|  |
| --- |
| IU |
| Threat Modelling |
|  |

# Learning Objectives

The complete course book is divided into seven units. In the first unit, the three main pillars of information security which are confidentiality, integrity, and availability, and how they could be preserved will be discussed. We will gain in-depth insight in the second unit into how a threat could be measured in order to make necessary preventions in advance to counter a potential threat if it exploits a vulnerability.

The third unit is the heart of this course book where it is explained in detail the well-known threat models. After finishing this unit, one would be able to easily model a threat by using any one of the threat models explained. Thereafter, the fourth unit is dedicated to the discussion of attack libraries. These are mostly related to offensive operations, but the ultimate goal of this unit is to get knowledge of how we could utilize these libraries for defensive operations before an attacker could utilize them to compromise a victim.

A thorough understanding of cyber laws and law enforcement is necessary for anyone who studies cyber security which has been addressed in unit five. Since only modeling a threat is not enough, we need to also manage it by applying risk management techniques which are explained in unit six. In unit six, we would gain a deep insight into each sub-process that is carried out under the risk management process. Lastly, in unit seven, we will learn some of the best practices that should be carried out to counter a threat and risk.

# Unit 1 – Thinking C.I.A. and Beyond

**Study Goals**

On completion of this unit, you will be able to …

… understand the three main key pillars of information security: confidentiality, integrity, and availability (CIA).

… apply CIA concepts in given scenarios.

… recognize the key differences between the different elements of CIA.

… identify which key pillar of CIA is compromised in a given situation.

… remember necessary security measures that need to be considered to protect the CIA of information.

… evaluate common information security issues.

# 1. Thinking C.I.A. and Beyond

## Introduction

Whenever there is a discussion of protecting and securing networks, systems, applications, and information from unauthorized tampering, usage, or access, the subject of information security is always invoked. Information security encompasses all types of security imaginable. But the main term here is “security,” which means to protect or to secure something. Readers should not confuse the terms security and safety. Safety ensures that no intentional or non-intentional harm is caused; security refers to the protection of only deliberate harm that could be the result of an attack. The main question here is how we know what key aspect of information needs to be secured.

To understand information security, one needs to understand the key aspects of confidentiality, integrity, and availability (CIA). As protection refers to security and security refers to CIA, it is imperative to understand these key aspects. Keep in mind that these three concepts, also known as the CIA triad, combine to form the pillars of information security which are discussed in subsequent sections (Deane & Kraus, 2021, pp. 4).

**Data Breach**

a disclosure of confidential or sensitive information to unauthorized people

All three of these key aspects operate together and are dependent on each other. Students, graduates, and even security professionals who belong to any field of information security must understand these three aspects and the corresponding countermeasures to secure their information from a **data breach**.

In the following sections, we will be discussing in detail the basics to intermediate concepts of CIA and how to protect them. Subsequently, we will analyze the most common security threats and issues that every organization faces regarding its assets in its day-to-day operations. An asset is anything that has some value to its owner. However, it should be noted here that we have two types of assets: primary and secondary. Primary assets are the ones that comprise the core information, process, or activity such as money and reputation. While secondary assets network, software, and hardware can be utilized to compromise the primary assets.

**Cyberattack**

cyber criminals obtaining unauthorized access to data and disrupting system resources

As per the annual cybersecurity report published by Cisco, the main aim of cyber criminals is to target those humans who lack cyber awareness and do not know how to deal with a situation if a data breach or a **cyberattack** happens. Thus, it is essential to achieve a good understanding of basic cybersecurity-related terminologies to efficiently lower the risk these situations (Ng et al., 2021, p. 1).

## 1.1 Confidentiality

**personally identifiable information**

any information that is used to identify someone such as name, date of birth, address, credit card number, etc.

Confidentiality is the protection of secret information from unauthorized or illegal disclosure. Many organizations are compromised by cyber criminals leading to data breaches, which can include leaks of **personally identifiable information** (PII), one of the assets targeted by attackers. Most of the training is being conducted in organizations to train individuals to become familiar with the basic terminologies of cyber and information threats. As humans are the weakest link in cyberattacks, it is imperative to train individuals with the basic terminologies used in the cyber domain.

Based on the above discussion, the following question might arise: Where should we start learning these concepts that relate to **cyber threats**? In this section, we will focus on confidentiality, which is one of the main concepts of the CIA triad.

**Cyber threat**

any act that potentially compromises the CIA of the data by stealing and damaging it or by making it unavailable

Confidentiality is the first pillar of the CIA triad. According to this concept, only those users who are authorized have access to data and systems, and unauthorized users are hindered. Simply put, confidentiality promises that those people who are intended can access resources and information. In a nutshell, the purpose of confidentiality is to restrict unauthorized and illegal access to private and non-private information and data. The point to be noted here is that confidentiality relates to viewing or reading the data. This means if somebody who is authorized and has permission to read some data is reading or viewing the data and no one else, we can say that confidentiality is preserved. And if someone is not authorized to read the data and somehow managed to access that data and read it, then a compromise of the confidentiality of the data has occurred.

Organizations or companies that do not comply with regulatory and contractual obligations by failing to protect the confidentiality of the data may face a data breach that impacts their business. These are some of the main consequences that an organization might face because of a lack of proper security controls.

The notion of confidentiality is related to one of the security best practices of least privilege. Least privilege is a concept in which access to sensitive data or information must only be given when needed. Under this rule, only adequate access is given to the users to perform their intended tasks.

One more important aspect that is related to confidentiality is privacy. When we talk about privacy in the security context, it relates to personal data. Information or details that can be utilized to unambiguously recognize a person are PII. This must be kept confidential by any entity or organization to comply with the country’s privacy laws.

Various malicious actors are targets to compromise the confidentiality of the data using social engineering and phishing techniques. Apart from malicious acts, confidentiality may get compromised by human negligence or error. Such situations include failure of the data encryption or showing highly sensitive information on computer screens while unauthorized employers or users are in proximity.

### Best Practices to Secure Data Confidentiality

Data owners often care about the preservation of confidentiality being one of the most important security concepts. Many security controls are available to help data owners protect the confidentiality of their data. These controls include but are not limited to the following (Security Operations Center, n.d.):

* encryption, a technique used to convert plain text data to cipher text
* multi-factor authentication, the utilization of tokens for strong authentication
* using a password manager to manage multiple account passwords
* passwordless authentication
* implementing security controls to prevent unauthorized physical access if the data cannot be access remotely
* using a passphrase
* using a lengthy and complex password that included numbers, special characters, and alphabet
* using a different password for each account rather than using the same password for all the accounts

But apart from all the above-mentioned security measures, extensive personnel training is imperative to mitigate human error which potentially leads to data breaches and compromises the confidentiality of the data (Deane & Kraus, 2021, pp. 4–5).

#### Understanding compromise of confidentiality using scenario-based examples

In order to understand confidentiality properly, some scenario-based examples are given below:

* A laptop or a mobile that is not encrypted or password protected and contains personal or sensitive information is robbed.
* Personal information is unintentionally published on the website or social media platform.
* Posting daily life activities such as birthday parties, marriage pics, etc., on social media would allow an attacker to find additional details relevant to the victim.
* A keylogger is installed on a victim’s host and records each key typed, leading to data leak e.g., passwords, credit card PINs, etc.
* A text chat that is going on between authorized persons is captured by a third unauthorized person to view it.

### Self-Check Questions

1. Please list three main reasons for a company to secure the confidentiality of data.

*To secure the personally identifiable information (PII) of the user.*

*To secure the privacy of the user.*

*To prevent the company’s economic and reputational loss that would result from a data breach.*

*To comply with the laws and regulations of the country.*

1. Please mark the correct statement(s).

* *Confidentiality is a part of the well-known CIA triad.*
* Security confidentiality of the data refers to allowing access to authorized people to change the data.
* *Reading secret data only by authorized people refers to confidentiality.*
* Companies need to secure confidential data just for their satisfaction.

1. Please complete the following sentence.

Extensive *personnel* training is recommended to mitigate *human* error.

## 1.2 Integrity

In information security, after confidentiality, the second concept that needs to be understood is integrity. Integrity refers to the correctness and perfection of the data, information, and systems (Lundgren et al., 2019, p. 421). This property of information security ensures the authorized handling and correctness of the data only. This means that the person who is allowed to access the data finds it correct. The main objective of integrity is to guarantee that the data remain entirely unchanged, reliable, and correct. If there is an unauthorized change found in the data, it would be perceived as a compromise of the integrity of the data as a whole. Failure to protect the integrity of the data may lead to incorrect decisions or damaging actions because the data upon which the decision or action was based has been tampered with (Deane & Kraus, 2021, pp. 5,6).

The integrity of the data, information, or systems might be compromised because of the following reasons:

* poorly written code by the software developers
* viruses

**Superuser**

In computing, the superuser is a special user account used for system administration

* a **superuser** or administrator of a system executing the wrong command for a database
* computer viruses
* an administrator changing the wrong portion of a configuration file
* malware downloaded into a system when a user clicks on a malicious link received via email in a phishing attack
* financial records modified through financial fraud
* human negligence or error
* malicious activities performed by an employee that would potentially alter the data

### Best Practices to Secure Data Integrity

We have discussed the concept of integrity and the main reasons that the integrity of the data could be compromised. To secure data integrity, proper security controls must be in place (Deane & Kraus, 2021, p. 6).

The following are some of the key security measures which, if considered, secure the integrity of the data or restrict unauthorized changes:

* continuously taking backups of the data to some external device such that original data could be restored if lost

**Version Control**

a centralized system to track changes made to the software code

* putting in place a proper software **version control** system
* putting rigorous permissions in place to allow only authorized people to access the data
* cryptographic **hashing**
* putting in place the practice of separation of duties, which means that more than one person is responsible to perform and complete the task rather than only one employee being given full control over the entire task (geeks for geeks, 2022).

**Hashing**

a technique used to check the integrity of the data which is received by the receiver

* practicing job rotation must be exercised, which continuously changes the users completing particular task and prevents a single user from having complete control
* proper and continuous user awareness training

It is worth noting here that two main concepts in information security are directly or indirectly related to integrity: authentication and nonrepudiation. This section is dedicated to understanding the concept of integrity, but we should not move forward without briefly discussing the concept of authentication and nonrepudiation. Authenticity or authentication refers to guaranteeing that all participants are who they claim they are, and data received is original and genuine. While nonrepudiation ensures that no participant is capable to refuse their actions (e.g., deleting, creating, or altering data). Digital signatures are the techniques used to protect the authenticity and nonrepudiation of the data (Deane & Kraus, 2021, p. 6).

#### Understanding compromise of integrity using scenario-based examples

The following are some real-world examples of data integrity breaches (Fruhlinger, 2020):

* manipulating business data that would potentially lead to poor decision-making
* illegally accessing a financial system to inflate stock values
* hacking into a bank account and then blocking the access
* altering the HTML code of a website by hackers for fun or revenge

### Self-Check Questions

1. Please complete the following sentence.

Two important security concepts that are not part of the CIA triad but are related to integrity are *authentication* and *nonrepudiation*.

1. Integrity of the CIA triad refers to...

* authorized data reading
* authorized data viewing
* correctness of data

1. What type of user has special permission over a normal user?

*Superuser or administrator*

1. Name three data integrity security measures.

*Using a version control system*

*Hashing*

*User awareness training*

*Job rotation*

*Strong permissions*

## 1.3 Availability

The third and final main pillar of the CIA triad is availability. Availability refers to a concept that ensures access to the data or a service by authorized users when needed. When the term availability is specifically mentioned in **enterprise networks** or environments, it refers to guaranteeing uninterrupted and timely access by authorized users and services to the data and systems that they require to accomplish their tasks. Threats that target availability can disrupt the business operations of the organization. If this happens, it might come along with the disruption of the crucial business system, which lead to further reputational harm, loss of income, and loss of customers (Deane & Kraus, 2021, pp. 6–7).

**Enterprise network**

This is a term that refers to the IT infrastructure of organizations.

The following are the concepts that should be considered as they are related to availability:

* **Accessibility** is a concept that relates to the ease and ability of the user to access the data or utilize a resource when required. This includes eliminating restrictions for users that are authorized to access the data and resources. For instance, let’s suppose there is a file that is stored on the internal hard drive of a company. This file is considered available if the file remains there and the hard drive is running. Nevertheless, if the same file needs to be moved to another folder on a shared hard drive, one may not be able to access the file, but we might still be able to say that the file is available. What this means is that the data is still available in this scenario but is not accessible.
* **Usability** is a concept that ensures that a user should be able to use the available and accessible data to meet their requirements in order to complete a task. For instance, if a document is shared via Google Drive and you try to edit it, you could notice that a shared document is not always editable as it can be restricted to read-only permissions. In this scenario, the file is available and accessible but it lacks usability due to strict permissions.
* **Timeliness** is the amount of time between when the information is requested and when it is accessible and available for authorized users to use. To ensure timeliness, data must be available to authorized users within a certain threshold of time. In situations where there is a third-party service that is managing the data such as cloud providers, timeliness is the critical component that must be mentioned in **service level agreements** (SLAs).

**Service Level Agreement**

A complete document that outlines services that must be provided by the service provider to the customer

### Common Threats to Availability

The availability of the data, information, or systems might be compromised due to the following reasons but not limited to (Deane & Kraus, 2021, pp. 6–7):

* **Denial-of-service (DoS)** attacks refer to a cyberattack in which a hacker tries to shut down or disrupt a network or machine and making it unavailable and inaccessible to authorized users or other services. It is accomplished through the flooding of unnecessary traffic to a target.
* **Distributed denial-of-service (DDoS)** attacks are similar to DoS attacks in the sense that an attacker tries to shut down a system or network and make data access unavailable when requested by the authorized user. The difference is that in DDoS, multiple compromised systems are utilized to initiate unnecessary traffic toward the target.
* **Natural disasters** such as tornados, storms, and earthquakes can lead to system destruction and disruption hence making it unavailable.
* **Deleting sensitive data** from the system makes it unavailable to the authorized users.
* **Ransomware** attacks involve an attacker who **encrypts** the system’s data of the victim and then demands a ransom in bitcoins to decrypt the data.

**Encrypt**

A process in which readable data are converted into a form that is non-readable is called encryption.

* **Non-malicious threats** refer to software configuration errors or environmental threats that lead to power disruption.
* **Malicious threats** refer to all those threats that potentially would be initiated by cyber criminals with bad intentions. These threats include attacks like ransomware, DoS, and DDoS, among others.

### Best Practices to Secure Availability

We briefly understood the concept of availability. We also discussed some of the main reasons that could compromise the availability of the systems. Now we talk about some of the security practices that must be considered to prevent availability from being compromised.

**Data redundancy**

This is the practice of storing data in two or more locations to access them if they become unavailable in the primary location.

The following are some key security measures which, if considered, secure the availability of the data, systems, or networks (Deane & Kraus, 2021, pp. 6–7):

* Continuously taking backups of critical systems’ data to ensure **data** **redundancy**
* Using multi-factor authentication
* Having more than one data storage
* Deploying backups for power supplies

**Cloud computing**

a concept in which a third party like Amazon or Google is hired to manage a company’s infrastructure

* Implementing Web Application Firewalls (WAFs) which, protect systems from DoS and DDoS attacks
* Considering **cloud computing** for systems that require 99.99% uptime

#### Understanding compromise of availability with a real-world example

The majority of cyberattacks have compromised the availability of systems. The following are brief details of the Colonial Pipeline ransomware attack, which disrupted the availability of jet fuels and gasoline (Wilkie, 2021):

The Colonial Pipeline ransomware attack was a sophisticated cyberattack that happened in 2021. Colonial Pipeline is the largest oil pipeline system in the US and consists of over 5,500 miles of pipelines. On 7 May 2021, just before 5 a.m., an employee realized that company had been attacked when he found a ransom notice on a system that was part of the Colonial’s IT infrastructure. It was mentioned in that note that the company’s data had been breached, and a ransom of $5,000,000 was demanded to get the data back.

The pipeline was instantly shut down to contain the attack to prevent the spread of the malware from other parts of the operational network that controlled the pipeline operations. This instant shutdown resulted in significant disruptions to gas delivery to the East Coast, and long lines of trucks formed at pumps. Airline operations were also disrupted (Wilkie, 2021).

The scenario discussed above exemplifies the devastating effects of the compromise of the availability of critical infrastructures.

### Self-Check Questions

1. Please complete the following sentence.

The third main important concept of the CIA triad is *availability*.

1. SLA is a written document that outlines the...

* Services provided by the customer to the service provider.
* *Services provided by the service provider to the customer.*
* Services provided by one customer to another customer.
* Services provided by one service provider to another service provider.

1. What are the potential consequences of DoS attacks?

Publishing confidential data

Reputational loss

*Unavailable service*

1. Name two common threats that target the availability of the systems.

*DoS attacks.*

*DDoS attacks.*

*Ransomware attacks.*

*Power disruption.*

*Storms.*

*Sensitive data deletion.*

## 1.4 Well-Known IT Security Issues

Any web application – whether it is a large bank processing millions and billions of dollars in daily transactions or any storefront for small to medium neighborhood businesses – could be a juicy target for malicious actors. Hackers or cyber criminals love to choose their victims by vulnerabilities. Systems that are smaller and might not even have sensitive data in them, could be more attractive targets just because they are much easier to compromise or hack. This could also be referred to as a cost-to-benefit approach.

In addition, it could be a security professional’s perspective that just securing a web application or a website gives you a strong protective measure around a server. A more professional approach is that every cyber security control or countermeasure serves as an additional layer of protection. With the addition of each layer, data become secure to an acceptable level. For instance, two- or multi-factor authentication gives you an additional layer of authentication under the presumption that the main password will be stolen one day. In this example, we have two layers of security, one is the password and the second is multi-factor authentication, which would increase the **work factor** of the hacker (Escobedo, 2021).

**Work Factor**

Time and effort needed by a hacker to compromise a system

### Understanding Security Issues

A security issue is an unmitigated **vulnerability** in your network, systems, or application that a hacker can utilize to harm. This might include vulnerabilities in the production servers and those applications that are responsible for connecting customers to the business. Web security issues must be considered as soon as they are uncovered because web applications are considered the first target that an attacker tries to compromise and leverages as an entry point to the internal network of an organization (Escobedo, 2021).

