University of Piraeus

School of Information and Communication Technologies

Department of Digital Systems

Postgraduate Program:

"Digital Systems Security"

Title:

Managing Cascading Threats in IT/OT Environments.

Supervising Professor: Prof. Konstantinos Labrinoudakis

	Full name	*E-mail*	*ID*
Author:	Nikolaos Gavriilidis	mte2103@unipi.gr	MTE2103

Piraeus,

April 2023

This page intentionally left blank.

Abstract

The concept of cascading threats has been the subject of increasing research in recent years, with a focus on identifying them and assessing their risk. Threat modeling, risk assessment, incident handling, and the development of mitigation strategies are considered core steps to defend against cascading threats. However, the complexity and interconnectivity of modern systems make it challenging to understand the potential impact of a cascading threat and to design effective models that predict dependencies. This research relies on an extensive examination of the relevant literature along with an analysis of applicable risk assessment techniques. Both Information Technology and Operational Technology environments are within the scope of this research. The main objective is the provision of a deeper understanding of cascading threats, their characteristics, and their impact on the information systems as well as to critical infrastructures. Thus, a systematic methodology and recommendations for identifying, assessing, and mitigating cascading threats are being proposed. Consequently, best practices and suggested architectures are presented both for IT and OT environments. The research also explores the role of data analysis tools for better visualizing and tracking the dependencies between assets and therefore a custom technical implementation is being presented. Finally, a promising approach for thoroughly evaluating cascading threats using a mathematical model has been proposed for future research. This research will be of interest to professionals/ researchers who are concerned to understand and manage cascading threats of the IT/OT world and will be particularly useful for those working in cybersecurity.

Περίληψη

Η έννοια των αλυσιδωτών απειλών (εφεξής ως cascading threats) έχει αποτελέσει αντικείμενο αυξανόμενης έρευνας τα τελευταία χρόνια, με έμφαση στον εντοπισμό και στην αξιολόγηση του κινδύνου τους. Η μοντελοποίηση απειλών, οι μελέτες εκτίμησης αντικτύπου, τα λειτουργικά μοντέλα χειρισμού περιστατικών ασφάλειας και η ανάπτυξη στρατηγικών αντιμετώπισης θεωρούνται βασικά βήματα ως προς την διαχείριση των cascading threats. Η πολυπλοκότητα και η διασυνδεσιμότητα των σύγχρονων συστημάτων καθιστούν δύσκολη την κατανόηση του δυνητικού αντίκτυπου ενός cascading threat και κατ' επέκταση καθιστά απαιτητικό το σχεδιασμό αποτελεσματικών μοντέλων πρόβλεψης κινδύνων και εξαρτήσεων. Η παρούσα έρευνα στηρίζεται σε εκτενή ανασκόπηση της σχετικής βιβλιογραφίας. Ταυτόχρονα αναλύονται σύγχρονες μεθοδολογίες εκτίμησης αντικτύπου για τον υπολογισμό του κινδύνου των cascading threats. Πεδίο αναφοράς είναι τα περιβάλλοντα που εντάσσονται στο φάσμα του IT αλλά και αυτά που χαρακτηρίζονται ως OT. Στόχος είναι να δημιουργηθεί μια βαθύτερη κατανόηση των cascading threats αφού αναγνωριστούν τα χαρακτηριστικά και οι επιπτώσεις τους. Ως εκ τούτου, προτείνεται μια ολοκληρωμένη μεθοδολογία για τον εντοπισμό, την αξιολόγηση, και τον μετριασμό των cascading threats. Επιπροσθέτως, παρουσιάζονται βέλτιστες πρακτικές και προτεινόμενες αρχιτεκτονικές για τα IT & OT περιβάλλοντα. Διερευνάται επίσης, ο ρόλος των εργαλείων ανάλυσης δεδομένων για την καλύτερη απεικόνιση των εξαρτήσεων μεταξύ των αγαθών ενός οργανισμού και παρουσιάζεται σχετική υλοποίηση. Τέλος, προτείνεται ένα μαθηματικό μοντέλο για την κατανόηση των cascading threats για σκοπούς μελλοντικής έρευνας. Η έρευνα προορίζεται για επαγγελματίες και ερευνητές του χώρου της κυβερνοασφάλειας.

Subject Area: Information Security.
Keywords: Risk Management, Cascading Threats, Data Analysis, Threat Modelling.

Table of Contents

List of Figures

List of Tables

Introduction

Cascading threats, also known as "domino effects," and refer to the propagation of a threat from one system or component to another, leading to a chain reaction of failures or disruptions. This domino effect, where one failure or attack leads to another and another, induces more risk than a simple attack. According to *(Federal Emergency Management Agency (FEMA) definition*, “cascading events are events that occur as a direct or indirect result of an initial event. Clearly, the increasing interconnectivity and complexity of modern systems have made systems more vulnerable to cascading threats. This fact cannot be confronted with a siloed approach for protecting systems in an isolated capacity because it becomes more and more obsolete, even though it is one of the most common used techniques, particularly in the domain of critical infrastructures [1]. Thus, I structured approach shall be followed for the purpose of identifying cascading threats and their corresponding risk; with the aim to enhance the organization’s cybersecurity posture. The core activities that should be included in this approach must include threat modeling, risk assessment / management, asset management and incident response operating models. Additionally, it is important to have a continuous monitoring and improvement process like an Information Security Management System (ISMS) to ensure that the organization is always prepared to detect and respond to cascading threats. This research, among others, aims to provide a thorough examination of the countermeasures and best practices are presented the following chapters as well as to create a structured approach to identify and respond to cascading threats / risks.

Cascading risks can be triggered by a wide range of threat events, such as natural disasters, cyber-attacks, equipment failures or human errors etc. It is notable that cascading risks do not only exist in information systems but also in every aspect of human life. A cascading event is, for instance, when a flash flood cuts out electricity to a region and, as a result of the electrical failure, a catastrophic traffic collision with a hazardous substance spill takes place. There are also excess cascading events if the spill of hazardous chemicals necessitates the evacuation of a community and the contaminating of a nearby stream [2]. When they occur all at once, cascading disasters can paralyze a community and dominate large scale disruptions. Respectively, information systems can also be affected from cascading events. One common example could be a single cyber breach at a software provider which not only affects them but may cascade and effect their customers, partners or vendors.

1. Understanding the Concept of Cascading Threats

1.1 Definition and Characteristics of Cascading Threats in IT

Nowadays, Organizations are required to maintain numerous dependencies on their information systems due to the increasing interconnectivity and complexity. This yields an increased risk of failure of the whole system because of a single point, or a particular asset that is fragile and sensitive to the failure of a component [2)]. As a result, larger parts of the organization will be affected with a higher impact.

Some of the characteristics of cascading threats include:

- They propagate through interdependencies between systems or components.
- They can be triggered by a wide range of events, such as natural disasters, cyber-attacks, or equipment failures.
- They can have a significant impact on the Availability, Integrity, and Confidentiality (CIA triad) of systems and data.
- They can be difficult to predict and prevent, as they often involve complex interactions between multiple systems and components. This makes it challenging to understand the potential impact of a threat and to design effective mitigations.
- They can lead to unexpected consequences, as the impact of a cascading threat can be greater than the sum of its parts. For example, a cyber-attack on a single component of a system can cause cascading failures in other parts of the system.
- They can be triggered by both internal and external events, such as human errors, natural disasters, cyber-attacks, or equipment failures.
- They are able to create disruption of essential services, loss of sensitive information, financial losses and many more.

Cybersecurity incidents can spread across borders due to similar dependencies and weaknesses that different technologies and organizations share, making it challenging to foresee, quantify, and manage cascading threats. Due to technological and comparative advantages, organizations from many industries frequently depend on the same third-party hardware, software, or service providers. When a widely used technology or shared service is interrupted by cyberattacks, this concentration of risk can generate problems for organizations that appear to be unrelated. As a result, a collaboration between the private sector, governmental organizations, and civil society is required, as well as a shared knowledge of the risks involved, to be ready for systemic cyber disasters [3].

1.2 Cascading threats and Cascading Failures in Critical Infrastructures

Critical infrastructures (CIs) face a complex and unpredictable risk environment with constantly changing threats, vulnerabilities, and impacts. As ICT systems are becoming more interconnected, CI sectors, which have historically faced physical dangers and natural disasters, are now subject to cyber-risks. Explaining dependencies is challenging due to the interdependencies between ICT systems and other CI industries (cross-border dependencies). A "system of systems" formed by interdependent Critical Infrastructure assets poses a danger to both the system as a whole and the individual assets within it. The resilience of the entire system and the area it serves can be negatively impacted by the breakdown of one or more infrastructural components. The possible effects of these dangers are illustrated by recent attacks on Ukrainian power infrastructure and the DDoS attack on DNS provider Dyn. In 2020, a ransomware attack on a hospital in Germany caused medical delays, which led to one patient's death [4]. These incidents demonstrate the important requirement for efficient risk management and mitigation techniques to safeguard Critical Infrastructures. Below are some of the most targeted sectors of CIs as regulated also with NIS2 so as to improve their resilience.

- Electric Grid Interruptions: A well-planned cyberattack on a crucial part of the grid can cause massive and widespread power outages, interrupting crucial services and resulting in huge financial losses.
- Water Distribution System Disruptions: A targeted attack on a water treatment facility may potentially result in a contaminated water supply, putting the general people at considerable danger for health and safety.
- Transportation Network Disruptions: A cyber-attack on a system that controls transportation could lead to the alteration of the timetables and routes for different nodes of transportation, including trains, aircraft, and buses, causing substantial delays and financial losses.
- Healthcare System Interruptions: An attack on the information system of a healthcare facility has the potential to seriously interrupt patient care and have life-threatening repercussions. Furthermore, it may result in the loss of critical patient information and data.
- Financial Institution Disruptions: A cyber-attack on a financial institution could jeopardize confidential data and financial assets, leading to serious economic repercussions and a decline in public confidence in the system.
- Airport Operations Disruptions: A targeted attack on an airport's control system might cause flight delays and cancellations, which would have a significant impact on business, communication, and transportation.
- Gas Pipeline Incident: A cyber-attack on the control system of a gas pipeline could cause an explosion, which would have major ramifications for air quality, energy generation, and transportation.

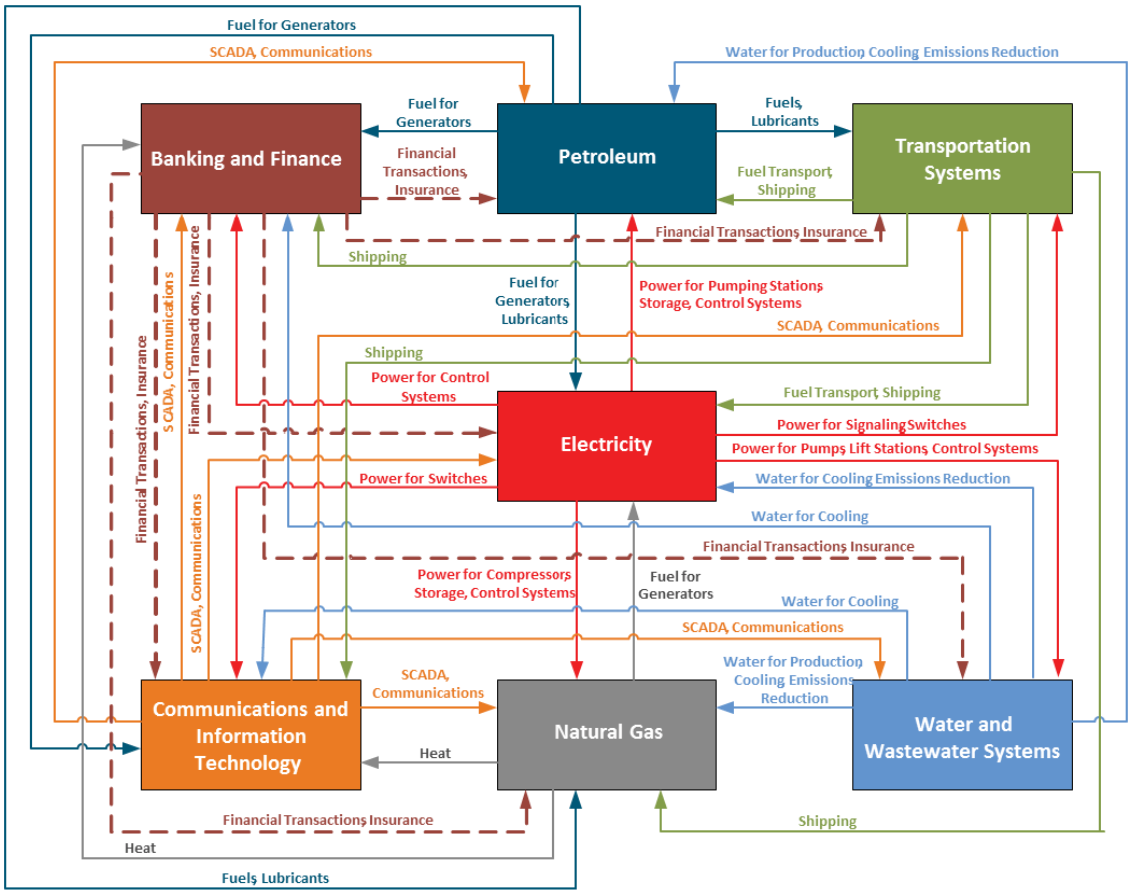


Figure 1 Cross Sector Dependencies

Source: https://www.hsaj.org

Recognizing dependencies between infrastructure systems is crucial, but it is insufficient to properly comprehend how crucial a connection is to the system's operational integrity. A greater comprehension of why and how a connection impacts the whole system is necessary to appropriately assess its relevance. Prioritizing the worst possible failure spots is a necessary step in protecting critical infrastructure in complex metropolitan regions. The prioritization process might be overwhelming due of the complexity of infrastructure systems, but it can help influence targeted planning and investment decisions. Protection programs frequently ignore system-level resilience when there is no prioritization procedure in place. Programs for protecting and ensuring the resilience of critical infrastructure should focus on identifying and prioritizing the most important contingencies because it is not practical for system operators and government organizations to examine and prepare for all potential interruptions [4]. The table below demonstrates some of the most common faults of CIs [5].

