Improvements.
	Intangible	1. Lost value of customer relationships. 2. Value of future lost contract revenue. 3. Insurance premium increases.

Table 4.2: Business Impact Categorization

or laws and regulations. These three violation penalties should be defined by contracts or regulations, and work as one-time impacts.

Intangible impacts mainly lie in the follow-up handling of business disruptions, including the possible loss of customer relationships and future contracts, which are general impacts all three types of information compromise will face and discussed in Section 4.2.4.

4.2.2 Business Impacts of Availability

The loss of data availability usually results in the breakdown of the ongoing business. It delays the process and the loss during the disruptive time should be intensively evaluated. This loss can be product quality degradation and sale loss, which is persistent before the information recovery. Penalty for the violation of delivery time with customers is also involved as a one-time impact.

For indirect impacts, as the current business is affected, further loss of customer relationships and future contracts will also be irresistible.

4.2.3 Business Impacts of Confidentiality

For the loss of data confidentiality, the most direct result will be information leakage, and remedies also emphasize how to stop the breach and handle negative outcomes. Usually, confidentiality loss doesn't affect business operations directly, and related business impacts are external. First, direct customer-facing businesses should release customer breach notifications, which may include printing, mailing, and call center services, and are generally mandated by state or federal law or industry regulation. Apart from this, post-breach customer protection costs should also be considered. It refers to the direct expenses which aim at identifying and safeguarding against potential attempts to illegitimately utilize customers' compromised personal information. Both impacts are recognized as one-time costs since this remedial measure usually takes place once in each threat scenario.

Some big corporations need to pay attention to public relations, as the data breach will harm the company's reputation. PR campaigns may cost differently and this is also a one-time impact. Some businesses include strict confidentiality agreements, and the penalty for violating commercial agreements with industrial partners is also involved. For companies with unique Intellectual Property (IP) as their core competitiveness, like trade secrets, copyrights, and investment plans, the theft of IP will lead to the loss of competitive advantage and possible attorney fees and litigation.

One of the intangible impacts of data confidentiality damage can be the increased cost to raise debt. It indicates that the loss of data confidentiality will cause a decrease in credit rating, thus forcing the victim company to encounter elevated interest rates for borrowed funds, whether they are acquiring new debt or renegotiating existing debt agreements. The increased expense can be either one-time for the estimation of the next debt, or persistent lasting for several years.

4.2.4 General business impacts

In addition to the ones discussed above, some impacts are more general and applied to every situation. In other words, these losses are quite likely to happen once a cyber attack occurs. In this work, two tangible impacts, technical investigation and cybersecurity improvements, and two intangible impacts, loss of customer relationships and future lost contract revenue, are involved to perfect the business impact list.

The technical investigation is a direct cost for analyzing what transpired during a cyber attack and identifying the perpetrators. Cybersecurity improvements, which also serve as instant remedies, are the cost to the infrastructure, security controls, monitoring capabilities, or surrounding processes to restore business operations so that the likelihood of similar events occurring in the future will be reduced. These two impacts should be often discussed, and identified as one-time costs during emergency response.

It takes time for the loss of customer relationships and future contracts to show up after the attack, and it is difficult to quantify the precise loss. According to the Deloitte report [58], marketing teams may estimate it by attaching a "value" to each customer in order to reckon how much revenue these customers may generate during a time. The loss then can be calculated with this kind of reverse thinking. Both two impacts last for a long period, therefore they are recognized as persistent impacts in this work. Additionally, some company may purchase insurance for important infrastructure or IT components. After a cyber incident, there may be higher costs for an insured company to pay to obtain or renew cyber risk insurance policies.

4.3 Loss Calculation and Visualization

After the critical business impact identification, the overall loss due to the attack is calculated. In this step, more input is required from users. The input step applies to each threat, including used currency, the MTPD of the interrupted business process, and two sections for one-time and persistent business impacts. The first section is for one-time business impacts, and users are requested only to provide the overall estimated loss. For persistent impacts, their daily loss and likely duration are required. In order to give a more accurate loss trend, the recovery level, defined qualitatively as the ratio of the current situation to normal, is also needed.

After getting all the required parameters, the framework automatically calculates the lost revenues. It first computes the loss for each threat based on the business impact tables. The formula is defined as follows:

$$\text{Loss} = \sum_i \left(\sum_t \text{BI\_persistent}_i \cdot (1 - \text{Recovery}_t) \cdot \text{Days}_t \right) + \sum_j \text{BI\_onetime}_j \tag{4.1}$$

The total loss of one threat consists of two parts, one-time loss, and persistent loss. `i` and `j` itemize each persistent impact and one-time impact, and `t` represents the recovery stages of each persistent impact. `BI_persistent` represents the input loss of persistent loss, `Recovery_t` is the recovered level of the business with time going on, and `Days_t` represents the time when the business restores to `Recovery_t`. The framework then adds all persistent loss which varies at different time and all one-time loss together.

For instance, a threat is determined to lead to these impacts: cybersecurity improvements, insurance premium increases, and product loss of revenue during the disruptive time. Among them, cybersecurity improvements and insurance premium increases are one-time impacts, which cost 1000 USD and 1200 USD respectively. The product loss is persistent and estimated as 500 USD per day before this threat is resolved. During the 1-3 days after the threat happens, the recovery is 0, during the 4-5 days, the disruptive business is recovered to 0.6, and on the sixth day, the business is completely restored. The loss calculation works in the following way: one-time impacts are directly added together:

$$\text{BI\_persistent} = 1000 + 1200 \tag{4.2}$$

while the persistent impact loss is summed up over time:

$$\text{BI\_onetime} = 500 * (1 - 0) * 3 + 500 * (1 - 0.6) * 2 \tag{4.3}$$

In the end, the overall loss of this threat is the sum of persistent and one-time impacts:

$$\begin{aligned} \text{Loss} &= \text{BI\_persistent} + \text{BI\_onetime} && (4.4)\\ &= 1000 + 1200 + 500 * (1 - 0) * 3 + 500 * (1 - 0.6) * 2 && (4.5)\\ &= 4100 && (4.6) \end{aligned}$$

Therefore, this threat is estimated to cause a loss of 4100 USD.

As each threat is inspected in detail, the framework collects the results from all of them and gives the visualization. The visualization of the loss focuses on both the overall loss and details of each threat scenario.

The overall loss collects all calculated losses of threats and adds them on the same time axis, and is visualized as a line chart, representing the relative revenue trend of the company with all threats happening. Then there are two threat prioritization lists, one is sorted according to the MTPD, and the other is ranked according to the estimated damage caused. The MTPD prioritization gives the emergency of each business that the threat influences, and the loss prioritization shows the order of decrease in revenue of each threat. Users may combine them to have a more objective insight into threats and take further measures.

After getting an overarching view of analyzed threats, there is also detailed visualization for each threat. The loss of each threat is visualized in a pie chart with proportions of different business impacts, which allows users to inspect these threats more in detail.

Chapter 5

Implementation

This chapter elaborates on the prototype implementation of the designed architecture based on Chapter 4, including technology stack use, interface design and implementation details, and other technical details.

Figure 5.1 provides an overview of the workflow of this framework. Firstly, the homepage allows users to input the threat scenario list and return a table with the C-I-A identification for each threat scenario, followed by an 'inspect' button. The button directs users to different pages with different business impacts based on the business impacts mapping discussed in Section 4.2. In this step, users can both choose applicable impacts and add customized impacts. For chosen impacts, an input page is generated next, which provides currency selection, MTPD input, and detailed numbers of each threat scenario. Inputted data on this page is collected and stored in the local storage. The homepage then extracts the data, calculates and prioritizes the overall loss as well as the detailed loss of each threat. Finally, the result is visualized through different forms of charts on the homepage, presenting users with a clear view of threat scenario prioritization and business impact composition.

Figure 5.2 presents a more detailed structure of each code file and function implementation. Codes shown in the rest of the chapter are quoted from files and functions depicted in this figure. All critical functions are extracted and shown here, with bidirectional arrows for the mapping of the page and JavaScript file, two-line connections for each file's composition, one-way arrows for the navigation between pages, and dotted lines for the connection to local storage. In the following sections, the logic and mechanism behind different files and how they communicate are explained comprehensively.

5.1 Technical Stack

The prototype is implemented with JavaScript, HTML, and CSS. Pico.css[1], which is a light CSS framework for semantic HTML, is deployed to improve the appearance of

[1] https://picocss.com/

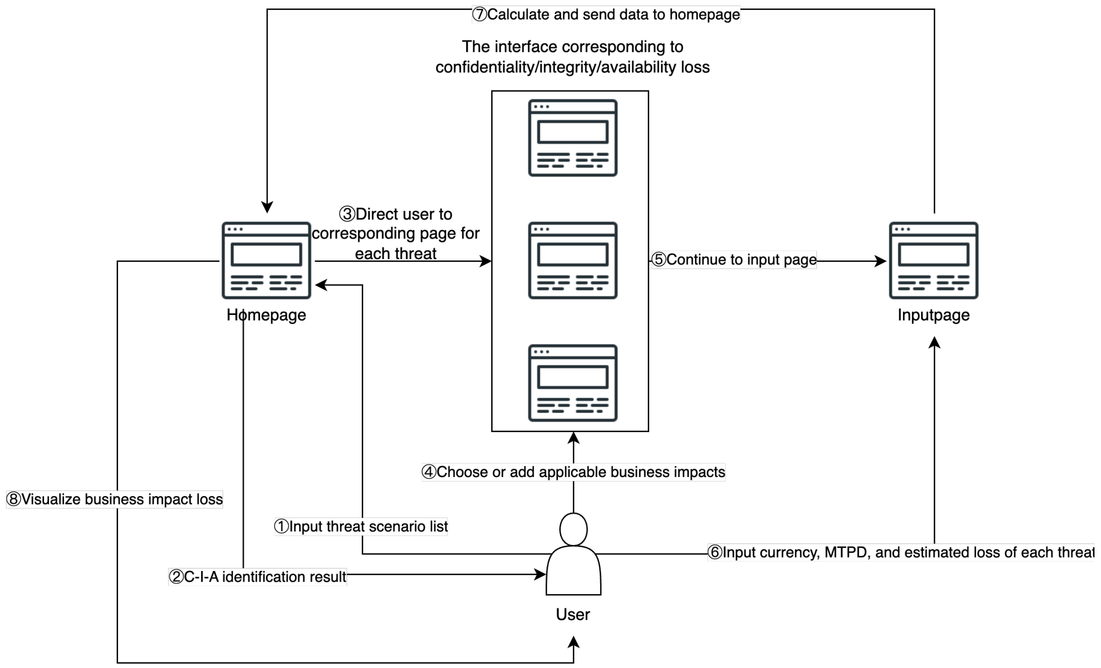

⑦Calculate and send data to homepage
The interface corresponding to confidentiality/integrity/availability loss
③Direct user to corresponding page for each threat
⑤Continue to input page
Homepage
Inputpage
④Choose or add applicable business impacts
⑧Visualize business impact loss
①Input threat scenario list
⑥Input currency, MTPD, and estimated loss of each threat
②C-I-A identification result
User

Figure 5.1: Workflow of the Framework Implementation

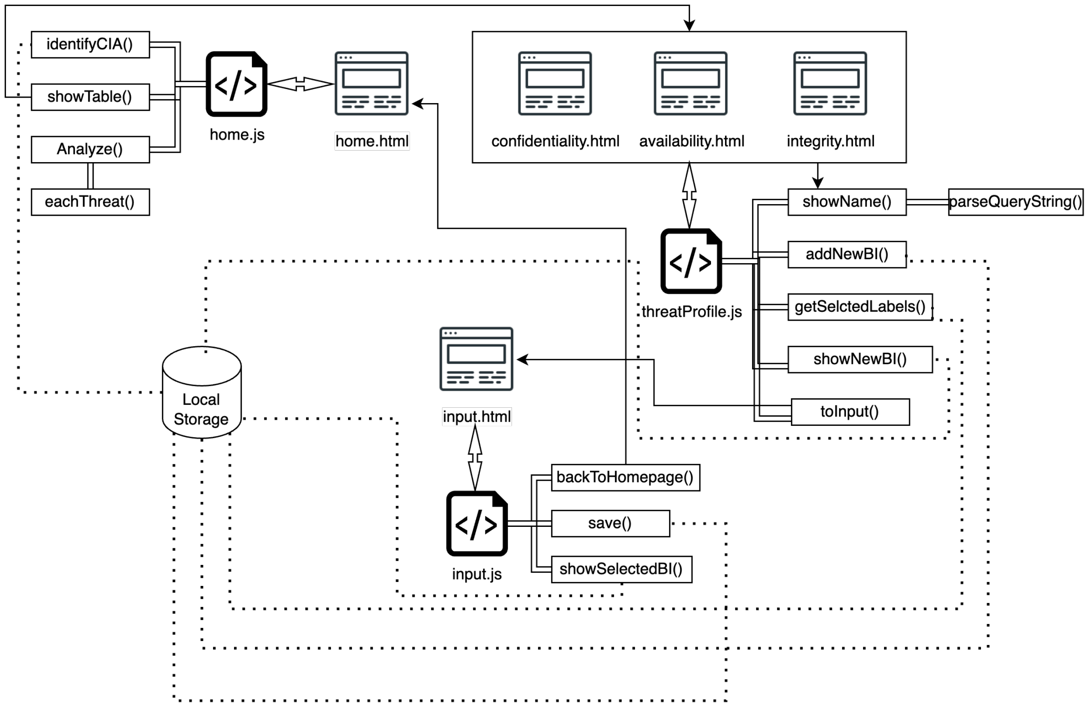


Figure 5.2: Detailed Coding Implementation Design

interfaces. All relevant data is stored in the local storage of the browser, and so far there is no back-end database applied. The implementation is completed in VScode, which is an IDE that provides an instant presentation of the prototype. What's more, all codes are stored in the repository of GitHub[2] for further check.