**Vulnerability**

a weakness that a hacker leverages to compromise a system, e.g., a weak password

If unauthorized access is allowed to customers’ data, businesses would lose customers’ regard and confidence. Therefore, businesses take cyber security and information security seriously. Data breaches are being increased exponentially despite the significance of securing customers’ data. These data breaches are the outcome of both insufficient security controls and cyber criminals with more technical skills (Lumen, n.d.).

In the following sections, we will be discussing some of the main security issues and some brief steps one can take to protect data and businesses (Escobedo, 2021).

#### Ransomware attack

The goal of a hacker in this attack is to gain complete control of the victim’s data. The attacker achieves this by encrypting the data and then demanding a ransom(payment) in bitcoin in exchange for the decryption of the data. Hackers may also threaten businesses or end users to release their sensitive data to the public if they fail to pay by the due date.

Taking frequent backups of the system’s data is one of the best protective measures against a ransomware attack.

#### Remote code execution (RCE) or code injection

RCE is all about the attacker gaining the privileges to execute his malicious code. To achieve RCE, the hacker tries to search for those parts of the web application that accepts input from the user like the admission form, registration form, search boxes, etc. The hacker may try to input his malicious code into those input forms that would eventually compromise the application.

Input sanitization is a security measure that checks for every malicious input and filters it for controlled input processing.

#### Malware Attack

Malware is also called malicious software. It is an umbrella term used for viruses, Trojan horses, rootkits, spyware, etc. All these are utilized for a common goal, namely system compromise or data breach. Malware involves a malicious code that runs on a target’s system to encrypt all the data for ransomware or to hide itself and capture the target’s activity (e.g., typed passwords). Apart from these two examples, several other malicious activities might be carried out by malware.

Updated antivirus solutions are the primary security measures to protect from downloading malware from malicious websites.

#### Distributed denial-of-service (DDoS) attack

The main goal of an attacker in this attack is not to steal any data but rather to disrupt the service. For instance, initiating unnecessary traffic overwhelms the server, making it unavailable to serve legitimate requests from authorized users.

Firewalls that are properly configured could be the first line of defense against DDoS attacks.

#### Credential stuffing attack

The reuse of a compromised email account and password is known as credential stuffing. This is a type of brute-force attack. If a hacker manages to find one of your email accounts and password, they may try to compromise other of your accounts that might have the same email and password.

The best security measure against this attack is to never reuse the same username and password or at least password to your multiple accounts. Also, two-factor authentication prevents this attack even if a weak password is used.

#### Brute force attack

In this attack, a hacker tries to find the actual password of a given account by trying every possible combination against that email account. He achieves this with the help of hacking tools that would eventually automate the whole process. For instance, for a given account, a combination of 1 million passwords would be used to discover the right one.

To prevent this, there must be some policy in place that enforces account lockout after some reasonable number of failed attempts. Today, most websites use a security feature that eliminates this attack vector.

#### Weak password issues

It is human nature to set passwords that can be easily remembered, such as birth date, a parent’s name, etc. But all these are weak passwords, and they are one of the vulnerabilities that could be leveraged by hackers to compromise a system by using hacking tools that contain databases of commonly used passwords.

To counter this issue, a strong password must be used for authentication that contains at least 18 characters. A password with a combination of special characters, letters, and numbers is referred to as complex. For instance, “2@abc!dgc” is considered a complex password, while “OnceUponaTimeinFloridaCity” is an example of a strong not complex password as it does not contain multiple characters. Cracking a strong password is much more difficult for a hacker than a complex password (Escobedo, 2021).

#### Social engineering

Social engineering refers to all non-technical techniques a hacker may leverage to compromise the victims’ data or system. The primary attack vector in social engineering is social media platforms to extract the personal information of a victim. In the next step, the hacker tries to gain the victim’s trust by influencing him through false information. For instance, a hacker may do it by impersonating a service provider or bank claiming to be an official. The main purpose of such an attack is to gain critical information or deceive an authorized user into unintentionally performing disastrous activities. Social engineering is all about **open-source intelligence** (OSINT) or information gathering.

**Open-source intelligence**

a framework used to gather information about the victim fom social media and other online platforms using free tools and resources

Rigorous security awareness training is the best preventive measure against social engineering.

#### Phishing and spear phishing

In a phishing attack, hackers send fake emails to thousands and or even millions of targets. These emails appear to be received from an official resource andcontain some links, compelling the receiver to click on them. After clicking on the link, malware downloads on the victim’s system eventually leading it to a system compromise.

Spear phishing is the same as phishing, but it is much more targeted at one or a few high-profile officials like the Chief Executive Officer (CEO) of an organization.

The best way to counter these attacks is to conduct human security awareness training every month. After the training, it would be highly beneficial to legally simulate a phishing attack to analyze how users would react to it.

#### Infrequent patching or updating

Using outdated or unpatched software is one of the most common security issues that we face. If the software is not continuously being patched or updated, it would allow an attacker to use this vulnerability to hack a system.

The simple way to counter this security issue is to frequently update all the system’s software to the latest versions.

#### Insider threat

A very common term used in the domain of information or cyber security is insider threat. Any person you can trust like an employee could be an insider threat that could damage an organization from within.

To prevent this, rigorous background screening of a new employee must be enforced. Additionally, granting limited access required to complete the assigned task would mitigate threats from the insiders or authorized employees.

### Self-Check Questions

1. Please complete the following sentence.

The reuse of a compromised email account with its password by the hacker refers to *credential stuffing*.

1. Which term is used for the “time and effort needed by a hacker to compromise a system”?

*Work Factor.*

1. Name any two common information security issues.

*Phishing.*

*Spear phishing.*

*Ransomware attacks.*

*Insider threats.*

*Unpatched software.*

*Weak passwords.*

Summary

When we study any domain of information security (e.g., cyber defense, penetration testing, and threat hunting), one should being with the three main pillars of information security: confidentiality, integrity, and availability, also known as the CIA triad. Being a security student or practitioner, it is imperative to have a very good understanding of these three key aspects.

In a given scenario, a student of cyber security must evaluate what aspect is being compromised. If there is unauthorized access to read the data, then confidentiality is involved. If there is unauthorized access to write or change the data, integrity is being compromised. If there a disruption happens in any service such as a website, then it refers to the compromise of availability. All three of these aspects of security are important, but their specific importance relies on the given scenario. For instance, confidentiality is important for PIIs and availability is important for emergency triggers.

Nevertheless, security issues and exploits occur. To protect an asset from a hacker or a cyberattack, a good understanding of well-known security issues is essential. To achieve this, frequent security awareness training must be enforced for both technical and non-technical employees.

# Unit 2 – Measuring the Cyber Threat

**Study Goals**

On completion of this unit, you will be able to …

… understand the concept of measurement in general and specifically in the context of cyber threats.

… analyze the concept of metrics and why they are used for measurements.

… apply threat measurement techniques using a threat matrix for a given scenario.

… remember the probability of the most common cyberattacks.

… evaluate the concept of black swan events in general and in specific in the context of cyber security.

# 2. Measuring the Cyber Threat

## Introduction

For almost all the enterprises or organizations of the world, the main enabler is information technology (IT). It is IT that ensures high impact and efficiency of various business operations such as sales, telecommunications, oil and gas, and finance, to name a few. The technology giants such as Meta, Google, and Amazon rely on their large IT infrastructures for day-to-day business operations. But the real problem is that humans are imperfect and thus invent imperfect technologies, technologies that are vulnerable to cyber threats. These threats can lead to cyberattacks and data breaches (Leirvik, 2022, p. 3).

Cyber threats have surpassed conventional threats that relate to terrorist activities. Every organization that is connected to the internet is vulnerable to cyber threats when necessary steps are not taken. It is imperative to have a strong strategy to evaluate how resilient an organization is to a cyberattack, and this is not possible without learning the concepts and strategies that relate to measuring a cyber threat and risk (Hubbard & Seiersen, 2016, pp. 7–8).

This unit explicitly discusses some of the main key concepts of measurement of cyber threats. You will be able to understand how one can think like an attacker and evaluate the impact of a cyber threat that could lead to a cyberattack and potential economic and reputational loss. We will discuss how to measure a threat by discussing some of the key techniques such as a threat matrix. Learning cyber threat measurement enables a security practitioner to evaluate the potential malicious activities of a cyber criminal and their impact.

## 2.1 Concept of Threat Measuring

In discussing how threats or risks are measured in the domain of cyber security, we need to first discuss and understand the concept of measurement. We also need to discuss the myth that some things are not measurable in cybersecurity.

There are three misunderstood elements based on which it could be perceived that cybersecurity is immeasurable. Wrong interpretation of these three elements might lead to the misconception that cybersecurity is immeasurable. These elements are concept, object, and method. Let’s have a brief overview of the basics of these three factors (Hubbard & Seiersen, 2016, pp. 20–21):

1. It is easy to misunderstand the concept of measurement. If we clearly understand what measurement means, we understand that anything could be analyzed in cybersecurity.
2. Attention must be paid to the object that needs to be measured. If the thing that is to be measured is not clearly defined, it would lead anyone to fail to start the measurement of the object.

**Tangible and Intangible**

Things or assets that can be touched are tangible, while those that cannot be touched are intangible.

1. Methods and procedures must be properly defined. If techniques used to measure are well known and clearly defined, one can easily end up measuring both **tangible and intangible** objects.

To remember these three elements, one can use the mnemonic “.com,” where c stands for the concept, o for an object, and m for misconception. Once we clarify our conceptions about these three common words, it becomes clear that anything is measurable.

### The Concept of Measurement

If a cybersecurity specialist or an expert is asked a question about measurement, the potential answers could be “to mitigate to some number,” “to quantify,” or “to calculate an accurate value.” One can perceive explicitly or implicitly from all these answers that no error is acceptable in measurement, and it should be some precise number.

The reader perhaps has said or heard phrases such as the following:

* If we don’t know the exact consequences of a cyberattack or a data breach, how can we measure its exact impact?
* Because of high uncertainty, we can’t calculate the probability that a victim will be compromised by a distributed denial-of-service attack.

Statements or perceptions like these show a hypothetical definition or concept that is unscientific and has nothing to do with the real decision-making processes. Therefore, if measurements are followed only in numbers, it will be tough to introduce these methods into cybersecurity (Hubbard & Seiersen, 2016, p. 21).

### Definition of Measurement

For practical decision-making processes, measurement needs to be treated as observations or opinions that quantitatively mitigate **uncertainty** or doubt. For measurement, simply a reduction in uncertainty would be enough, rather than complete elimination. To some scientists, measurement is a probabilistic practice. Measurement can be defined as the quantitative reduction of uncertainties established on observations. To understand this definition, let’s have a look at the statement that gives results based on some measurement such as the following: “There is an 80% chance that a malware attack on a web server would make it unavailable for the users between 2 and 9 hours.” There is still some uncertainty in the statement, but at least it has been reduced to some extent by giving us the indication and probability of an attack. This would enable the cyber defense teams to consider necessary security measures before an attack happens. This would not have been possible without understanding the concept of measurement in the context of cyber security. These types of measurement results are the ones that would be termed as pass based on some security standards and would give results having some amount of uncertainty (Hubbard & Seiersen, 2016, p. 21).

**Uncertainty**

If the probability of some outcome like a cyberattack is not known, it would be termed as uncertainty.

### Classification of Measurement Scales

In this sub-section, we will focus on different measurement scales. This will help us to enhance our concepts of measurement in the domain of cyber security. Whenever we talk about the measurements, we think of some specific units of measure such as hours of duration of network downtime or loss of money in terms of dollars per month.

In contrast, cybersecurity experts and professionals consider scales like high, medium, or low to measure threats and risks. These scales are common in the cybersecurity industry, international standards, and best practices for risk assessments. We often see measurements in cybersecurity like “likelihood” and “impact” which is a subjective assessment and is given a scale of 1 to 5. These scales are then combined for further risk assessments and give a scale of low, medium, and high.

It should be noted here that even in cybersecurity, measurements do not work entirely without quantitative expressions. At least, the uncertainty must be given in some numbers, i.e., quantified, but keep in mind that the subject which is to be assessed may not need to be a quantity. A subject that is to be measured could be completely qualitative. The following are some of examples of qualitative measures of subjects:

* a subject that is to be measured in just “yes” or “no”
* whether it is probable that cyberattack or a data breach will happen at the end of this year
* whether we will claim a cyber insurance company

But what about the quantitative measure that is to be given for the uncertainty of our above analysis? This still needs to be expressed in quantity. Please have a look at the following examples that represent qualitative measures:

* There is a 60% chance of a cyberattack at the end of this year.
* There is a 25% chance that a cyber insurance claim would be made.

The above-discussed concepts about measurement are important and comprise many key lessons for cybersecurity specialists and managers. The common impression that assumes measurements are precise quantities overlooks the benefit of lowering uncertainty if eradicating uncertainty is not feasible or cost-effective. And by no means must all measurements be a traditional quantity.

To wrap up our discussion of measurement, it addresses discrete values of interest such as “Will we encounter a horrible cyberattack?” along with continuous values or quantities such as “If a data breach occurs, how much would it cost?” Decision makers, in business, make their decisions under uncertainty (Hubbard & Seiersen, 2016, pp. 22–24).

### Self-Check Questions

1. Please complete the following sentence.

There is a myth in cybersecurity that some things are not *measurable*.

1. The mnemonic used to remember the three misconceptions about the measurement is *.com.*
2. Name any two misunderstood elements about measurements in cybersecurity.

*Concept*

*Object*

*Method*

## 2.2 Cyber Threat Metrics

A threat is any organization or person that has the intention to cause damage. It is much easier to just list the threats instead explaining what threats ultimately are. Moreover, it is much simpler to explain than to measure. Consequently, listing threats is preferred by most organizations. Few organizations explain them in meaningful terms, and still fewer measure them in useful ways. This results in vague descriptions of cyber threats. A domain does not allow effortless measurements. Organizations and senior management are responsible for threat management as they are supposed to sign off for budget approvals after proper threat management.

Cyber threat measurement is a domain that resists easy measurements. That is why, unfortunately, there is a lack of understanding in applying and defining threat metrics and why measuring threats is skipped most of the time.

Measuring threats precisely and consistently has many benefits. For example, an accurate threat measurement helps in improving the analysis of the situation. It can also help analyze the potential impact or to determine the criticality of threats. In a nutshell, a good and consistent threat measurement supports proper risk management.

To understand all these important concepts and to address these problems in the cyber threat domain, we discuss and explain threat metrics for characterizing and describing threats clearly and consistently (U.S. Department of Energy et al., 2017, p. 3, 7). But before comprehending threat metrics and threat matrices, we need to first discuss the concept of a metric explained in the following sub-sections (U. S. Department U.S. Department of Energy et al., 2017, pp. 9–10).

### What is a Metric?

Generally, a metric is defined as “a standard of measurement”. But in the security domain, it is referred to as “a consistent standard of measurement” that enables the measurement of behaviors and attributes of concern. For instance, a *kilogram* is used as a unit in a metric to measure weight while the *number of students passed* can be used ina metric that allows us to measure the overall quality of the students and their studies (U.S. Department of Energy et al., 2017, p. 9).

The terms “metric” and “measure” should not be confused. To clarify, “metric” is some unit that helps us to measure, while “measure” is the precise observation that characterizes the performances Hence, if the number of cyberattacks per year is the metric, the measure would be the observed value, for instance, 12.

### Why are Metrics Used?

When something is measured using consistent metrics, we enhance our ability and capability to control it, manage it, understand it, compare it, and, in the situation of a threat, protect and defend against it. According to H. James Harrington (U.S. Department of Energy et al., 2017, p. 9), a performance engineer, “If you cannot measure something, you cannot understand it. If you can’t understand it, you can’t control it. If you can’t control it, you can’t improve it.”

### What Makes a Good Metric?

A good metric usually exhibits various traditional characteristics. The following are some of the features of a quality metric:

* A quality metric is clear, explicit, and unambiguous.
* A good metric helps in quality decision-making that prevents subjective interpretation.
* Good metrics help in implementing quantitative instead of qualitative scales, for example.
* A good metric enables us to express our findings in numbers (quantitative) rather than low, medium, and high ratings (qualitative).
* A good metric helps in assigning a number to even intangible assets.

### What Defines a Quality Threat Metric?

A good and quality threat metric is efficient, unambiguous, and clear. It is also able to support quality decision-making as mentioned in the preceding sub-section.

### Understanding a Threat Matrix

Threat matrix is all about understanding threat metrics. A metric is not equal to a matrix; rather, multiple metrics are combined to make a matrix. For a better understanding of a threat metric, it is imperative to grasp the basic concept of a threat matrix given below in the table. Measuring threats is beyond the scope of this subsection, so we will go through a high-level overview of the threat matrix given below. The main goal of a generic threat matrix is to recognize the attributes that might help threat analysts characterize modern threats based on their capabilities (U.S. Department of Energy et al., 2017, p. 13).

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| General Threat Matrix | | | | | | | | |
| **Threat Level** | **Threat Profile** | | | | | | | |
| **Commitment** | | | **Resources** | | | | |
| **Intensity** | **Stealth** | **Time** | **Technical**  **Personnel** | **Knowledge** | | | **Access** |
| **Cyber** | **Kinetic** | |
| 1 | H | H | Years to decades | Hundreds | H | | H | H |
| 2 | H | H | Years to decades | Tens of tens | M | | H | M |
| 3 | H | H | Months to years | Tens of tens | H | | M | M |
| 4 | M | H | Weeks to months | Tens | H | | M | M |
| 5 | H | M | Weeks to months | Tens | M | | M | M |
| 6 | M | M | Weeks to months | Ones | M | | M | L |
| 7 | M | M | Months to years | Tens | L | | L | L |
| 8 | L | L | Days to weeks | Ones | L | | L | L |

Source: U.S. Department of Energy et al. (2017).

Threat characterization allows analysts to completely define a specific threat. However, it is not possible to identify each specific threat consistently, the general threat matrix allows government and intelligence organizations to classify threats with common terminology.