Table 1 Industrial Control System's Common Faults

Common faults	Description
Faults and inaccuracy in data collection	It might be particularly difficult to obtain and acquire data that is accurate and effective. This is due to the fact that these systems frequently make use of extensive networks of equipment, sensors, and devices that can produce enormous amounts of data. Additionally, the data produced by these systems may be distributed across a number of places and systems and may be corrupted or interfered with in numerous ways. For organizations in this industry, ensuring that the data gathered is accurate, thorough, and dependable may be very difficult.
Sensor faults	Sensors are frequently used in severe conditions, which can cause them to malfunction, fail, and degrade significantly. As a result, sensors may create outliers, which are values that are odd or incorrect. It may be challenging to obtain correct data and analyze it because of these outliers, which also makes it challenging to spot and address possible risks and system breakdowns.
Actuator faults	Any issues that a cyber-physical system's actuators are included in this section. In a cyber-physical system, the components known as actuators are in charge of managing and regulating the external physical environment. Due to prolonged usage and aging, these components may develop a variety of problems, such as bias issues and efficiency loss.
Failure in emergency and fault management.	Refers to the fault management system's incapacity to manage emergencies efficiently as a result of its poor situational awareness and hidden faults. This may make it difficult to identify and manage failures, perhaps resulting in more harm or jeopardizing the security of the system.
Memory exhaustion	exhaustion. Devices may become unresponsive or stop functioning properly when they run out of memory, which can result in system failures or even security breaches. For IoT devices to operate reliably and securely and to avoid memory exhaustion, memory utilization must be properly managed. Low memory capabilities are another factor that prevents the

Common faults	Description
	computation of complicated cryptographic algorithms to obtain a better level of security.
Hardware malfunction	Systems that are critical to the nation's infrastructure may be vulnerable to cyberattacks, natural catastrophes, and other disruptive occurrences due to flaws in the design of their hardware and software components.
Communication failure	This kind of failure impair the cyber-physical systems' availability and integrity (CPSs). Hardware malfunctions, network congestion, and software defects are only a few of the causes of communication failures. As a result, maintaining secure and reliable communication is essential for the efficient operation of critical infrastructure systems.

1.3 The Challenges of IT & OT Convergence

The demand for greater efficiency, cost savings, and the capacity to make better business decisions based on real-time data are some of the powerful factors driving this IT & OT convergence. Another significant issue is the rising reliance on computer networking and digital communications, as well as the expanding interconnectivity of wired and wireless communications among intelligent devices. Likewise, the desire to accelerate time to market, enhance scalability, and boost insight into security concerns and performance are also key factors. Obviously, using IT services and service models for OT can also aid in managing assets, vulnerabilities, patches, and privileged access. To ensure successful integration, there are a few issues raised by the convergence of OT and IT. Dealing with proprietary systems that are difficult to expand across different technologies and suppliers is one of the major obstacles. Furthermore, implementing security and interoperability without affecting crucial services or necessitating excessive resources is difficult due to the lengthy equipment lifecycles. Any convergence attempt must prioritize reliability and integrity, and there can be skills gaps to fill because OT is still in need of dated IT capabilities. Budgets and personnel headcounts may need to be verified along with the reorganization of the IT and OT divisions, which will also necessitate the adaptation, retirement, or replacement of functional business processes. Since many sensors only transmit events or deviations from the norm, data analytics may contain partial or incorrect information. Another challenge is the perception of risk, as IT and OT do not share the same perspective on the risk. Clearly, the integrity and availability are the most important requirements of the OT world. On the other hand, the confidentiality of data is the priority (or should be)

of the IT world. Consequently, both sides find it challenging to manage the plethora of vulnerabilities and attack vectors that IT and OT bring. Instrumentation, sensors, and mechatronics are examples of physical components that restrict systems' flexibility and futureproofing, making it difficult to update or switch suppliers or move from wired to wireless networks. In contrast to IT environments, OT environments do not have a centralized or unified antivirus solution. The vendor of the antivirus solution in the industrial environment often undertakes validation testing before issuing updates in order to avoid negative effects. So, the update frequency for antivirus engines and signatures may vary from the IT environments. Antivirus programs for control systems must function in specific ways, specifically by alerting the user or sending a warning when a virus is found, but without implementing any countermeasure to contain or reduce the threat. Finally, until appropriate data models are implemented, growing traffic and connection may result in storage and bandwidth issues. To overcome these obstacles and successfully integrate OT and IT, careful planning and implementation actions are needed. In general, the OT and IT convergence process is a complex one that needs careful planning, execution, and continuous management to be successful [6] [7].

2. Managing the Threat Landscape

The identification and the definition of all possible threat actors and threat vectors shall be the first stage in developing a threat model. For that reason, the initial step in addressing cascading risks is considered to be the understanding of all the threats that an organization might be exposed. This could entail performing a threat assessment to identify potential threats both from the inside and the outside as well as determining their likelihood, their potential impact, their motive etc. This chapter will undertake a thorough analysis of the complete threat management process. This analysis will go in-depth on each phase, giving readers a thorough knowledge of the mechanisms and approaches employed to reduce and control threats. In the following sections of this study, the subsequent stages of managing cascading risks will be presented. After this chapter, one important step that will be covered is the identification of specific assets and their corresponding dependent assets that support an organization's business process. This entails the assessment of asset's vulnerabilities to the known threats (that have already been identified) and figuring out what might happen to the asset if one threat is materialized to a dependent asset. Consequently, a dependency graphic with the use of data analysis tools will be developed to highlight the relationships between the assets. This dependency graphic will also demonstrate the assets' threats and their degree of dependency. Another equal important step of the methodology is the calculation of the control's strength that the organization has implemented. The proposed approach, which will be detailed further in this study, provides to the practitioners a comprehensive methodology for not only identifying potential cascading risks and threats, but also conducting a thorough analysis of their own systems and processes. This approach is beneficial in assisting organizations to enumerate the interconnections between various assets and understand the business processes that they support. The main output is the development of a proactive approach. In summary, the goal is to shape a more resilient system which is better prepared to withstand disruptive events, whether they are cyberattacks, natural disasters, or other types of incidents, and regardless of their source.

Managing threats firstly requires acknowledging them using signals/ alerts. Signals or alerts denote the existence of events and could point to the presence of a threat or incident and can be used to its identification and categorization. Both manually and automatically, such as through monitoring tools, anti-virus, firewalls, or SIEM systems, can detect these events. More specifically, a manual example could be when a user who reports strange activity or issues with an asset. Precursors and indicators are the two categories used to categorize cybersecurity signals. Accordingly, precursors are signals that could point to the existence of an incident in the future, for example they could be security bulletins that show the existence of a new vulnerability affecting a category of assets. On the contrary, indicators are signals that show a cybersecurity problem may be occurring or has already occurred. Examples include

alerts from monitoring tools for unintended changes in communication parameters, notifications from antivirus software for infected assets or malicious traffic etc. [8]

2.1 Understand Threats

An organization cybersecurity posture may be impacted by a number of threats, including, but not limited to, network threats, host threats, and supply chain threats, as well as a number of attack vectors like botnets, worms, trojans. Indeed, the organization needs to understand the motive (goals) that the malicious actors might have. The disambiguation of the idea that the target system maintains or process something important could clarify the motive of a malicious actor. Multiple motives exist, for example a common motive is to steal valuable information with a view to capitalize it and earn money. Another similar reason could be a competitor who wants to imitate and disrupt critical business processes, leading to a financial gain from the disruption caused. The equitation bellow decomposes the main characteristics of an attack which are: the motive, the method, and the vulnerabilities.

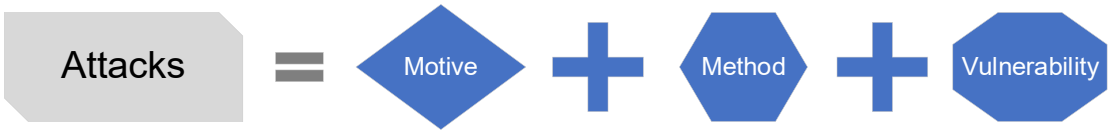


Figure 2 Attack Definition

Thus, attacks shall be analyzed in terms of motive, method, and vulnerabilities along with other variables which also can be included like the malicious actor's capacity to carry out the attack and the likelihood they have to exploit the system.

When taking a threat-driven risk scenario approach, understanding the data at risk is a critical aspect. Before embarking on the creation of a threat program, an organization should undergo a formal definition of its business drivers and "crown jewels". This includes assets and information as well as business processes that should be thoroughly evaluated in terms of financial loss, operational disruption, reputational damage, or other negative impacts. It is important to remember that malicious actor's motivations may often lead to events that don't always fall into the category of cyber events. On the contrary, events such as product sabotage or threats to human-life can also happen. As a consequence, the preservation of human life shall be the number one priority of every organization and especially those from the Critical Infrastructure sector, pursuant to NIS2. When building a threat program, all these considerations should be included for a robust and complete approach.

2.2 Identify Threats

Threat actors and threat vectors play a crucial role in the threat landscape. To begin with, the threat actors are groups with the intention of engaging in malicious activities

by exploiting security flaws and causing harm to their intended targets. For more effective cyber threat management and incident response programs, it is crucial to comprehend how threat actors behave, think, and act as well as their motives and objectives. With a view to retain a strong cybersecurity posture in the present environment, it is necessary to keep up with the most recent advancements in the methods and strategies used by malicious actors for accomplishing their objectives [9]. These methods are commonly referred to as threat vectors.

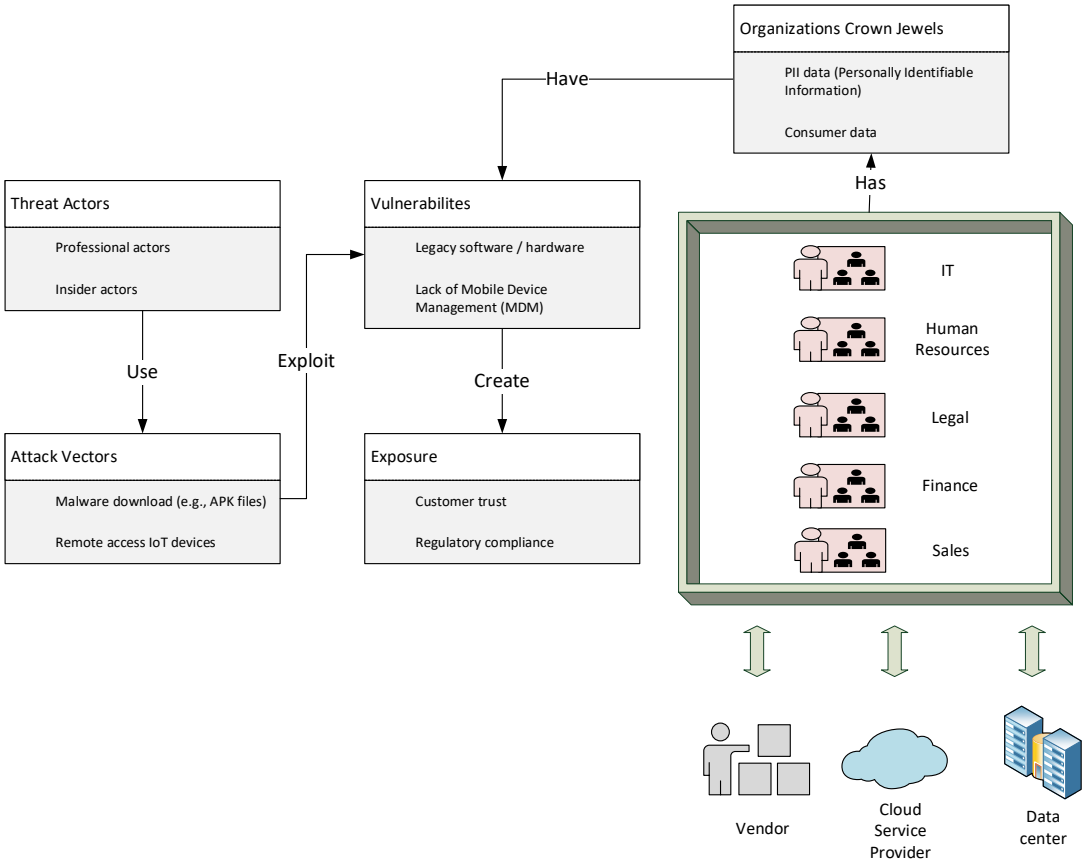


Figure 3 Conceptual Model of Threat Vectors / Actors

The figure above illustrates at a high-level how threat vectors and threat actors can affect an organization. The two main categories which was also the main subject of this chapter are further explained in the tables bellow.

Table 2 Threat Actors

Threat Actors	Description
Professional Actors	These actors are professional hackers, and they intentionally exploit vulnerabilities of specific targets for profit. They invest time in researching their target and customizing their attack, which may include intercepting financial records, personal information, and secret information.
State-sponsored Actors	State-sponsored actors are skilled individuals that attack specific targets on behalf of a state and under its instructions.
Hacktivists	Hacktivists are groups that launch coordinated cyberattacks in favor of political motives. Hacktivists frequently target entire sectors of the economy, although they occasionally target particular companies which they believe to be in opposition to their political beliefs or ethical standards [10].
Insider Actors	Any individual in a position where insider credentials, status, or access are utilized to disrupt or damage an organization is considered an insider threat. Insiders are typically given some level of power and access to the organization's resources since they are trusted by it. They include not just present employees but also past employees, third-party partners, contractors, and outsiders who have acquired credentials and are now de-facto insiders (whether by theft, coercion, or an insider's neglect).