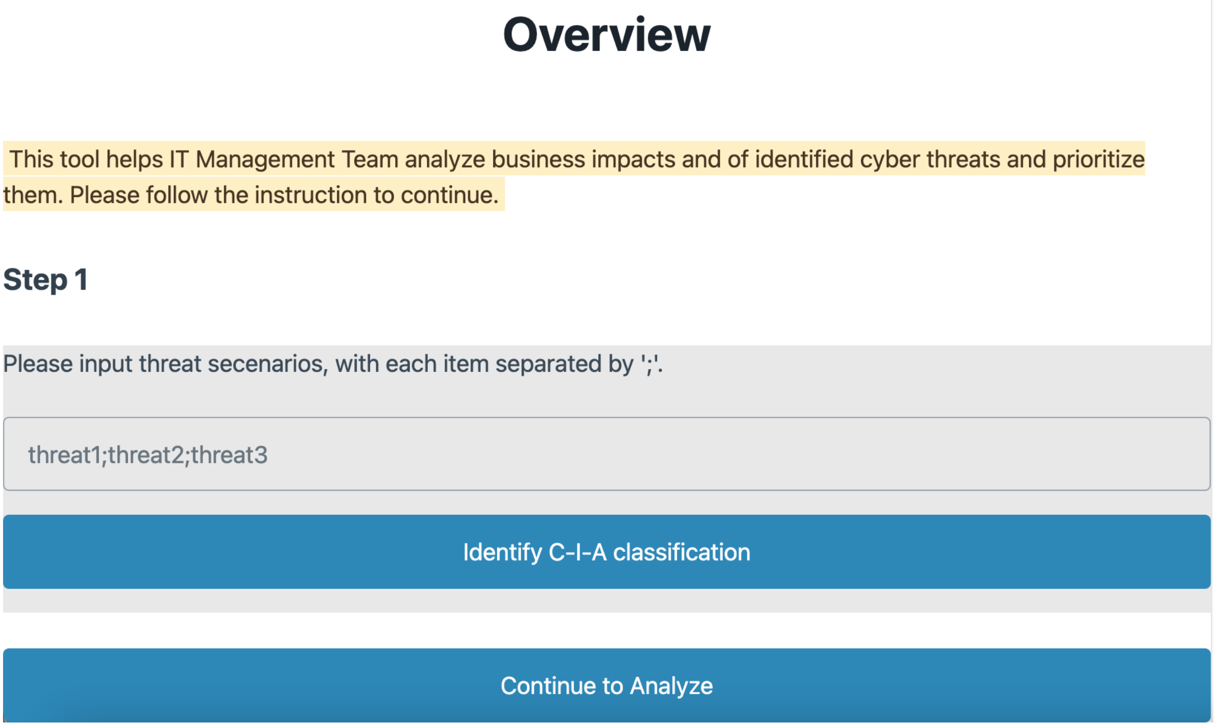
[2] https://github.com/Dmmmmy/BIA-prototype

Technical Stack Components	***Technology***
Programming Language	JavaScript, HTML, CSS
Frameworks and Libraries	pico.css
Development Environment	Visual Studio Code 1.80.1

Table 5.1: Technical Stack

5.2 C-I-A Identification and Implementation

Serving as the beginning page, the home page mainly undertakes two tasks: classify input threat scenarios and visualize the final calculation result. All relevant functions are implemented in the home.js file. Here, functions related to C-I-A identification are first discussed.



Overview

This tool helps IT Management Team analyze business impacts and of identified cyber threats and prioritize them. Please follow the instruction to continue.

Step 1

Please input threat secenarios, with each item separated by ';'.

threat1;threat2;threat3

Figure 5.3: Initial Page

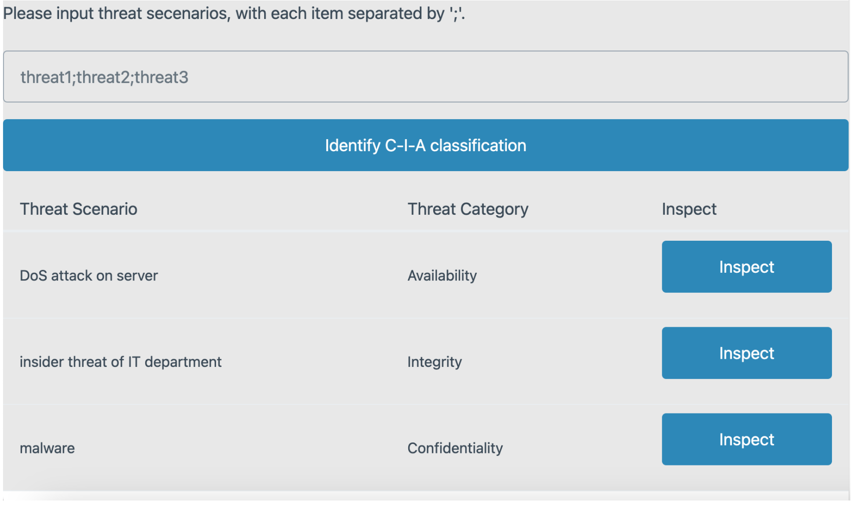
In the beginning, only an input box and a classification button are shown on the homepage for input threat scenarios classification (see Figure 5.3). The highlighted words indicate the usage of the framework, and the section 'Step 1' marked in grey helps users get started. The function `identifyCIA()` bonded with this 'Identify C-I-A classification' button receives and maps each threat scenario to confidentiality, integrity, or availability loss as Listing 1 implements.

The variable `ts` refers to the input threat scenarios, `dicCate` is a dictionary that maps keywords of cyber threats to a kind of loss, which then serves as a filter credential during

```
function identifyCIA(){
    ...
    var ts = inputValue.split(';').map(item => item.trim());
    const dicCate = {
      "Confidentiality": ["Zero-day attack", "Malware", "Ransomware",
      ↪   "MitM(man in the Middle) attack", "Web-based attack","Social
      ↪   Engineering", "Physical attack", "Eavesdropping",
      ↪   "Disinformation", "Insider threat", "Data breaches",
      ↪   "Cyberfraud", "Phishing"],
      "Integrity": ["Web-based attack for modification", "Physical attack
      ↪   for modification", "Insider threat for modification"],
      "Availability": ["DoS attack", "Botnet", "Unavailability",
      ↪   "shutdown"]
    };
    const categorizedResults = {};
    ts.forEach(item => {
        for (const category in dicCate) {
            if (dicCate.hasOwnProperty(category)) {
                const keywords = dicCate[category];
                const foundKeywords = keywords.filter(keyword =>
                ↪   item.toLowerCase().includes(keyword.toLowerCase()));

                if (foundKeywords.length > 0) {
                    categorizedResults[item] = category;
                    break;
                }
            }
        }
    });
    localStorage.setItem('homeData', JSON.stringify(categorizedResults));
}
```

Listing 1: Core Codes of Function identifyCIA()

the iteration of `ts`. The function `includes()` is utilized in the second loop of each key in the `dicCate`, to check if the threat scenario belongs to a certain cyber attack or destroys the data in what way, and the corresponding type of loss is identified and stored in the variable `categorizedResults`. The result is stored in the local storage with the key `homeData`, which allows the page to keep showing the result when reloading it.



Please input threat secenarios, with each item separated by ';'.

threat1;threat2;threat3

Threat Scenario	Threat Category	Inspect
DoS attack on server	Availability	Inspect
insider threat of IT department	Integrity	Inspect
malware	Confidentiality	Inspect

Figure 5.4: Presentation of the Classification Result

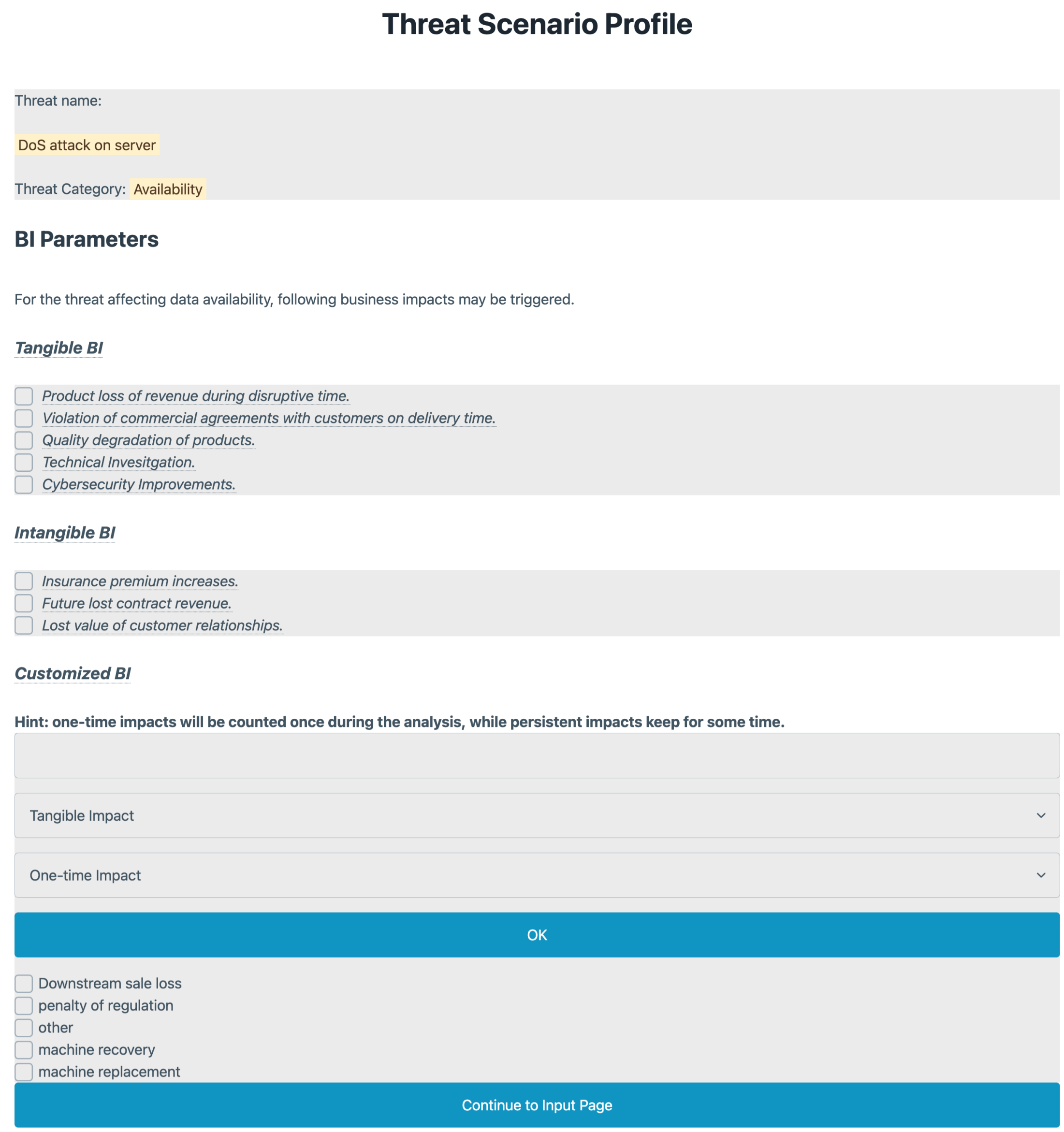
After the identification, the result is presented in a table with an `inspect` button followed in each line (Figure 5.4) with the function `showTable()`. Each `inspect` button is bonded with different interfaces according to the type of information loss. For instance, the first threat scenario 'DoS attack on server' is identified as Availability loss, then its `inspect` button directs users to the page that shows business impacts related to availability loss. In addition, to inform users which threat is being analyzed clearly, the name of the threat scenario is encoded and sent to the next business impact mapping page as well as shown in Listing 2.

```
function showTable(){
    ...
    button.onclick = function (){
        if (category === 'Availability')
        {
          var url = 'availability.html?param'=encodeURIComponent(item);
          window.location.href = url;
        }
        //else if ...
      }
}
```

Listing 2: Implementation of Function `showTable()`

For the threat identified as availability loss, the variable texttturl is defined as the combination of the availability business mapping page and the threat name. How the transferred threat name is used and how the business impact mapping page is generated are discussed in the next section.

5.3 Business Impacts Mapping Page



Threat Scenario Profile

Threat name:

DoS attack on server

Threat Category: Availability

BI Parameters

For the threat affecting data availability, following business impacts may be triggered.

Tangible BI

□ *Product loss of revenue during disruptive time.*
□ *Violation of commercial agreements with customers on delivery time.*
□ *Quality degradation of products.*
□ *Technical Invesitgation.*
□ *Cybersecurity Improvements.*

Intangible BI

□ *Insurance premium increases.*
□ *Future lost contract revenue.*
□ *Lost value of customer relationships.*

Customized BI

Hint: one-time impacts will be counted once during the analysis, while persistent impacts keep for some time.

Tangible Impact

One-time Impact

OK

□ Downstream sale loss
□ penalty of regulation
□ other
□ machine recovery
□ machine replacement

Continue to Input Page

Figure 5.5: Example of Threat Profile Page

In order to conveniently organize the structure of the framework, three interfaces are designed for different types of loss. These pages are named 'Threat Profile', consisting of the threat name received from the home page, C-I-A classification, and applicable business impacts. Business impacts are subdivided into three parts, tangible, intangible, and customized areas. All functions controlling components in these three interfaces are integrated into the `threatProfile.js` file. Figure 5.5 shows an example of the threat

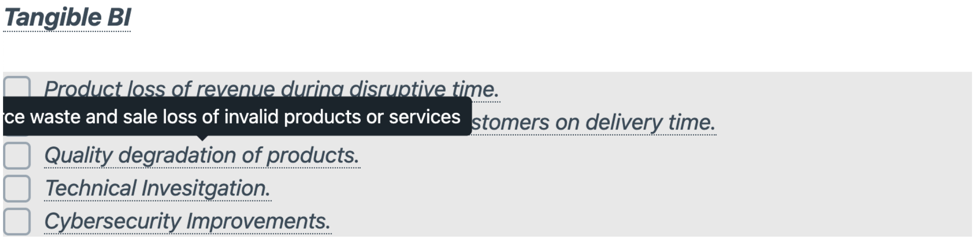
```
function showName(){
    //Display threat name
    var queryString = window.location.search;
    var searchParams = parseQueryString(queryString);
    var name = searchParams['param'];
    var nameContainer = document.getElementById('threatName');
    var threatName = this.document.createElement('mark');
    threatName.textContent = name;
    nameContainer.appendChild(threatName);
}
function parseQueryString(queryString) {
    var params = {};
    var pairs = queryString.substring(1).split('&');

    for (var i = 0; i < pairs.length; i++) {
      var pair = pairs[i].split('=');
      var key = decodeURIComponent(pair[0]);
      var value = decodeURIComponent(pair[1] || '');
      params[key] = value;
    }
    return params;
}
```

Listing 3: Core Codes for Parsing the Threat Name

profile of the threat ’DoS attack on the server’. At the top of the page, its name, as well as the threat category, are displayed with highlights. The threat name transmitted from the last page is decoded and presented in a container, which requires a parsing function (see Listing 3).