As shown in the table above, columns in a threat matrix define the potential attributes of a threat, while threat capability is described in rows. At this point, questions may arise in the mind of the reader about why we are talking about attributes and capabilities and what their relation to the metric is. The answer is that a unique and specific metric determines each attribute. Some metrics follow qualitative results (for instance, high, medium, and low), while the rest use quantitative ones (for example, the annual cost). Since we have these two types of metrics in threat modeling, we need a framework that organizes these into one place. In a nutshell, a matrix is a model or framework used for organizing metrics (U.S. Department of Energy et al., 2017, p. 13–14).

Until now, we discussed the basics of the threat matrix in the context of threat metrics or attributes. But what about the concept of capabilities? Since capabilities are related to the observations and measurements that are made based on metrics or attributes, going into these concepts in depth is beyond the scope of this section, as these will be covered later in the context of threat measurement.

### Self-Check Questions

1. Please complete the following sentence.

It is much easier to list the threats than to *explain* them.

1. Anything that has the intention to harm is referred to as a...

* Attack.
* Risk.
* *Threat*.
* Vulnerability.

1. Which domain of Cyber Security resists easy measurements?

*Cyber Threat Domain.*

1. Name any two characteristics of a quality metric.

*Clear*

*Concise*

*Unambiguous*

*Support good decision-making*

*Quantitative measures*

## 2.3 Measuring the Threat for an Organization

To understand the concept of measuring a threat for an organization, we refer to the table “General Threat Matrix,” which we briefly discussed in section 2.2. Before going into the details of the matrix, let us first recall what a measurement is in the context of a threat. A measurement is nothing but an observation that can be made based on some metric. If we map these concepts of measurement and metric to table like the “General Threat Matrix” one, then columns are the metrics or attributes based on which observations are made and represented as rows or capabilities. This means that we can easily measure a threat if we manage to draw a threat matrix for a given set of attributes of a particular organization.

### Threat Attributes

A threat attribute is a distinct characteristic of a threat. Threat characteristics collectively define the ability and willingness of a threat to achieve its objective. Nevertheless, both ability and willingness are based on multiple separate and multiple attributes. Hence, each attribute of a threat is distinctive, and no two attributes are dependent on each other.

Threat attributes are divided into two sections: commitment attributes and resourceattributes (U.S. Department of Energy et al., 2017, p. 14–15).

#### Commitment attribute family

Commitment attributes are those properties that define the willingness of a threat to achieve its objective. These characteristics indicate the ability of a threat because they illustrate the force of a threat to attain its goal. Threats with greater commitment will achieve their goal at any cost and will not stop, while threats with less commitment will not have that much drive to accomplish their objective.

We have three separate attributes in the commitment family:

1. **Intensity**: It is defined as the strong determination and persistence of a threat in pursuit of its target. It is the measure of a threat that how far it is willing to proceed and what it is ready to risk to achieve its goal. Hence, threats with higher intensity are considered more lethal and dangerous because of their compelling desire to pursue a goal.
2. **Stealth:** While achieving the goal, a threat can remain hidden. To maintain consistent secrecy, a threat may obscure the details about its goal, the threat organization, and its inside operations. A threat with high stealthiness will make sure to hide its internal operations and structure from the external world. Open source intelligence (**OSINT**) is relevant here.

**OSINT**

a framework used to gather information about the victim from social media and other online platforms using free tools and resources

1. **Time:** This refers to a time in which an attacker managed to plan, develop, and implement techniques to attain their objective. In the context of a cyberattack, it refers to the time needed from the planning phase to the implementation and the execution phases. The more a threat invests time in pursuit of a goal, the greater its ability for harmful impact.

#### Resource attribute family

What access, people, and knowledge are available to an attacker for accomplishing their goal comes under the umbrella of resource attribute family. Explanations of these three resource characteristics are given below (U.S. Department of Energy et al., 2017, p. 15–16):

1. **Knowledge:** This includes the practical and theoretical skills of an attacker and how these skills are utilized to achieve their goals. Knowledge also comprises the attacker’s capability to obtain training in a required domain, share information, and keep up to date with the current tools and techniques. Fewer resources and time would be required for a threat to achieve its goal if it has extensive knowledge of both **defensive and offensive** operations. Knowledge can be differentiated as two types. The first is cyber knowledge, which is the practical and theoretical expertise that relates to networks, computer systems, and applications. The second is kinetic knowledge,which is related to cyber-physical systems like the oil and gas industry, manufacturing, power generation, etc.

**Defensive and offensive**

The protection of an asset refers to the term defense while attacking an asset in offense.

1. **Technical personnel:** This is a group of people that a threat dedicates to achieve a specific task. These people are highly skilled in their respective domains and can innovate new tactics and techniques that may not have been created in the past.
2. **Access:** This is the ability of a threat to place one of its group members inside a restricted system. A restricted system cannot be accessed without having a higher privilege. This characteristic outlines the skill of a threat to penetrate a restricted and secured system. The greater the access capability of a threat, the more security measures need to be in place to protect that system.

### Threat Capabilities and Profiling

Measuring the threat relates to the observations that are made from analyzing and reviewing the general threat matrix. And to observe a threat matrix, one should have a very good understanding of the attributes that we have previously discussed in detail. Now we will discuss attributes with their capabilities, which collectively help us to analyze, observe, or measure a threat. To establish a strong threat profile, first and foremost, two boundary conditions must be considered (U.S. Department of Energy et al., 2017, p. 16–17):

* Threats with a Level 1 profile will be considered with the highest capability under each attribute.
* Threats with Level 8 are the ones that have the lowest capability under each attribute.

Secondly, for good measurement and observation, the threat’s power of technical personnel can assist to understand and derive other threat’s attributes:

* A threat with strong technical personnel will surely have more access, knowledge, and intensity. This is an assumption that an experienced threat analyst or researcher makes to derive capabilities of other attributes (U.S. Department of Energy et al., 2017, p. 16).
* Threats that are marked as “ones” under the category of technical personnel, for instance, will not have that much knowledge as compared to those that fall under the category of “tens.” This is because threats with little human resources will not have the capacity to acquire knowledge and eventually share them.
* To have an attribute with a high intensity, the threat’s strength of technical personnel must be greater. Technical personnel with a level of “ones” lacks high intensity because it doesn’t have persistence and determination (U.S. Department of Energy et al., 2017, p. 16).

A threat organization’s knowledge is also very handy to make measurements and observations: Threats with a high level of knowledge will always have one step ahead of the target if the target is not up to date with the current trends of cyber security. Threats with strong cyber knowledge refer to both theoretical and practical knowledge.

The last attribute that could be helpful to measure a threat is its capability and ability for access: A threat with strong knowledge (kinetic and cyber) will be able to maintain its access after it manages to compromise a target. A target could be a network, system, or application. The attacker could maintain their access by escalating their privileges from a low-level user to a high-level user, such as “Root” in the case of Linux or “Administrator” in the case of the Windows operating system.

To wrap up, what we have studied in this section is to analyze a general threat matrix to make our observations to measure a threat based on its attributes and capabilities. Since the matrix discussed in this section is generic, it could be used as a reference to measure the threat to an organization by filling the values against each attribute accordingly. If you can profile a threat, which means labelling it as LEVEL 1 or LEVEL 2 (etc.) based on the given set of attributes and their capabilities in a threat matrix, then you have learned how to measure a threat.

### Self-Check Questions

1. Please complete the following sentence.

One must refer to the *general threat matrix* to measure a threat.

1. A measurement closely relates to...

* Attack.
* Attribute.
* Capability.
* *Observation*.

1. Which term is used to define a distinct characteristic of a threat?

*Attribute*

1. Name any three attributes of a threat from a threat matrix.

*Intensity*

*Time*

*Stealth*

*Knowledge*

*Technical personnel*

*Access*

## 2.4 Major Cyberattacks and their Impact

2021 is considered one of the critical years in terms of massive data breaches and cyberattacks that wreaked havoc on critical infrastructures. These infrastructures included Colonial Pipeline, Solar Winds, and lots of others which after the attack had a high impact on security and the economy. Attackers considered and still consider Ransomware as their primary tool to target small and medium organizations and critical infrastructures. When discussing the likelihood of cyberattacks, we need to quantify them in terms of numbers or percentages to better understand the impact of the potential attack and to make necessary security measures. Without knowing the likelihood of an attack, one cannot be able to identify how much money should be invested to implement security controls to prevent and detect the potential cyberattack. In the following subsections, we will discuss some of the key trends of the major cyberattacks in different sectors of the industry. This will broaden our horizon of understanding the landscape of major cyberattacks and their likelihood (Brooks, 2022).

### Businesses and Cyberattacks

Although large businesses suffered massive data breaches, the lack of proper security measures and technical expertise in small to medium businesses means they have always been the easiest target for hackers. Almost 43% of attacks are targeted at small businesses, but only 14% have the necessary security measures to counter those attacks. The likelihood of a cyberattack increases if proper security controls are not implemented. Because of this, small to medium size businesses always struggle to defend themselves.

The following are the three most common cyberattacks and their likelihoods in terms of percentage on small to medium size businesses (Brooks, 2022):

1. Social engineering/Phishing: 57%
2. Stolen or compromised devices: 33%
3. Compromised credentials: 30%

### Healthcare and Cyberattacks

According to a recent survey of the healthcare sector, 70% reported facing ransomware attacks that resulted in delays for tests and procedures, delays that have caused severe consequences, including a rise in patient death. More than half of the internet-facing devices found in hospitals have vulnerabilities that could be exploited and end up compromising patients’ data and safety (Brooks, 2022).

### Internet of Things (IoT) and Cyberattacks

As reported by Semantic, IoT devices face 5,200 attacks on average per month. The reality is that most IoT devices are in their inception and that the attack surface is much bigger for the attackers to exploit vulnerabilities related to them (Brooks, 2022). Cyberattacks on an IoT device impact the device’s usability, performance, and services that are offered by the device. For instance, an IoT device that is compromised could end up in battery drain, causing a device to switch off and thereby rendering the service offered by the IoT device unavailable.

To minimize the risk of the cyberattacks, each industry must follow best practices in security. For example, the health sector must comply with the Health Insurance Portability and Accountability Act (HIPAA), a law that enforces the security of the patient’s data, preventing it from being disclosed without the knowledge and consent of the patient. Similarly, businesses and organizations must implement security controls as per the requirements of the ISO 27001 standard, an international standard used for the implementation of an information security management system (ISMS). Furthermore, IoT devices could be protected by following the best practices in security mentioned in ISO standard 27400.

### Self-Check Questions

1. Please complete the following sentence.

The technique which is mostly used by hackers to target healthcare is *ransomware*.

1. What businesses are most likely to be targeted by cyberattackers in terms of their size?

*Small*

## 2.5 Black Swan Events

A black swan is an uncertain event that has potentially serious consequences, is expected beyond a normal situation, and is difficult to predict. Incidents like 9/11, World War I, the 2008 Financial Crisis, and COVID-19 are examples of black swan events.

There is no doubt that cyberattacks and breaches are becoming more common and attackers are becoming more skilled and sophisticated in their tools and techniques. From phishing campaigns to malware, from reconnaissance attacks to denial-of-service, attackers are becoming determined and bolder with every passing day. To beat hacktivists and cyber criminals, organizations must focus on increasing their security measures to boost resiliency against data breaches (Financier Worldwide, 2017).

Nevertheless, companies must think beyond traditional security planning for a cyberattack and implement different defense strategies for uncommon threats, like a black swan cyber event.

In the context of cyber security, black swan events are termed black swan cyber events. Black swan cyber events could follow different techniques and approaches as opposed to conventional cyberattacks. The motivation behind most cyber breaches is financial gain, they could be from malicious employees or hacking organizations. Comprising an organization’s network or the critical infrastructure of industries such as oil and gas, manufacturing, and telecommunication is the most severe threat from cyber criminals (Financier Worldwide, 2017).

The following are the key points that summarize the concept of black swan events (Investopedia, 2022):

* A black swan is an event that is considered highly rare with severe impact.
* They are unpredictable.
* These events could negatively impact investments and markets and cause disastrous damage to economies.
* Even with the use of strong modeling techniques, black swan events cannot be predicted.
* Forecasting techniques and tools may also fail to predict such events.

### Self-Check Questions

1. Name any two characteristics of a black swan event.

*Rare*

*Unpredictable*

*High Impact on Economy*

Summary

This unit discussed the concept of measurement, how a threat could be measured and rated for any organization, and how a threat matrix could be leveraged for the analysis of the overall threat posture of an organization. We briefly discussed some of the key terms used in a threat matrix such as metric, measurements, observations, attributes, capabilities, and threat profiles or profiling.

We have also discussed the probabilities and the impact of major cyberattacks on critical infrastructure and small to medium-sized organizations. Then, to understand the concept of those events or attacks that are unpredictable and cannot be forecast, we briefly discussed the concept of black swan events and their manifestation in cyberspace.

# Unit 3 – Threat Modeling

**Study Goals**

On completion of this unit, you will be able to …

… understand the concept of threat modeling.

… identify the nature of the threats that might impact systems, networks, and applications.

… create attack tree diagrams that describe attacks on a system.

… evaluate the STRIDE model used by software developers.

… analyze a DREAD modeling technique to prioritize and rate the intensity of threats.

… apply the conceptual model of the Pyramid of Pain for the effective utilization of threat intelligence.

# 3. Threat Modeling

## Introduction

This unit explicitly discusses and explains various valuable models one can utilize to address and alleviate potential threats. People or organizations that built networks, systems, software, or applications must address various threats their infrastructure might face (Shostack, 2014, p. xxi).

Threat modeling is a term that can be used for some acts we all perform intuitively in our daily lives. If somebody asks you to model a threat for your house, it is natural that your thought process might start by thinking about the valuable assets within it such as heirlooms, family photos, or other valuables. You might also start worrying about the different ways someone might break in, like open doors and windows. And you might also think about who could be able to break in, such as professional robbers, stalkers, or perhaps somebody from a neighborhood.

Each of the above-mentioned examples concerning the thought process of a person creating a threat modeling process for his house are analogous to the cyber world. This is because the same thought process is applied to threat modeling in cyber security. However, these questions are simply those that arise in the mind of a person as an analyst. What about the subsequent processes that need to be implemented to address these questions to mitigate the potential threats? This requires proper skills and techniques, and we will discuss such in the upcoming sections of this unit. These techniques are various threat models which are the tools that assist a threat analyst not only to think about the necessary questions about a potential threat but to address them as well (Shostack, 2014, p. xxi).

The term “threat” can be interpreted in many ways. It could be used to address a disgruntled employee as an “Insider Threat”. It can be used to represent an event, for instance, “At the end of this month, there is a threat of a tornado.” It can also be used to define malware and viruses or the possibility of a certain cyberattack.

Similarly, there are different ways of describing threat modeling, but these generally fall under the following two conceptualizations (Shostack, 2014, pp. xxii–xxiii):

1. Carrying out the analysis process to identify what might go wrong in case a threat potentially exploits a vulnerability

**Risk**

the potential damage or loss caused due to the exploitation of vulnerability by a threat

1. Utilizing abstractions that help in the thought process about **risks**

For a stronger defense, threat modeling is one of the key techniques. Different threat models, like attack tree, STRIDE, DREAD, and the pyramid of pain will be discussed in subsequent sections.

Some people genuinely understand information security. Software developers might have knowledge of IT but not of information security; this is why they generally do not see the design of an application from the attacker‘s point of view. In reality, within cyber security, it is important to understand that there is no security measure that cannot be bypassed, and this usually happens in a way the architect never envisioned. And as security bugs are reported everyday by the newspapers and reports, it becomes obvious that the concept of “security“ does not have significance unless you find answers to the questions like “Security from whom and for how long?”

**Network Infrastructure**

This refers to a combination of hardware, network services, and software.

It is evident that we need certain techniques to model threats against **network infrastructure**. If one can perceive the different methods that can be leveraged to attack network infrastructure, once can potentially plan countermeasures to hinder these attacks. Then, one can implement those countermeasures to tackle real-world threats (Schneier, 1999).

## 3.1 Attack Tree Methodology

A useful way of approaching the attack tree methodology is through analyzing real-world examples.

### Understanding Attack Trees with Real-World Examples

Attack trees is a threat modeling technique that was invented by Bruce Schneier (1999). This technique offers an organized approach based on the diverse nature of the attacks. The attack is represented against a target in a hierarchical tree structure. The root node represents the main objective, and the leaf node describes the ways of attaining that objective. Using the attack trees technique, we can model various paths through which a target can be invaded, and the resulting graph helps security practitioners for better analysis of potential security threats. The following paragraphs give a detailed explanation of the attack trees from Schneier (1999), and students may look at the attack tree models found on the source’s website in tandem with this section.

Schneier’s first attack tree models an attack targeting a physical safe (1999). The main objective is to open a safe. To unlock a safe, attackers could pick a lock, learn a combination, cut and open a safe, or improperly install a safe so that it could be easily opened afterwards. To get the combination, they have to find it either from the combination that is written down or get it from the safe’s owner. Every node will become a subgoal, and each node’s child represents the approach to attain that subgoal. Certainly, the attack tree described here is subjective. Based on skills and expertise, one can add various other potential attacks that would be leveraged to achieve the goal.

It should be noted that nodes are represented as OR and AND nodes. A node that is not marked as an AND node is considered an OR node. OR nodes give an option. For instance, there are four different ways to achieve a goal (e.g., to open a safe). Anyone of the four options could be used to open a safe. In contrast, AND nodes give you various steps to be performed collectively to achieve the goal. For instance, according to the first of Schneier’s figures (1999), to **eavesdrop** for getting the safe’s combination, the attacker must listen to the conversation AND somehow compel the safe’s owner to disclose the combination. In this example, an attacker would fail to achieve the objective (that is, successful eavesdropping), if either (or both) of the conditions is not met.

**Eavesdropping**

unauthorized intercepting of a confidential communication

After completing the main attack tree, two more values can be assigned: P (possible) and I (impossible) to the nodes to make further analysis and calculations. Once these values are assigned, forecasting the security of the root node becomes much easier. OR nodes will be marked as P if any one of its child nodes is P and I if all of its child nodes are I. AND nodes will be marked as P as long as all of its child nodes are P and I if any of the child nodes is I, as demonstrated in Schneier’s second figure (1999).