Insider actors or insider threats are one imports category from the ones discussed above that needs to be specifically acknowledged. Insiders broadly fall into two major categories of motivations: the conscious or malicious and the unwitting. These conscious insiders who wish harm on others seem to be less common than the unintentional ones. Unwitting insiders now have more capabilities and opportunities to inadvertently cause harm on a regular basis, including posting sensitive materials to cloud storage, sharing sensitive data with suppliers without authorization, using information in an illegal manner, and allowing an outside attacker to steal their credentials. Many organizations' initiatives place an undue emphasis on the malicious, conscientious insider and ignore the unwitting, but in the end, a well-designed program should include strategies for both. Programs should also be attuned to third parties as these are essentially insiders as well. Third parties are trusted partners who are frequently granted logical and physical access to data, networks, and facilities, whether they are vendors, contractors, contingent workers, or other designations. If those

parties are not thoroughly investigated and kept under surveillance, they may pose a greater risk than the company's personnel [11].

The majority of organizations use behavior analytics as their main tool for keeping an eye out for insider threats. Although many cybersecurity programs have not yet grasped this relatively new field, it is important and has a lot of potential. However, insider threat necessitates a significant amount of non-technical oversight as well, for as through whistleblower programs, HR considerations, background checks and credit checks, etc. For a complete picture of insider risk, each of these needs to be taken into account and coordinated. Finally, a successful treat roadmap depends on the accuracy of well-defined use cases that specify precise goals for insider threat identification and response, including the people, process, and technology components and many mitigation programs seem to lack this [12]. Bellow the most common threat vectors are being presented [9].

Table 3 Threat Vectors

Attack Vectors	Description
Phishing techniques	Phishing is a method to manipulate people into disclosing sensitive information and frequently lead to threat actors gaining unauthorized access to networks or sensitive data.
Supply chain	This kind of attacks targets insecure vendor infrastructure with an ulterior motive to disrupt multiple organizations' business processes.
Internet of Things (Io & IIoT)	Internet of Things and Industrial Internet of Things devices like PLCs and HMIs frequently have legacy software and weren't built with security as their top priority.
Malware / Ransomware	Today's most widespread attack method, which is typically propagated by email attachments, infected infrastructure, infected web applications, etc.
Advanced Persistent Threats (APT)	One of the main characteristics of APTs is that they can remain undetected for an indefinite period while the victim is unaware of the infection. They are well-organized attacks with the goal of stealing strictly confidential information and are usually organized at the state level.

Mobile Security Threats	Mobile devices are widely used and contain sensitive information. A lack of structured Mobile Device Management program within an organization can result in data leaks.
Networking Threats	Botnets, viruses, warms, session hijacking, Man-in-the-Middle, sniffing, eavesdropping, spoofing, information gathering are some of the most used network vectors.
(Web) Applications Threats	The (web) application attacks include misconfiguration, input validation, buffer overflow, SQL injection, hidden field manipulation, and many others.
Cloud Threats	Many organizations are working on cloud transformation projects. However, a large number of attack vectors may allow malicious actors to gain unauthorized access to information.
Endpoint / Host Threats	Attack vectors that could affect a specific system include arbitrary code execution, privilege escalation, backdoor attacks, and unauthorized access.

2.3 Introduction to Threat Modelling

Threat modeling is a structured approach to identifying and mitigating potential attacks, threats, and risks in a system. It is typically used in the design phase of software development (SDLC Lifecycle) and/or risk assessments projects focusing on the understanding of the goals and motivations of adversaries when attempting to attack a system. IT also aims to shed light shed light on the security implications and the overall operation of a system (e.g., data flows). Threat modeling methods can be classified into various categories such as manual, automatic, formal, and graphical modeling. Formal modeling depends on mathematical models and graphical modeling can be structured based on techniques like attack trees, attack and defense graphs, or tables. Threat modeling can be used from both system evaluation and application development perspective, it helps to represent and analyze the system architecture, identify potential security threats, and select appropriate mitigation techniques. It is an industry accepted practice that assists the relevant stakeholders to identify and document potential security threats associated with a system / asset, providing a periodic and efficient approach for discovering strengths and weaknesses.
Threat modelling answers questions like:

- Where an organization is most vulnerable to attack?
- What are the most relevant threats?
- What actions are required for an organization to be secure from these threats?

Organizations can benefit from a threat modelling processing and create a view of their own operation. Benefits include, among others, the following [13]:

- It helps to identify and eliminate preventable errors, including software bugs, unpatched vulnerabilities, and misconfiguration.
- It reduces risk exposure by minimizing and mitigating vulnerabilities in the attack surface.
- It contributes to the validation and testing of existing security controls and systems.
- It provides leverage of the right tools, it empowers the organization to adapt faster to a constantly changing threat landscape, keeping pace where traditional risk management frameworks might fall behind.
- It identifies and eliminates bottlenecks, single points of failure, and ineffective controls/policies.
- Threat modelling can detect threats and potential risk early stage so that mitigations can be incorporated to reduce the findings during the penetration testing so that save the cost, time, resources in later stage of life cycle.

It’s easy to understand that a vulnerability that cannot be seen, and an attack that is not known could not be mitigated. Overall, these are the issues that threat modelling

addresses and therefore is important; as it promotes a deeper understanding of software and hardware systems, particularly from a risk perspective.

One valuable point that should be mentioned is that collaboration is required for a threat modeling project. taking under consideration perspectives of business-related people, engineers, adversary / defender as well as customer view. The major threat modelling steps that should be followed are the bellow [13]:

- Define the scope: Define if threat modeling will be conducted for a full system or for example a small design change. Decide which elements of the system will be part of the threat model.
- Identify all important assets: The aim of this step is to includes all relevant parts of the system. Primarily, a top-level description of the system is conducted and consequently the process is being repeated for more detailed views of smaller parts.
- Draw diagram(s): Diagrams of the system are made based on the scope. They should at the very least cover the system's users (users, administrators, operators, etc.), how they interact with it, browsers, desktop clients, servers, load-balancers, firewalls, and other related items. The team shall determine that the diagram accurately depicts the system's component parts once it has been created.
- Draw dataflows: Visualize the interactions as data flows between the components. Provide information on the protocol version, the authentication method, etc. Include questions such as:
    - How do each of the components communicate? (What protocol is in use for each data flow?),
    - Who stores what and where? (For example, what is stored in the DB?), What are the authentication and authorization checks in place for each data flow?
    - In what order do they occur? What is exchanged in each data flow (what information does it have?
    - What is the purpose of the request/response? What type of data is it? Example: credentials, authentication, HTML).
- Mark the areas where crucial data resides, flows, and transforms: Detect which data should be protected and where it appears in the system.
- Define security requirements: Assess the security requirements that the system has implemented.
- Identify threats: Based on the context that has been created from the previous steps identify the threats.
- Mitigate Threats: Create effective response mitigation plans for the identified threats and validate that those have been mitigated.

The output, a threat model, is a document that should be appropriately stored so that only authorized stakeholders have access because it is a document that reflects the

present situation of the organization and malicious actors can advantage of this information. Once several findings have been identified and the relevant team cannot come up with additional findings, these need to be assessed and mitigated by priority. The process is only complete if these findings are mitigated.

There are several well-known and effective threat modeling methods that can be used to assess and manage threats [14].

- STRIDE: Microsoft created this method, which stands for Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege. This method entails identifying and categorizing each potential threat, as well as determining the impact of each threat on the system.
- PASTA (Process for Attack Simulation and Threat Analysis): Using this technique, the system's boundaries are defined, prospective threats are found, and attacks are simulated to see how they might affect the system. The PASTA approach offers a thorough framework for comprehending a system's attack surface and risk mitigation.
- Trivy This threat modeling tool employs automated techniques to find potential security holes and threats in a system. Rapid and effective threat assessments, the identification of key risk areas, and the prioritization of mitigation activities may all be done with Trivy.
- VAST (Visual, Agile, and Simple Threat modeling): Visual diagrams and flowcharts are used in the VAST method to describe the system architecture, identify potential risks, and assess the impact of each threat. The VAST approach is a common option for organizations that must quickly assess and reduce cybersecurity risks because it is easy and uncomplicated in design.
- S-TAM (System-Theoretic Accident Modeling): S-TAM (System-Theoretic Accident Modeling): Using this technique, the system is fragmented into a complex network of interconnected parts. The S-TAM technique models the relationships between components and assesses the potential effects of threats on the system using system dynamics and graph theory.

The table below depicts the different threat domains that are taken into consideration pursuant to the STRIDE methodology which will be further analyzed in the next chapter, as the proposed threat modelling methodology.

Table 4 STRIDE Overview

STRIDE Domains	Security Principle	Definition	Examples
Spoofing	Authentication	Masquerading as an entity or individual	Spoofing a website, ARP Spoofing, DNS spoofing, Ip spoofing, Voice spoofing.

STRIDE Domains	Security Principle	Definition	Examples
Tampering	Integrity	Code or data alteration	Deleting, files, altering log files, changing configurations, planting false information.
Repudiation	Non-repudiation	Denying involvement in an action	Counterfeiting digital certificates, Digital signature forgery, Email interception.
Information Disclosure	Confidentiality	Unauthorized disclosure of information	Unsecured data storage, information leaking, unsecure data transition, inadequate access control, e-mails to false recipients.
Denial of Service	Availability	Disrupt legitimate users to access services	Ping, SYN, HTTP, UDP flood attacks, smurf attack.
Elevation of privilege	Authorization	Acquiring capabilities without appropriate permission	Privilege escalation, unauthorized access to sensitive information, installing software without admin permissions.

2.4 Implement Threat Modelling

This chapter provides guidance for implementing threat modelling, based on the STRIDE methodology and recommended best practices [15]. The first step that the organization needs to organize is a collaborative approach. All the relevant stakeholders from different teams and different perspectives shall be included in the whole process. Project managers, cloud, network, and security engineers, among others, could be some of the stakeholders. The next and equal important step is to define the scope of the threat modeling process. One of the most common objectives is a new feature in a critical application or a new infrastructure component. The next step is to model the information that is being discussed in the workshops with the relevant teams. Data Flow Diagrams (DFDs) that present all the applicable layers (e.g., system layer, process layer) needs to be developed and depict all the required information. The information shall represent how the system and its component interact with each other in order to function. DFDs can be created with various methods like diagrams tools (e.g., Microsoft Visio, Draw.io) but also specific application such as

OWASP Threat Dragon and Microsoft Threat Modelling Tool. Consequently, with the use of the STRIDE Methodology, the applicable threats must be recognized when the under-examination issue has been closely investigated. The threats that are most frequently covered through the domains of the STRIDE Methodology are shown in the table 5 [16]. It should be highlighted that this table is not exhaustive, and all relevant stakeholders should come up with additional potential threats. Accordingly, the countermeasures need to be determined. Once more, the table below lists some possible countermeasures that correspond to the dangers that have been discovered based on best practices. The final step is to validate that the threats have been adequately identified and countermeasures are planned to be implemented. The organization must explicitly outline the timeline for implementation and document all the countermeasures that will be used. Consult the table below for the aforementioned steps.

Table 5 STRIDE Methodology Attacks & Countermeasures

STRIDE Domains	Security Principle	Common Threats	Examples	Countermeasures
Spoofing	Authentication	Spoofing an identity.	Phishing attacks, Impersonation attacks, social engineering.	Methods for authentication including passwords, tokens, and biometrics or other identifiers. A comprehensive process for managing new additions, departures, and changes within the system.
		Spoofing a 'file' on disk.	Generating a file within a local folder, modifying the link prior to user access, and generating a fake file in the anticipated directory.	Complete file paths, verifying access control lists, and confirming that pipes are correctly established.
		Spoofing a network address.	ARP spoofing, IP spoofing, DNS spoofing, IP redirection.	DNSSEC, HTTPS, IPses, access control lists (ACLs), authentication protocols, such as CHAP or MS-CHAP.
		Spoofing a program in memory.	Obfuscation & steganography techniques.	Data Execution Prevention (DEP) and Address Space Layout Randomization (ASLR) technologies, anti-malware software,

STRIDE Domains	Security Principle	Common Threats	Examples	Countermeasures
				isolation techniques (e.g., sandboxing and virtualization).
Tampering	Integrity	File alteration.	Link redirection, file modification, Remote code execution attacks.	ACLs, Digital Signatures, Keyed MACs, private directory structures, regular backups, system monitoring, file integrity monitoring tools, encryption, network segmentation.
		Memory Tampering.	Altering the code that is currently executing, tampering with data input an application programming interface (API), Injecting malicious code into running programs, Inserting malicious code into data inputs.	ACLs, Secure Development Lifecycle (SDLC) process, runtime application self-protection (RASP) or application shielding techniques to monitor and protect running code from tampering.
		Network packets tampering.	Traffic redirection to the malicious actors' machine, modify traffic flowing over a network.	HTTPS, IPsec, Network isolation, Virtual Private Networks (VPNs) or Secure Shell (SSH) tunnels, Domain Name System (DNS) security techniques (e.g., DNSSEC), network intrusion detection and prevention systems (IDS/IPS).