In the next section, business impacts relevant to availability loss are displayed in the form of checkboxes. Tangible and intangible impacts are grouped separately in two containers and stored directly in HTML files. Each checkbox is assigned a unique ID, which will be used for later recognition. What’s more, each impact label is decorated with a tooltip, offering users an explanation of what this impact evaluates, in case users have no clue about it. Figure 5.6 presents the appearance of the tooltip use. ’Quality of degradation of products may be hard to estimate, while the hint ’Resource waste and sale loss of invalid products or services’ indicates that users should take the expense of waste and sale loss of invalid products caused by this cyber attack into consideration.

In the *add area* for customized impacts, an input box and two selection boxes for its attribute are provided. Users should choose its tangibility and persistence. After finishing the new business impact definition, users click the `OK` button, and the newly added impact will be shown immediately on the page. The triggered function creates a checkbox and a label with the impact name as its content, and the attribute `id` of the checkbox is defined as the combination of the impact’s name and its two attributes, which will be later extracted for visualization and calculation.



Tangible BI

□ Product loss of revenue during disruptive time.

ce waste and sale loss of invalid products or services stomers on delivery time.

□ Quality degradation of products.

□ Technical Invesitgation.

□ Cybersecurity Improvements.

Figure 5.6: Tooltip Design for Business Impact

At the same time, the inputted impact and its two attributes are stored in the local storage with the key `data` (see Listing 4):

```
function addNewBI(){
    ...
    //Get inputs from the HTML
    var inputField = document.getElementById('BIInput');
    var inputValue = inputField.value.trim();
    var timeselectValue = document.getElementById('timeAttribute');
    var timeselectData = timeselectValue.value;
    var tanselectValue = document.getElementById('tanAttribute');
    var tanselectData = tanselectValue.value;
    var data = {
        input: inputValue,
        attribute: [timeselectData,tanselectData]
        };
    var storedData = localStorage.getItem('data');
    if (storedData!==null){
        storedData = JSON.parse(storedData);
    }
    else{
        storedData = [];
    }
    storedData.push(data);
    localStorage.setItem('data', JSON.stringify(storedData));
}
```

Listing 4: Core Codes of Function `addNewBI()`

Furthermore, in Listing 5 another function `showNewBI()` is implemented to present the new customized business impact that has just been added, so that in the function `getSelectedLabels()` it can be captured and transmitted to the next page by the id of its checkbox. The `filter()` function identifies this impact from stored data to get its attributes, and the id is defined as the combination of the impact name and two attributes.

To transmit chosen business impacts to the next input page, another function `getSelctedLabels()` is implemented. The function presented in Listing 6 queries all containers

```javascript
function showNewBI(){
    ...
    var storedData = JSON.parse(localStorage.getItem('data'));
    var contentArray = storedData.split('\n');
    contentArray.forEach(function(content) {
        if (content) {
            var checkbox = document.createElement('input');
            var filteredElements = storedData.filter(item => item.input === content);
            var att = filteredElements[0]['attribute'];
            checkbox.id = content+att[0]+att[1];
            contentContainer.appendChild(checkbox);
            ...
            }
        });
}
```

Listing 5: Core Codes of Function `showNewBI()`

on this page to collect selected checkboxes, and an array `selectedBI` is created to store them in the form of a dictionary. This variable is then stored in the local storage with the key `selectedCheckboxes`. On this page, except for the function `addNewBI()` which is triggered by the button, all other functions are executed once the page is loaded.

5.4 Input Page for Business Impacts Details Design and Implementation

The input page displays all required inputs to calculate and visualize chosen business impacts, including the currency used, MTPD of each threat, and estimated loss of each selected business impact. Particularly, business impacts here are re-classified as persistent or one-time. For one-time impacts, they are displayed as a label, and an input box is followed. For persistent impacts, an input box and a table are attached. Users are asked to input the loss per time unit, and estimated recovery progress. For the two extreme cases of complete recovery and no recovery at all, users should input 0 for no recovery at all, and 1 for complete recovery. For instance, the user chooses impact 'Technical Investigation, 'Product loss of revenue during the disruptive time', and 'Future lost contract revenue'. The technical investigation is defined as a one-time impact, therefore it is shown in the container `One-time BI Parameters`. Product loss during the disruptive time and future lost contract revenue are categorized as persistent impacts, and shown in the `Persistent BI Parameters` group. For the recovery progress, a table is initialized, and users may click the `Add row` button to input more details.

In the last step, all selected impacts are stored in the local storage. The function `showSelectedBI()` in the `input.js` file reads this data and re-classifies impacts once the page

```
function getSelectedLabels() {
    var selectedBI = [];
    var containers = document.querySelectorAll('.cont');
    containers.forEach(container =>{
        var checkboxes =
         ↪  container.querySelectorAll('input[type="checkbox"]:checked');
        checkboxes.forEach(function(checkbox) {
            var label = checkbox.nextElementSibling.textContent;
            var id = checkbox.id;
            dic = {label: label, id: id};
            selectedBI.push(dic);
        });
    });
    localStorage.setItem('selectedCheckboxes',
     ↪  JSON.stringify(selectedLabels));
}
```

Listing 6: Core Codes of Function `getSelctedLabels()`

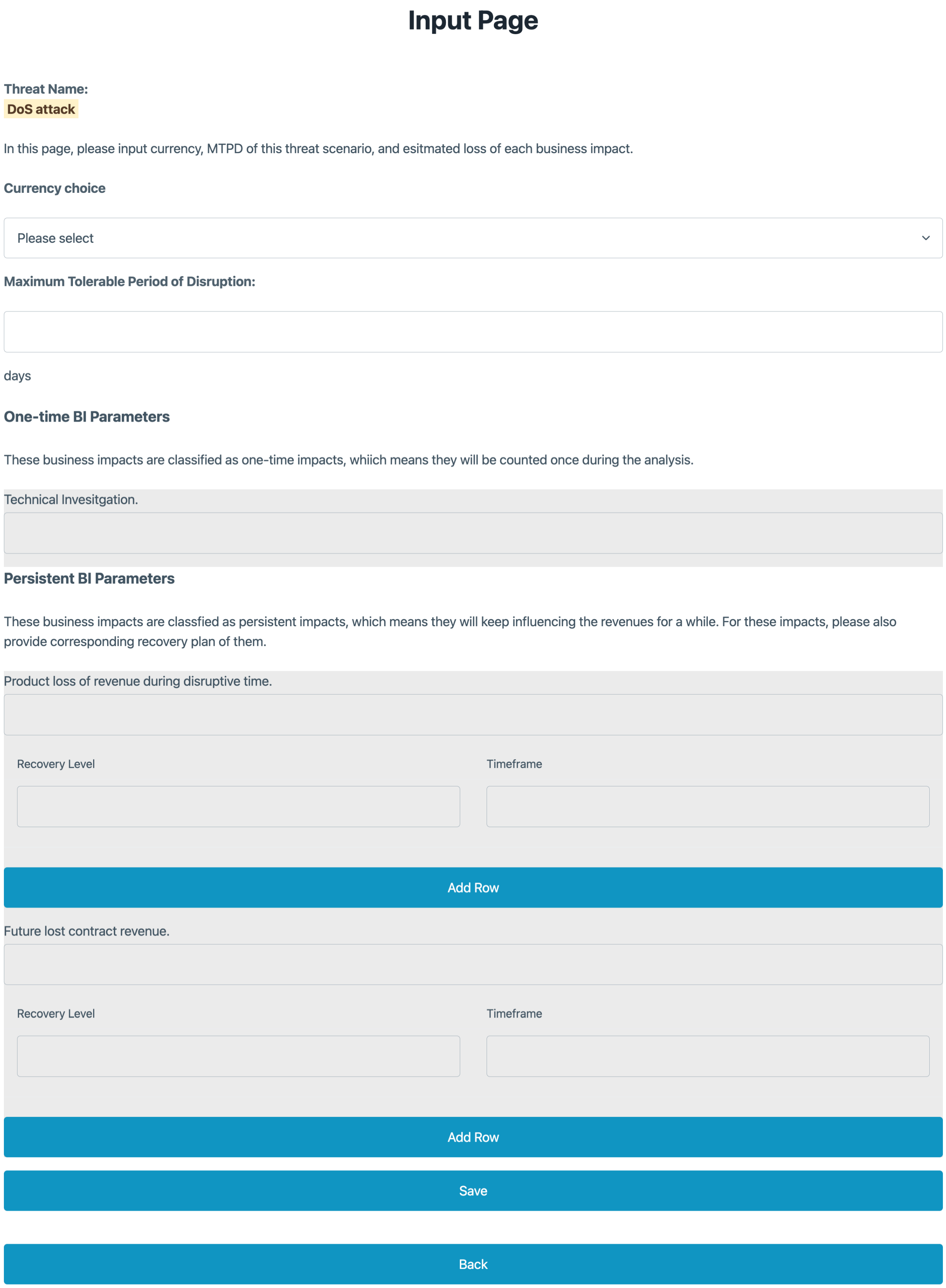
is loaded (see Listing 7). As all impacts are stored with their unique IDs, the function checks each of them. For newly added impacts, as its id is a combination of its name and two attributes, the `include()` method is called to check if it is persistent.

In this function, variables `labelElement`, `inputElement`, and `tableElement` refer to the impact text, matching input box, and matching recovery table. Especially, these three elements are assigned an attribute `classList` as `dynamic-label`, `dynamic-input`, and `dynamic-table`, which serve as an identifier for later data collection. For persistent impacts, the label, input box, and table are appended successively. For one-time impacts, only the label and input box are added.

After inputting all required data, users should click the `Save` button to store it in the local storage. A pop-up window will appear to inform users of the operation's success. The `save()` function collects all inputted data and combines it into a dictionary as Listing 8 shows.

The threat name is stored with the key `id`. The currency is stored as a string with the key `currency`, and the MTPD is stored directly as a number for prioritization. The variable `onetimeBI`, defined as a dictionary, contains all one-time business impacts with the impact name as its key, and inputted data as its value. The variable `persistent BI` stores all persistent impacts and relevant data in a dictionary as well. For each persistent impact, the corresponding value is another dictionary, which consists of the loss per time unit and the recovery progress. The overall data is saved in the local storage with the threat name as its key.

At the bottom of the page, a `Back` button is set to instruct users to get back to the home page and continue inspecting other threat scenarios.



Input Page

Threat Name:

DoS attack

In this page, please input currency, MTPD of this threat scenario, and esitmated loss of each business impact.

Currency choice

Please select

Maximum Tolerable Period of Disruption:

days

One-time BI Parameters

These business impacts are classified as one-time impacts, whiich means they will be counted once during the analysis.

Technical Invesitgation.

Persistent BI Parameters

These business impacts are classfied as persistent impacts, which means they will keep influencing the revenues for a while. For these impacts, please also provide corresponding recovery plan of them.

Product loss of revenue during disruptive time.

Recovery Level

Timeframe

Future lost contract revenue.

Recovery Level

Timeframe

Figure 5.7: Example of the Input Page

```
function showSelectedBI() {
    ...
    var selectedBI =
     ↪  JSON.parse(localStorage.getItem('selectedCheckboxes'));
    var labelElement = document.createElement('label');
    labelElement.textContent = checkbox.label;
    labelElement.classList.add('dynamic-label');

    var inputElement = document.createElement('input');
    inputElement.type = 'text';
    inputElement.classList.add('dynamic-input');

    var tableElement = document.createElement('table');
    tableElement.classList.add('dynamic-table');
    if (checkbox.id === 'qualDeg' || checkbox.id === 'lc' || checkbox.id
     ↪  === 'lr' || checkbox.id == 'lostSale' ||
     ↪  checkbox.id.includes('per')) {
        persistentContainer.appendChild(labelElement);
        persistentContainer.appendChild(inputElement);
        persistentContainer.appendChild(tableElement);
        persistentContainer.appendChild(document.createElement('br'));
    else{
        persistentContainer.appendChild(labelElement);
        persistentContainer.appendChild(inputElement);
    }
}
```

Listing 7: Core Codes of Function `showSelectedBI()`

5.5 Loss Calculation and Visualization

After finishing all threat scenario inspections, users are guided back to the home page. Below the inspection table, there is an `Analyze` button, which is bonded with the function `Analyze()`. This function implements the following four tasks: loss calculation of each threat, loss and emergency prioritization of all threat scenarios, the loss trend over time, and overall tangible and intangible impact loss calculation.

The loss calculation of each threat scenario is implemented in the `eachThreat()` function (shown as Listing 9), which is called in the `Analyze()` function in the threat scenario iteration. It first extracts data from the local storage with the threat's name, and assigns its currency, MTPD, and each business impact loss to corresponding variables.