In Schneier’s second figure (1999), all achievable attacks are shown with dotted lines as a hierarchy from the leaf nodes to the goal (the root node). According to this model, a goal could be achieved via two possible attack techniques: Opening the safe by cutting it or bribing the safe’s owner to learn the combination. Having this knowledge gained through an attack tree model, one knows precisely how to implement proper security measures to defend the infrastructure against the potential modeled attack. For instance, hiring a security service to check the safe at regular intervals is an example of the implementation of a security measure in this scenario.

Assigning “P“ and “I“ values to the nodes is just one way to model an attack via an attack tree. One can assign any other values to the nodes such as “difficult against easy,” “inexpensive against expensive,” “illegal against legal,” “no special equipment needed against special equipment,” and so on. The third figure from Schneier (1999) shows the attack tree with the same goal but with different values.

Assignment of the values like “not expensive“ and “expensive“ would also be beneficial, but showing it exactly in numbers would be great for better analysis of a model. The fourth figure from Schneier (1999) shows the attack tree in which the nodes are assigned different costs as values. Costs of the cheapest child nodes are assigned to their parent OR nodes, while the sum of the costs of all the children is assigned to their parent AND nodes. The attacker always tries to utilize those techniques that would cost less. Therefore, the attack with the lowest cost is illustrated in the fourth figure (Schneier, 1999).

The fourth figure of the Schneier’s attack tree shown in could be utilized to identify the system’s vulnerability (1999). Moreover, if a threat analyst is only interested in modeling the less expensive attacks, then only those attacks should be considered in the attack tree as shown in Schneier’s fifth figure in (1999). It is assumed that a safe might have an asset worth $100,000, therefore all attacks that potentially cost the attacker less than $100,000 are shown. The motive behind this model is that the attacker might not want to achieve his goal by spending money that would cost him more than the value of the asset itself.

Other continuous values apart from the one shown in Schneier’s fifth figure in could also be used for the nodes such as the likelihood of the attack’s success or the probability that an attack will be tried by an attacker, and so forth.

In any real-world scenario, threat modeling via attack trees is mostly carried out by assigning more than one value to the nodes. This would help to identify the system’s vulnerabilities even better. For instance, the sixth figure from Schneier (1999) models the cheapest attack that requires no special equipment.

An attack tree threat model helps in implementing the proper security measures. For instance, in Schneier’s sixth figure (1999), it would cost $20,000 for an attacker to achieve his goal. Because it is assumed in the model that the attacker would try the cheapest attack that requires no special equipment, namely bribing a person who knows the safe’s combination. Based on this analysis, we could implement a countermeasure by paying that human more to make him less vulnerable to bribes. For instance, if we assume that it would cost $60,000 for an attacker to bribe him, then the cost would increase to $40,000. Probably a third party could be hired to check the resiliency of that person against the bribe.

It should be noted that these are just examples and modeling the attacks and assigning values to nodes depends on the given situation. Understanding these real-world examples enable the students to utilize the attack trees technique for threat modeling for a given scenario. Briefly, security is a continuous process – it is not a product. Attack trees enable us to understand this process (Schneier, 1999).

### Self-Check Questions

1. Please complete the following sentence.

A threat can be interpreted in *many* ways.

1. Please choose the correct answer: An attack tree is a...

* defense modeling technique.
* *threat modeling technique.*
* offense modeling technique.

## 3.2 STRIDE

STRIDE is an abbreviation for Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege. STRIDE is a threat modeling technique that was invented by Praerit Garg and Loren Kohnfelder in 1999. The technique was designed for the software developers to help them identify the potential attacks that software might experience (Shostack, 2014, p. 61).

Threats that are mentioned in STRIDE are basically the opposite of some of the security aspects one would like their infrastructure to have. These security aspects are authentication, integrity, non-repudiation, confidentiality, availability, and authorization. The table “STRIDE Threat Model” presents a list of STRIDE threats, the security property that one would like to preserve against that corresponding threat, the threat’s description and definition, and some examples (Shostack, 2014, p. 62).

It should be noted that the STRIDE model is not used to categorize threats but rather to identify and list them which would lead to cyberattacks. In the following sections, we will discuss each one of the STRIDE threats in detail.

### Spoofing

Spoofing refers to claiming yourself as someone else’s identity. The table given below contains examples of pretending to be Elon Musk, system32.dll, a police officer, amazon.com, or an anti-fraud officer. Each one of these belongs to different subcategories of spoofing. In the examples of pretending to be amazon.com, it refers to identity spoofing of a well-known entity. In this case, there is no intermediate authority who takes obligation about the site authenticity. This varies from the example of system32.dll, which is a windows registry file, where the operating system acts as an intermediate authority between the user and these files to ensure their authenticity. An attacker might be able to insert his .dll file that looks original but contains malicious code. This is an example of spoofing a file or process on a system. Spoofing Elon Musk is an example of claiming to be an individual. An individual could be a well-known person or some employee. If somebody pretends to be some anti-fraud officer, police officer, or the prime minister of some country, these examples would fall under the category of spoofing a specific role (Shostack, 2014, pp. 64–65).

|  |  |  |  |
| --- | --- | --- | --- |
| STRIDE Threat Model | | | |
| **Threat** | **Security violation** | **Threat description** | **Examples** |
| Spoofing | Authentication | Claiming someone else’s identity | Wrongly claiming to be Elon Musk, system32.dll, amazon.com, a police officer, or an anti-fraud officer |
| Tampering | Integrity | Modifying something on memory or in a disk | Modifying the binary of a crucial program, a spreadsheet, or the database kept on disk |
| Repudiation | Non-repudiation | Denying something you did | A person saying that “I did not email you” when, in fact, the person emailed the day before |
| Information disclosure | Confidentiality | Giving information to an unauthorized person | Giving access to private emails, databases, or files |
| Denial of service | Availability | Compromising the resources required to run the service | To trick a web server to utilize all of the system’s resources such as disk, memory, and network’s bandwidth |
| Elevation of Privilege | Authorization | Accessing the resources for which someone is not allowed | Permitting a normal user to run the administrative commands as a superuser |

Source: Adam Shostack (2014).

### Tampering

In the STRIDE model, tampering refers to a threat that modifies something, in memory, or on a disk. As given in the table above, examples of tampering are modifying data in spreadsheets such as Microsoft Excel or any other editor, changing the contents of a database on a disk, or modifying configurations and binaries on a disk. Packets that travel over the network could also be changed by the addition of extra unnecessary packets to damage the communication (Shostack, 2014, p. 67). The implementation of strong hashing algorithms could prevent tampering threats.

### Repudiation

Repudiation is the act of denying something you did or claiming that you are not accountable for what took place. As in the example given in the table above, someone who emailed you the day before could denying doing so. **Logging** systems and processes are also related to repudiation threats. If logs are not enabled for the network infrastructure, log retention is not considered, or one cannot be able to analyze the logs, it would be hard to counter the repudiation threats (Shostack, 2014, pp. 68–69). Strong logging systems, if deployed in organizations, enable security teams to prevent repudiation threats.

**Logging**

the process of recording events happening in an organizaton’s network and systems

### Information Disclosure

Information disclosure is a type of threat in which unauthorized people are permitted to view information. It also refers to the unintentional revealing of information by the application about its architecture that could be leveraged by the attackers to attack the system.

Following are some of the well-known examples of information disclosure (Bauernfreund, 2022):

* information about the application that could be disclosed by the comments that are written by the software developers
* errors that comprise crucial details
* application’s source code that gives parameter information, or it could be technical information related to infrastructure or application.

Since the STRIDE threat model is designed for software developers, therefore they are the core people that could prevent vulnerabilities related to information disclosure. The following are some of the best security practices that, if followed by the developers, could prevent information disclosure (Bauernfreund, 2022):

* Information about the application such as response headers, error messages, and sensitive background information must be kept generic to prevent disclosing clues related to the behavior of the application.
* Proper authorization mechanisms and access controls must be configured to avoid unauthorized access.

**Web application penetration testing**

legally attacking a web application to identify its weaknesses to mitigate them in time

* The developed application must be checked from a user’s viewpoint to confirm that sensitive information and comments left by the developer are not exposed. This can be done by **web application penetration testing** using the best industry practices and standards.

### Denial-of-Service Attacks

Denial-of-service (DoS) attacks fall under the threats of denial of service of the STRIDE model and the security violation class availability. These attacks flood the victim with unnecessary traffic, instigating a crash and making it unavailable for legitimate traffic. These attacks usually cost their victims in terms of money, time, and reputation in terms of reliability. One of the most famous examples of DoS attacks is a buffer overflow that overloads the reserved memory buffer by injecting more data than intended, causing the application to crash.

**Web application firewall (WAF)**

It provides protection for a web application by HTTP traffic filtering between an internet and web application.

The application could be prevented from DoS attacks by configuring a **web application firewall** **(WAF)**, which could include blocking the incoming traffic from suspicious IP addresses or limiting the packet rate for better traffic management (Bauernfreund, 2022).

### Elevation of Privilege

Elevation of privilege (also called privilege escalation) is an attack that exploits misconfigurations mostly in the web application to obtain illegal access to privileged rights. These attacks might exploit authentication and credential processes, leverage the misconfigurations in the design and code, or utilize social engineering or malware techniques to gain privileged access. After gaining privileged access, an attacker can execute administrator or root-level commands and could wreak havoc. It should be noted here that gaining access to a higher privileged account is known as vertical privilege escalation (e.g., gaining access from a normal user to a root user account). However, gaining access to an account that has the same privilege level as yours is known as horizontal privilege escalation (e.g., gaining access to a student account from another student account).

Security against these threats needs to be enforced at the software’s development stage. This includes hardening mechanisms such as least privilege, closing unnecessary open ports, eradicating unneeded access and rights, and so forth (Bauernfreund, 2022).

### The Merits of STRIDE Threat Modeling

Many well-known techniques are used for identifying vulnerabilities (penetration testing, **code reviews**, etc.) once all or some of the web application is developed. Nevertheless, it is much easier and cheaper to fix the bugs while the application is in the development phase than to fix them once the application is live. STRIDE is a threat modeling technique that supports the developers to recognize potential vulnerabilities early in the development phase when mitigating them is easier and cheaper (Bauernfreund, 2022).

**Code reviews**

the process of assessing a source code to determine bugs

### Self-Check Questions

1. Name any two threats of a STRIDE model.

*Spoofing*

*Tampering*

*Repudiation*

*Information Disclosure*

*Denial of Service*

*Elevation of Privilege*

## 3.3 DREAD

Attack trees and STRIDE as we just discussed in the previous sections are used more for the identification of threats while DREAD is a threat assessment technique used to prioritize threats. Prioritization is based on the potential impact of the threats on a web application or software system, the likelihood of their occurrence, and the techniques used to potentially exploit them. This prioritization is performed after the identification of the threats as discussed in sections 3.1 and 3.2. These characteristics can be utilized to assign a qualitative rating such as low, medium, and high for threat prioritization.

Techniques used to prioritize threats are usually based on threat-risk ratings. (Please note that ratings and rankings in this section are used interchangeably.) The DREAD model is an example of a threat-risk assessment model that prioritizes threats based on their rankings (Ingeno, 2018, pp. 363–364).

DREAD is a model used for security threats’ prioritization based on a **risk**

**assessment**. It was developed by Microsoft like the STRIDE model. DREAD is an abbreviation for the following risk components:

**Risk assessment**

a process to identify high priority threats that could potentially damage the assets

* damage potential
* reproducibility
* exploitability
* affected users
* discoverability

The DREAD model at Microsoft is used to calculate risk. We give a risk rating to a given threat by asking questions based on the above-mentioned risk factors of the DREAD model. Let us first discuss each risk factor of the DREAD model and then investigate some of the examples to understand how a threat can be prioritized and ranked based on the DREAD model’s risk rating factors (Microsoft Corporation, 2003, p. 63).

### Damage Potential

Damage potential refers to the degree of damage that could potentially be done to an organization or users if the attack succeeds. For instance, the rating would be lower for damage caused to user data than for a cyberattack that can take down the whole system. Assessing damage depends upon the type of the cyberattack and assets being targeted, e.g., damage to a company’s prestige or financial liability (Ingeno, 2018, p. 364).

### Reproducibility

Reproducibility represents how simple it is to reproduce a specific cyberattack. A cyberattack is rated higher that could be reproduced easily and reliably than an attack that cannot be reproduced easily (Ingeno, 2018, p. 364).

**Exploit**

a software or technique used to take advantage of a vulnerability to compromise a system

### Exploitability

Exploitability is a risk factor based on which it is assessed how hard it is for a threat to damage an asset by exploiting a vulnerability. Some **exploits** can easily be understood and might be executed even by unauthenticated users, while some require more technical skills to execute advanced tools and **scripts** (Ingeno, 2018, p. 365).

**Script**

special instructions that are used to automate the process

### Affected Users

This risk factor represents the users’ percentage that would be impacted by a specific threat. Some cyberattacks might impact all users while some may impact a small number of them. This risk factor should be rated higher if the number of users who might be impacted by a threat is higher (Ingeno, 2018, p. 365).

### Discoverability

Discoverability indicates how simple it is to find a vulnerability. A threat that is already in the public domain has a higher discoverability rate than one that is difficult to find. It is worth mentioning here that some security professionals and organizations feel that the discoverability risk factor should not be considered as it honors a security control called **security through obscurity**. They believe that considering a vulnerability less risky just because it is not easy to discover is not a wise approach. Therefore, many security professionals use a DREAD-D (DREAD without the last D) model or give a maximum discoverability rating for all threats (Ingeno, 2018, p. 365). Since our focus is to discuss DREAD in this section, we will not consider rating this factor based on DREAD-D.

**Security through obscurity**

the process of keeping a system secure by maintaining its knowledge secret, e.g., hiding a key under a doormat for a locked door

The five risk factors of the DREAD model that have been discussed above are basically the questions that should be asked to find out the risk rating for a specific threat. The five questions could be asked as follows:

1. **Damage potential**: How much damage would happen to an asset?
2. **Reproducibility**: How simply could a cyberattack be reproduced?
3. **Exploitability**: How simply could a cyberattack be carried out?
4. **Affected users**: How many users would be affected?
5. **Discoverability**: How simply could a vulnerability be learned?

The above-mentioned questions could be used for rating the threats by using the scales of low (1), medium (2), and high (3). If each value of the rating system is clearly defined, it is easier to rate a specific threat by correlating it with a suitable scale. The table “Threat Ratings and Prioritization” given below show a rating table that assists in prioritizing the threats (Microsoft Corporation, 2003, pp. 63–64).

After asking the aforementioned questions for a specific threat, mark the ratings from 1 to 3 for each category of DREAD and then add them. The result could be in the range of 5-15. Then a threat could be prioritized as a low risk when it has ratings of 5–7, a medium risk with ratings of 8–11, and a high risk with ratings of 12–15 (Microsoft Corporation, 2003, p. 64). The complete process of rating a specific threat is shown in the table “DREAD ratings.”

For instance, let’s have a look into two threats to understand the process of DREAD ratings better:

1. Malicious SQL commands are inserted into an application.
2. The attacker acquires authentication credentials through network monitoring.

Once the risk rating for each threat has been obtained, this should be updated in the documentation against each threat that is labeled “high” for both threats shown in the table “DREAD Ratings.”

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Threat Ratings and Prioritization | | | | |
|  | **Ratings** | **Low(1)** | **Medium(2)** | **High(3)** |
| **D** | Damage potential | Trivial information is leaked. | Sensitive information is leaked. | The attacker can run administrative commands. |
| **R** | Reproducibility | Reproducing an attack is extremely difficult even if the attacker has a good knowledge of a vulnerability. | The attack can be reproduced only in a specific situation. | The attack can easily be reproduced in every situation. |
| **E** | Exploitability | A highly skilled and informative person is required to launch a cyberattack. | A good programmer could launch an attack with some attack skills and knowledge. | A programmer who is a beginner could also launch an attack. |
| **A** | Affected users | Very few users would be affected. | Some groups of users would be affected. | All users would be affected. |
| **D** | Discoverability | The vulnerability is obscure and the probability of finding it is very low for the users. | The vulnerability is rarely used and requires some thinking to exploit it. | The vulnerability is publically available and could be easily exploitable. |

Source: Microsoft Corporation (2003).

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| DREAD Ratings | | | | | | | | |
| **Threats** | **D** | **R** | **E** | **A** | **D** | **Total** | **Rating** |
| Malicious SQL commands are inserted into an application. | 3 | 3 | 3 | 3 | 2 | 14 | High |
| The attacker acquires authentication credentials through network monitoring. | 3 | 3 | 2 | 2 | 2 | 12 | High |

Source: Microsoft Corporation (2003).

One of the examples of a resultant documented threat is shown in the table below.

|  |  |
| --- | --- |
| A Complete Documented Threat |  |
| **Threat Description** | The attacker acquires authentication credentials through network monitoring. |
| **Threat target** | Authentication process |
| **Risk rating** | High |
| **Attack technique** | Network monitoring |
| **Countermeasure** | Encryption to preserve the confidentiality |

Source: Microsoft Corporation (2003).

The countermeasure mentioned in the table above is the security control that should be enforced for an asset. We can also see that if a threat is properly documented with its risk ratings and other details as described in the above table, decision-making to secure an asset would be easier in terms of selecting an appropriate security control.

### Self-Check Questions

1. Name any two attributes DREAD.

*Damage potential*

*Reproducibility*

*Exploitability*

*Affected users*

*Discoverability*

## 3.4 The Pyramid of Pain

David J. Bianco, a security professional, first presented the concept of the Pyramid of Pain in 2013. It is a conceptual model that assists in threat detection with a specific focus on augmenting the attackers’ cost. The main objective of introducing this technique was to assist in identifying the potential attack indicators or threats to perform threat modeling. A complete model of The Pyramid of Pain is shown below.

Pyramid of Pain

A picture containing text, businesscard

Description automatically generated

Source: Zohaib Hassan (2023), based on Bianco (2013).

### Understanding Attack Indicators

In the graphic above, a pyramid is shown in which there are six levels. Each level represents various forms of attack indicators. The pain is defined by the level where the corresponding indicator is mapped. For instance, if an attacker is utilizing **malware** to infect a system and you are utilizing hashes to detect this behavior of the attacker, it would be trivial for an attacker to recompile that malware with a different hash value than the one you are using for the detection, hence making your hash value relatively useless (Chenette, 2019).