STRIDE Domains	Security Principle	Common Threats	Examples	Countermeasures
Repudiation	Non-Repudiation	Insufficient log analysis.	Modification of log files or and deletion	Log analysis and monitoring tools, Security Operations Center services
		Insufficient protection of log analysis.	Tampering logs by inserting false or misleading information.	Access controls and authentication mechanisms, Security Information and Event Management (SIEM) Systems, log backup and retention policies.
Information Disclosure	Confidentiality	Network sniffing.	Database exploitation, Man-in-the Middle attacks, Understanding network connections through DNS analysis.	Secure File Transfer Protocol (SFTP), avoid public WIFI, implement guest networks.
		Data source exposure.	Database exploitation, misconfigured cloud storage, unprotected shared files, inadequate security for IoT devices.	Encryption, access control, security configuration for cloud storage and APIs.
		API information disclosure.	Accessing API data without proper authentication.	Enforce strict API permissions, implement encryption for data in transit & rate limiting, monitor API activity.

STRIDE Domains	Security Principle	Common Threats	Examples	Countermeasures
Denial of Service	Availability	Network flooding.	Network resource exhaustion.	Implement load balancing, content delivery networks (CDNs), firewalls, SIEM.
		Program resource flooding.	Overwhelm memory, Overwhelm CPU, excessive requests.	Efficient resource utilization, Efficient resource utilization.
		System resource flooding.	Overloading data storage, High CPU utilization, Excessive demand on memory.	Implement load balancers, throttling incoming requests for example limite the number of requests that can be made per second.
Elevation of Privilege	Authorisation	Data / code confusion.	Tampering with code execution, Unvalidated input injection.	Implement prepared statements or stored procedures in SQL, clear separators with canonical forms, code signing, input validation.
		Control flow / memory corruption attacks.	Gaining access to read or write memory inappropriately.	Adopt coding techniques in type-safe programming languages like Java or C#, use modern operating system sandboxes, implemented modern operating system memory protection facilities, creating

STRIDE Domains	Security Principle	Common Threats	Examples	Countermeasures
				separate accounts for each application or function and don’t use a generic "nobody" account.
		Command injection attacks.	SQL injection, script injection, code execution.	Encoding and escaping techniques, use libraries and frameworks that have been previously tested and proven to be secure and able to reduce the risk of command injection attacks, run applications with the least amount of privilege.

3. Understand Dependencies

Dependencies are relationships of reliance within and among assets and systems that must be identified with a view to proactively mitigate potential impacts. An organization's email server, for instance, might be dependent on a certain kind of hardware or software, which in turn might be dependent on a particular kind of operating system or data storage system. The entire email system, as well as the underlying hardware and operating system, may be compromised if a vulnerability in the email server software is found. Furthermore, the email server's critical data storage could potentially be under risk.

Critical business processes are usually dependent on systems and organization are often able to recognize those critical cyber processes. Organizations, however, might not be aware of the multiple nodes/components that those vital cyber services rely on [17].

Dependencies can be one-directional or bi-directional (that are also known as interdependencies) and may traverse organizational or geographic boundaries as described later on this chapter. Managing asset dependencies in cybersecurity is a critical aspect of protecting an organization's posture. By understanding and actively managing these dependencies, potential threats from one asset to another can be identified in order to minimize the impact of potential security incidents. It is important to note that dependencies extend beyond just physical connections between assets and systems [18]. All different types of independencies shall be considered. The types of independencies are the followings [18] [19]:

- Physical: The type of interdependency can be defined according to the Layer 1 of OSI Model. It is one of the most easily dependency type that can be identified as it is responsible for the actual physical connection between nodes. On the contrary, the cascading impact of physical connected nodes can be high.
- Cyber: The type of interdependency when a node relies on IT and communication systems to operate.
- Geographic: The type of interdependency when multiple nodes can be affected due to similar hazards or a single disruption.
- External: The type of interdependency when an organization use specific services provided by third parties. A typical example are software vendors.

The following figure depicts how threats can affect assets and create impact. Three different impact categories have been identified: direct, synergistic, cascading [18].

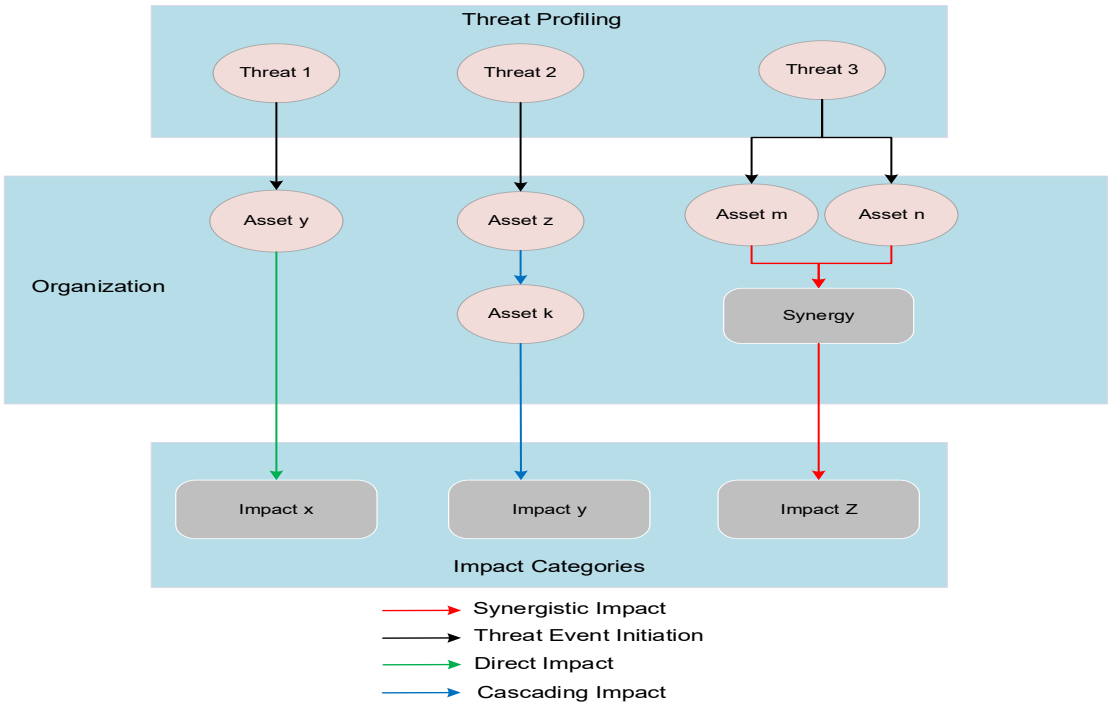


Figure 4 Model of Cascading Threats & Impact

3.1 Calculating & Visualizing Dependencies

To manage the dependencies as described in the previous chapter organizations shall have a thorough awareness of the linkages and relationships among their assets. This understanding will help to the creation of dependency matrices in an attempt to identify and manage the potential risks associated with a system's architecture. Additionally, potential single points of failure or weak links in the system can be found for example, if a critical application relies on a specific component (e.g., software library, database) the dependency graphic can help to pinpoint the potential risks associated with the failure of that component. It is recommended that the key components of a risk assessment project to include dependency matrices and the linking of assets with business processes. Consistent asset mapping and inventorying can help with the previously describes actions. The identification of potential vulnerabilities and dependencies can also be aided by regular security assessments and penetration testing. Additionally, incident response teams need to be knowledgeable about how various organizational systems interact with one another. They ought to be capable of promptly identifying and prioritizing critical systems and dependencies, as well as creating and putting into practice efficient plans to reduce the risks these dependencies pose.

The proposed methodology for the visualization of dependencies is part of the overall methodology that is presented in this research in order to manage cascading threats. First, after a thorough analysis of various data visualization methods, the most suitable ones were selected and assessed with test data. The Microsoft Power BI tool

was adopted and the chart that were selected are the Sunburst Chart and the Decomposition Tree.

Sunburst Chart is ideal for presenting Hierarchical data. Each level of the hierarchy is represented by one ring or circle with the innermost circle as the top of the hierarchy [20]. It has been selected due to its hierarchical structure, as the user is able to identify assets and dependent assets. The figure bellow depicts a test scenario with assets and their dependent assets along with the dependency value that is subsequently described.

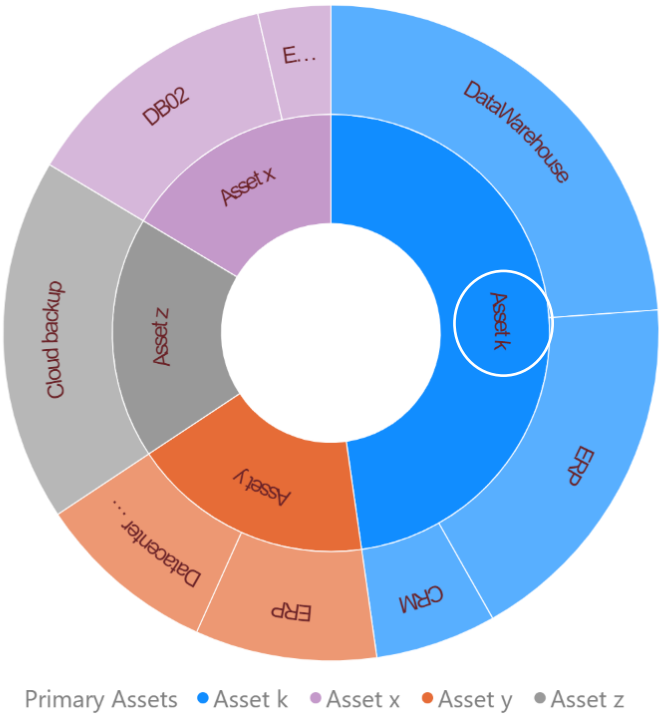


Figure 5 Sunburst Chart

This chart also offers the functionality where users can click on each asset and analyses their dependent one, as shown in the figure below.

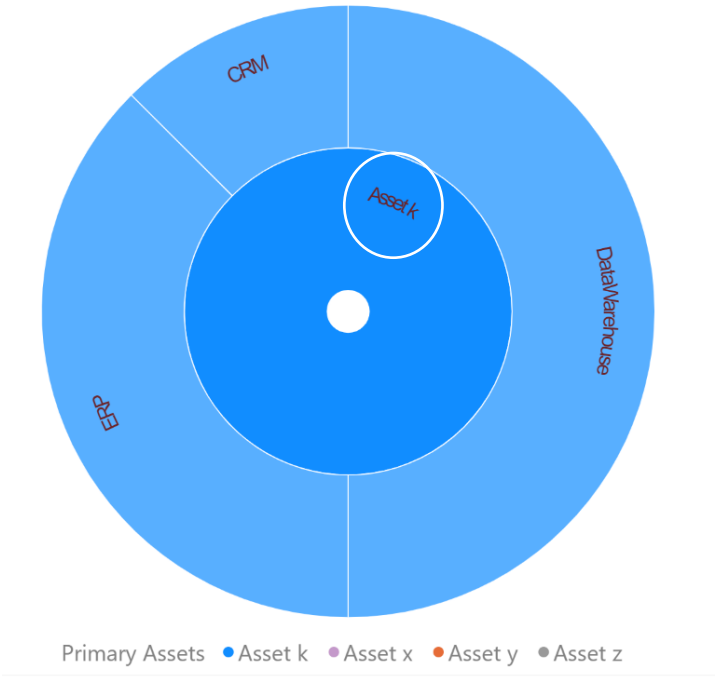


Figure 6 Sunburst Extended Functionality

The second diagram that was used, as it was previously aforementioned, is called Decomposition tree [21]. It can support multiple levels and this diagram could be useful also during the threat modelling process. Again, this visualization was tested with the same test data and is presented in the following figure.

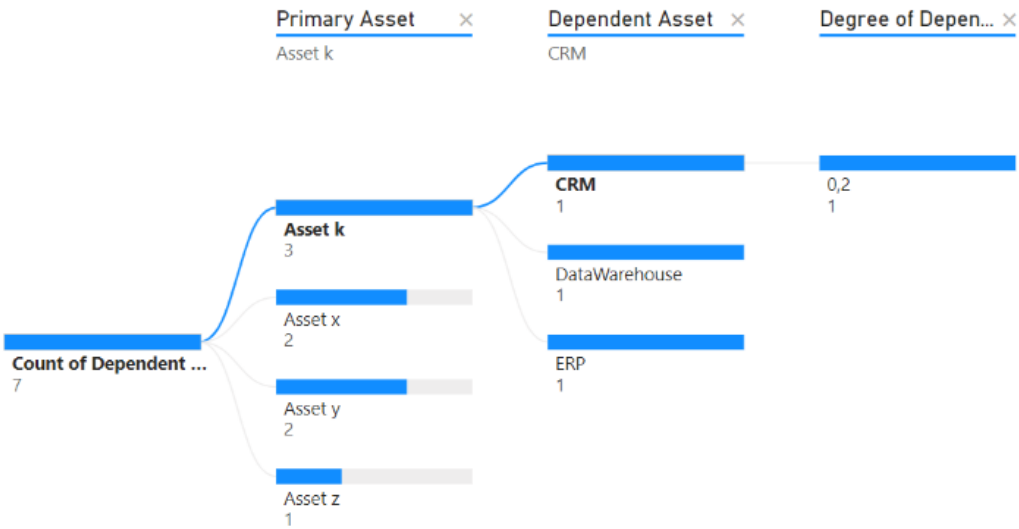


Figure 7 Decomposition Tree

As we can see this visual in Power BI offers data visualization across multiple dimensions. It automatically aggregates data and enables drilling down into multiple components in any order. This can help to identify the whole dependency path of an asset. Decomposition trees are also ideal to model data when multiple tables exist. In the scenario that is presented below, except from the dependency model, the threats

of the assets have been included in the visualization. But before moving to the creation of the visual, the table's relationships need to be managed, as show in the figure 9. In this scenario three different tables exist, the first one is the table with dependency information and the other two contain information with the threats. The Threat table (Threats_Assets) could be the result of the threat modelling process that was previously presented.