Variable `persistentSum` represents all persistent business impact losses. It is initialized as 0 and increased with the iteration of persistent business impacts. The variables `recovery`, `days`, and `pBIvalue`, defined as three arrays, store the recovery table and inputted loss of each persistent impact respectively. The variable `totalLoss` counts the overall loss of

```
function save() {
    var onetimeBI = onetimeBIContainer.querySelectorAll('.dynamic-input');
    var onetimeBIlabels =
     ↪  onetimeBIContainer.querySelectorAll('.dynamic-label');
    var persistentBI =
     ↪  persistentBIContainer.querySelectorAll('.dynamic-input');
    var persistentBIlabels =
     ↪  persistentBIContainer.querySelectorAll('.dynamic-label');
    var persistentBItable =
     ↪  persistentBIContainer.querySelectorAll('.dynamic-table');
    ...
    // combine all inputs
    var inputData = {
        id: name,
        currency: currency,
        MTPD: MTPD,
        onetimeBI: onetimeBIValue,
        persistentBI: persistentBIValue,
    };
    localStorage.setItem(name, JSON.stringify(inputData));
}
```

Listing 8: Core Codes for Saving Inputs

this threat scenario, which will also be called later to sum the loss of one-time business impacts. `pBIRealvalue` is also defined as an array to store the loss of each persistent impact, which is designed for the visualization of the threat scenario composition. This part is implemented based on the formula (4.1), within each recovery stage the persistent loss increases by the multiplication of loss per time unit, 1-recovery level, and the time frame.

The one-time loss is directly added to the variable `totalLoss` (see Listing 10). It is worth noting that all business impact loss-related data is inputted and stored as a string, and the function `Number()` is called to convert the string to a number.

After both persistent and one-time impacts are processed, these two types are integrated for visualization. As Figure 5.8 shows, the threat scenario 'Malware' will cause three business impacts: theft of IP, technical investigation, and increased cost to raise debt. The pie chart depicts them with their corresponding loss.

For the task of prioritization threats, as the total loss of each threat is calculated, and its MTPD is retrieved from the local storage, these two variables are returned to the main function `Analyze()` and added to the arrays storing all threats' overall loss and MTPDs as Listing 11.

The loss-based prioritization chart lists threat scenarios with their loss descending, while the MTPD-based chart prioritizes threats with their MTPD time ascending, indicating

```
function eachThreat(){
    ...
    // Calculate the first part of the formula, persistent impacts: (((BI_persistent, * (1 - recovery) * days)))
    let persistentSum = 0;

    for (let t = 0; t < days.length; t++) {
        persistentSum += pBIvalue * (1 - recovery[t]) * days[t];
    }
    totalLoss += persistentSum;
    console.log(persistentSum);
    pBIRealvalue.push(persistentSum);
  }
```

Listing 9: Core Codes for the Calculation of Persistent Impacts

```
function eachThreat(){
    ...
    // Calculate the second part of the formula, one-time impacts
    let persistentSum = 0;
    for (let j = 0; j < BIvalue.length; j++) {
        //console.log(BIvalue[j]);
        v = Number(BIvalue[j]);//convert str to int
        totalLoss += v;
    }
}
```

Listing 10: Core Codes for the Calculation of One-time Impacts

that the first threat could be the most emergent one to address. These two prioritization lists provide users with different analysis views of threats, allowing users to get insights from both sides and take more reasonable measures (shown in Figure 5.9).

Meanwhile, the loss over time is also calculated in the `forThreat()` function as Listng 12. First, when iterating persistent impacts, the variable `rDays` stores the whole time frame the recovery table covers, and the variable `lossValues` is initialized as an array with the time frame as its length to store the loss per time unit. The `currentDay` works as an index to store the matching persistent loss. After finishing the iteration of each line of the recovery table of the current impact, the `lossValues` is pushed as an element into the array `date_loss`, which is initialized outside the loop to store the loss of all persistent impacts over time.

The variable `date_loss` consists of multiple arrays with different lengths, indicating that each impact may take different periods to restore. To unify this array for visualizing the loss trend over time of this threat scenario, the longest period of recovery should be first identified. Then a new array equaling the longest period is defined to store all loss from

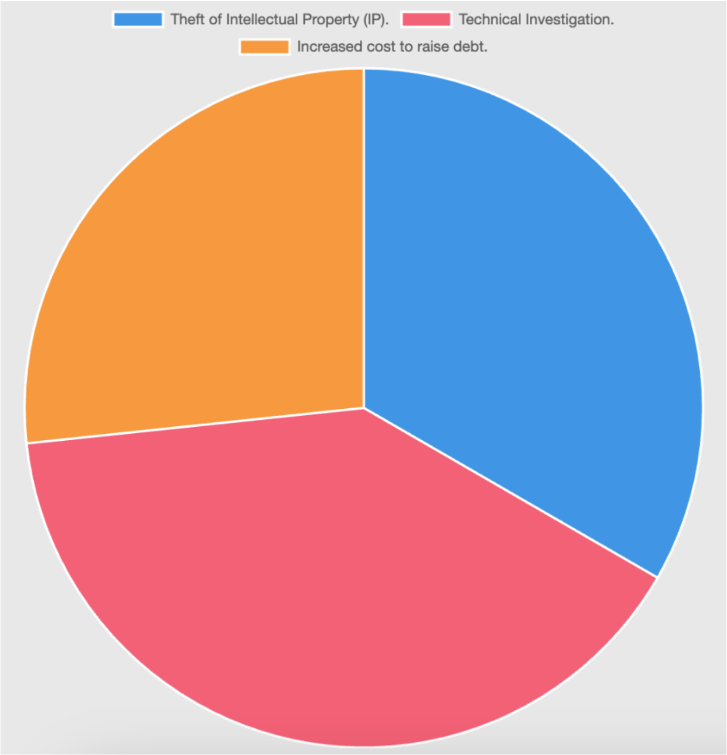


Figure 5.8: The Impact Composition of Threat 'Malware'

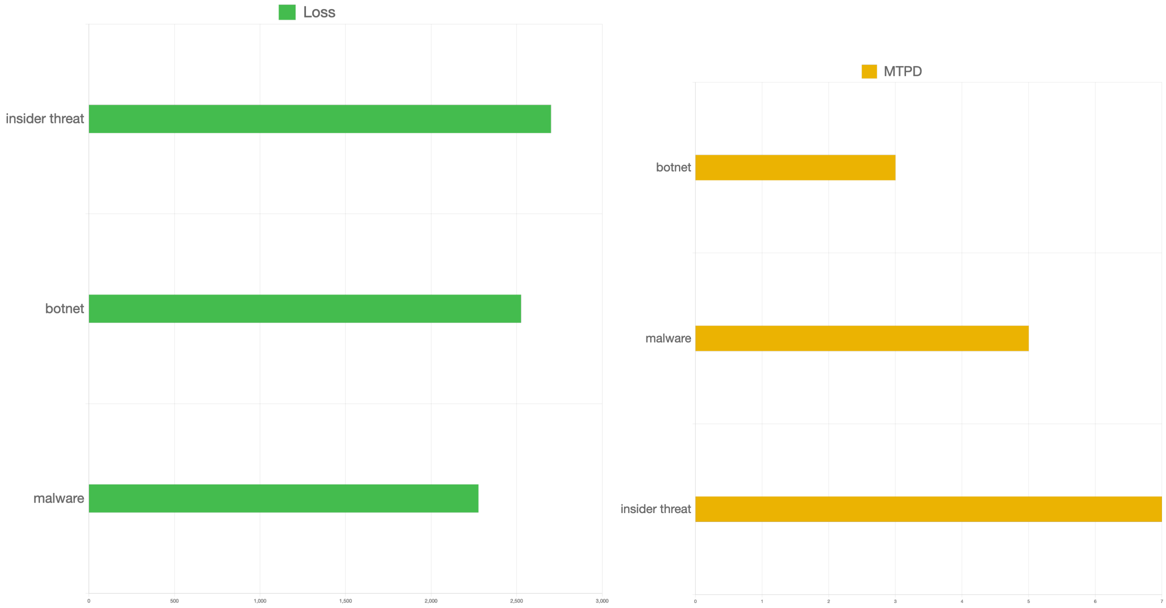


Figure 5.9: Threat Prioritization by Loss and Emergency

```
function eachThreat(){
    ...
    pBIName.forEach((element) => {
        BIlabel.push(element);
    });
    pBIRealvalue.forEach((element) => {
        BIvalue.push(element);
    });
}
```

Listing 11: Core Codes for Integrating Persistent and One-time Impacts

different persistent impacts on the same time unit during the iteration of the `date_loss`, as Listing 13 shows.

The variable `result` is returned to the main function `Analyze()`. Before starting the iteration of each threat scenario in `Analyze()`, a dictionary `dayLoss` is initialized to collect each threat's loss trend over time with the threat name as its key.

Similarly, in the main function `Analyze()`, first the longest recovery period among threats is identified and a dictionary of this length is initialized. This variable then records each threat name as its key and the loss trend array as its matching value. For the shorter threat, the rest time unit is mapped with the value 0. For instance, after the iteration of these three threat scenarios, 'insider threat' and 'botnet' lead to several persistent business impacts each, and loss trends over time in the line chart with different colors (see Figure 5.10).

For the overall tangible and intangible impacts visualization, total tangible and intangible impact losses are collected in the evaluation of each threat (see Listing 14).

For those pre-defined impacts displayed on the threat scenario page, the variable `intangible_keyword` collects keywords of all intangible impacts, and the function `includes()` is to check if the current impact name belongs to intangible impacts. For new business impacts users define, as they are stored with their chosen attributes in the local storage before, the stored data is extracted and the `filter()` function is called to get its attribute. According to the data format, if the second attribute is 'tan', this impact is defined as tangible, and added to the variable `tangibleBI`, otherwise it is added to the variable `intangibleBI`.

These two variables are also returned to the function `Analyze()` and all tangible losses and intangible losses are summed up for visualization.

As Figure 5.11 shows, the respective proportions are shown in the pie chart, and when the mouse hovers over each element, a tooltip will display the specific loss amount of tangible or intangible impact losses. For users who need an estimation of the tangible and intangible impacts proportion, this chart can help users immediately have some insights.

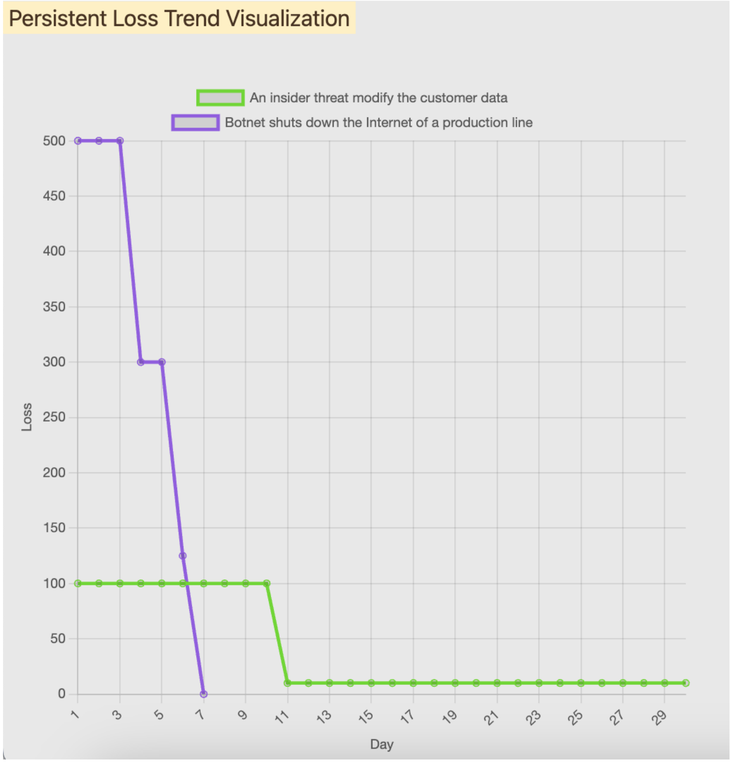


Figure 5.10: The Visualization of Impact Loss Trend over Time

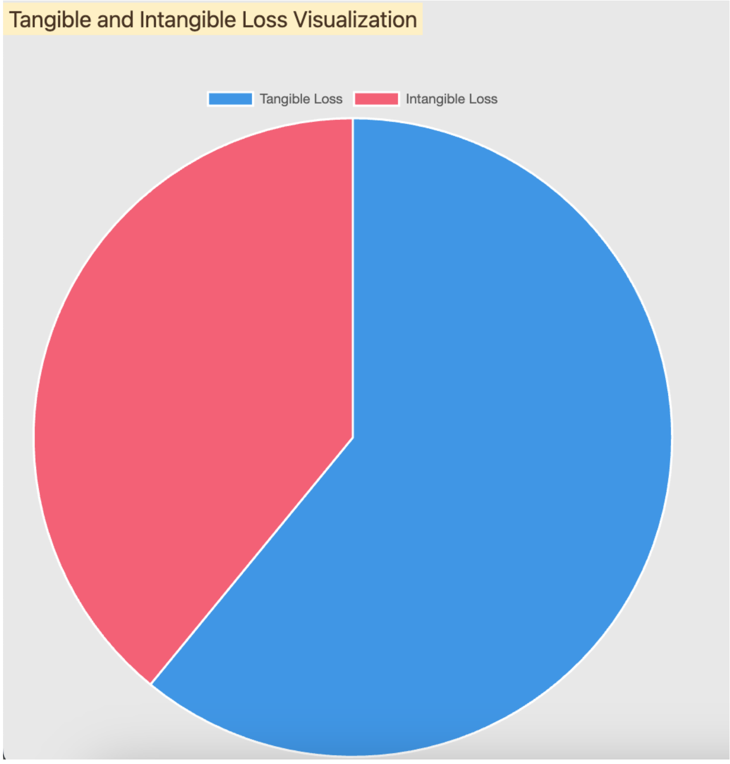


Figure 5.11: The Visualization of Tangible and Intangible Impact Loss Proportion

```
function eachThreat()
{
    ...
    //Calculate everyday loss for line chart
    var date_loss  = [];
    for (var key in persistentBI){
        if (persistentBI.hasOwnProperty(key)){
            var rDays = days.reduce((accumulator, currentValue) =>
             ↪  accumulator + currentValue, 0);
            var lossValues = new Array(rDays).fill(0);
            let currentDay = 0;
            rp.forEach(({ column1, column2 }) => {
                for (let day = 1; day <= column2; day++) {
                    lossValues[currentDay] = (1-column1)*pBIvalue;
                    currentDay++;
                }
            });
            date_loss.push(lossValues);
        }
    }
}
```

Listing 12: Core Codes for the Calculation of Everyday's Loss

```
function eachThreat()
{
    if (date_loss.length!==0){
        var maxLength = Math.max(...date_loss.map(array =>
         ↪  array.length));
        var result = new Array(maxLength).fill(0);
        for (let i = 0; i < maxLength; i++) {
            for (const array of date_loss) {
                if (array[i] !== undefined) {
                    result[i] += array[i];
                }
            }
        }
    }
}
```

Listing 13: Core Codes for the Loss Trend Visualization

```
function eachThreat()
{
    ...
    intangible_keyword = ["debt", "relationships", "contract",
     ↪  "premium"];
    intangibleBI = 0;
    tangibleBI = 0;
    var storedData = localStorage.getItem('data');
    storedData = JSON.parse(storedData);
    for (var i=0; i<BIlabel.length; i++){
        var filteredElements = storedData.filter(item => item.input ===
         ↪  BIlabel[i]);
        if (intangible_keyword.some(keyword =>
         ↪  BIlabel[i].includes(keyword))){
          intangibleBI+= JSON.parse(BIvalue[i]);
        }
        else if (filteredElements.length !== 0){
            attribute = filteredElements[0]['attribute'];
            if(attribute [1] === 'tan'){
                tangibleBI+= JSON.parse(BIvalue[i]);
            }
            else{
                intangibleBI+= JSON.parse(BIvalue[i]);
            }
        }
        else{
            tangibleBI += JSON.parse(BIvalue[i]);
        }
    }
}
```

Listing 14: Core Codes for the Overall Tangible and Intangible Impacts Visualization

Chapter 6

Evaluation

Due to the fact that there is no available ground-truth data to evaluate the accuracy of the framework, a full quantitative evaluation is not feasible. Therefore, in the evaluation stage, the usability and effectiveness of this framework are mainly tested with the usage scenario and focus group evaluation. Particularly, the usage scenario demonstrates the effectiveness of this framework with a hypothetical scenario, and the focus group pays attention to both usability and effectiveness by involving a group of target users.