**Malware**

This refers to a malicious software created to damage a network, system, or application.

Let’s briefly define all eight indicators upon which the pyramid is built (Bianco, 2013):

1. **Hash values:** These are the values that refer to specific malware. MD5 or SHA1 are examples of hashes that point to some specific malicious file based on which the detection is carried out.
2. **IP addresses:** This is an address or group of addresses that uniquely identify a machine over the network or internet. 15.2.1.2 is an example of an Ipv4 address.
3. **Domain names:** A domain refers to a web page such as google.com or a sub-domain like sites.google.com. It could also refer to a sub-sub-domain like site1.sites.google.com.

**Artifact**

This is evidence submitted after an incident for further investigations.

1. **Network artifacts:** The observables or the **artifacts** that are left behind by the attacker on the network after compromising it. For example, the IP address information of the adversary is found in network logs.
2. **Host artifacts:** The observables or the artifacts that are left behind by the attacker on the host after compromising it. For example, malicious .dll files could be dropped in specific places using legitimate names.
3. **Tools:** These could include software or the utilities utilized by the attacker to achieve his goal. For instance, attackers mostly leverage a Linux distribution known as Kali Linux for their malicious activities.
4. **Tactics, techniques, and procedures (TTPs):** This refers to a complete strategy that an attacker follows to attack a network, system, or application. Spear phishing is one of the examples of TTPs in which malicious attachments are used in the structure of .zip or .pdf files. TTPs refers to the techniques and activities to perform malicious activities and are not related to some specific tool. This is associated with a significant amount of pain for the attacker, since we not only detect the activities of an attacker but also the attacker himself.

We have gone through the basic details of each of the indicators. Now let’s discuss the pyramid in detail. The pyramid’s widest part is in green, and its peak is in red. Both color and width have their significance in the evaluation of each indicator. The indicator placed on the bottom would cause minor pain to the adversary, while the one placed on the pinnacle would have an enormous impact and would require an immense effort by the security analyst to disclose it (Panhalkar, 2020).

At the bottom of the pyramid, hashes are positioned. This is because the disclosure of the hashes does not significantly impact the adversary. Furthermore, hashes need to be accurate to analyze a threat such as malware. This means that incorporating unnecessary bits would make hashes useless for further analyses. Moreover, less effort is required by an analyst to calculate the hashes.

**The Onion Router**

an open-source software that provides services for anonymous communication

Above hashes, IP addresses are placed. IP addresses occupy the wider region of the pyramid, as huge databases of IP addresses are available to utilize and is key information that an attacker needs to set up a connection with the victim. The attacker can easily hide his original IP using proxy services like **The Onion Router** (TOR) and go undiscovered. If somehow the fake IP gets blocked, then he could continue the attack process by instantly changing the IP to a new fake one. Hence, this indicator is mentioned in green.

Level three from the bottom up is dedicated to domain names. Since it would cost an adversary to purchase a domain name to launch himself on the internet, it is mentioned in light green, which refers to greater pain as compared to below two levels.

The section above the domain names in the pyramid is occupied by the host and network artifacts. It is mentioned in light yellow which indicates the start of the painful effect on the adversary because of the greater struggle of a security analyst in discovering that indicator. It always requires a greater effort for an analyst to understand and detect a well-structured attack. Once he manages to detect it, it means the attack needs to be restructured by the attacker to not get detected again. So, for that, an attacker would suffer pain by reconstructing the attack keeping in mind how it got detected before and he would also need to know through research what methods are utilized by an analyst for the detection. This discovery of the host and network artifacts would make an adversary rebuild the tool by discerning the artifact that caused the discovery. Discovering, fixing, and conquering such barriers requires the great effort and time of an adversary.

Further up is the section of the tools in the pyramid that is represented in yellow color. If a security analyst detects a tool, it would cause an adversary to spend more time in research to develop a new tool that would be more efficient to perform an attack. This would lower the attacker’s performance and lengthen the amount of time required to make their attack.

Lastly, the pinnacle of the pyramid is dedicated to TTPs which, if identified and detected, would cause the worst effect on the adversary. This would compel an adversary to either restart the complete attack process or. At this point, a security analyst knows the complete approach of the adversary.

### Self-Check Questions

1. Name any three levels of The Pyramid of Pain model.

*Domain Names*

*IP Addresses*

*Hash Values*

*TTPs*

*Tools*

*Network/Host Artifacts*

Summary

The unit discussed the concept of threat modeling with some of its well-known techniques. The technique of attack trees was discussed, and it assists in identifying a threat by modeling it in a hierarchical structure in terms of nodes. We also discussed the STRIDE threat modeling technique, which is utilized by software developers for threat identification. Then, the DREAD model was explained in detail. This model describes the prioritization of a threat after its identification. Finally, the Pyramid of Pain model was explained. This models various levels of the threats in terms of the impact (or pain) caused to an adversary if that threat is detected by an analyst.

# Unit 4 – Attack Libraries

**Study Goals**

On completion of this unit, you will be able to …

… recognize publicly available attack techniques by using the CAPEC attack library.

… understand privacy violations and their harms using Solove’s Taxonomy of Privacy.

… apply the MITRE ATT&CK framework to discover the attacker’s advanced techniques and tactics.

… identify new attack types based on current threats.

# 4. Attack Libraries

## Introduction

In the domain of cyber security, a security practitioner must keep himself updated with the current threats landscape and attack vectors. To provide an up-to-date, centralized, and ever-evolving knowledge database to security practitioners, the concept of attack libraries is evolved. An attack library refers to various centralized databases that are considered and consulted to evaluate and understand the current techniques utilized by adversaries. In this unit, various well-known attack libraries will be discussed.

A Common Attack Pattern Enumeration and Classification (CAPEC) will be discussed in detail to understand the operations of the adversary. This is also useful in the implementation of a strong cyber security program. CAPEC is an extensive dictionary that comprises the well-known techniques utilized by the attacker to exploit vulnerabilities in network infrastructure.

Afterwards, a detailed discussion will be carried out on the concept of privacy and the different harms and consequences one could face if it is compromised. We will investigate the detailed discussion of privacy in reference to Solove’s Taxonomy of Privacy (2006). This would help us to identify the privacy problems and to categorize the damages that could potentially arise from its compromise.

Subsequently, we will study and discuss the MITRE ATT&CK framework. It is one of the well-known globally accessible databases mostly leveraged by threat intelligence analysts to identify an adversary’s tactics, techniques, and approaches to execute a cyberattack against a victim. Since MITRE ATT&CK is a continuously updated database, therefore it also helps in modeling and identifying cyberattacks which then enable an organization to implement proper security controls according to the current threat landscape.

## 4.1 CAPEC

CAPEC is an attack library from MITRE that provides a publicly accessible centralized catalog for security professionals. It was established and proposed by the U.S. Department of Homeland Security and was first released in 2007 (CAPEC™, 2019).

CAPEC contains well-known attack patterns that help professionals comprehend the behavior of **adversaries** in exploiting vulnerable applications. It continuously updates the public’s contribution and participation to create a standard procedure for the identification, collection, improvement, and sharing of attack patterns among the cyber security community. The term “attack patterns” is worth noting here. It refers to the descriptions and explanations of the techniques and approaches utilized by adversaries to exploit vulnerabilities that lead to a compromise. Attack patterns describe the difficulties and challenges that attackers might face and how they could overcome them. An attack pattern gives you complete knowledge about designing and executing an attack and provides guidance and direction about how to mitigate the impact of the potential attack by selecting appropriate security controls. It should be noted here that, unlike MITRE ATT&CK, CAPEC focuses on application security (CAPEC™, 2019). A detailed discussion of MITRE ATT&CK is covered in section 4.3.

**Adversaries**

individuals or organizations that execute malicious operations

The main benefits and usage of CAPEC attack vectors include

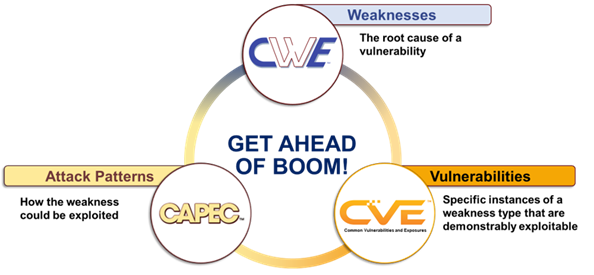
* penetration testing,
* the education and training of software developers,
* applications threat modeling,
* the definition of potential threats, and

**Buffer overflow**

This is an attack that takes place when the size of data surpasses the capacity of memory.

* risk analysis of applications architecture.

CAPEC listings are related to Common Vulnerabilities and Exposures (CVE) and Common Weakness Enumeration (CWE). The term CWE refers to the baseline for weakness identification, mitigation, and prevention efforts, whereas CVE is a specific instance of weakness within some system or product that is exploitable. For example, a **buffer overflow** attack would be termed as CWE but the mistake in an application code by the developer that helps an attacker compromise an application leading it to a buffer overflow attack is called CVE. CAPEC attack pattern leverages a CWE to carry out an attack as shown in the figure below. Therefore, the CAPEC attack patterns contain a complete “execution flow” – complete instructions for an attacker to compromise a target. An example of an execution flow of CAPEC’s attack pattern is discussed next sub-section.

The Relationship Between CAPEC, CWE, and CVE

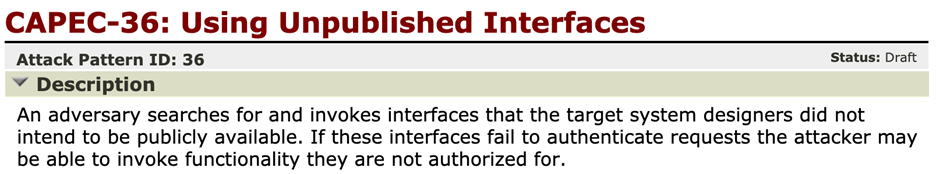
Source: MITRE (2021b). © 2023 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation.

### Understanding CAPEC’s Attack Pattern With an Example

To understand the concept of attack pattern in detail, let us discuss in detail one of the CAPEC’s well-known attack patterns – “Using Unpublished Interfaces” – and discern how different characteristics of attack patterns are beneficial.

An ID is associated with each CAPEC entry. This numerical ID does not indicate any information, except to specify when this entry was added to the database. Each entry has a title and description. The description is a complete summary of an attack pattern and what it is all about. This information is shown in the figure below. The number 36 is the ID and “Using Unpublished Interfaces” is the name of the attack pattern in the example shown in the figure below.

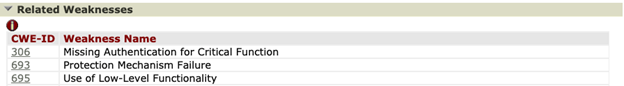
Name, ID, and Description of CAPEC’s Attack Pattern



Source: MITRE (2021b). © 2023 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation.

The weaknesses for each attack pattern can be found under the “Related Weaknesses” portion that an adversary could exploit. The “Related Weaknesses” section for CAPEC-36 is shown in the figure below.

Related Weaknesses for CAPEC-36

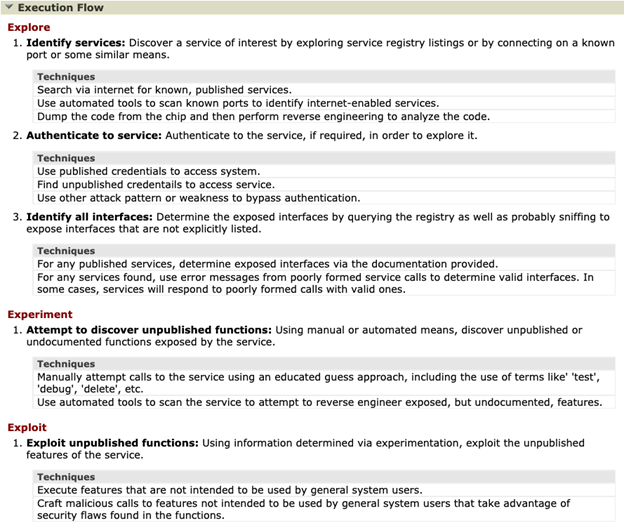


Source: MITRE (2021b). © 2023 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation.

If we analyze the above two figures, it could be seen that the attack pattern and the weaknesses do not seem to be related and there does not necessarily need to be a one-to-one relationship. The attack pattern needs to leverage these weaknesses to execute an attack.

Next is the portion of the “Execution Flow,” which shows complete step-by-step instructions on how to execute an attack. The “Execution Flow,” portion for CAPEC-36 is shown in the figure below.

Execution Flow of CAPEC-36



Source: MITRE (2021b). © 2023 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation.

The execution flow is divided into three phases:

1. **Explore:** In this phase, multiple ways are described in order to discover a potential victim to attack. There is more than one step in each of the three phases. Each step describes multiple techniques to perform that step.
2. **Experiment:** Once a victim or target has been discovered, techniques presented in the experiment phase are leveraged to identify whether the target has weaknesses that this specific CAPEC wants to exploit.
3. **Exploit:** This phase of the execution flow suggests techniques to execute the actual attack.

It should be noted here that the execution flow of any CAPEC attack pattern not only helps to execute an attack but also assists in determining if the victim is vulnerable.

Subsequently, there is a section named “Consequences” that shows the potential repercussions after the successful execution of the attack by using the attack pattern. For example, the figure below shows the “Consequences” section for CAPEC-36.

Consequences of CAPEC-36



Source: MITRE (2021b). © 2023 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation.

A significant point to note here is that entries listed in CAPEC are not established on the attack’s consequences. These are based on how to successfully exploit a target’s weakness that causes the consequence. For example, for denial-of-services (DoS), there is no CAPEC entry. However, various attack patterns could be utilized which cause DoS. Here, DoS is a consequence, not an attack pattern.

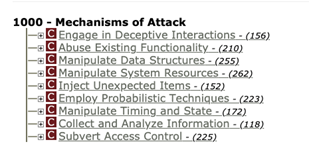
**Views**

CAPEC’s view is the representation of a perspective that assists one looking at the different collections of attack pattern inside CAPEC.

Additionally, there are two **views** through which CAPEC entries are demonstrated. CAPEC entries are pre-defined and arranged under these views. These views are:

* **Mechanism of Attack:** This view is used to emphasize the different entries of the CAPEC that could be utilized to attack various domains of cyber security. An example of the “Mechanism of Attack” view is shown in the figure below.
* **Domains of Attack:** Similar attacks are grouped in this view. An example of this view is shown in the figure below.

Mechanisms of Attack View



Source: MITRE (2021b). © 2023 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation.

Domains of Attack View



Source: MITRE (2021b). © 2023 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation.

In both of the figures above, the next level of the subtree could be opened by clicking on the “+” sign.

### Exploring CAPEC Website

This sub-section explains how one could use the CAPEC website for research, for example, if you are asked by your chief information security officer (CISO) to check whether the new system is vulnerable to SQL injections. Then you could leverage two common methods to navigate through the CAPEC website to extract necessary information according to the requirements.

#### Keyword search

A search feature is available on the CAPEC website as shown in the figure below.

Exploring CAPEC using Keyword Search - I



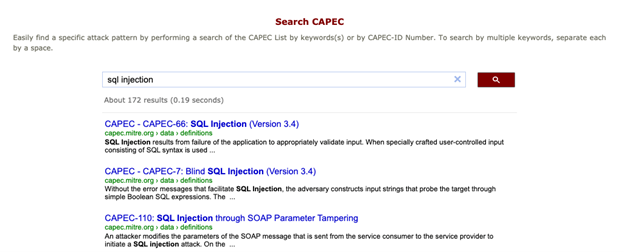
Source: MITRE (2021b). © 2023 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation.

Any keywords, IDs, or common terms could be searched. For instance, imagine we want to search for information related to a structured query language injection, known as an **SQL injection**. The process that should be followed is given in the figure below, in which we get different results after typing “sql injection” in the search bar.

**SQL Injection**

This is a web application vulnerability that is leveraged by an attacker to send malicious commands to database via web application.

Exploring CAPEC using Keyword Search - II

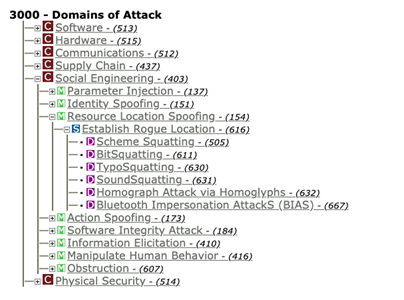


Source: MITRE (2021b). © 2023 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation.

#### Using views

We already discussed how CAPEC entries are organized into views. We can traverse any view according to the area of our interest. For example, if we are interested in the attack patterns of social engineering, we explore the “Domains of Attack” view to see the CAPECs associated with this domain as shown below.

Exploring CAPEC Using Views



Source: MITRE (2021b). © 2023 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation.

### Self-Check Questions

1. Please complete the following sentence.

In the domain of *cyber security,* a security practitioner must keep himself updated with the current *threat* landscape.

## 4.2 Solove’s Taxonomy of Privacy

“Privacy” is a broad term that refers to a diverse group of connected things. Using such a term could be helpful at times, but it might be unhelpful when using it in other contexts. For instance, consider the word “animal.” The term “animal” encompasses a huge group of creatures such as reptiles, mammals, fish, birds, etc. There are then sub-groups inside each of such groups. Using the term “animal” will be enough in some scenarios. Suppose Alice asks Dimitri, “What is the exact count of animals in that zoo?” John does not have to know precise details to reply to this question as the usage of the word “animal” in the question is clear in this context. Now assume Alice wants to buy a cat and ask John for it. In this context, using the term “animal” will not suffice as she will have to specify the type of animal she desires. Like the broader term “animal,” we can use the term “privacy” in general. But at times using the term “privacy” by itself may lead to confusion when the issues are placed before policymakers and courts.

This taxonomy illustrates the connections between various problems and harms. It is not uncommon that many problems are stated as violations of privacy as they are very similar. But we must also understand where they differ. The objective is to determine the problem according to the context, its uniqueness, how it varies from other problems, and how other privacy problems are related to it.

Usually, these problems cause harm to people. Harm such as injuries could be understood easily. A violation of privacy represents a difficult case. When we speak about privacy, it should be considered as something intangible or nonphysical rather than a physical injury. Security researchers and authors Warren and Brandeis contended that the violation of the privacy of an individualleads to injury to emotions and feelings (as referenced in Solove, 2006).