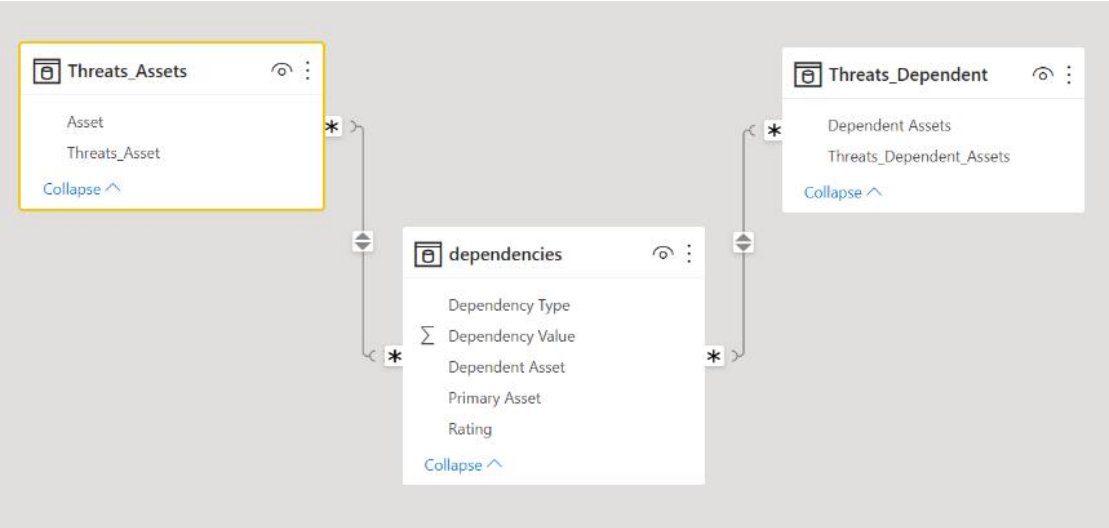


Figure 8 Table Relationships

The output of the tables' relationships is presented in the following figure.

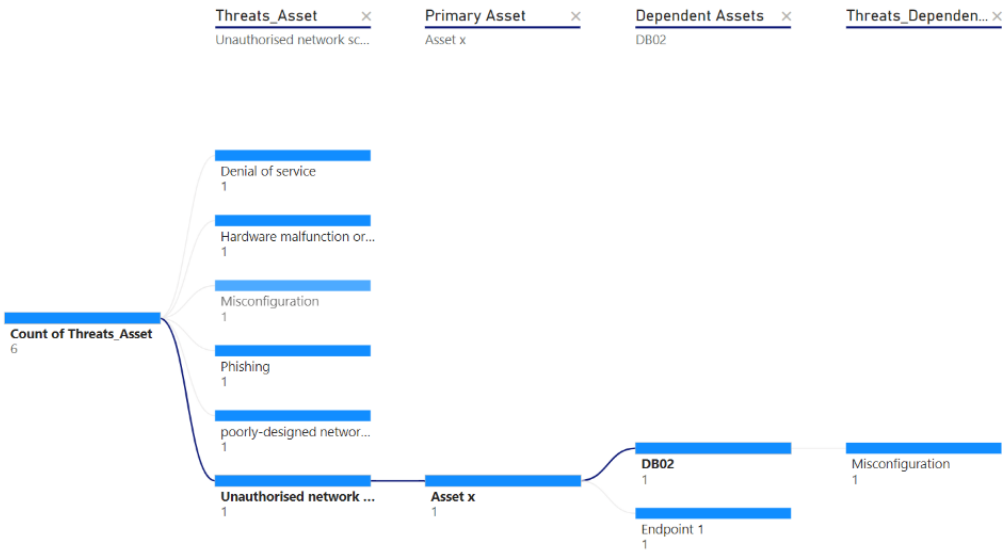


Figure 9 Decomposition Tree with Threats

It should be noted the scenarios that were used above are for indicative purposes of the functionality of the tools and potentially multiple scenarios and analyses can be

created. But when assessing cyber dependencies, it is not sufficient to only visualize those data. Therefore, a methodology should be followed in order to assess the overall dependency risk of an organization's assets. This will help practitioners to identify the assets with the highest dependency risk and accordingly prioritize and monitor those assets. A methodology is being proposed based on literature review and any additional changes deemed necessary. Three different variables have been identified to calculate the overall dependency risk [18].

- Criticality of dependent assets: There are several levels of criticality that by extension modify the impact of a cyberattack. It should be noted that the impact table is not something than can be horizontally created and each organizations needs to define and formally approve a different instance. Short-term interruptions, a decline in quality or integrity, or the failure of a cyber dependency can all be brought on by potential threats, including unacceptable physical phenomena. The criticality of the assets that would be lost or deteriorated as a result of the potential threats which will affect the dependent asset should be measured when estimating the dependency risk. The practitioner can evaluate the level of criticality in a range between 0-1 with the highest criticality level being indicated by a score of 1, and the lowest by a score of 0.
- Degree of dependency: There are several levels of cyber dependence. A dependency is considered high if the primary asset directly contributes to the failure of its dependent asset and as result a critical cyber service or of a business process is being interrupted. The dependency is medium if primary asset's failure forces the organization to implement its backup plans or other procedures (e.g., replace the dependent asset). The dependency is low if the organization can maintain operations even without the dependent asset. Similarly, this variable is not being calculated with a qualitative value, instead a number between 0-1 is being assigned upon the degree of dependency.
- Control Strength: The term of control strength and how this is calculated will be presented in chapter 4. Now, practitioners can utilize the result of the control calculation to assess the overall dependency risk of a system or a particular asset. The range of the control strength value is 0 to 1, with 1 denoting the highest level of control and 0 denoting the lowest amount of control. In contrast, a score closes to 0 suggests that the organization has few safeguards in place to lessen the effects of unfavorable incidents. A control strength value near to 1 shows that the organization has strong safeguards in place to prevent adverse events from damaging the system. A system's overall dependency rate can be determined by considering the control strength, which has a major effect on the impact and degree of dependency.

The calculation of the dependency risk is based on the 3 variables that were described above. Consequently, the picture bellow depicts the calculation formula.

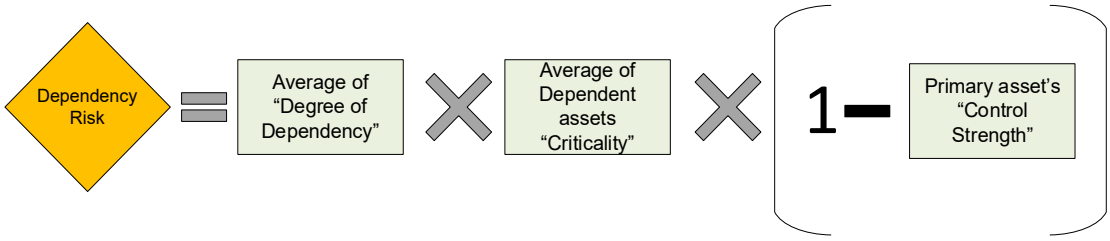


Figure 10 Dependency Risk Calculation

This dependency risk calculation provides an overview of the risk based on the calculation of three variables as described and illustrated above. The overall dependency risk will be in the range of 0 to 1, with values close to 1 indicating that if an asset's dependency risk is high, its dependent assets are more likely to be impacted with a higher impact in the organization. Above 2 different tables are presented in order to provide further guidance regarding the assignment of values at the "degree of dependency & the "criticality of dependent assets" variables.

Table 6 Dependency Risk Reference Table

Value Range	Dependency risk	Description
0 - 0.24	Negligible	A non-critical website outage, a non-essential software bug, a minor delay in receiving/providing non-essential supplies or equipment. All these examples will bring minor legal or compliance issues that do not result in fines or penalties.
0.25 - 0.49	Low	A temporary disruption of a non-critical service, a minor hardware failure, a delay in receiving/ providing critical supplies or equipment, a temporary loss of access to non-critical data. All these examples will bring minor legal or compliance issues that do not result in fines or penalties but will causes a slight impact on customer satisfaction or reputation and to the continuity of the business processes of the organization.
0.50 - 0.74	Moderate	A temporary disruption of a critical service, a moderate hardware failure, a delay in receiving/ providing critical supplies or equipment, a temporary loss of access to critical data, a temporary loss of internet connectivity. These examples will result in significant fines or penalties for moderate legal or compliance violations, as well as prolonged service interruptions that have a notable

Value Range	Dependency risk	Description
		negative impact on consumer satisfaction or reputation and to the business processes of the organization.
0.75 - 1	High	A major hardware failure, a prolonged delay in receiving/ providing essential supplies or equipment, a permanent loss of access to vital data, a major cyber-attack, a major natural disaster, the loss of critical services, such e-banking, are all examples of events that could cause a high dependency risk. This dependency risk will lead to severe reputational damages brought by the preceding examples that seriously affects clients or the public. Severe compliance or legal difficulties that bring up stiff penalties, punishments, or legal action will come up along with severe business interruptions.

Table 7 Criticality of Dependent Assets Reference Table

Value Range	Criticality Level	Impact
0 - 0.24	Negligible	The asset has negligible or minimal impact on its function. The loss or degradation of the asset would not significantly affect the overall organization's ability to function.
0.25 - 0.49	Low	The asset has a minor impact on the non-critical operations of the organization. The loss or degradation of the asset may cause some disruption or inconvenience, but the organization would be able to continue functioning with available resources without the need of recovery, continuity, or backup plans.
0.50 - 0.74	Moderate	The asset has a significant impact on operations. The loss or degradation of the asset would cause substantial disruption to the organization's ability to function and provide services to clients or any affected parties, and additional resources may be required to restore operations (e.g., additional hardware resources).

Value Range	Criticality Level	Impact
0.75 - 1	High	The asset has a high impact on the critical operations of the organization. The loss or degradation of the asset could cause a severe disruption to the organization's ability and as a result customers or any affected partis which might have a range of adverse effects. As a result, urgent actions are required to restore operations.

Table 8 Degree of Dependency Reference Table

Value Range	Degree of dependency	Description
0 - 0.24	Negligible	The asset depends on other systems or assets only to a limited extent, which means that it has fewer interconnections to other assets and may operate independently with little interference from other failures.
0.25 - 0.49	Low	The asset depends on other assets or systems to a low extent, demonstrating some degree of interdependence, but it is still capable of operating independently with little negative impact from other failures.
0.50 - 0.74	Moderate	The asset has a moderate dependency on other assets or systems, which means it is linked directly to other assets or systems and is potentially vulnerable to other failures while still being somewhat functional.
0.75 - 1	High	The asset is critically dependent on other assets or systems, meaning that without these other components, it may not be able to function at all. This dependency indicates that the asset is substantially dependent on other assets or systems to function.

To sum up, it has been discussed how to calculate and define the degree of dependency and the dependent asset's criticality. In the next chapter the method for the calculation of the control strength is being presented.

4. Calculating Control Strength

Control Strength is an important variable for the identification of the cascading threats and consequently the calculation of dependency/ cascading risk. Cascading threats from on asset to another cannot be calculated without a thorough understanding of the state of the controls. The proposed methodology is based on The ISF Quantitative Information Risk Assessment (QIRA) Methodology which is a five-phase process that aids in the evaluation and management of information risk by risk practitioners. QIRA offers instructions on how to do all steps of a comprehensive information risk assessment, including defining, calculating, modeling, and reporting information risk [22], but our focus is the calculation of control strength. According to QIRA control strength is calculated with the following expression: *Relevance X Implementation = Control strength* [22]*.* This formula has been modified to include the effectiveness of the control which is considered important too [23].

Table 9 Control Strength Calculation

Threat	Control ID	Relevance		Implementation		Effectiveness		Control Strength
SQL Injection	C1	100%	✖	75%	✖	75%	=	**56%**
	C2	75%		75%		50%		**28%**
	C3	75%		50%		50%		**28%**

After the above-mentioned modification, the formula for calculating Control Strength is:

*Control Strength[i] = Relevance[i] * Implementation[i] * Effectiveness[i] Where i represents the i-th control.*

Measurements should be assigned as a percentage (%), ideally in a range (e.g., a control is 40%–60% relevant) or between 0-1 (e.g., 0.45=45%). Some practitioners use a binary viewpoint in which a control is either completely vulnerable or completely successful in stopping threats. Binary calculations are less flexible than percentage calculations because, for instance, control relevancy on a scale of 1 to 5 can be 3 or 4, not 3.7. Instead, this flexibility is provided by percentage computations.

This formula provides insights about how well or not a control functions against a specific threat. But usually, to address a specific threat multiple control are combined, and the effectiveness of these controls cannot be identified with this equitation. The equitation needs to be modified in the following manner. Firstly, Aggregated control strength for a given threat event, X, can be calculated by using the following formula:

*Aggregated Control Strength[X] = (SUM(Control Strength[i] * Relevance[i]) where i = 1 to n) / SUM(Relevance[i]) where i = 1 to n*

The i represents the i-th control, n represents the total number of controls in scope for threat event X, and SUM() represents the sum of the values within the parentheses.

In this way controls are assessed based on their relevance and a new “Weighted Strength” variable is being created. Then the sum of this new variable is being multiplied against the sum of the relevance variable. Aggregated control strength calculation is depicted illustratively in the following picture. The picture does not depict the “Effectiveness” field as it is not taken under consideration in the QIRA methodology and is an additional amendment. The only difference is that with our approach “Control Strength” is being calculated against three variables and not two.