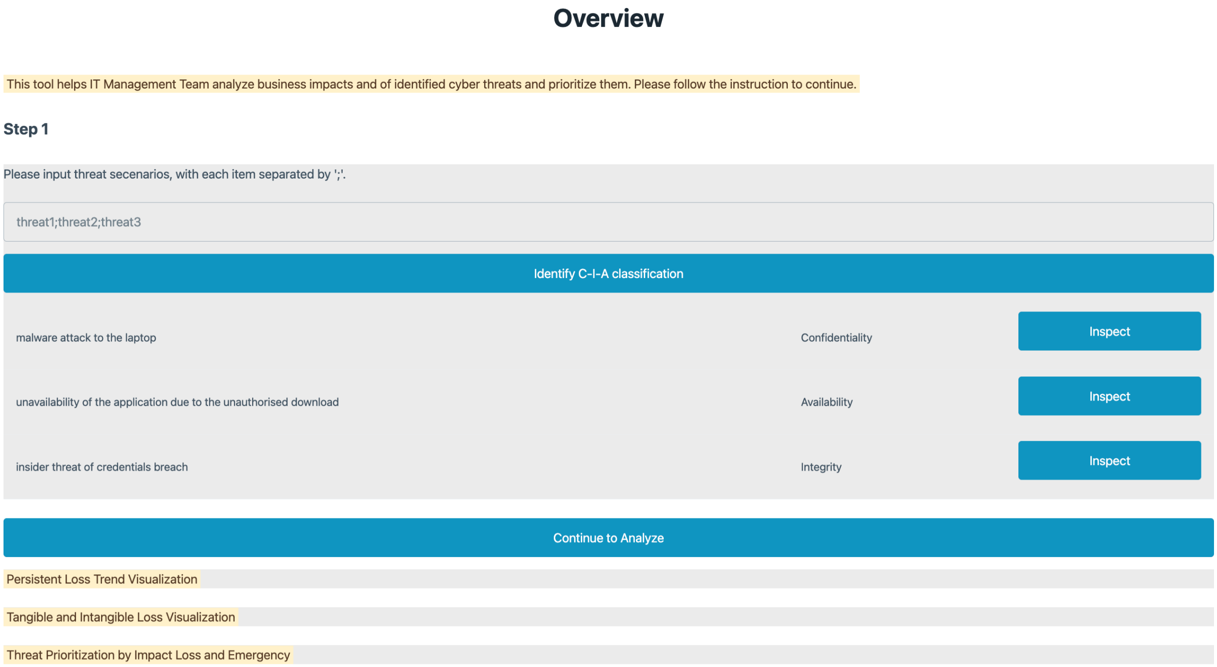
6.1 Usage Scenario

The Usage scenario method depicts a practical scenario which a specific user or a persona may encounter. By the real interactions between the system and the persona, usage scenarios can help designers comprehend users' pragmatic requirements and actions.

For the evaluation of this framework, the usage scenario is deployed from a Deloitte report about business impacts of cyberattacks [58]. In this hypothetical scenario, the user Mary works as an IT consultant in a technical consulting company, and recently took over a cyber threat case for a US health insurer. This company utilizes a patient care application that offers medical notifications and enables healthcare professionals within its network of providers to access patient records and information about insurance coverage. It is regulated by both state and federal authorities and pays $7 million annual premium for a $100 million cyber insurance policy. The task for Mary is to cooperate with the insurer company to evaluate the economic loss of these incidents and provide recovery insights for follow-up measures as soon as possible.

In the past week, the insurer company has experienced the following cyber threats successively in a short time. In May, the company learned that a laptop containing 2.8 million of its personal health information (PHI) records had been attacked by a virus. Five days later, they detected that an additional one million patient records had been downloaded from the application database and were unable to confirm it was for authorized use. As a result, the company immediately shut down physician's access to the patient care application for two weeks tentatively, during which period the coverage and claims validation between the company and its physicians and providers had to be done manually. Meanwhile, there was a notable rise in the number of newly registered user accounts that were in active use. After a rough technical investigation, it turned out that one staff's privileged credentials to the database had also been stolen.

After learning about the general situation, Mary forms a cyber incident response team with an IT expert, a business manager, a staff from the marketing department, and a lawyer from the law firm working with this company. This team analyzes the situation and extracts three main threat scenarios: malware attack on the laptop, unavailability of the application due to the unauthorized download, and an insider threat of credentials breach. Mary inputs the threat scenario list into the framework and gets the classification table (see Figure 6.1):



Overview

This tool helps IT Management Team analyze business impacts and of identified cyber threats and prioritize them. Please follow the instruction to continue.

Step 1

Please input threat secenarios, with each item separated by ';'.

threat1;threat2;threat3

malware attack to the laptop	Confidentiality	Inspect
unavailability of the application due to the unauthorised download	Availability	Inspect
insider threat of credentials breach	Integrity	Inspect

Identify C-I-A classification
Continue to Analyze
Persistent Loss Trend Visualization
Tangible and Intangible Loss Visualization
Threat Prioritization by Impact Loss and Emergency

Figure 6.1: Home Page After Getting and Analyzing the Threat Scenarios

Each threat scenario now is classified as a type of information loss, and the 'inspect' button will guide Mary to different pages with different applicable business impacts. Based on the discussion with the response team and the suggested impacts provided by the framework, Mary finally obtains three tables of business impacts for each cyber attack, which can be seen in Tables 6.1, 6.2, and 6.3.

Business Impact	***Tangibility***	***Persistence***	***Cost(in millions)***
Customer breach notification	Tangible	One-time	10.00
Post-breach customer protection	Tangible	One-time	21.00
Public relation	Tangible	One-time	1.00
Increased cost to raise debt	Intangible	Persistent	10.00(per year)
Insurance premium increases	Intangible	One-time	30.00
Regulatory compliance (HIPAA fines)	Tangible	One-time	2.00

Table 6.1: Business Impacts of the 'malware attack on the laptop'

Business Impact	***Tangibility***	***Persistence***	***Cost(in millions)***
Human labor costs during shutdown	Tangible	Persistent	0.30(per day)
Future lost contract revenue	Intangible	Persistent	21.00(per year)
Lost value of customer relationships	Intangible	Persistent	16.00(per year)

Table 6.2: Business Impacts of the 'unavailability of the application due to the unauthorized download'

Business Impact	***Tangibility***	***Persistence***	***Cost(in millions)***
Technical Investigation	Tangible	One-time	1.00
Cybersecurity improvements(for upgrading the internal authority security system)	Tangible	One-time	14.00

Table 6.3: Business Impacts of the 'insider threat of credentials breach'

For persistent impacts, recovery details are provided by the lawyer and staff. The recovery level is the ratio of the current level of business to the normal level before the cyber attack, and the term is the timeframe that this unrecovered level persists. For instance, if the production line is totally stopped for 4 days due to the unavailability of product data, then the recovery level should be 0, and the term is 4.

Persistent Impact	***Recovery level***	***Term (year)***
Increased cost to raise debt	0.5	2
	0.7	1
	0.95	1
Human labor costs during shutdown	0.0	0.03
Future lost contract revenue	0.6	1
	0.8	1
	0.99	1
Lost value of customer relationships	0.6	1
	0.95	1

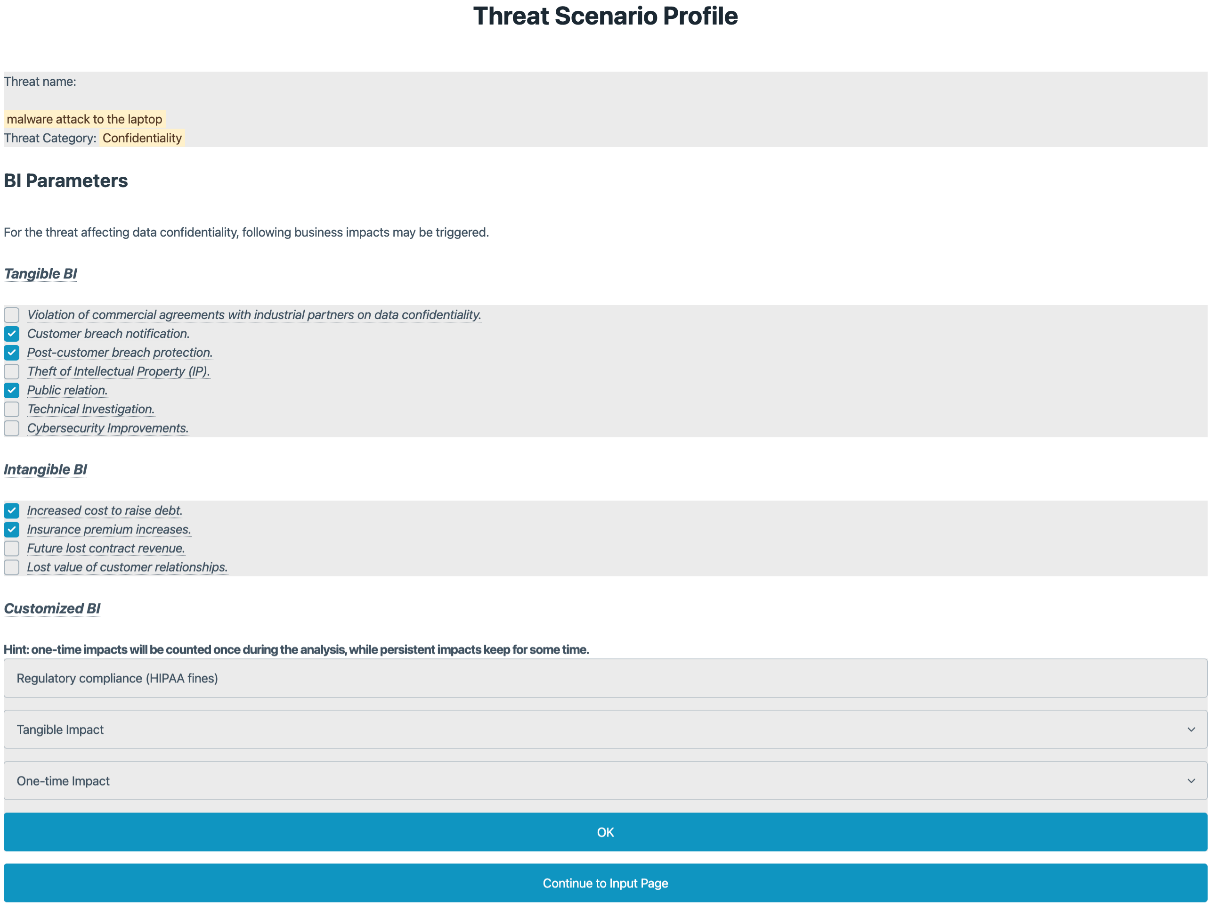
Table 6.4: Recovery Plan for the 'Increased cost to raise debt'

According to the experience of the IT expert, the MTPD of each threat scenario is also acquired in Table 6.5:

Threat	***MTPD (days)***
malware attack on the laptop	20
unavailability of the application due to the unauthorized download	12
insider threat of credentials breach	14

Table 6.5: MTPD of Each Threat Scenario

Then Mary selects all applicable impacts on each threat profile. Especially, for the threat ’malware attack on the laptop’, there is a customized business impact proposed by the lawyer named ’Regulatory compliance (HIPAA fines)’ as this company is regulated by the federal authorities, and the leakage of the customers’ data leads to a Health Insurance Portability and Accountability Act (HIPPA) fine. On the threat file page (see Figure 6.2) of this threat, this business impact is manually added:



Threat Scenario Profile

Threat name:

malware attack to the laptop

Threat Category: Confidentiality

BI Parameters

For the threat affecting data confidentiality, following business impacts may be triggered.

Tangible BI

□ *Violation of commercial agreements with industrial partners on data confidentiality.*
☑ *Customer breach notification.*
☑ *Post-customer breach protection.*
□ *Theft of Intellectual Property (IP).*
☑ *Public relation.*
□ *Technical Investigation.*
□ *Cybersecurity Improvements.*

Intangible BI

☑ *Increased cost to raise debt.*
☑ *Insurance premium increases.*
□ *Future lost contract revenue.*
□ *Lost value of customer relationships.*

Customized BI

Hint: one-time impacts will be counted once during the analysis, while persistent impacts keep for some time.