Brandeis and Warren spoke about the dignitary harms of an individual. Reputational injury is a classic example of such harm. They intended to indicate that these types of harms are genuine and legally cognizable in which they succeeded (as referenced Solove, 2006, pp. 485–487).

In this taxonomy, harmful activities are divided into four groups (Solove, 2006, p. 488):

1. Information collection
2. Information processing
3. Information dissemination
4. Invasion

These groups are arranged around a paradigm that starts with a data subject. A data subject is an individual who is directly impacted by the events and activities arranged in this taxonomy. Different entities such as governments, businesses, and people collect information from such individuals. Entities that collect, store, manipulate, combine, search, and utilize the data are called data holders. All these activities are called “information processing” in Solove’s Taxonomy of Privacy. After the information processing, data holders share, release, or transfer the information with others. This step is termed “information dissemination” in the taxonomy. The model of the taxonomy shows that data is moving away from the power and control of an individual as it is aggregated, collected, processed, and disseminated. The last activity is termed “Invasion” which directly impacts the individual (Solove, 2006, pp. 488, 489).

Information collection is the primary group that contains the activities impacting the privacy of a subject. These activities are the following:

* **surveillance**: In this activity, recording, listening to, or watching the subject’s activities is performed.
* **interrogation**: Multiple ways of questioning and information probing falls under this category.

The second group refers to the activities that include the techniques through which information is manipulated, stored, and used. This collection is referred to as Information processing. Activities included in this group include the following:

* **aggregation:** This refers to the process of combining multiple bits of data about an individual.
* **identification:** This is the process of linking the information to specific individuals.
* **insecurity:** This is the lack of protection of collected information from unauthorized access and leaks.
* **secondary use:** This refers to the utilization of collected information for a purpose other than the one it is collected for without the consent of the subject.
* **exclusion:** This activity considers the failure of allowing the data subject to be aware of the information that other people have about him and take part in its use and handling.

All the above activities of the second group discuss the approaches to data used and maintained rather than gathering data, which has already been collected in the first group of activities (Solove, 2006, p. 490).

Dissemination of information is the third group that involves the following activities:

* **breach of confidentiality:** This involvesfailing to keep a data subject’s personal information confidential.
* **disclosure:** This is revealing genuine information about an individual that would influence the judgment of others towards him.
* **exposure:** This involves the revelation of another’s grief, bodily functions, or nudity.
* **increased accessibility:** This is amplification in access to information.
* **blackmail:** This is a threat given to disclose personal information.
* **appropriation:** The utilization of an individual’s identity to assist the interests and aims of another.
* **distortion:** This is the dissemination of misleading and fake information about data subjects.

All the activities that are discussed above involve the transferring or spreading of an individual’s data (Solove, 2006, p. 491).

The last group involves activities that target invasions into individuals’ private affairs. The activities in this group include the following:

* **intrusion:** This is the act of disturbing the individual’s solitude or tranquility.
* **decisional interference:** This is the involvement of government in the individual’s decisions impacting his private affairs.

### Self-Check Questions

1. Please complete the following sentence.

Privacy is a *broad* term.

## 4.3 Mitre ATT&CK®

MITRE ATT&CK was developed in 2013, and ATT&CK is an acronym that stands for Adversarial Tactics, Techniques, and Common Knowledge. It was created by the researchers in the Fort Meade Experiment (FMX) at MITRE where they emulated both defender and adversary behavior to improve the detection of threats after compromise through behavioral analysis. The essential question that researchers faced was “How efficient are we performing in detecting adversarial behavior through documentation?” To answer this, the researchers created ATT&CK, which then was utilized as a useful tool to classify adversary behavior (Trellix, n.d.).

The MITRE ATT&CK framework reflects the different stages of the attack performed by the adversary as well as the victims and platforms they typically target. The concept of tactics and techniques shown in the model gives a common classification of adversary activities that can be easily perceived by both defensive and offensive teams of cyber security (Trellix, n.d.).

The following main components are given in the behavioral model of ATT&CK (Strom et al., 2018):

* **tactics**: This denotes the short-term adversary goals and objectives during the attack (and is presented in columns).
* **techniques**: This shows the broader ways using which the adversaries achieve their tactical goals (and is presented in individual cells).
* **Sub-techniques**:This concerns more specific ways the adversary utilizes to achieve the tactical goals.

MITRE ATT&CK can also be viewed as three main iterations also known as matrices:

|  |  |  |  |
| --- | --- | --- | --- |
| MITRE ATT&CK VIEWS | | | |
| **ATT&CK for ENTERPRISE** | **ATT&CK for MOBILE** | **ATT&CK for ICS** |
| This matrix highlights the adversary’s  behavior in Linux, Mac, Windows, and  Cloud environments. | This matrix highlights the adversary’s  behavior on Android and IOS operating systems. | This matrix focuses on the actions that an adversary might take while attacking an industrial control system (ICS) network. |

Source: Zohaib Hassan (2023), based on Trellix (n.d.).

MITRE ATT&CK is leveraged worldwide within various domains that include but are not limited to red teaming, intrusion detection, security engineering, threat hunting, and risk management (Strom et al., 2018).

### The MITRE ATT&CK Matrix

The MITRE ATT&CK framework or model is represented in the form of a matrix that contains a collection of techniques utilized by adversaries to achieve a specific goal. These goals are categorized and called tactics in ATT&CK Matrix. The goals are represented linearly starting from “reconnaissance” to the last objective, “impact.” Looking and analyzing the extensive version of ATT&CK for Enterprise (which comprises Linux, macOS, Windows, Office 365, Azure AD, and Cloud Networks), the following fourteen adversarial tactics are grouped and categorized (Trellix, n.d.):

1. **Reconnaissance**: This involves collecting information to plot future adversarial operations such as target organization’s information.
2. **Resource Development**: This concerns setting up resources to assist operations such as establishing a command & control infrastructure.

**Spear phishing**

a technique used to target an individual using an email scam or through any other means through the internet

1. **Initial Access:** This is the process of getting access into the victim’s network, for example, via **spear phishing**.
2. **Execution**:This involves trying to execute the malicious code on the victim’s network or system i.e., executing a running tool that could be controlled remotely.
3. **Persistence**: This concerns attempting to maintain the foothold, for example by manipulating the target’s configurations.
4. **Privilege Escalation**:This involvestrying to obtain access to high-level privileged accounts such as root user accounts on Linux or administrator accounts on Windows. This could be done by exploiting a vulnerability in a compromised system. This is because the system has already been compromised at this stage but the adversary has the access to low-level user permissions.
5. **Defense Evasion**: In this case, an adversary tries to avoid being caught or detected, for example, by utilizing a trusted process to conceal malware.
6. **Credential Access**: In this situation, the adversary tries to steal passwords, names, and accounts. For instance, this could be via keylogging.
7. **Discovery**: In this case, an adversary tries to find out the target’s environment to explore what could be controlled.

**Pivoting**

leveraging a compromised system to attack another system

1. **Lateral Movement**:In this case, once the adversary gets the authorized credentials, he legitimately moves through the environment by **pivoting** through various systems.
2. **Collection**: This involves collecting data that is in the interest of the adversary for achieving the objective. For example, this could involve gaining access to the cloud’s data.
3. **Command and Control**: This is the stage where compromised systems and networks are controlled and communicated by the adversary, i.e., mimicking the legitimate web traffic in order to communicate and control the victim’s network.

**Ransomware**

a special malware created to prevent organization and user accessing the files on the computer by encrypting it and demands a ransom (payment) to undo the operation

1. **Exfiltration**: This concerns stealing the victim’s data and transferring it.
2. **Impact**: This involves interrupting, manipulating, or demolishing data and the system. For example, encrypting the victim’s data through **ransomware**.

The actual operation performed by an adversary is described by techniques mentioned inside each tactic that is discussed above. Some techniques are further divided into sub-techniques that define how a particular technique is carried out by the adversary. The complete Enterprise ATT&CK Matrix 2021 is shown below, and it lists complete tactics with their techniques. To view it more clearly, the same matrix could also be accessed from the MITRE ATT&CK website.

### Utilizing a MITRE ATT&CK Matrix?

Organizations and security professionals could leverage the ATT&CK Matrix in multiple ways. Generally, the following are the most common benefits of utilizing the matrix (Trellix, n.d.):

#### Red teaming

This is a complete attack that is emulated within an organization from the adversary’s perspective to determine the potential impact after a breach. This process could also be termed “adversary emulation.” The process is also carried out to test the security defenses of the organization. The ATT&CK matrix could be utilized to organize and execute red team operations.

Grouping of Activities in Solove’s Taxonomy of Privacy

Table

Description automatically generated

**Advanced persistent threat**

This is a special cyber-attack also known as state-sponsored or nation state in which the attacker manges to hide himself for a very long time on a compromised system and remains undetected.

Source: MITRE (2021a). © 2022 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation.

#### Threat intelligence

ATT&CK could be utilized by threat analysts as a vast source of information to keep up to date with the latest cyberattacks and threat landscape. It allows the defense teams to assess how resilient they are to a cyberattack by assessing their security measures against **advanced persistent threats** (APTs).

#### SOC assessment

The Security Operations Center (SOC) is a dedicated environment within an organization whose function is to detect, monitor, investigate, detect, and respond to cyberattacks. Since the ATT&CK Matrix is used to emulate an attack, this emulation would also help to assess the effectiveness of SOC in detecting the attack.

The implementation of MITRE ATT&CK usually is carried out by mapping the threats manually or integrating them with cyber security tools, and the most-utilized tool is called Security Information and Event Management (SIEM). Integrating SIEM with MITRE ATT&CK involves collecting **logs** from the enterprise network, identifying the threats, and then mapping them to ATT&CK Matrix.

**Logs**

automatically generated, detailed information of events

Apart from utilizing MITRE ATT&CK for the above-mentioned and common activities, this framework could also be leveraged for other cyber defense operation, e.g., cyber forensics and threat hunting.

### Self-Check Questions

1. Please complete the following sentence.

ATT&CK was developed in the year *2013* by the *MITRE* organization.

## 4.4 Identifying new Cyberattacks

A security professional, an employee, a student, or even a normal internet user should have at least basic knowledge for identifying a cyberattack or malicious activities that could lead to a cyberattack. It is imperative because attackers usually try to gain human trust and then force them to perform some illegal activity such as sharing confidential company information. When people are trained and aware of the different techniques attackers use, it becomes much more difficult to compromise them.

In this section, we will be discussing how to identify a cyberattack or any malicious activity by looking for some of its important signs. Identifying some of the most common cyberattacks that might lead to massive data breaches are discussed below (Stanfield, 2022):

### Hacked Email Account

The following are signs that indicate an email account has been compromised:

* The password has been altered.
* Unusual activity is seen in the inbox and among sent emails.
* Emails for password resets are received in the inbox from other websites.
* The email account is accessed from some unexpected location and IP address.
* You have been informed by your email contacts that they are continuously receiving strange emails from your email account.

### Hacked System Account

The following are signs that indicate a system account and its details have been compromised.

**Add-on**

a small program that extends the features of a browser

* There is a significant decrease in computer speed.
* Your system’s antivirus has been compromised or disabled automatically.
* Suspicious **add-ons** start appearing on your browser.
* Random restarts and shutdowns are happening.
* You lose access to the system account.
* You experience unusual activities such as the automatic movement of the mouse pointer and flipping off the monitor screen.

### Hacked Cloud Storage Account

Cloud storage accounts are where users store their data online. Examples of cloud storage accounts are OneDrive, DropBox, Google Drive, and iCloud. The most common signs that an online account has been hacked include the following:

* You see some unusual content uploaded to your online account.
* The account cannot be accessed.
* Data is missing or altered.
* There is bizarre traffic going out from the network via your account.
* You get notifications that the account is being accessed from multiple locations.
* There are enormous read operations on your online account.
* Your contacts receive fake emails with malicious attachments and links from your account.

### Hacked Social Media Account

Social media accounts such as those offered by Facebook, Instagram, Twitter, and TikTok, are being used by billions of people in today’s digital era. Hacking a social media account is a lucrative target for an attacker to gain further access to sensitive information and wreak havoc. Signs that should be looked for in a hacked social media account include the following:

* Changes occur in the follower count.
* Unnecessary friend requests flood out from your account.
* Your previous posts are deleted.
* The password suddenly changes.
* You get notifications that that account is being accessed from multiple locations.

### Hacked Network

A network is the collection of two or more electronic devices (e.g., computers) that are joined together to share data and information. If a network of a small, medium, or even large organization is hacked, it might lead to a massive data breach as sensitive information is kept in the systems forming a network. The most common indications of a hacked network are the following:

* The files have been encrypted.
* The network becomes unusually slow.
* Network utilization becomes very high.
* Programs are constantly crashing.
* Systems are operating without any input.
* Users are getting ransomware messages on their computer screens.

### Self-Check Questions

1. Please complete the following sentence.

Usually, the hacker first tries to exploit human *trust*.

Summary

In this unit, we explicitly discussed CAPEC, a dictionary that contains the most popular techniques used by adversaries. We understood how we can improve the cyber defense program of an organization by figuring out what could potentially be the next move of the adversary and applying proper security measures beforehand. We then looked into research work where the concept of privacy is presented as A Taxonomy of Privacy. We discussed how we can utilize this concept in understanding the problems related to privacy and the potential consequences as a result of its compromise.

Furthermore, the MITRE ATT&CK framework was addressed in detail. This is a database that is constantly being updated with the tactics and techniques used by the adversaries. We saw how a threat intelligence analyst could utilize this database to stay one step ahead by modeling threats using tactics and techniques mentioned in the framework. Lastly, we discussed some of the major signs of hacking and compromised accounts that would help even a normal internet user to identify and remedy a cyberattack.

# Unit 5 – Rules, Regulations, and Law Enforcement

**Study Goals**

On completion of this unit, you will be able to …

… understand the concept of cyber laws.

… explain the concept of compliance and regulatory requirements.

… identify the concept of and need for law enforcement in cyberspace.

# 5. Rules, Regulations, and Law Enforcement

## Introduction

In the domain of cyber security, we often use the word “cyberspace.” This term was first coined by William Gibson in the early 1980s in his science fiction novel Neuromancer (Bussell, 2013). Gibson illustrated cyberspace as a virtual landscape that is created by computer networks. Today, cyberspace is considered an environment where communication takes place over a computer network. Cyberspace could also be called a virtual medium because communication takes place over the internet between electronic devices with no physical boundaries. Understanding the term cyberspace is imperative whenever there is a need to discuss laws and regulations in cyber security, as it is the frequently used term in the literature.

When the internet was developed, developers and researchers realized that it would become a beast that can be leveraged for various immoral and illegal activities and that, eventually, strong laws would be needed to control its usage in cyberspace. Various alarming activities occur in cyberspace such as money laundering, terrorism, and identity theft. These are grey areas that created a necessity for cyber laws.

**Regulatory compliance**

Rules that must be followed by organizatons to protect critical information and individuals from cyber criminals

This unit discusses and explains the cyber laws that need to be followed when communication takes place in cyberspace. Subsequently, the concept of compliance will be discussed to outline how an organization should follow international standards to ensure **regulatory compliance** or security of the information from a cyberattack. Furthermore, the concept of law enforcement will be discussed in the context cyberspace, as well as how organizations get assistance in addressing cyber criminals by sharing threat intelligence data with the agencies.

## 5.1 Cyber laws

In today’s digital era, the internet has grown to be an essential aspect of everyone’s daily life, from simple communication to web-based shopping. Almost every organization utilizes the web for its day-to-day operations. This resulted in the growth of **eCommerce**. Various governmental operations are also occurring online, and **eFinance** is also on the rise. With the rapid increase in the usage of the web, the threats affiliated with it also augmented. Cyber law works as a safeguard for the communications that took place over cyberspace and also hinders cybercrimes from taking place to some extent. Creating a cyber law is although a challenging task for lawmakers, and they are constantly creating, updating, and establishing these laws to restrict illegal and questionable activities that happen online or in cyberspace (UNext Editorial Team, 2020).

**eCommerce**

Also known as electronic commerce, this refers to the selling and purchasing of services and goods through the internet.

**eFinance**

financial services carried out over the internet

### What is Cyber Law?

Cyber law is also known as internet law or information technology (IT) law. It is defined as a legal structure created to tackle the communications that take place over the internet and associated legal issues. Since we are talking about a law that deals with an environment that has no physical boundaries, Cyber law can also be referred to as a “paper” law for a “paperless” world (UNext Editorial Team, 2020).

Cyber law comprises aspects of contract law, intellectual property, data protection, jurisdiction, freedom of speech and expression, and privacy. It directs and ensures (UNext Editorial Team, 2020)

* how the digital circulation of information should be carried out,
* the provisioning of legal identification and acceptance of eDocuments, and
* the creation and establishment of a legal structure for online transactions.

In a nutshell, cyber law could be perceived as an infrastructure that provides legal grounds to tackle cybercrimes (UNext Editorial Team, 2020).

Cyber laws that are enforced for cyber security differ from jurisdiction to jurisdiction and from country to country. The penalties also vary from fines to jail sentences on the basis of the cybercrime committed. Therefore, citizens must understand the cyber laws that they are supposed to follow within their countries. It is worth noting here that the Computer Fraud and Abuse Act was the first law introduced in cyberspace in 1986 that restricted unauthorized and illegal access to digital assets (such as computers) and the unlawful utilization of digital information (UNext Editorial Team, 2020).

### The Significance of Cyber Law

**Due diligence**

doing proper research to discover weaknesses

Cyber law comprises rules and regulations that instruct people, companies, and organizations on how the internet should be used. There are some rules within the law that give protection to people from cybercrimes executed by cyber criminals through the internet. Cyber law could be comprehended by the below-given points (UNext Editorial Team, 2020):

* It preserves the tracking of all electronic records.
* It dictates what actions and reactions are to be performed within cyberspace.

**Due care**

The implementation of proper security measures after the identification of weaknesses

* It regulates every online activity.
* It provides security for the digital information of organizations, the government, and individuals.
* It enforces performing **due diligence** and **due care.**
* It assists in establishing electronic governance.