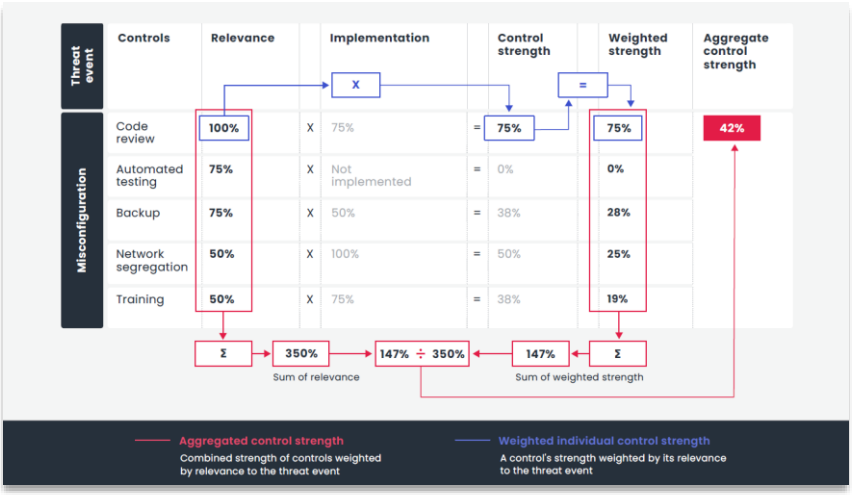


Figure 11 Aggregated Control Strength Calculation

Source: ISF QIRA Methodology

To summarize, the process that is described above can be outlined in 4 steps as follows:

- Identify the controls that are within scope and relevant for the loss event.
- Multiply the control strength by the control’s relevance.
- Sum this score together for all the controls.
- Divide the figure produced by the sum of the control’s relevance.

The final score reflects the aggregated strength of the implemented controls against the threat event. However, assets usually are not fully (100%) protected, so the inverse of this score is the extent to which the control does not protect against the threat event to which it is mapped (e.g., control strength of 75% has a corresponding 25% control-gap) [22]. It is important to note that is weighted aggregation by the control’s relevance values provides better results than an arithmetic approach. An arithmetic approach would produce the following result:

*(Sum of Controls' Strength) / (Number of Controls) = 75%+0%+38%+50%+38% / 5=**40%***

*versus the **42%** that was calculated with the weighted approach.*

This result does not reflect a real use case and it is outlined that the weighted approach is considered more comprehensive and representative.

5. Monitoring Cascading Threats

Key Risk Indicators are statistics or measurements that can provide a perspective of an organization's risk position [24]. These indicators usually represent the impact on organizations, are specific and measurable. In some cases, they might stand in for important ratios that management monitors - across the entire organization - as signs of evolving threats and prospective opportunities, which indicate the necessity of taking actions. They are designed to offer a proactive approach and contribute to the creation of a forward-looking strategy. As a result, they help in identifying and monitoring areas of risk in order to prioritize actions and develop effective mitigation plans. All KRIs shall have a fixed threshold, based on the needs of the organization, as a minimum requirement. There are many KRIs that could be utilized in the context of cybersecurity and cascading threats, and a few of them are listed below.

- Percentage of successful cyber-attacks: This KRI measures the number of successful cyber-attacks against an organization's systems and applications (assets) as a percentage of the total number of attempted cyber-attacks. The higher the percentage indicates that the organization needs to implement more security measures.
- Average incident detection time: This KRI calculates the time taken to detect a security incident from the moment it occurred. In consequence organizations can assess their ability to timely detect and respond to security incidents. A low average time proves that the organization has a robust monitoring strategy and detection capabilities. On the other hand, a high average time is a sign for potential improvements in the monitoring strategy.
- Average Incident closure time: This KRI estimates the time taken to fully resolve a security incident from the moment it is detected. As a result, organization understand how capable they are to effectively manage and resolve incidents. Thus, a low average pinpoints that the organization has efficient incident response procedures / policies. However, a high average must trigger corrective actions to the incident response framework.
- Percentage Successful backups: This KRI demonstrates the success rate of data backup processes. Therefore, the reliability of an organization's backups is being assessed. The higher the percentage the safer the (critical) data of an organization.
- Percentage of corrective actions with overdue status: This KRI evaluates the number of corrective actions that have not been completed within the specified timeframe. A high percentage suggests that the organization needs to immediately address those corrective actions to enhance its cybersecurity posture.
- Percentage of privilege users (in-house & outsourced personnel): This KRI designate the number of personnel who have elevated privileges within an

organization's IT systems. Hence, organization can evaluate the need of those privileges of the average number is too high.

- Percentage of End-of-Life systems: This KRI shows the number of systems within an organization's IT infrastructure that have reached the end of their product life cycle and/or are no longer supported by their vendor (e.g., security patches). Correspondingly, the organizations will become aware of its own infrastructure condition and if the percentage is high, essential actions, such as replacement, shall be done.
- Percentage of changes in IT production that was classified as “emergency”: This KRI quantifies the number of changes made to an organization's IT production environment that are flagged as "emergency" changes. Organization thereby, are able to assess their change management framework. Changes that are being classified as emergency are usually done out of the normal change management process (unscheduled changes) and if the percentage is high, this can lead to inconsistencies and inefficiencies to the change process.
- Percentage of Critical IT audit findings: This KRI counts the number of critical findings identified during IT audits. Critical finding may relate for example to security vulnerabilities, compliance violations, inadequate controls and can pose significant impacts, and other significant risks, ergo they must be prioritized and promptly mitigated.
- Number of non-active users: This KRI displays inactive users that have not logged in to the Privilege Access Management (PAM), Active Directory (AD) or other similar solution for a period of time that may range from one to two months dependending on the organization’s policies. Accordingly, it is useful to trach the total number of active users, too.
- Service / system availability: This KRI is particularly useful to track Service Level Agreements (SLAs). It could be measured as an output of the total system, downtime <time period> with the total of system runtime during <reference period>.
- Percentage of privileged accounts with an expired password: This KRI helps to assess risk level, as this percentage rises the risk of password leakage grows. Calculating the proportion of privileged accounts on an identity solution with an expired password is considered very important.

Supplementally organizations could benefit from benchmarking data to compare with relevant peers. Organizations can better understand their entire security posture and enhance their cybersecurity strategies by comparing metrics of other similar organizations within their field. As a result, the organizations can proactively detect possible vulnerabilities and take action to stop cascading attacks before they happen.

#	Metric Description	Implementation Evidence	Frequency	Formula	Goal	Tolerance	Answer A	Answer B	Answer C	Outcome	Gap	Comments
1	Percentage of incidents that affected more than one assets.	A. How many incidents did the organization face in the reference year? B. How many of the aforementioned incidents affected more than one assets?	e.g., Annually	(B/A)*100	100%	10%	5	4		80.00%	20.00%	
2	How many assets are dependent to other assets in order to function?	A. How many assets have been identified? B. Of which, how many assets are not dependent to other assets? C. Number of assets that are dependent to other assets.	e.g., Annually	[C/(A-B)]*100	100%	10%	10	4		40.00%	60.00%	
3	Percentage of vulnerabilities that have been remediated within the reference year?	A. How many vuknerabilities have been identified within the reference year? B. Of which, how many vulnerabilites have been remediated?	e.g., Annually	(B/A)*100	100%	10%	100	50		50.00%	50.00%	

Figure 12 KRIs Example

For demonstration purposes an example of KRIs has been created using Microsoft Excel. The KRIs that were selected address cascading threats. The first and the second column describe the Metrics. The other columns highlight crucial factors that should be taken into account, such as frequency and the intended goal of the metric. Subsequently, one of the most important columns is the “Formula” one as it describes how the metrics will be calculated. This formula is based on the user's answer and the initial fixed tolerance that needs to be established from the practitioner.

6. Defend Against (Cascading) Threats (IT)

Organizations must establish efficient risk management and mitigation techniques as a means to anticipate and respond to cascading threats. Risk assessment, which entails identifying and analyzing potential risks that could have a negative impact on the business, is one of the major components of a cybersecurity strategy. This procedure ought to be continual / periodical and should take into account both internal and external elements, such as shifting economic situations, emerging technologies, and world politics (if applicable). Contingency planning is a crucial component of cascading threat preparation. This entails creating an action plan that can be promptly put into place in the case of a disaster. The plan should specify the duties of key employees, the channels of communication, and the steps to activate the plan. To ensure the plan's efficacy and applicability, it should also be evaluated, tested, and updated on a regular basis. Businesses facing cascading threats must also be able to communicate effectively during times of crisis. This entails promptly and clearly informing shareholders, consumers, and other important parties about the issue and the steps being taken to handle it. Thus, comprehensive communication plan includes also the key escalation point within the organization. To preserve confidence and limit reputational and/or economic harm (ref. GDPR fines), transparency, honesty and timely notification are necessary. Similarly, risk management in the supply chain is among the best practices to predict threat from vendors. This entails recognizing and minimizing potential supply chain interruptions including natural catastrophes, political unrest, or cyberattacks. To lessen their exposure to supply chain risks, organizations might use risk mapping, supplier appraisals, and supplier diversification, vendor assessment & vendor monitoring / auditing. By doing this, organizations can guarantee the availability of the supplies required for their operations and reduce operational disruptions. Business continuity planning is an additional best practice. This entails creating a strategy to guarantee that essential corporate operations can continue both during and after a crisis. This may entail identifying and prioritizing critical business processes, creating back-up plans, defining Recovery Time Objectives (RTO) / Maximum Tolerable Period of Disruption (MTPD), Recovery Point Objectives (RPO) and putting the plan through testing to make sure it works. Organizations can reduce the effects of cascading risks on their operations and guarantee that they can keep delivering goods and services to customers by putting in place a continuity plan. Another crucial best practice is employee education and awareness. Employers should instruct their staff on cascading threats and how to handle them. This may entail offering instruction in crisis communication, business continuity planning, and emergency procedures as well as compliance standards / regulations. Organizations can ensure that their staff members are ready to respond to cascading hazards and minimize their effect on the company by educating them. Systematic monitoring and early warning are also essential best practices. Systems / software solutions for monitoring possible threats, such as (Distributed) Denial of Service attacks (D)DoS

and providing early warning of potential crises shall be in place. This can involve utilizing early warning systems (SIEM) offered by the external companies, social media monitoring, and data analytics. Organizations can prevent possible dangers from having a negative impact by simple monitoring them and giving the appropriate alerts. A recommended practice that can assist organizations in preparing for and responding to cascading threats is collaboration and partnerships. To exchange information and resources about cascading dangers, organizations should develop alliances and work together with other groups, including other enterprises, governmental bodies, and non-profits. Organizations that cooperate in tandem can take advantage of one another's resources and knowledge to better prepare for and respond to cascading risks. By putting these tactics into practice and focusing on a program that highlights the security in terms of people, processes and technology organization can achieve a high level of cyber resilience.

One of the state art cybersecurity architectures that the organizations need to implement is the Zero Trust Architecture (ZTA). ZTA is based on three principles:

- Verify explicitly: check everything and take decision considering multiple variables.
- Use least privilege access: Follow a just-in-time and just-enough-access (JIT/JEA) approach.
- Assume breach: Do not trust anything / anyone and always assume breach.

The idea behind the cybersecurity paradigm known as "zero trust" is that trust is never given automatically but rather must be constantly assessed. In the past, organizations (and enterprise networks generally) have concentrated on perimeter defense, and once an identity has been authorized, they are granted access to a wide range of resources on the internal network. Unauthorized lateral mobility within the environment has therefore been one of the main problems for government organizations [25].

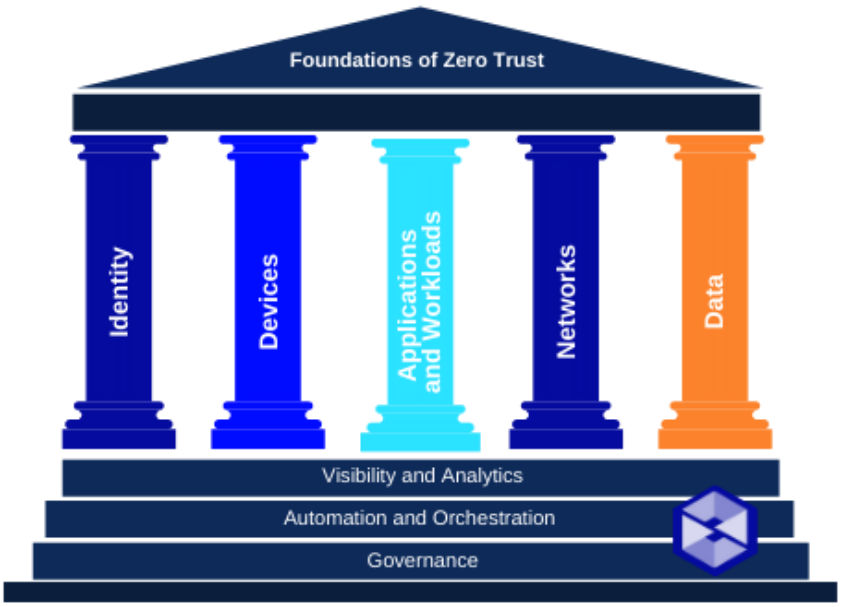


Figure 13 CISA Zero Trust Architecture

The idea behind the ZTA architecture is those pillars as displayed above. The 'Identities' are considered not only users but also other attributes that should be continuously evaluated to gain access to the resources. Some possible examples to validate identities' security are behavior-based authentication and multi-factor authentication (MFA). The "Devices" or better known as "endpoints" are the hardware that needs access to resources and should be assessed, inter alia, with compliance mechanisms (e.g., operating system version). The "Applications and workloads" cover tasks or services provided by systems living in on-premises or in the cloud environment. The preservation of "Data" is regarded as a vital component for almost every organization; thus, its absence would be deemed unacceptable in a ZTA architecture. Data Loss Prevention Systems (DLP), Digital Rights Management (DRM) are some of the security techniques that can be implemented. Following the previously mentioned categories, it is crucial to monitor performance and behavior, as well as sensor and telemetry data, and establish an activity baseline, all of which fall under the category of "Visibility and Analytics". As a result, organization can detect unusual activity and enable real-time access control adjustments. Indicatively, SIEM, event monitoring tools, Unified Access Management (UAM) can be used to enable visibility and analytics capabilities. The final pillar "Orchestration / Automation" aims to promote a comprehensive and timely assessment of threats through for example, Security Orchestration, Automation, and Response (SOAR) solutions which extracts actionable insights from diverse security tools across an organization, allowing for automated responses and the accomplishment of a thorough and prompt evaluation of threats [26].