Regulatory compliance (HIPAA fines)

Tangible Impact

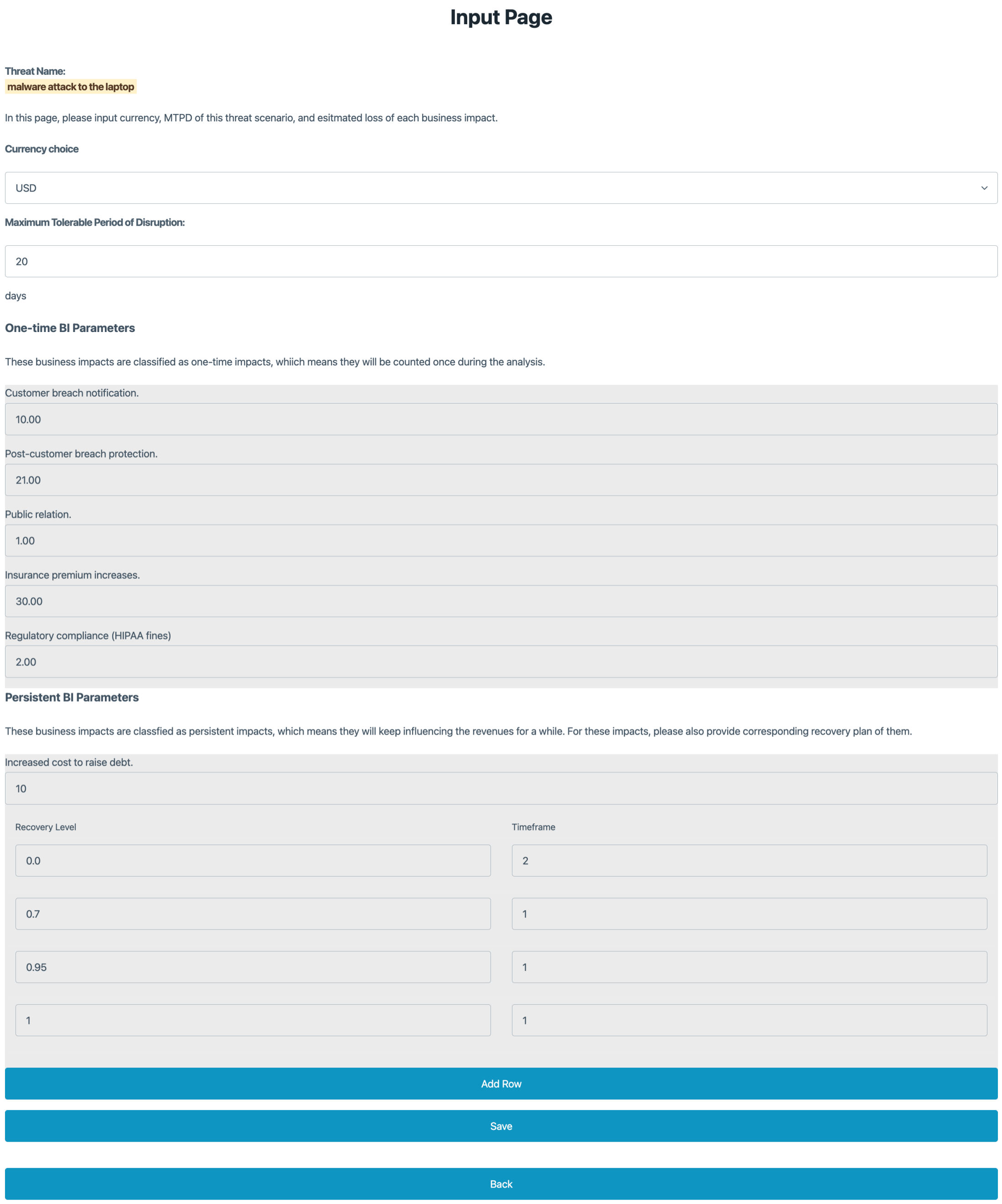
One-time Impact

Figure 6.2: Threat Profile Page of the Threat ’malware attack on the laptop’

The button ’Continue to Input Page’ directs Mary to the input page, and on this page (see Figure 6.3), business impacts are automatically re-classified into one-time and persistent ones, which appear in different parts of the page and allow Mary to input above data. Moreover, after finishing all inputs, Mary clicks the ’save’ button and sees the ’Saved!’ alerts, which confirms that all her input is stored and she can click the ’Back’ button to get back to the home page for the next threat inspection.

The remaining two threat inspections work similarly, which is not elaborated on further. Mary then clicks on the button ’Continue to Analyze’ at the bottom of the home page, and Figure 6.4 is what she gets:

From the visualization result, Mary soon gets the information that the malware attack leads to the most economic loss among these threat threats, while the application shutdown is the most urgent one. What’s more, the intangible loss takes up more than the



Input Page

Threat Name:
malware attack to the laptop

In this page, please input currency, MTPD of this threat scenario, and esitmated loss of each business impact.

Currency choice

USD

Maximum Tolerable Period of Disruption:

20

days

One-time BI Parameters

These business impacts are classified as one-time impacts, whiich means they will be counted once during the analysis.

Customer breach notification.

10.00

Post-customer breach protection.

21.00

Public relation.

1.00

Insurance premium increases.

30.00

Regulatory compliance (HIPAA fines)

2.00

Persistent BI Parameters

These business impacts are classfied as persistent impacts, which means they will keep influencing the revenues for a while. For these impacts, please also provide corresponding recovery plan of them.

Increased cost to raise debt.

10

Recovery Level	Timeframe
0.0	2
0.7	1
0.95	1
1	1

Figure 6.3: Input Page of the Threat ’malware attack on the laptop’

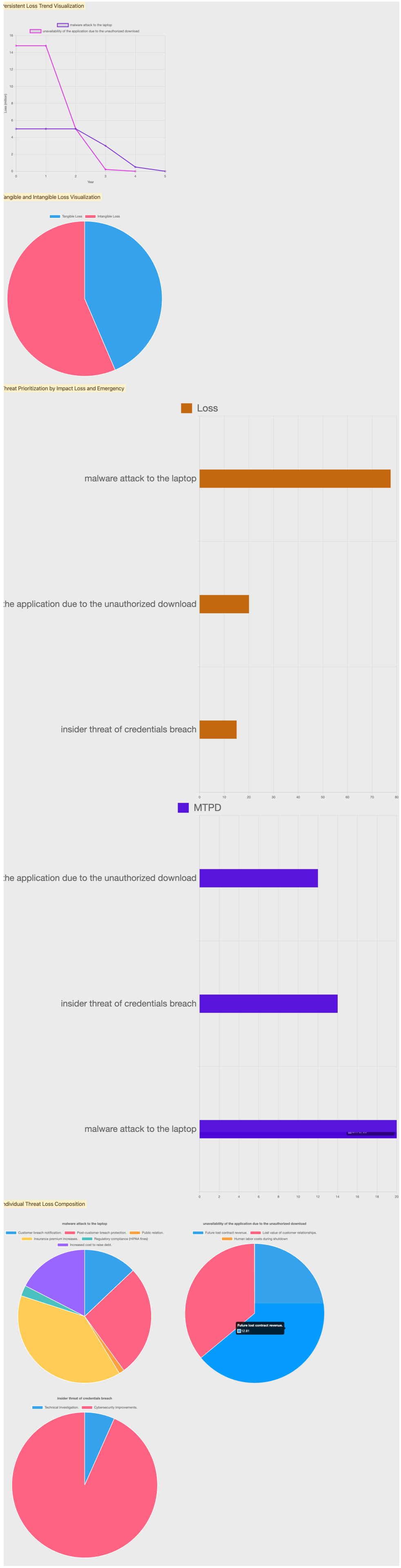


Figure 6.4: Visualization Result of the Usage Scenario

tangible one, indicating that the insurer company should invest more in these intangible impacts. The persistent impact loss trend suggests that these threats will keep affecting the company's economic situation in the next five years. If the manager or other experts want to figure out the specific composition and share of business impacts of each threat, they can view the section 'Individual Threat Loss Composition' and gain more insights.

6.2 Focus Group Evaluation

Focus group is a qualitative research method that involves a group of people to discuss insights based on their personal experiences regarding the subject under investigation [59]. It is an effective tool to collect comprehensive insights about the strengths, drawbacks, and potential improvements of the framework from different participants. In this thesis, a focus group discussion is deployed to evaluate the effectiveness and usability of the proposed framework. Through the view of the focus group, this section illustrates the design and discussion of the focus group discussion on the framework.

6.2.1 Methodology

In this section, the setting of the focus group is elaborated, including how the discussion is organized, the participants' details, and what analysis method is applied to draw findings from the discussion.

Design

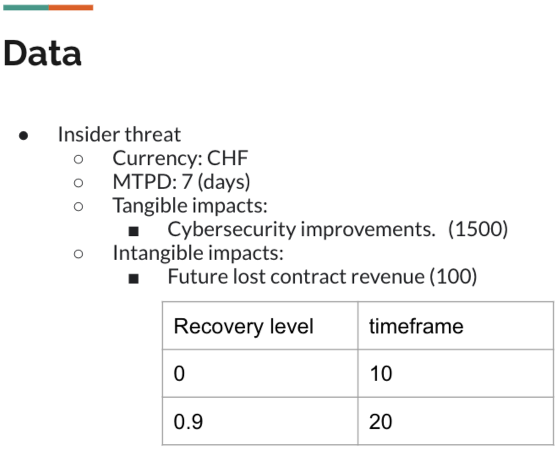
The focus group discussion is designed to take place within a small group of about 4–5 people through a recorded online meeting. The evaluated framework is the prototype implemented, as Chapter 5 demonstrates. Participant recruitment should be finished 1–2 days before the discussion, and participants do not have to do extra work before and after the discussion.

Before the discussion, a brief introduction is also prepared for participants to help them quickly learn the topic and the framework. The introduction consists of the following sections: **a)** an overview of the workflow and design purpose of the framework, **b)** background knowledge including general cyber threats, the concept of BIA, meaning of MTPD, and business impacts categorization by tangibility and persistence, **c)** agenda of the discussion, **d)** the specific task participants will be requested to finish with the framework, **e)** a questionnaire containing the System Usability Scale (SUS) and an open question for the suggestion.

The discussion begins with an introduction to the framework, followed by the hypothetical scenario and data elaboration, and task distribution:

> ”Assume that you are a risk manager of a US technology manufacturer company, and the situation is that three cyber attacks happened in the past weekend:
>
> - A malware invaded the main server of the core product;
> - An insider threat modified the customer data;
> - Botnet shut down the Internet of a production line.
>
> You are required to analyze the business impacts of these threats and prioritize them to plan the next step.”

The hypothetical data is provided as Figure 6.5 shows. It is made up mainly to test usability rather than to get close to the actual situation. Impacts of different threat scenarios cover different situations, which requested participants to use every function of the prototype to have a thorough evaluation. The expected time for participants to complete the task is 15 minutes, but it should be carried out without time limits for participants, and they are allowed to ask for instructions freely.



Data

- Insider threat
  - Currency: CHF
  - MTPD: 7 (days)
  - Tangible impacts:
    - Cybersecurity improvements. (1500)
  - Intangible impacts:
    - Future lost contract revenue (100)

Recovery level	timeframe
0	10
0.9	20

Figure 6.5: Example of Hypothetical Data for Focus Group Discussion

After all participants finish their tasks, they should answer the following questions based on the visualization result they get:

Q1 When choosing the business impacts, do you have an idea of what it evaluates?

Q2 Which threat costs the most to address, and which is most emergent?

Q3 At what time does the loss caused by the malware threat drop sharply?

Q4 Do you have an estimation of tangible and intangible impacts proportion?

Q5 Which threat costs the most to address? And which threat is most emergent?

Q6 Do you have a clear picture of the business impact composition caused by the insider threat?

These six questions are designed to test the effectiveness of the prototype. Each question corresponds to one of the main functions implemented by the prototype, and if participants can give the answer quickly and correctly, it can be recognized that critical functions have a high degree of validity.

At the end of the discussion, participants are asked to finish a questionnaire for a wrap-up evaluation. This questionnaire contains the SUS with 10 questions, one additional ranking question for the effectiveness:

> **Q7** Do you think this product will help analyze the business impact of cyber threats? To what extent? Rank it from 1-5, 1 for hardly useful, and 5 for very useful.

and one open question of suggestions for a better user experience. Among them, the SUS and the open question are designed for usability testing. The SUS is a 'quick and dirty' usability scale that can be used for global assessments of systems usability [60]. As it is easy to get on and low-cost while not losing reliability, the SUS is suitable to be applied here for a systematic evaluation. It consists of a 10-item questionnaire with five response options for users, from Strongly agree, represented by 1, to Strongly disagree, represented by 5.

S1 I think that I would like to use this system frequently.

S2 I found the system unnecessarily complex.

S3 I thought the system was easy to use.

S4 I think that I would need the support of a technical person to be able to use this system.

S5 I found the various functions in this system were well integrated.

S6 I thought there was too much inconsistency in this system.

S7 I would imagine that most people would learn to use this system very quickly.

S8 I found the system very cumbersome to use.

S9 I felt very confident using the system.

S10 I needed to learn a lot of things before I could get going with this system.

Participants submit answers to Q7, SUS, and suggestions with Google Forms. All qualitative and textual results, including answers to Q1-Q7, notes taken during the discussion, SUS results, suggestions, and transcription of the recorded meeting, are collected for usability and effectiveness analysis.

Participants

Participants were recruited by a simple questionnaire within a small scope among students. The recruitment questionnaire includes the following three questions:

- Do you have basic knowledge of information security or cyber security?
- Do you have a basic knowledge of business impact analysis or business continuity management?
- Do you have some experience in testing prototypes or new products?

Among these questions, the first question is a necessary condition for selecting participants as the whole framework is constructed under cybersecurity. The remaining two questions test whether participants have a richer background of knowledge. Participants are good to have BIA or prototype evaluation knowledge – but it is not necessary. In total, 14 people submitted the questionnaire, and 5 people met the criteria for recruiting participants. Table 6.6 shows the critical information about them.