### Why do we Need Cyber Law?

More than 4.6 billion of the world’s population are using the internet not only for their daily communication but also for online transactions and eCommerce activities (UNext Editorial Team, 2020). With the rapid growth of the utilization of cyberspace, enforcement of rigorous cyber rules assists in setting up a secure environment on the internet. A cyber law provides deterrence in a way that a victim could take action against the person who is discovered breaking cyber laws or rules which would not have been possible if no cyber law existed (UNext Editorial Team, 2020).

### The Multiple Elements/Sections of a Cyber Law

There are various components within a cyber law that address the protection of digital information. Some of these components are discussed below (UNext Editorial Team, 2020):

* **protecting privacy and data**:To comply with cyber law, organizations must ensure the protection of data and private information from cyber criminals. These laws enforce deterrence for people in the digital environment and hinders them from the misuse of private information of any user.
* **cybercrime**:Cybercrimes are referred to as any illegal activities that are carried out on the internet. Examples of such crimes are hacking, extortion, money laundering, and cyberbullying, to name a few. Cyber law provides accountability against such acts if it exists in the country.
* **intellectual property**: Anything that the work of a group or individual, including inventions, designs, symbols, or any intangible element that is copyrighted, is known as the intellectual property of that group or individual. Cyber law gives protection from the illegal use or stealing of intellectual property.

### Types of Cybercrimes

Cybercrimes are divided into multiple categories but generally, they are grouped into three types discussed below (UNext Editorial Team, 2020):

1. **Property**:Illegal possession and usage of digital information, transmission, and usage of malicious programs, theft of financial information, etc., are examples of property cybercrimes.
2. **Individual**: Stealing personal information, online harassment, sharing child pornography, and using vulgar and obscene data are the most common examples of cybercrimes that are carried out against individuals.
3. **Government**: Cybercrimes that one government executes against another government fall under this category. These crimes are also known as advanced persistent threats (APTs) or nation-states and are carried out by a group of experts.

**Digital Signatures**

A mathematical calculation or technique applied to confirm the integrity and authenticity of a digital document, software, or electronic message

### Objectives of a Cyber law

The main objective of introducing a cyber law is to control and maintain the rule of law in each type of online activity and to mitigate cybercrime. Some of the main objectives that are achieved through cyber law apart from this are given below that will help us understand it better (UNext Editorial Team, 2020):

* Unlike paper-based transactions and communications, legal authentication and recognition of the transactions that are carried out on the internet are provided by cyber law.
* Because of cyber law, the concept and implementation of **digital signatures** has become widespread.

**eFiling**

The submission of tax returns through the internet

* Cyber law promotes the **eFiling** of documents to government agencies and departments.
* It permits fund transfers through the internet, namely electronic funds transfer between banks, financial institutions, persons, and so on.
* It legally allows banks to keep account information electronically.

### Types of Illegal Online Activities Addressed by a Cyber Law

In this sub-section, we will discuss some of the important types of illegal online activities that are addressed by cyber law. These are discussed below (UNext Editorial Team, 2020):

* **copyright**:This protects individuals’ and companies’ rights to earn revenue from the original work they created. Therefore, the misuse of copyrighted material is indirectly violations of the cyber laws of that country or jurisdiction. Hence, nowadays, in the presence of cyber law, violation of online copyrighted material is extremely hard.
* **defamation**: Spreading fake statements on the internet or social media could lead to defamation of public figures, businesses, or even a common person. This is an offense that is addressed by a defamation law that allows an internet user to execute a legal procedure against an adversary. It should be noted here that the adversary could be a professional or a normal internet user, because spreading fake statements could even be done by creating a fake social media account in the name of the victim that does not require any special technical expertise.
* **fraud**: Cyber law offers protection to individuals from fraud carried out on the internet. Online fraud includes but is not limited to money-related illegal activities that are carried out on the internet, **identity theft**, and credit card data theft. People face criminal charges if they carry out online fraud.

**Identity theft**

Committing scams or frauds by using a stolen identity is called identity theft.

* **stalking and harassment**: Stalking and harassment involve posting threatening or intimidating statements on social media about an innocent person. This is a malicious act and violates civil and criminal laws, which will be discussed later.
* **freedom of expression**: The internet is a medium that allows its users to express their expressions with freedom. However, there are certain boundaries that if crossed, would lead to the violation of the cyber law.
* **trade secrets:** Trade secrets are a kind of intellectual property, for example, a technique designed and utilized by an organization to manufacture their products. Stealing trade secrets is also a violation of cyber law and therefore, cyber law also gives protection to companies by empowering them to take legal action against the suspect organization.
* **employment and contracts laws:** It is always seen on websites or when downloading software that one needs to agree with the terms and conditions before accessing or using it. Usually, most people don’t take it seriously; regardless, this also falls under a cyber law that protects online privacy.

When discussing laws in cyberspace, it is important to know and understand the difference between criminal law and civil law as they are also thoroughly discussed when cyber laws are discussed. The following section explicitly discusses criminal and civil law.

### Distinguishing and Understanding Criminal and Civil Law

There are some differences between criminal and civil law that should be outlined.

#### Criminal law

Criminal Law refers to a law that forbids behavior hated by society. This law is generally enforced by state agencies, for example, inhibitions against computer hacking and bank fraud. Criminal law could be described as the combination of the following (Rashid et al., 2019, p. 55):

* **deterrence**:This involves discouraging bad behavior, for a criminal specifically and society members in general.
* **incapacitation**: This is restricting a criminal’s ability to further damage society.
* **retribution**:This concerns causing some kind of loss to the criminal to make him suffer in reaction to a crime he committed.
* **restitution**:This involves compelling a criminal to give some compensation to a victim.
* **rehabilitation**:This is seeking to transform the long-lasting behavior of the criminal.

Terms like “innocent” and “guilty” are usually reserved as explanations of outcomes (verdicts) in criminal proceedings. Hence, these wordings should not be utilized when explaining the verdicts of a civil case (Rashid et al., 2019, p. 55). Punishments that are available in criminal law encompass criminal fines usually paid to a state, forfeiture and seizure of proceeds of crime, financial or any other restitution paid to a victim, and prison sentences (Rashid et al., 2019, p. 55).

#### Civil (non-criminal) law

#### Civil law governs private relationships between and among persons. For example, this includes laws of negligence and contract. Injuring a person because of a violation of civil law could initiate legal proceedings against the culpable party (Rashid et al., 2019, p. 55).

Remedies that a civil law provides based on the situation might contain a few combinations of the following:

* Compensation is paid to the injured by the liable.
* Legal relationships between the parties is terminated.
* A liable party is given the order to terminate harmful activities.
* A liable party must perform an affirmative, act such as transferring ownership of property.

The rules of civil law are usually created in an attempt to rectify the negative outcomes of the behavior in society. Furthermore, people who are aware of the laws would make them more responsible and ultimately change their behavior toward cyber security (Rashid et al., 2019, pp. 55, 56).

### Self-Check Questions

1. Please list any two key activities companies or people perform in their day-to-day activities on the internet.

*eCommerce*

*eFinance*

*Online transactions*

*Web-based shopping*

*Communication*

## 5.2 Compliance and Law Enforcement

Implementing cyber security in an organization is a complex task that integrates a resilience-centered strategy towards hardware and software infrastructures that are exposed to the internet to eliminate the potential vulnerabilities which might impact customers, companies, and pertinent **stakeholders**. Regulatory compliance assists and enforces organizations in implementing that resiliency against cyberattacks (NordLayer, 2022).

**Stakeholder**

An organization or individual that has the right, claim, interest, or share in the system that meets their expectations and needs.

### What is Compliance in Cyber Security?

Cyber security compliance is the implementation of security controls that are aligned with the industry standards such as ISO 27001. The **information security management system** (ISMS) of any organization which is compliant with the regulatory requirements enables them to implement necessary security measures that would potentially decrease the probability of a data breach. This also enables an organization to set a plan for a situation if a breach happens such as communicating the impact and facts of a breach to the affected parties (NordLayer, 2022).

**Information security management system**

a framework of controls and policies that manages risks and security methodically across an entire organization

### Importance of Cyber Security Compliance

It is imperative to admit cyber security compliance is not only a bunch of mandatory and strict requirements that come from a regulatory body, but also influential to the overall success of the business.

Any organization that exists in cyberspace is a potential target of a cyberattack. If a data breach happens, the situation could probably escalate to a complex situation that could impact the organization financially and reputationally, resulting in disputes and legal proceedings. Hence, a company that meets cyber security compliance requirements or standards would alleviate the risk of a cyberattack (NordLayer, 2022). The following are some of the advantages of cyber security compliance:

* It assists in evading heavy sanctions and fines.
* It protects the organization’s prestige by evading non-compliant activities.
* It supports and ensures clients’ privacy right to access, modify, or erase their data, which would eventually bolster business functions.
* It helps organizations to establish trust among the stakeholders by proving that the organization has performed its due diligence to protect the collected data.
* It assists organizations in meeting the requirements of pertinent laws and regulations by implementing the necessary security controls.
* It promotes accountability and transparency in organizations.

#### Industry standards

Aligning security standards into businesses helps security professionals avoid misinterpretations among the companies and assists in coordination when there is a need to discuss whether cyber security compliance is taking place. For example, if a company claims that it is ISO 27001 compliant, then the one who knows about this standard would understand whether the company is following the stringent security measures as suggested by the standard (NordLayer, 2022). Several standards exist that organizations follow per their requirements, such as ISO 27001, PCI-DSS, and the German IT baseline protection, some of which are explained in the next section.

#### Avoidance of regulatory fines

Implementing best security practices and measures that comply with regulatory requirements enables organizations to protect themselves from regulatory penalties following a data breach (NordLayer, 2022). For example, a bank that has the credit card data of customers is supposed to protect it to comply with the Payment Card Industry Data Security Standard (PCI-DSS) and, in case of a breach, the bank would face severe penalties. The most common international security standards being followed in the security industry are discussed in the next section.

**Regulation**

directives or rules that forces the organization to protect data from cyberattacks

### Common Cyber Security Compliance Requirements

Cyber security **compliance** standards are established by the relevant **regulation** requirements. Although the methods described in each standard are distinct the goal is the same i.e., develop such rules that could be easily followed and implemented in an organization for safeguarding sensitive information.

**Compliance**

Any entity that follows the federal, state, or international regulations and laws is said to be in the state of compliance.

Compliance requirements depend upon the location of the business and the market in which it processes and operates the data. The primary goal is to implement ISMS that ensures the protection of the data from cyberattacks. Organizations that have access to confidential data are the most common victim of cyberattacks (NordLayer, 2022). Some of the most common security standards and regulatory requirements are discussed below:

#### ISO/IEC 27001

One of the most common international standards used by organizations to implement ISMS is ISO/IEC 27001. This standard belongs to the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

Any business that is ISO 27001 certified shows that the organization complies with all controls mentioned in ISO 27001 standard. The standard addresses the best practices to establish a reliable and resilient cyber security program in an organization (NordLayer, 2022).

#### PCI-DSS

PCI-DSS is an information security standard that must be implemented for the protection of data related to the credit card or cardholders. The standard applies to all merchants who handle credit card payments. Entities are at risk of losing their merchant license if they do not comply with PCI-DSS. Losing a merchant license would prevent them from further accepting payments through credit cards. Businesses operating without PCI-DSS might eventually become possible victims of cyberattacks (which cause a reputational loss) and also face heavy fines from the regulatory bodies (NordLayer, 2022).

#### GDPR

The General Data Protection Regulation (GDPR) is a privacy and data protection law that was published in 2016 and became enforceable in 2018. It covers the European Economic Area (EEA) and European Union (EU) countries. The GDPR provides a legal structure that provides protection for the personal data of EU and EEA-based individuals.

The GDPR binds organizations to give clear and concise terms and conditions that show how exactly customer data will be processed. Therefore, to comply with the GDPR, businesses must get the consent of the individual before processing their personal data, while guaranteeing its confidentiality and being obligated to notify them if a data breach happens (NordLayer, 2022).

#### HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) is a federal regulation enacted in 1996 by the U.S. It was specifically enforced for the protection of health-related information. All those entities who are responsible for the processing and storage of health-related information on the internet must comply with HIPAA. HIPPA’s rules assist health organizations (such as hospitals and healthcare providers) by recommending necessary security controls that would give protection to the individual’s data from a data breach and also restricts an organization not to disclose the data without the individual’s consent. HIPPA rules are only applicable to organizations working inside the U.S. (NordLayer, 2022).

#### FISMA

The Federal Information Security Management Act (FISMA) is a U.S. legislation enacted in 2002. It is a comprehensive framework that specifies the requirements for the security of U.S. federal systems or systems that contain highly confidential data related to the national interest of the country. The statute is aligned with active country laws and executive orders to ensure cyber security compliance (NordLayer, 2022).

### The Law Enforcement

In cyber security, it is imperative to arrest cyber criminals and disrupt their illegal activities in such a way as to stop those activities. Organizations could deter cyber criminals from perpetrating crimes by removing the infrastructure utilized by them to execute cyberattacks. Law enforcement also enables to thwart cyberattacks, trace incidents, and seek prosecution. Law enforcement not only assists in incident response but also in prevention by discouraging cyber criminals with through deterrence (U.S. Department of Justice, n.d.).

**Sophisticated attack**

a cyber-attack targeted to an organization by highly skilled professionals

Law enforcement agencies stop and disrupt ongoing cyber-criminal operations through lawsuits and arrests and impede others from becoming involved in the same activities. These agencies better understand the techniques and tactics of threat actors. Moreover, since they also have access to resources and threat intelligence data, they have significant insight into **sophisticated attacks**. For example, investigating a criminal organization could yield invaluable details about the techniques and infrastructure leveraged by other criminal organizations. Agencies also depend on international relationships and resources to combat international criminal organizations. The international reach of the agencies is imperative to tackle cyberattacks that are executed and controlled by criminal organizations in other countries (U.S. Department of Justice, n.d.).

Investigations that are carried out by law enforcement against cybercrimes is initiated by victim organizations or customers; the agency cannot start its investigation until it is informed that the incident has happened as the result of a cybercrime. Therefore, in such situations, victims should report such incidents and malicious activity to law enforcement agencies. This encourages an organization to develop a strong culture of communication and sharing exact threat information with law enforcement, because effective punishment of cyber criminals requires strong assistance from the victims. Once the victims report cybercrimes to law enforcement, they then quickly preserve the digital evidence. Therefore, reaching out to law enforcement officials within time ensures that the evidence of the cybercrime is correctly secured and that the crime scene is available for investigations to hold perpetrators accountable (U.S. Department of Justice, n.d.).

Strong coordination is required between organizations and law enforcement to tackle cybercrimes. Leveraging the organization’s knowledge and information to assist law enforcement to carry out investigations that follow criminal sanctions could be a pivotal deterrent to criminals and make them think twice before attacking someone (U.S. Department of Justice, n.d.).

### Self-Check Questions

1. Please list any two international standards or regulations that are followed by organizations to ensure regulatory compliance or data protection from cyberattacks.

*ISO 27001*

*FISMA*

*GDPR*

*HIPAA*

*PCI-DSS*

Summary

In this unit, we discussed the concept of cyber law and explained how civil and criminal laws could be leveraged when cyber laws are violated. Moreover, we investigated the consequences that a cyber criminal would face if he violated these laws. Furthermore, the concept of regulatory compliance was discussed, whereby we explained how organizations must follow various international standards to keep their customer’s data secure from cyberattacks, which could further prevent them from regulatory fines. Lastly, the role of law enforcement agencies in cyber security was discussed, along with how they could make a deterrent environment for cyber criminals.

# Unit 6 – Risk Management

**Study Goals**

On completion of this unit, you will be able to …

… understand the concepts of risk, risk management, risk assessment, and risk mitigation.

… recognize the notion of incident management and crisis management.

… define the concept of performing continuous monitoring and reevaluation of the risk management process.

… identify and analyze the concept of black swan events.

# 6. Risk Management

## Introduction

Organizations are heavily dependent on technology assets to attain their business goals. If the information technology (IT) of any business or organization fails to function, there would be negative consequences as normal business operations would be stopped, objectives could not be achieved, resulting in significant economic loss beyond the organization itself. The **cyberspace** offers continuously progressing threats to organizations and their IT infrastructure capability to accomplish business objectives and to deliver core functions. Hence the cyber security domain is the responsibility of both IT professionals and senior management. A comprehensive approach to risk management in cyber security across an organization is needed for the effective implementation of a cyber security program.

**Cyberspace**

a virtual world where communication takes place through the internet

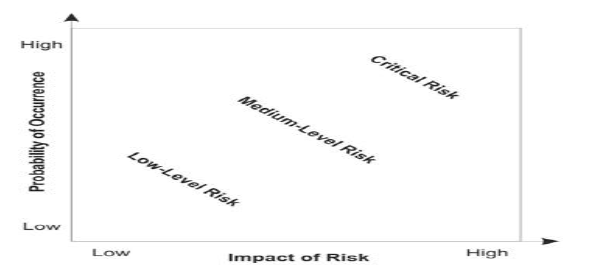
In this unit, the concept and implementation of risk management in cyber security will be discussed in detail. The concept and processes of risk assessment, risk mitigation, and continuous monitoring and reevaluation, which fall under the umbrella of risk management will also be discussed. Furthermore, incident management and crisis management are addressed. These are applicable when an incident that could lead to a crisis happens despite having a robust risk management process in an organization. Lastly, black swan events and how they affect the market is briefly described.

## 6.1 Risk Management: An Overview

Risk is the likelihood or probability of occurrence of an event that would impact an organization’s accomplishment of objectives. Risk can be mathematically defined as follows:

The figure given below shows how risk could be represented in a matrix as a combination of impact and probability.

The Probability Impact Risk Matrix



Source: Verma et al. (2016, p. 152) CC BY-SA 4.0.

Risk comes in many forms: Financial, IT, personnel, and operational risk are just some of the possibilities. To tackle risk more efficiently, organizations use a risk management technique to identify, assess, and mitigate these risks. Risks that organizations might face could be categorized based on their severity, ranging from a trivial inconvenience to those that might threaten the critical business operations of the entire organization. Risk in cyber security is the function of the probability of a threat source exploiting a vulnerability, and the resulting impact of this harmful event on the overall system and mission of an organization. Organizations must develop and enforce rigorous risk management processes, which are sometimes required by law, to protect from cyber-attacks and their ability to achieve their business objectives (Verma et al., 2016, pp. 152–153).