The core Zero trust logical components are considered the Policy engine (PE), Policy Administrator (PA) and the Policy Enforcement Point (PEP). The interaction of these components is presented beneath.

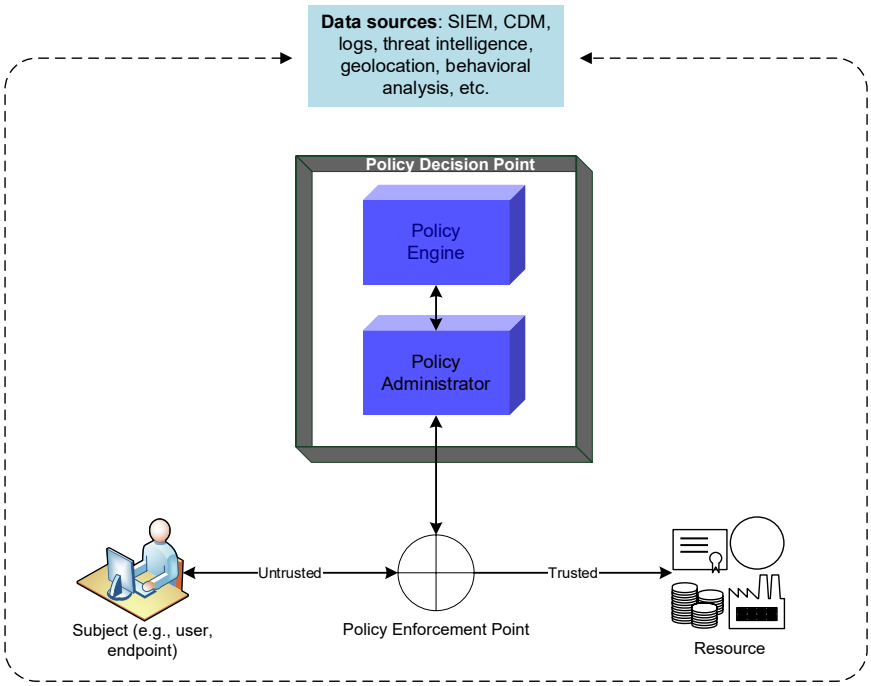


Figure 14 Core Zero Trust Components

The PE component serves as the brain of the Zero Trust model, it evaluates data from different data sources and oversees the decision to grant or not assess to a resource. The PE directly communicates its decision with the Policy Administrator. The PA is in responsible for controlling the channel of communication between a resource and a subject by approving or disapproving access though commands to PEPs in accordance with the policy set out. It is also capable to create authentication tokens credentials or in general session specific attributes for authentication. PA and PEP could be also implemented as a single component. The PEP operates under the instruction of PA in order to allow, monitor and terminate connections. It receives any policy updates from the PA. Eventually, everything beyond PEP is considered trusted.

7. Defend Against (Cascading) Threats (OT)

The objective of this chapter is to outline the recommended approach for the organization of the OT sector —often referred to as "Critical Infrastructures"— to design their architecture as a way to prevent (cascading) threats. In the current digital era, where cyber-attacks are happening more frequently than ever, it is crucial for organizations to take the required measures to safeguard their systems from malicious activities and actors. One essential and initial step is to ensure the safety and integrity of safety instrumented systems. To achieve this, organizations must first determine which SIS they manage, and if an appropriate forum is nonexistent, organizations shall gather safety and cyber security specialists to enable the execution of the subsequent mitigation procedures, as described in this chapter. Another essential and equally important factor to think about is the connectivity. Whether the SIS is connected to the rest of the control system or not must be documented by the organization (e.g., architecture diagrams), and in cases where there is connectivity, the connection mechanism must be investigated and documented. Apart from this, organizations shall check to see if the SIS has a mechanism in place to stop reprogramming or network access to the device while it is in use, as well as physically check that the devices are in "run-mode" or a similar state. Moreover, to stop intentional or unintentional breaches of the safety loop integrity, the SIS must be physically protected. Furthermore, organizations make sure that the trust architecture prevents ICS boundaries and environments from implicitly trusting Active Directory, which is prone to compromise. Equally, a strong authentication mechanism is essential for safeguarding the SIS. Organizations shall assess the authentication, authorization, and access control processes for OT devices. Strong authentication shall be required for any equipment connecting to the ICS from the corporate network. In ICS or administrator environments, end-user devices and critical systems shouldn't have internet access, and SIS administrative systems like laptops shouldn't either. Whitelisting is considered the proposed method to manage connectivity. Lastly, software deployed to SIS environments should be validated with the vendor using a proper (and preferably cryptographically secure) mechanism, and only modern and patched components should be placed on the boundaries of OT networks. Organizations can considerably lower the risk of cyber-attacks on their SIS by putting these steps in place.

In the OT sector, the Purdue Model of Computer Integrated Manufacturing is a widely accepted standard as adopted by ISA-99 that is renowned for its advice on the architecture of industrial control systems. The model's promotion of layer separation and explicit definition of how machines and processes should operate and interact have been helpful in improving industrial communication security. As a result, the Purdue Model has established itself as a recognizable security baseline in the OT sector, offering insightful advice and industry-recognized best practices for assuring the security, reliability, and availability of industrial control systems [27]. Purdue model

is constituted by 5 independent layers as illustrated in the figure below and explained afterwards [28]:

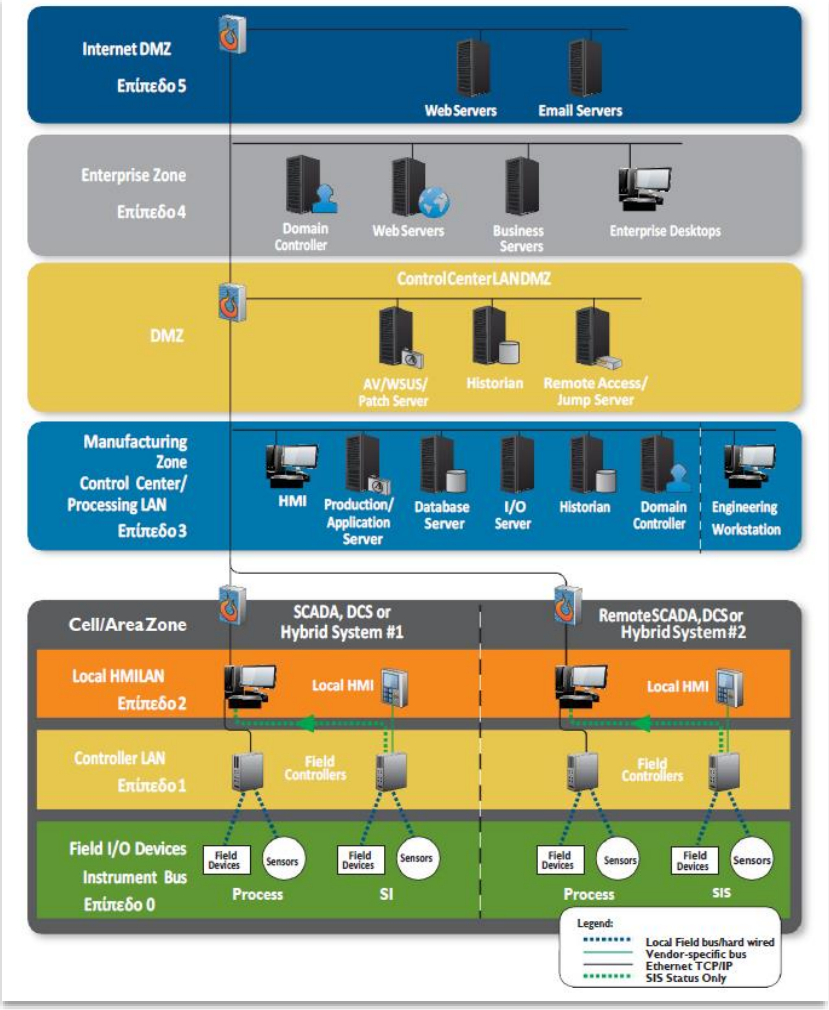


Figure 15 Purdue Model

Source: Defense-In-Depth in the natural & oil industry, oil and Natural Gas Subsector Coordinating Council [28]

- Layer 0: The Layer 0 encompass the physical components (e.g., sensors, robots) that build products. Level 0 devices include motors, pumps, sensors, valves, etc.
- Layer 1: The layer 1 is composed of sensors that monitor, receive input from the nodes, processes the inputted data by using control algorithms, execute specific actions (actuators) and send the outputted data to the nodes at different layers.
- Layer 2: The Layer 2 are devices that control the overall processes within the system based on the information from IIoT devices (Layer 1). For example, human-machine interfaces (HMIs) and SCADA software enable humans to monitor and manage the process.
- Layer 3: The Layer is situated in the middle of the OT and IT environments. It includes systems for controlling manufacturing operations. Systems Like

Manufacturing operations management (MOM), Manufacturing execution systems (MES) and Data historians are some of the most common systems that can be found in this layer and are able to communicate with both the IT & OT environment.

- Layer 3.5 DMZ: The layer 3.5 is the implementation of a Demilitarized Zone between layer 3 and 4. Jump boxes and similar devices can limit access to ICS systems from IT environments, but this data diodes can also stop threats in the IT environment from propagating to OT systems, and vice versa.
- Level 4: The layer 4 is the IT systems that support the operations at the enterprise level such as business planning and logistics. This Layer is frequently considered to be an extension of Zone 5 and more specifically includes services like e-mail, phones, printing, reporting, scheduling, inventory management, and capacity planning and ERP. The IT organization typically manages and runs the services, systems, and applications in Zones 4 and 5.
- Level 5: The Layer 5 encompass the required components of an organization like e-commerce services. Systems located at this level directly communicate with the public internet and are separated again through a DMZ.

But while Purdue model is commonly used and as mentioned before a widely accepted architecture a lot of difficulties have come to the surface with the emergence of new technologies. Nowadays, more and more data are required to travel between layers 0-3 to the layers 4 & 5 for data analytic purposes and monitoring processes. Adopting the old Purdue model architecture inevitably organizations strictly restrict data flows, slowing the process as a DMZ or/and a firewall is intercalated between the layers [29] [30]. On the contrary, smart devices have emerged providing real-time operational data and transforming the traditional Industrial Control Systems (ICS) to the Industrial Internet of Things (IIoT). Alongside the traditional zones, a separate IoT Zone has been added, allowing IoT systems and devices from both OT and IT to connect directly to the cloud. With this modification IIoT are connected directly to the manufacturing zone and each one of them transmit the information to the IT environment (including cloud). Clearly, in this way a single point of failure is avoided since if an IIoT device is down, only the data from this specific device will be lost. The following figure demonstrate how the Purdue model can be modified because of the evolution of cloud technologies and IIoT.