Participant	***Background***	***BIA Knowledge***	***Prototype Evaluation Experience***
1	master student	No	Yes
2	junior software developer	No	Yes
3	master student	No	No
4	master student	No	No
5	financial practitioner	Yes	No

Table 6.6: Brief Introduction of Participants

Among the selected participants, one of them learned about BCM during the course of her studying for a master's degree in finance, and two of them have webpage evaluation experience from their work or academic project experience. All of them command cybersecurity knowledge at different levels, which is suitable to have them as potential actual users of this framework.

Discussion Process

The entire discussion took place online and lasted for 57 minutes. To enhance the observation of the participants' experimental process and improve the efficiency of solving issues, participants were asked to share their screens while encountering problems. Including the moderator, a total of 6 people participated in this discussion.

During the discussion, all sections were executed in turn with recording. The discussion started with an introduction to the framework together with background knowledge illustration. For the introduction to the framework workflow, Figure 4.1 was referred to instead of a detailed live demo for participants to have a general understanding of how it works, as whether interfaces and hints of this prototype can assist users work efficiently is the main subject to be evaluated. In addition, when introducing every stage of the framework, relevant background knowledge was also interwoven and briefly introduced within them. Then the moderator presented the hypothetical scenario and data and explained them to the participants. For the impacts of each threat, tangibility and persistence classification and particularly stressed in case participants got confused.

After distributing the task, participants began to work on the framework independently. During this stage, they were also encouraged to carefully review and try each interactive component on the interface to have a complete view of the prototype, instead of completing the task in a hurry. Some participants had various questions which were documented as well.

It took about 35 minutes for all participants to complete the task. The moderator then asked participants Questions (1)-(6) for effectiveness evaluation. The result is recorded as the ratio of correct answers to total. Later, participants filled in the questionnaire for about 5 minutes. After 5 questionnaires were successfully received, the focus group discussion came to an end.

6.2.2 Analysis

From the discussion, two main types of information are paid attention to and collected. One is the transcription extracted from the recording and notes taken during the discussion, and another kind of information is the result of the wrap-up questionnaire.

Effectiveness Evaluation

For the evaluation of effectiveness, useful information falls in answers to Q1-Q7. Answers to Q1-Q6 were almost correct, except for the question 'Which threat is most emergent?'. One participant wrongly gave the least emergent threat as the answer, and after inquiring deeply, this participant immediately realized she mistakenly took it for granted that the threat with the longest MTPD was the most urgent one. Apart from this case, all participants could give correct answers to 6 other questions instantly and without difficulty. For Q7 which was integrated into the questionnaire, three participants rated the usefulness of the framework as 4, and the other two ranked it as 5. It indicates that within this small group, the framework generates a positive response overall. Based on all results related to effectiveness evaluation, it can be inferred that general users may think it with a relatively high level of usefulness on average.

Usability Evaluation

For the usability analysis, notes taken during the discussion, transcription of the meeting, the SUS questionnaire, and collected suggestions are the primary materials. As there is a lot of textual and non-quantitative information, notes, transcriptions, and opinions submitted through the questionnaire are analyzed with thematic analysis.

First, all textual data is gathered and listed. Each piece of text is reviewed and tagged with a code. For contents discussing the same issue, they are marked with one code. After all texts are inspected, they are categorized into five groups, which reveal issues and possible improvements of the framework. As Table 6.7 shows, problems center on button usage, as some participants got puzzled about the functions of some buttons like ”Is the ‘back’ button on the input page directs to the original table for the next threat inspection?”. This indicates that the design of the button like the text on it or its direction should be put in a clearer way. Additionally, most participants suggested the need for more tips and guidance on the page to instruct users on what to do next. This opinion is consistent with participants taking longer than expected to complete the task. The tooltip design still requires refinement, since this feature does not perfectly fulfill the original design intent of explaining business impact to the user. Input checks and data storage are also mentioned to enhance the usage of the framework, which focuses more on the optimization of functions behind interfaces. Although these two issues are not discussed in detail, they are considered equally important, as convenient operations also contribute to a better user experience.

As Table 6.8 shows, two themes are further distilled from these codes, which summarize two aspects of feedback of the framework. One theme stands for the UI design issue of the framework, involving tooltip improvement and instructions and hints improvement. Items belonging to this theme can be developed through continuous user testing iterations. The other theme is defined as functions and workflow, which pays more attention to function implementation and workflow optimization. This theme consists of unclear buttons, unchecked inputs, and data storage. Functions of relevant buttons and input boxes should be modified, such as using the local storage and window.addEventListener() function to store the inputted data on the input page as long as there is an input to address the issue ”After I finish the input, I click the ’inspect’ again to check it, but the data disappeared, so I have to input it again”.

Theme	***Code***
Functions and Workflow	Unclear Buttons Unchecked Inputs Data Storage
UI Design	Tooltip Improvement Instructions and Hints Improvement

Table 6.8: Themes Drawn from Codes

To interpret the SUS score result, for each question the score is normalized: for positively-oriented questions, deduct one from the initial score, while for negatively-oriented questions, subtract the initial score from five. All scores then fall in the range of 0-4, and the sum of all scores is amplified by a factor of 2.5 to obtain the ultimate score [61]. For instance, if the cumulative score of a user’s responses to the ten questions is 30, it should

Code	***Text***
Unclear Buttons	*1. The timing of buttons should be more reasonable.* *2. Is the 'back' button on the input page directs to the original table for the next threat inspection?* *3. After the submission on the input page, the button can directly submit and jump to the next page, instead of the user manually jumping.* *4. The 'OK' button resembles the 'Continue to Input Page' button although they represent different functions, I got a little confused after I added the new customized impact.*
Unchecked Inputs	*1. Shall I add an apostrophe when inputting the customized business impact?* *2. You can regulate the input data type, such as inputting the wrong data type pop-up window to report errors so that the operation is more rigorous.*
Tooltip Improvement	*1. What does 'customer breach notification' mean?* *2. I cannot read the full sentence in the tooltip as part of the text is obscured. Could it be moved to the next line of the checkbox?* *3. The design of the tooltip could be optimized.*
Instructions and Hints Improvement	*1. What should I do after getting the classification table? There should be more guidance language like 'Prompt to inspect after entering threat'.* *2. Guidance for users should be strengthened.* *3. I think maybe some instructions appearing on the page could be better.*
Data Storage	*1. After I finish the input, I click the 'inspect' again to check it, but the data disappeared so I have to input it again.* *2. After filling in the data, this threat can be marked on the main home page, for example, there is a checkbox in front of it, so that those that have been filled in by the user can be automatically checked, and the user can also choose the number of threats that need to be analyzed.*

Table 6.7: Codes for Textual Information

be multiplied by 2.5 and yield an SUS score of 75. Table 6.9 collects the SUS scores of all participants.

Participant	***SUS Score***
1	75
2	85
3	55
4	72.5
5	72.5

Table 6.9: SUS Scores of Participants

It is worth noting that the SUS score is a percentile instead of a percentage number. The average SUS score is 68, and for level A the score is 80.3, which is the top 10% score [61]. From the score table, it can be drawn that 4 out of 5 participants think the performance of the prototype is above the passing level, and one of them thinks it is excellent. Overall, the level of usability of this prototype is at least acceptable.

Index	***Question***	***Disagree***	***Neutral***	***Agree***
S1	I think that I would like to use this system frequently.	0%	40%	60%
S2	I found the system unnecessarily complex.	100%	0%	0%
S3	I thought the system was easy to use.	0%	40%	60%
S4	I think that I would need the support of a technical person to be able to use this system.	40%	20%	40%
S5	I found the various functions in this system were well integrated.	0%	20%	80%
S6	I thought there was too much inconsistency in this system.	60%	40%	0%
S7	I would imagine that most people would learn to use this system very quickly.	0%	20%	80%
S8	I found the system very cumbersome to use.	80%	20%	0%
S9	I felt very confident using the system.	0%	20%	80%
S10	I needed to learn a lot of things before I could get going with this system.	100%	0%	0%

Table 6.10: SUS Result

Table 6.10 shows a detailed result of the SUS. S4 and S10 test the learnability of the prototype, and the rest evaluate the usability [62]. Participants had evenly different opinions on S4, while for S10, all participants disagreed. The results for the two questions point in different directions, indicating that the learnability of the framework is hard to assert and needs a wider investigation. What' more, S1, S3, and S6 gets 40% neutral answers. S1 and S3 relate to the practical use of the framework, as 2 participants maintained a neutral attitude, the reason can be either the framework is somewhat time-consuming or intricate, or there can be some differences between actual users and participants, and for real users, they can give clearer judgment. For S6, 3 participants held reservations about the consistency of the system, which may suggest that the consistency of the framework can be improved for a better user experience.

Chapter 7

Summary and Conclusions

This thesis works on a framework that deploys the BIA method to quantify and prioritize the impact of cyber threats in business contexts. First, cyber threats and the BIA method are introduced as background knowledge. Next, the thesis focuses on current threat modeling methodologies. Totally 23 modeling methodologies are studied and classified in depth, and their threat prioritization work is especially discussed. It can be drawn from the literature that there is little work aiming at quantifying and prioritizing threat impacts from a business view, and a framework for threat analysis and visualization is proposed to address this gap.

The BIA framework first categorizes the threat belonging to confidentiality, integrity, or availability loss, then provides users with corresponding business impacts. At the same time, the framework allows users to add customized impacts for convenience. After choosing applicable impacts, users can input the estimated loss of each impact and other necessary information. The framework will finally generate a visualization report based on the inputted information, including loss trend over time, tangible and intangible impact loss overview, threat prioritization by loss and emergency, and detailed business impact composition of each threat. Users can derive insights more efficiently based on the visualization.

Last but not least, the usability and effectiveness of this framework are evaluated through a usage scenario and focus group discussion. The result is both qualitatively analyzed by the SUS and textually discussed. It turns out that effectiveness is fully achieved as the business impact losses suggestion, calculation and visualization are all validated. The usability also gets satisfactory SUS scores from different participants of the focus group, and suggestions and opinions collected from participants are also classified and inspected for the improvement of the framework.

7.1 Future Work

Although the framework is well-developed and gets positive feedback from evaluation, there are still many aspects and details that need to be refined and improved. Potential directions for improvement are collected from both the architecture design and implementation process, and opinions from participants during the evaluation stage.

1. First, the implementation of the mapping between cyber threats and types of loss can be extended. As presented in Table 4.1, one cyber threat may lead to different kinds of information loss. For instance, malware can damage both data confidentiality and integrity. This mapping is constructed according to the most possible outcome that the cyber threat can cause, while in practice the scenario is more complicated. A more comprehensive mapping mechanism should be implemented to cover more practical situations.

2. Second, according to the feedback of the focus group discussion, more instructions and better button design should be considered to provide users with clearer guidance to utilize this framework. What's more, the design of the workflow should also be optimized. For instance, it will be more convenient for users to directly jump to the home page after clicking the "save" button on the input page instead of manually getting back to the home page.

3. The design of the visualization result can be further refined. During the effectiveness evaluation of the framework, one participant mistakenly thought the longest MTPD stands for the most emergent threat. This indicates that the visualization should be presented in a more straight way, like giving out the emergency list of threat scenarios from most emergent to the least one.

Bibliography

[1] E. Wheeler, *Security risk management: Building an information security risk management program from the Ground Up*. Elsevier, 2011.

[2] L. F. Eliyan and R. Di Pietro, "Dos and ddos attacks in software defined networks: A survey of existing solutions and research challenges", *Future Generation Computer Systems*, vol. 122, pp. 149–171, 2021, ISSN: 0167-739X. DOI: https://doi.org/10.1016/j.future.2021.03.011. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167739X21000911.

[3] L. Bilge and T. Dumitraş, "Before we knew it: An empirical study of zero-day attacks in the real world", in *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, ser. CCS '12, Raleigh, North Carolina, USA: Association for Computing Machinery, 2012, pp. 833–844, ISBN: 9781450316514. DOI: 10.1145/2382196.2382284. [Online]. Available: https://doi.org/10.1145/2382196.2382284.

[4] S. S. Silva, R. M. Silva, R. C. Pinto, and R. M. Salles, "Botnets: A survey", *Computer Networks*, vol. 57, no. 2, pp. 378–403, 2013.

[5] A. Singh, A. Sharma, N. Sharma, I. Kaushik, and B. Bhushan, "Taxonomy of attacks on web based applications", in *2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT)*, vol. 1, 2019, pp. 1231–1235. DOI: 10.1109/ICICICT46008.2019.8993264.

[6] M. Wazid, A. K. Das, J. J. P. C. Rodrigues, S. Shetty, and Y. Park, "Iomt malware detection approaches: Analysis and research challenges", *IEEE Access*, vol. 7, pp. 182 459–182 476, 2019. DOI: 10.1109/ACCESS.2019.2960412.

[7] T. Reshmi, "Information security breaches due to ransomware attacks - a systematic literature review", *International Journal of Information Management Data Insights*, vol. 1, no. 2, p. 100 013, 2021, ISSN: 2667-0968. DOI: https://doi.org/10.1016/j.jjimei.2021.100013. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2667096821000069.

[8] A. Mallik, "Man-in-the-middle-attack: Understanding in simple words", *Cyberspace: Jurnal Pendidikan Teknologi Informasi*, vol. 2, no. 2, pp. 109–134, 2019.

[9] J. M. Biju, N. Gopal, and A. J. Prakash, "Cyber attacks and its different types", *International Research Journal of Engineering and Technology*, vol. 6, no. 3, pp. 4849–4852, 2019.

[10] Z. Wang, L. Sun, and H. Zhu, "Defining social engineering in cybersecurity", *IEEE Access*, vol. 8, pp. 85 094–85 115, 2020.

[11] J. M. Hatfield, "Social engineering in cybersecurity: The evolution of a concept", *Computers & Security*, vol. 73, pp. 102–113, 2018.