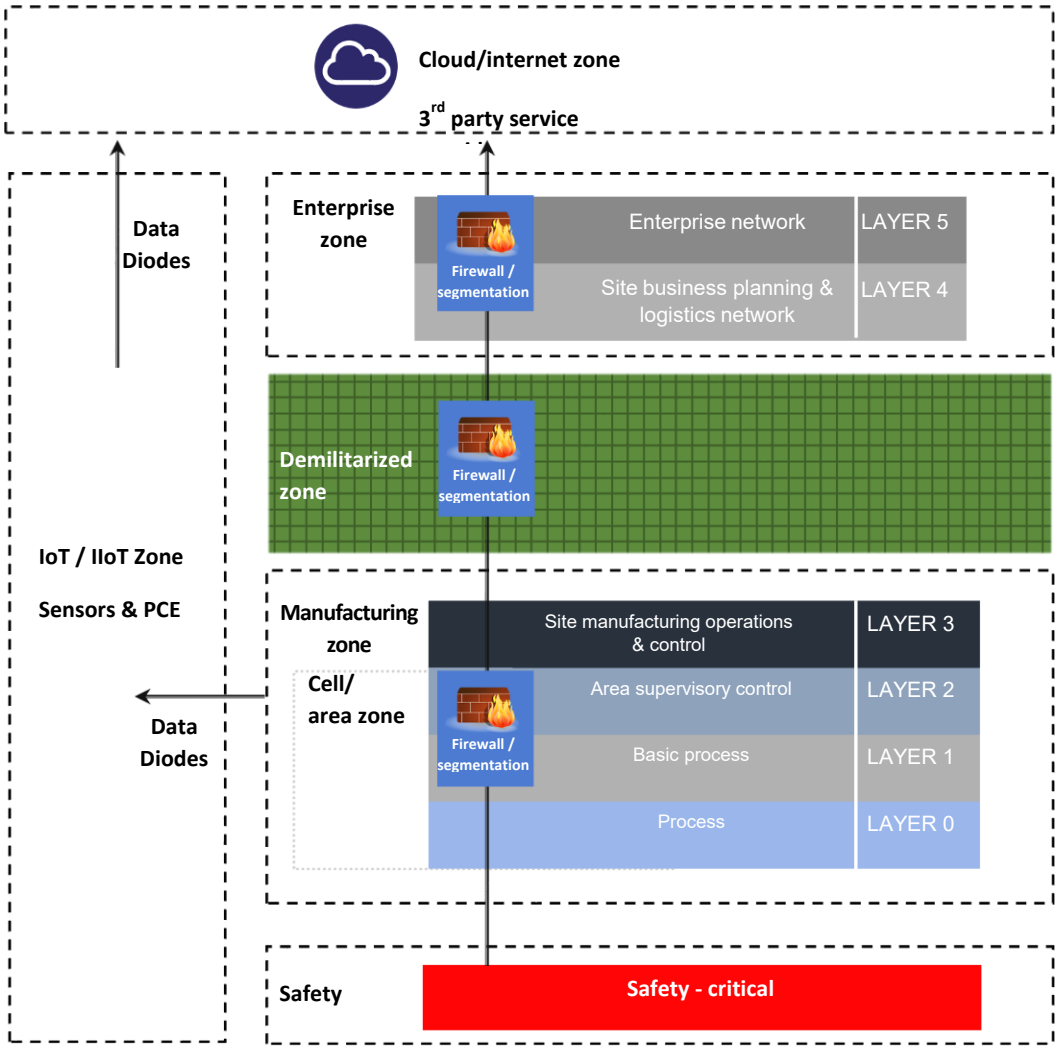


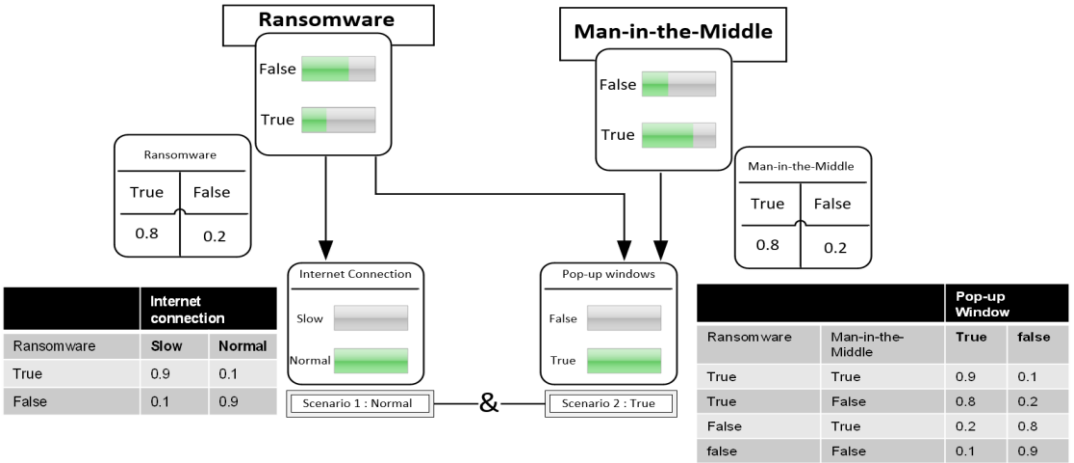
Figure 16 Evolved Purdue Model

The shape has been created with MS PowerPoint. Source: owlcyberdefence.com [30]

It is equally important though, to mention security issues that derive from the adoption of IIoT devices. The communication between IIoT and manufacturing layer shall ensure the security of both nodes. A compromised IIoT device can affect its connected device in the manufacturing layer but also cascade a threat to the other devices within the same layer. Ultimately, IIoT devices Impact the production process and at the same time new security issues and cascading threats.

8. Future Work

Bayesian networks (BN) also called belief networks or/and Bayes nets combine two distinct areas of mathematics: graph theory and probability theory [31]. They have been applied to various fields finance, healthcare, machine learning, language processing to model uncertain and complex conditions, and are considered as a probabilistic graphical model. These networks depict the probability distribution of a set of interdependent random variables that could be related dynamically. The network consists of nodes that stand in for the variables, edges that show how nodes are connected causally, and conditional probability distributions inside each node. Modeling the posterior probability distribution of outcome variables in light of new evidence is the main goal of Bayesian networks. These networks can be built manually using the context of the organization or automatically using appropriate software that gathers data from massive datasets (e.g., historical data) and benchmarking analysis [32]. In terms of cybersecurity, Bayesian networks could be useful for modeling cascading threats. By simulating the dependencies between various attack scenarios and calculating the likelihood that they will occur, Bayesian networks have demonstrated potential for assessing the risk of cascading threats. The two components of Bayesian networks are the quantitative and qualitative. The quantitative part is Directed Acyclic Graph (DAG) made up of nodes and edges represents the qualitative portion. The edges between the nodes, on the other hand, reflect the conditional relationships among the corresponding nodes which are also considered as random variables. The quantitative component takes the form of conditional probabilities, which define a conditional probability distribution for each connected node in the DAG and quantify the dependencies between them. A mockup of a simple BN model that illustrates the probabilistic connections between cyber-attacks (ransomware and conde injection). Given the cyberattacks outcome (Internet connection and Pop-up Windows) the BN can determine the posterior probability of different cyber-attacks. According to the figure above, ransomware is less likely to be present in the above scenario than is the presence of a code injection attack [33].



	Internet connection	
Ransomware	Slow	Normal
True	0.9	0.1
False	0.1	0.9

		Pop-up Window	
Ransomware	Man-in-the-Middle	True	false
True	True	0.9	0.1
True	False	0.8	0.2
False	True	0.2	0.8
false	False	0.1	0.9

Figure 17 Example of Bayesian Networks

9. Conclusions

It is by now generally accepted that the wide development of technology and the increased need of interconnectivity has raised the issue of cascading threats. Indeed, cascading attacks cannot be easily predicted without a solid understanding of how the organization, as well its third parties, function. The overall approach for managing cascading threats, that is presented in this research, will prove useful in expanding their importance both for OT & IT environments. An equal important contribution of this research is the development of a tailor-made methodology for calculating dependency risk, based on a synthesis of industry approved risk assessment methodologies and guidelines. It has been noted that there is a gap in bibliography regarding cascading threats/ risks/ attacks, hence this work could be a solid starting point for discussion and further research. For this reason, an interesting and promising mathematical method has been proposed. It is important enough to mention that ransomware attacks became the biggest threat in 2022, surpassing data related attack, which were the biggest concern in 2021 [34]. Undoubtedly, threats and attack vectors will continue to evolve, which means that organizations need to continuously monitor the applicable threat landscape and enhance their cybersecurity maturity. At this geopolitical moment in time, it should be also highlighted that cascading threats and in general attacks has raised the amount of hacktivism [34]. Thus, not only organization but also governmental agencies shall be aware of the cascading impact of a cyber-attack in other countries so as to protect their citizens.

Terminology

Assets	Assets could be either physical or logical (tangible or intangible) that have value to the organization, as well as the people, process and technology that interact with them (e.g., business applications, technical infrastructure or physical locations).
Business Continuity	An organization's[1] ability to sustain its mission/business processes during and after a significant disruption.
Business Impact Assessment	The process by which the business processes of an organization's Business Units are examined and classified as critical and non-critical based on specific evaluation criteria (hereinafter referred to as "BIA").
Countermeasures	A safeguard prescribed for an information system, or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements (NIST).
Data flow diagram (DFD)	A data-flow diagram is a way of representing a flow of data through a process or a system. The DFD also provides information about the outputs and inputs of each entity and the process itself (Wikipedia).
Control Components	The industrial process relies on various components which facilitate the control of the field devices and processing of variables such as pressure, flow, temperature, and electrical values like voltage and current. These components operate based on preconfigured logic and include PLCs, RTUs, controllers as well as I/O modules.
Impact	The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability.

[1] The term "organization", in the context if this report, is used synonymously with other comparable nouns such as "company" or "enterprise" while acknowledging the subtle distinctions in meaning among them.

Inherent Risk	The risk that arises when no security measures are in place.
Risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence (NIST).
Risk Appetite	The types and amount of risk, on a broad level, that an organization is willing to accept without the need to adopt further corrective measures.
Residual Risk	The risk that remains after security measures and risk appetite has been applied.
Threat Actor – Threat	The malicious actor(s) (inside or outside the organization) that is responsible for the initiation of an incident (e.g., hacker, employee).
Threat	Any action or event with the potential to adversely impact the organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

* A common terminology confusion happens between threats and risks. The difference between a threat and a risk is that a threat is a negative event by itself, whereas a risk is the negative event combined with its probability and its impact (Bugcrowd)

10. References

1) Giulio Z, Daniale de G, Mattia F.L (2018). Theoretical model for cascading effects analyses, International Journal of Disaster Risk Reduction.
2) König et al. (2019). Cascading Threats in Critical Infrastructures with Control Systems, WiPe Paper – Protecting Critical Infrastructures in Crisis Situations Proceedings of the 16th ISCRAM Conference.
3) World Economic Forum. (2022) Systemic Cybersecurity Risk and role of the Global Community: Managing the Unmanageable.
4) Duane V. Frederic P. Kibaek K. (2017). Incorporating Prioritization in Critical Infrastructure Security and Resilience Program. available at https://www.hsaj.org/articles/14091, [Accessed: 10/03/2023].
5) Ahmed H, El-Kady, Syeda H, Mahmoud M. El-Halwagi, Faisal L. (2023). Analysis of Safety and Security Challenges and Opportunities Related to Cyber-Physical Systems. Journal Pre-proof.
6) Yassine M. (2021). IT/OT convergence and cyber security. Computer Fraud & Security, p. 13-16.
7) Ike C, Michael A. (2020). Understanding the influence of IT/OT Convergence on the adoption of Internet of Things (IoT) in manufacturing organizations: An empirical investigation. Computers in Industry.
8) NIST. (2012) NIST SP 800-61 Rev 2. Computer Security Incident Handling Guide
9) ENISA. (2022). ENISA Threat Landscape 2022.
10) Kevvie Fowler. (2016). An Overview of Data Breaches, chapter 1. p.1-26
11) Marc Lee. (2012), Cyber crimes: preparing to fight insider threats. Computer Fraud & Security, p. 14-15
12) CISA. Insider Threat Mitigation. available at https://www.cisa.gov/topics/physical-security/insider-threat-mitigation, [Accessed: 20/01/2023].
13) Continuous Threat Modeling Handbook. [Online] Available at: continuous-threat-modeling/Continuous_Threat_Modeling_Handbook.md at master · Autodesk/continuous-threat-modeling · GitHub
14) Threat Modeller. (2019). STRIDE, VAST, TRIKE, & MORE: Which Threat Modelling Methodology is Tight for Your Organization? available at https://threatmodeler.com/threat-modeling-methodologies-overview-for-your-business/, [Accessed: 28/02/2023].
15) Jim G. (2020). A Guide to Threat Modelling for Developers available at https://martinfowler.com/articles/agile-threat-modelling.html, [Accessed: 28/02/2023].
16) OWASP. STRIDE Reference Sheets. available at https://owasp.org/www-pdf-archive/STRIDE_Reference_Sheets.pdf, [Accessed: 28/02/2023].

17) What are dependencies? Cybersecurity & Infrastructure Agency. [Online] Available at: https://www.cisa.gov/what-are-dependencies [10/01/2023].
18) Rehak, David & Patrman, David & Brabcová, Veronika & Dvorak, Zdenek. (2020). Identifying Critical Elements of Road Infrastructure Using Cascading Impact Assessment.
19) Evans, N. & Horsthemke, W. (2023). Assessing Cyber Resilience: Cyber Dependencies. Argonne National Laboratory, a U.S. Department of Energy National Laboratory.
20) Microsoft. Create a sunburst chart in Office. [Online] Available at: https://support.microsoft.com/en-us/office/create-a-sunburst-chart-in-office-4a127977-62cd-4c11-b8c7-65b84a358e0c#:~:text=The%20sunburst%20chart%20is%20ideal,similar%20to%20a%20doughnut%20chart. [Accessed: 20/02/2023].
21) Microsoft. Create and view decomposition tree visuals in Power BI. [Online] Available at: https://learn.microsoft.com/en-us/power-bi/visuals/power-bi-visualization-decomposition-tree [Accessed: 20/02/2023].
22) Information Security Forum (ISF). (2021). QIRA Methodology, Quantitative Information Risk Assessment.
23) M.Y. Measuring Aggregated Control Strength When Quantifying Cyber Risk. LinkedIn. [Online] Available at: https://www.linkedin.com/pulse/measuring-aggregated-control-strength-when-quantifying-m-y- [Accessed: 20/01/2023].
24) Coleman, L. (2009). Risk Strategies: Dialling up optimum firm risk. London: Routledge
25) Scott Rose, Oliver Borchert, Stu Mitchell, Sean Connelly. (2020). Zero Trust Architecture, NIST Special Publication 800-207.
26) Cybersecurity and Infrastructure Security Agency. (2022). Applying Zero Trust Principles to Enterprise Mobility, Version: draft for public comment.
27) Is the Purdue Model Still Relevant? [Online] Available at: https://www.automationworld.com/factory/iiot/article/21132891/is-the-purdue-model-still-relevant. [Accessed: 30/02/2023].
28) Defense-In-Depth in the natural & oil industry, oil and Natural Gas Subsector Coordinating Council (ONG SCC) and Natural Gas Council (NGC). [Online] Available at:: https://www.api.org/-/media/Files/Policy/Cybersecurity/2018/Defense-in-Depth-Cybersecurity-in-the-Natural-Gas-and-Oil-Industry.pdf. [Accessed: 01/03/2023].
29) Matteo I, Alessandro T, Valerio C. (2023). Identification of cyber-risks for the control and safety instrumented systems: a synergic framework for the process industry. Process Safety and Environmental Protection
30) How IIoT and the Cloud are Upending the Purdue Model in Manufacturing. [Online] Available at: https://owlcyberdefense.com/blog/how-iiot-and-the-cloud-are-upending-the-purdue-model-in-manufacturing/. [Accessed: 30/02/2023].

31) Todd A, Stephenson. (2000). An Introduction to Bayesian Networks Theory and Usage. IDIAP Research Report.
32) Michal Horny. (2014). Bayesian Networks. Boston University School of Public Health.
33) Chockalingam at al. (2017). Bayesian Network Models in Cyber Security: A Systematic Review. Proceedings of the Nordic Conference on Secure IT Systems
34) ENISA (2023). Threat landscape: Transport Sector.