[12] Z. Wang, H. Zhu, and L. Sun, "Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities and attack methods", *IEEE Access*, vol. 9, pp. 11 895–11 910, 2021. DOI: 10.1109/ACCESS.2021.3051633.

[13] F. Salahdine and N. Kaabouch, "Social engineering attacks: A survey", *Future Internet*, vol. 11, no. 4, 2019, ISSN: 1999-5903. DOI: 10.3390/fi11040089. [Online]. Available: https://www.mdpi.com/1999-5903/11/4/89.

[14] K. M. Caramancion, "An exploration of disinformation as a cybersecurity threat", in *2020 3rd International Conference on Information and Computer Technologies (ICICT)*, 2020, pp. 440–444. DOI: 10.1109/ICICT50521.2020.00076.

[15] G. Magklaras, S. Furnell, and P. J. Brooke, "Towards an insider threat prediction specification language", *Information management & computer security*, vol. 14, no. 4, pp. 361–381, 2006.

[16] L. Cheng, F. Liu, and D. Yao, "Enterprise data breach: Causes, challenges, prevention, and future directions", *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, vol. 7, no. 5, e1211, 2017.

[17] I. KARA and M. AYDOS, "Cyber fraud: Detection and analysis of the crypto-ransomware", in *2020 11th IEEE Annual Ubiquitous Computing, Electronics Mobile Communication Conference (UEMCON)*, 2020, pp. 0764–0769. DOI: 10.1109/UEMCON51285.2020.9298128.

[18] S. Baror and H. Venter, *A Taxonomy for Cybercrime Attack in the Public Cloud.* Mar. 2019, ISBN: ISBN-10: 1912764113 ISBN-13: 978-1912764112.

[19] D. D. Caputo, S. L. Pfleeger, J. D. Freeman, and M. E. Johnson, "Going spear phishing: Exploring embedded training and awareness", *IEEE security & privacy*, vol. 12, no. 1, pp. 28–38, 2013.

[20] R. Alabdan, "Phishing attacks survey: Types, vectors, and technical approaches", *Future Internet*, vol. 12, no. 10, 2020, ISSN: 1999-5903. DOI: 10.3390/fi12100168. [Online]. Available: https://www.mdpi.com/1999-5903/12/10/168.

[21] W. A. Al-Khater, S. Al-Maadeed, A. A. Ahmed, A. S. Sadiq, and M. K. Khan, "Comprehensive review of cybercrime detection techniques", *IEEE Access*, vol. 8, pp. 137 293–137 311, 2020. DOI: 10.1109/ACCESS.2020.3011259.

[22] M. Sakshi, A. Vashishth, *et al.*, "An analysis of cyber crime with special reference to cyber stalking", *Journal of positive school psychology*, pp. 1279–1287, 2022.

[23] A. Shah and D. Chudasama, "Investigating various approaches and ways to detect cyber crime", vol. 9, pp. 12–20, Nov. 2021. DOI: 10.37591/JoNS.

[24] M. Ahmed, D. Cox, B. Simpson, and A. Aloufi, "Ecu-ioft: A dataset for analysing cyber-attacks on internet of flying things", *Applied Sciences*, vol. 12, no. 4, 2022, ISSN: 2076-3417. DOI: 10.3390/app12041990. [Online]. Available: https://www.mdpi.com/2076-3417/12/4/1990.

[25] J. Carr, *Inside cyber warfare: Mapping the cyber underworld.* " O'Reilly Media, Inc.", 2012.

[26] E. Reddy and A. Minnaar, “Cryptocurrency: A tool and target for cybercrime”, *Acta Criminologica: African Journal of Criminology & Victimology*, vol. 31, no. 3, pp. 71–92, 2018.

[27] N. Ali, “Crimes related to cryptocurrency and regulations to combat crypto crimes”, *Journal of Policy Research*, vol. 8, no. 3, pp. 289–302, 2022.

[28] J. T. Force, “Security and privacy controls for information systems and organizations”, National Institute of Standards and Technology, Tech. Rep., 2017.

[29] I. Tarandach and M. Coles, *Threat Modeling: A Practical Guide for Developing Teams*. O'Reilly Media, Incorporated, 2020, ISBN: 9781492056553. [Online]. Available: `https://books.google.ch/books?id=WcbFyQEACAAJ`.

[30] N. Shevchenko, T. A. Chick, P. O'Riordan, T. P. Scanlon, and C. Woody, “Threat modeling: A summary of available methods”, Carnegie Mellon University Software Engineering Institute Pittsburgh United ..., Tech. Rep., 2018.

[31] ISO, *Iso/ts 22317:2021(en) security and resilience — business continuity management systems — guidelines for business impact analysis*, Last accessed 14 May 2023, 2021. [Online]. Available: `https://www.iso.org/obp/ui/#iso:std:iso:ts:22317:ed-2:v1:en`.

[32] S. Tjoa, S. Jakoubi, and G. Quirchmayr, “Enhancing business impact analysis and risk assessment applying a risk-aware business process modeling and simulation methodology”, in *2008 Third International Conference on Availability, Reliability and Security*, 2008, pp. 179–186. DOI: `10.1109/ARES.2008.206`.

[33] A. Corallo, M. Lazoi, and M. Lezzi, “Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts”, *Computers in industry*, vol. 114, p. 103 165, 2020.

[34] NIST, *Nist sp 800-34*, Last accessed 15 May 2023, 2021. [Online]. Available: `https://www.nist.gov/privacy-framework/nist-sp-800-34`.

[35] S. Torabi, H. Rezaei Soufi, and N. Sahebjamnia, “A new framework for business impact analysis in business continuity management (with a case study)”, *Safety Science*, vol. 68, pp. 309–323, 2014, ISSN: 0925-7535. DOI: `https://doi.org/10.1016/j.ssci.2014.04.017`. [Online]. Available: `https://www.sciencedirect.com/science/article/pii/S0925753514001027`.

[36] R. L. Tammineedi, “Business continuity management: A standards-based approach”, *Information Security Journal: A Global Perspective*, vol. 19, no. 1, pp. 36–50, 2010.

[37] ISO, *Iso 22301:2012(en) societal security — business continuity management systems — requirements*, Last accessed 14 May 2023, 2012. [Online]. Available: `https://www.iso.org/obp/ui/#iso:std:iso:22301:ed-1:v2:en`.

[38] A. Corallo, M. Lazoi, M. Lezzi, and P. Pontrandolfo, “Cybersecurity challenges for manufacturing systems 4.0: Assessment of the business impact level”, *IEEE Transactions on Engineering Management*, pp. 1–21, 2021. DOI: `10.1109/TEM.2021.3084687`.

[39] R. Phillips and B. Tanner, “Breaking down silos between business continuity and cyber security”, *Journal of business continuity & emergency planning*, vol. 12, no. 3, pp. 224–232, 2019.

[40] R. Khan, K. McLaughlin, D. Laverty, and S. Sezer, "Stride-based threat modeling for cyber-physical systems", in *2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*, IEEE, 2017, pp. 1–6.

[41] F. Kammüller and C. W. Probst, "Modeling and verification of insider threats using logical analysis", *IEEE Systems Journal*, vol. 11, no. 2, pp. 534–545, 2017. DOI: 10.1109/JSYST.2015.2453215.

[42] J. Wynn, "Threat assessment and remediation analysis (tara)", MITRE CORP BEDFORD MA BEDFORD United States, Tech. Rep., 2014.

[43] P. Saitta, B. Larcom, and M. Eddington, "Trike v. 1 methodology document [draft]", *URL: http://dymaxion. org/trike/Trike v1 Methodology Documentdraft. pdf*, 2005.

[44] J. Cleland-Huang, "How well do you know your personae non gratae?", *IEEE software*, vol. 31, no. 4, pp. 28–31, 2014.

[45] C. Alberts, S. Behrens, R. Pethia, and W. Wilson, "Operationally critical threat, asset, and vulnerability evaluation (octave) framework, version 1.0", Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, Tech. Rep. CMU/SEI-99-TR-017, 1999. [Online]. Available: http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=13473.

[46] K. Wuyts and W. Joosen, "Linddun privacy threat modeling: A tutorial", *CW Reports*, 2015.

[47] B. Potteiger, G. Martins, and X. Koutsoukos, "Software and attack centric integrated threat modeling for quantitative risk assessment", in *Proceedings of the Symposium and Bootcamp on the Science of Security*, 2016, pp. 99–108.

[48] N. Mead, E. Hough, and T. S. II, "Security quality requirements engineering technical report", Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, Tech. Rep. CMU/SEI-2005-TR-009, 2005. [Online]. Available: http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=7657.

[49] N. Mead and F. Shull, *The hybrid threat modeling method*, Carnegie Mellon University, Software Engineering Institute's Insights (blog), Accessed: 2023-May-25, Apr. 2018. [Online]. Available: https://insights.sei.cmu.edu/blog/the-hybrid-threat-modeling-method/.

[50] Z. Rodionova and L. Bobrov, "Protection of the information resources of a library based on analysis of business processes", *Scientific and Technical Information Processing*, vol. 43, pp. 20–27, 2016.

[51] G. Brændeland, A. Refsdal, and K. Stølen, "Modular analysis and modelling of risk scenarios with dependencies", *Journal of Systems and Software*, vol. 83, no. 10, pp. 1995–2013, 2010.

[52] X. Li, R. Liu, Z. Feng, and K. He, "Threat modeling-oriented attack path evaluating algorithm", *Transactions of Tianjin University*, vol. 15, no. 3, pp. 162–167, 2009.

[53] B. A. Sabbagh and S. Kowalski, "A socio-technical framework for threat modeling a software supply chain", *IEEE Security Privacy*, vol. 13, no. 4, pp. 30–39, 2015. DOI: 10.1109/MSP.2015.72.

[54] S. Singh, H. Tu, J. Allanach, J. Areta, P. Willett, and K. Pattipati, "Modeling threats", *IEEE Potentials*, vol. 23, no. 3, pp. 18–21, 2004. DOI: `10.1109/MP.2004.1341780`.

[55] X. Li, K. He, Z. Feng, and G. Xu, "Unified threat model for analyzing and evaluating software threats", *Security and Communication Networks*, vol. 7, no. 10, pp. 1454–1466, 2014.

[56] H. Suleiman, I. Alqassem, A. Diabat, E. Arnautovic, and D. Svetinovic, "Integrated smart grid systems security threat model", *Information Systems*, vol. 53, pp. 147–160, 2015.

[57] B. Al Sabbagh and S. Kowalski, "A socio-technical framework for threat modeling a software supply chain", *IEEE Security & Privacy*, vol. 13, no. 4, pp. 30–39, 2015.

[58] E. Mossburg, J. Gelinne, and H. Calzada, "Beneath the surface of a cyberattack: A deeper look at business impacts", 2016.

[59] R. A. Powell and H. M. Single, "Methodology matters–v", *International journal for quality in health care*, vol. 5, no. 8, pp. 499–504, 1996.

[60] J. Brooke, "Sus: A "quick and dirty'usability", *Usability evaluation in industry*, vol. 189, no. 3, pp. 189–194, 1996.

[61] P. Jeff Sauro, *Measuring usability with the system usability scale (sus)*, Last accessed 23 Aug 2023, 2011. [Online]. Available: `https://measuringu.com/sus/`.

[62] J. R. Lewis and J. Sauro, "The factor structure of the system usability scale", in *Human Centered Design: First International Conference, HCD 2009, Held as Part of HCI International 2009, San Diego, CA, USA, July 19-24, 2009 Proceedings 1*, Springer, 2009, pp. 94–103.

Abbreviations

BIA	Business Impact Analysis
BCM	Business Continuity Management
DDoS	Distributed Denial of Service
DoS	Denial of Service
TCP	Transmission Control Protocol
SYN	Synchronize Sequence Numbers
ICMP	Internet Control Message Protocol
UDP	User Datagram Protocol
HTTP	HyperText Transfer Protocol
MitM	Man-in-the-Middle
RFID	Radio-Frequency Identification
PKI	Public Key Infrastructure
PC	Personal Computer
IT	Information Technology
WPA2-PSK	Wi-Fi Protected Access2-Pre-shared Keys
XSS	Cross-site Scripting
NIST	National Institute of Standards and Technology
MTPD	Maximum Tolerable Period of Disruption
ISO	International Organization of Standards
PASTA	Process for Attack Simulation and Threat Analysis
TARA	hreat Assessment and Remediation Analysis
CVSS	Common Vulnerability Scoring System
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
VAST	Visual, Agile, and Simple Threat
hTMM	Hybrid Threat-Modeling Method
SQUARE	Security Quality Requirements Engineering
PnG	Persona non Granta
HMM	Hidden Markov Model
C-I-A	Confidentiality-Integrity-Availability
IP	Intellectual Property
SUS	System Usability Scale
PHI	Personal Health Information
HIPPA	Health Insurance Portability and Accountability Act

Glossary

In the context of cybersecurity, some concepts have broad meanings. Here in this thesis, some meanings of glossaries are narrowed or re-defined to precisely describe the scenario. In addition, we assume that audiences are familiar with front-end development, and some implementation glossaries are not introduced in the main text.

Threat Analysis Threat analysis is a general concept in cybersecurity, which refers to the process of determining which components of the system need to be protected, and the types of threats they should be protected from. In this thesis, threat analysis mainly focuses on threat quantification and prioritization and is particularly differentiated from risk analysis.

Hybrid Threat This kind of threat is difficult to be simply dichotomized as technical or non-technical, as they may result from different causes or motivations and be accomplished by a combination of technical and non-technical cyberattacks. Hybrid threat is proposed by this thesis to more accurately classify cyber threats.

Container The Container mentioned in Chapter 5 is a kind of layout element of HTML that organizes the content of the interface.

Local storage Local storage is an attribute in HTML5 that Allows data to be stored as key-value pairs in the browser. In this thesis, the prototype is implemented in the front end, and all relevant data is stored in the local storage.

List of Figures

List of Tables

Appendix A

Installation Guidelines

The prototype is implemented in the front end completely. Users can directly open the `home.html` file in the code folder to start. For detailed usage guidelines and codes please refer to the GitHub repository [1].

[1] https://github.com/Dmmmmy/BIA-prototype