The process of assessing the risks and taking appropriate actions to reduce them to an acceptable level or avoid them is termed risk management. Usually, the steps taken in the process of risk management are risk assessment and risk mitigation.

## Risk Assessment

Risk assessment is the process of identifying threats to information systems or information, determining their probability or likelihood, and identifying the network, system, and application vulnerabilities that can be exploited by them. The first step in the process of risk management is risk assessment. Risk is evaluated or assessed by first identifying the vulnerabilities and threats, and subsequently determining the impact and likelihood of the risk. The following is a typical risk assessment process (Verma et al., 2016, p. 153):

1. Identification and classification of assets
2. Identification of the threats
3. Identification of the vulnerabilities
4. Analyzing the risk
5. Selecting a methodology for risk assessment

#### Identification and classification of assets

The first step in the process of risk assessment is the identification and classification of information assets. Classification is a title, or a naming, assigned to an asset from a pre-defined scale based on its sensitivity.Information assets comprise all forms of information, such as databases, files, or specific digital and non-digital assets. An organization is responsible for protecting the confidentiality, integrity, and availability of information assets.

It is the information owner who determines the value of an asset. Information assets are valuable to an organization based on its goals. Hence, it is imperative to identify all information assets. It is preferable to make a complete list of information assets and then classify them as public, restricted, or confidential. The information regarding the classification of each asset should also be included in a centralized list (Verma et al., 2016, p. 154).

#### Threats identification

A threat is a person, organization, or a force that aims to compromise or access information. By analyzing the capabilities and resources of a threat, one could identify the likelihood of its occurrence in the process of the risk assessment. The threat could be assessed in respect of the probability of an attack. Information security threats can be categorized as follows:

* social engineering
* natural disasters, such as tornadoes, floods, earthquakes, and fires
* malware, such as viruses, worms, and trojan horses
* insider threats, such as disgruntled employees
* network attacks, such as routing attacks, man-in-the-middle attacks, and denial of service attacks

#### Vulnerabilities assessment and identification

Vulnerabilities are the weaknesses in the network, system, or applications that an attacker could exploit. Vulnerabilities could be any means through which the cyber attack would potentially be successful. Some examples of the vulnerabilities are as follows:

* unpatched software
* insecure application
* disclosure of confidential information to unauthorized individuals
* usage of simple and same passwords on multiple accounts
* no multi-factor authentication

#### Risk analysis

Some risks are inherently involved in transferring and containing information. Information could be subject to unintentional and intentional activities. There might be unauthorized people, such as disgruntled employees or competitors, who wish to access and see confidential information. People might also try or want to hack into the systems containing sensitive information or may also try to intercept it during transfer. They might also acquire confidential and sensitive information completely by accident. Moreover, information systems could be accidentally or purposefully damaged. Such breaches of information security could seriously damage an organization. Generally, the risk for an asset could be written as given below:

*Risk = (Probability or likelihood of occurrence of threat targeting an asset) x (Value of an asset)*

Simply put, the greater the probability of a threat impacting the asset and the greater the value of the asset, the greater the risk. If the threat has no or less likelihood of occurring, or if an asset has no value, the risk would be either zero or low (Verma et al., 2016, p. 155).

#### Methodology for risk assessment

Organizations must develop some methods to quantify and measure risks so that the results of the risk assessment could be easily communicated. There are various risk assessment methodologies some of the most commonly used ones are discussed in the next sub-section and every organization must select what is best suited for them as per the compliance requirements. Values of assets and the degree of risk vary from company to company.

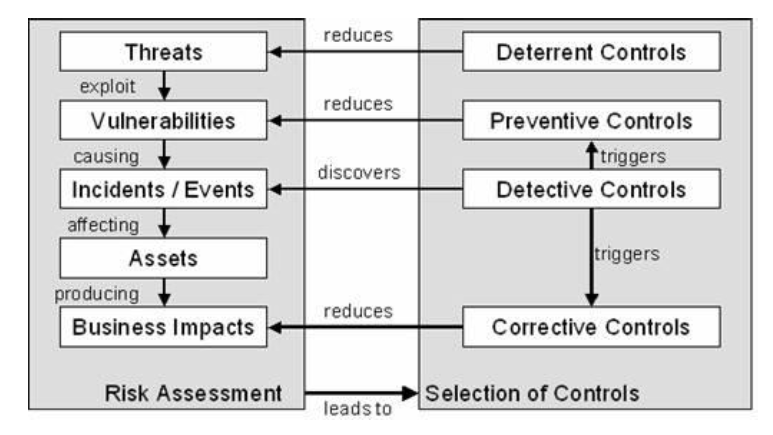
### Risk Mitigation

Taking necessary actions to reduce the likelihood of a threat to an acceptable level is known as risk mitigation. In business terms, risk mitigation is the implementation of security controls against potential threats. The number of controls based could be categorized as follows:

* Deterrent control – implemented to mitigate a threat
* Preventive control – implemented to mitigate a vulnerability
* Detective control – implemented to detect the incident that has occurred
* Corrective control – implemented to reduce the impact of an incident

The representation of the relationship between the security controls and the risk assessment process is shown in the figure below.

Relationship Between Controls Selection and Risk Assessment



Source: Verma et al. (2016, p. 156). CC BY-SA 4.0.

After risk assessment, generally, three steps are followed to perform the risk mitigation process of identifying, choosing, and implementing the controls (Verma et al., 2016, p. 156).

After the risk has been assessed, the decision must be made to select one of the four options given below:

1. Accepting the risk. Organizations might choose to accept the risk if the risk is deemed very low or the cost of risk acceptance is less than the cost of limiting or transferring the risk.
2. Transferring the risk. This refers to the utilization of the insurance provided by third-party companies. These organizations, on payment, compensate the asset owner for the potential damage if happens.
3. Limiting the risk. This refers to the implementation of the proper security controls such as installation of the antivirus solutions, Intrusion detection and prevention systems, firewalls, and user awareness and training to name a few.
4. Avoiding the risk. Normally carried out when controls could not be implemented, this may be due to high cost or preventing assets from such threats that are natural and could not be controlled. For example, constructing a building outside the zone of an earthquake or an organization decides not to install a specific solution due to its continuous compromise across different organizations.

#### Choosing and implementing risk mitigation options

Once an organization has determined different options for risk mitigation, one of them must be picked and put into action. For each asset there is an assigned risk and an option for risk mitigation has also been chosen. Implementing the selected option results in following some procedures and putting new controls in place. Implementing controls to limit risk is the commonly selected option by the organization to protect its information systems and assets (Verma et al., 2016, p. 157).

### Risk Assessment and Management Methodologies

There are several risk management and assessment methodologies. The top management of an organization decides and chooses a framework for risk management and assessment techniques. Organizations when considering and selecting the risk assessment technique might include the scope of a project, the cost, and ensuring that the required resources are viable and proportionate. Each organization selects a risk assessment method per its requirements and tailors the method according to its needs (Verma et al., 2016, p. 158). In this sub-section, we will look into some of the methodologies commonly used for risk assessment:

* ISO/IEC 27005
* NIST SP 800-30 and SP 800-39
* OCTAVE
* COBIT

#### ISO/IEC 27005

ISO 27005 is the international standard that provides guidelines and instructions for risk management. This standard is part of the family of ISO 27000 standards. ISO 27005 is used by organizations considering it one of the main requirements of implementing ISO 27001 which is a standard for implementing an information security management system (ISMS; Verma et al., 2016, p. 158).

The main requirement of the risk assessment carried out according to ISO 27005 is to take vulnerabilities, threats, and impacts into account. These factors must be contextualized to the business and considered for the risk evaluation, which then helps the decision makers how to tackle the risks. The principles of the ISO 27005 framework could be applied to different sizes and types of organizations. Since the guidance provided in this framework is generic and broad, skilled resources would be required for the tailored implementation as per the business requirements (Verma et al., 2016, p. 158).

#### NIST SP 800-30 and SP 800-39

The National Institute of Standards and Technology (NIST) *SP 800-30- Guide for Conducting Risk Assessments* and *NIST SP 800-39 Managing Information Security Risk* are the preferred methodologies of the US government for performing risk assessments. These standards provide a detailed piecemeal process starting from the initial phases of planning for assessment, through managing and conducting it, communicating the findings, and reevaluating it to maintain the assessments. These standards are free from the official NIST website. Organizations of any size, both public and private, can utilize these standards. Moreover, they are designed to work with various other ISO frameworks (Verma et al., 2016, pp. 158–159).

**Scope**

the information assets that need to be protected

The steps provided in SP 800-30 to carry out the process of risk assessment are as follows:

1. Establish the **scope**.
2. Utilize the identified vulnerabilities and threats to determine the **impact**, likelihood, and risk.
3. Communicate the outcomes to stakeholders.
4. Monitor the effectiveness of the security controls.

#### OCTAVE

The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) originated from Carnegie Mellon University in the USA. It provides a structured way to evaluate the risk and addresses best security practices, **operational risk**, and technology that is utilized to reduce the identified risk. This approach is different from the others in a way that it provides more of a strategic approach as compared to tactical ones. Companies could learn and utilize this methodology without requiring security experts. OCTAVE is designed to be handled as a workshop, with a few groups of participants from the IT and operational departments of the business without requiring broad expertise. Resources related to OCTAVE to perform risk assessments are free to download (Verma et al., 2016, p. 159).

**Impact**

the loss of confidentiality, integrity, availability, as well as losses like reputational and income loss

**Operational risk**

the risk of the losses resulting from the disruptions to the operations, e.g., human or technological errors

The OCTAVE steps are as follows:

1. Establish the criteria to measure the risk according to the business objectives.
2. Identify assets.
3. Consider the threats and their potential impacts according to the current threat landscape.
4. Identify risks.
5. Prioritize risks based on the criteria set for risk measurement.

#### COBIT

Control Objectives for Information and Related Technologies (COBIT) was developed by ISACA. ISACA is an international and professional association specialized in **IT governance**. It is a prescriptive and thorough framework that includes risk assessment. ISACA members are granted access to the standard, while non-members may purchase it. Implementing this standard would probably need a substantial investment of skilled personnel and time. COBIT is best suited to those organizations where regulatory compliance is paramount. COBIT is lined up with some famous risk management standards like ISO 27005 (Verma et al., 2016, pp. 159, 160). To implement COBIT, organizations must consider the following aspects:

**IT governance**

This practice defines the processes in an organization that guarantee the efficient and effective utilization of IT.

* identification of threats and vulnerabilities
* identification of the potential impact
* specialist resources are needed

|  |  |  |  |
| --- | --- | --- | --- |
| Summary of the Differences Between Risk Management Methodologies | | |  |
| **ISO 27005** | **NIST SP 800-30** | **OCTAVE** | **COBIT** |
| Part of the ISO 27000 series family | Part of NIST special publications | Carnegie Mellon University (USA) | Developed by ISACA |
| Utilized by organizations considering it one of the main requirements of implementing ISO 27001 | Preferred by the US government for performing risk assessments | Any organization can utilize it, without requiring security experts | Best suited to those organizations where regulatory compliance is paramount and needs investment in skilled people |
| Not freely available | Freely available | Freely available | Freely available to ISACA members |

Source: Zohaib Hassan (2023)

### Self-Check Questions

1. Please list any two well-known international frameworks that are followed by organizations for risk management.

*ISO 27005, NIST SP 800-30, NIST SP 800-39, OCTAVE, COBIT*

## 6.2 Incident Response and Crisis Management

A cybersecurity threat might come in various forms and could badly impact brand reputation and business operations, even leading to legal action. Organizations must be prepared to manage and reduce the effect of successful attacks and increase the recovery process (Gorecki & Sullivan, 2020).

### Resilience

In the day-to-day operations of the business, minor incidents are unavoidable, such as a temporary issue in the internet connection. Organizations must act quickly to evaluate and respond to a circumstance. “Crisis” and “incident” are frequently used interchangeably, but the comparison is more akin to apples and oranges.

### Incident

An incident is a cyber event and refers to a situation that is initially on a minor scale and might lead to a crisis resulting in much bigger losses, like the disruption of business. Incidents such as a computer or a laptop crash, poor WIFI connectivity, website crash, or a printer problem disturb the day-to-day business operations. Incidents are usually on a small scale and manageable with swift actions (Shahane, 2021).

### Crisis

A crisis is much more serious. A crisis might disturb crucial activities of a business and pose greater uncertainty. Incidents that are incorrectly resolved or left unresolved can become crises, requiring strategic intervention. A chain of incidents happening one after another or an incident that triggers another could result in a crisis.

**Financial crimes**

for example gaining unauthorized access to financial accounts or theft of credit card information to initiate illegitimate transactions

Examples of such crises are serious data breaches and cyber-attacks, **financial crimes**, theft of critical business assets, or any such events that could pose risk to an organization’s stability (Shahane, 2021).

The following questions might help in differentiating between an incident and a crisis:

* Does the situation create significant pressure?
* Does the event pose a significant threat to an organization?
* Does the situation have a surprise or shock element?

If the answers to the questions are “yes,” the situation is a crisis (Shahane, 2021).

The situations discussed above could affect the businesses if they aren’t prepared. Business must understand the differences between an incident and a crisis. Many organizations falsely assume they are well-prepared to respond to an incident or crisis (Shahane, 2021). Hence, to resolve and tackle both situations well, it is vital to recognize their nature first. This leads us to the discussion of crisis management and incident management.

### Incident Management

Incident management is an approach to handling events that disturbs the day-to-day, normal operations of an organization or a business. It comprises identifying the event that disrupted the normal activities of a business, assessing it, and then responding to it. Incident management enables organizations to return to their normal operations after the disruption has happened.

**Events**

Any happening that occurs in an IT environment is an event. All incidents are events, but not all events are incidents; an incident is an event that negatively impacts the organization’s data by compromising its confidentiality, integrity, and availability

Incident management could be achieved by crafting a proper plan to handle all potential incidents that might disrupt normal operations and could cause loss or damage. **Events** leading to an incident could occur in any small to large-sized organizations impacting the normal workflow (Shahane, 2021). Therefore, incident management planning is beneficial and enables an organization

* to take crucial steps for a swift recovery
* to immediately inform the people impacted by an incident
* to identify the potential risks and tackle them with targeted planning
* to gain a hawk-eye view of all potential incidents
* to enhance the productivity and efficiency of daily operations.

### Crisis Management

As we already discussed, a crisis is a situation with a greater magnitude than an incident and could badly affect the organization’s reputation. To tackle the crisis, there must be a dedicated crisis management team in an organization whose job it is to take necessary steps to limit the impact. Organizations that do not take crisis management seriously could have severe impacts on various aspects of the business such as employee morale, sales, the company’s reputation, leadership reputation, and productivity (Shahane, 2021). A proper plan developed for crisis management could save the business by

* decreasing the downtime of normal business operations
* reducing negative impact
* helping organizations to avoid reputational and financial damage
* preventing legal consequences

To better understand the differences between the incident and crisis management, some major points are summarized in the table below.

|  |  |
| --- | --- |
| Incident Management Versus Crisis Management | |
| **Incident management** | **Crisis management** |
| Small and quick actions | Taking much bigger steps to tackle the situation |
| Might not need the involvement of the senior leadership of the organization | Might need the involvement of senior leadership |
| Could mostly be managed within days, hours, or minutes | Could take days, weeks, or months |
| Might only impact a few people or teams | Might impact the whole organization |

Source: Renuka Shahane (2021).

### Self-Check Questions

1. Please complete the following sentence.

A *threat* could be posed to an organization in variousforms.

## 6.3 Unpredictable Events (Black Swan)

A black swan is an unpredictable and rare event that has serious repercussions and anticipating such events is almost impossible. Black swan events could lead to huge losses and harm to the markets and economy. Incidents such as the 2008 financial crisis, 9/11, and the COVID-19 pandemic could be categorized as black swan events.

### Preparing for Black Swan Cyber Events

Large organizations implement information security management systems to overcome cyber attacks. But as cyber attacks hit utilities, governments, hospitals, and companies with greater force, it is becoming evident that organizations now must have two **playbooks**, one for countering known cyber threats such as denial-of-service attacks, phishing, and malware and another that counters much worse through robust resiliency. Organizations must be prepared both for a cyber crisis that cripples and disrupts their own day-to-day business operations, as well as one that affects the whole industry (Herbolzheimer, 2016).

**Playbooks**

A key component in IT operations and incident management, a playbooks could include exercises and trainings to prepare incident response teams for the next potential incident.

Hence, organizations need to devote time to analyzing what kinds of cyber disasters they could face. Like other calamities, a cyber attack could occur suddenly. But they could also emerge slowly and gradually, like a plague or pandemic that steadily spreads over time before becoming a global crisis. Therefore, effective plans and strategies must be considered and enforced by organizations, such as building up redundancy to counter both known cyber threats and black swan cyber events (Herbolzheimer, 2016).

Organizations also need to examine if they could contain and survive black swan cyber attacks or whether they might disseminate like an infection within the industry and maybe beyond. Already, many organizations have prepared extreme containment and fallback plans like preparing to function offline if hit by a black swan cyber event. For example, hospitals and healthcare providers impacted by ransomware attacks in Germany and the United States have taken their systems of critical infrastructure partially offline and have prepared to resume their operations manually with paper and pen if an incident impacts their day-to-day digital operations (Herbolzheimer, 2016).

Companies may also consider establishing industrywide special weapons and tactics (SWAT) teams for regularly monitoring and addressing cyber threats. These teams would identify the trigger points beyond which a potential cyber crisis might occur, what kind of data and service they could afford to lose, and which data and service loss would lead them to a complete disaster (Herbolzheimer, 2016).

To summarize, black swan events are defined by their severe impact, consequences, and extreme rareness. Black swan events are highly unusual, and rarely have a serious impact. These events adversely affect markets by causing devastating damage to revenues. Even with the use of strong threat modeling and risk management techniques, black swan events cannot be predicted by forecasting tools (Investopedia, 2022).

### Self-Check Questions

1. Please complete the following sentence.

Black swan events have a *severe* impact on businesses.

## 6.4 Continuous Reevaluation

Periodic and continuous reevaluation and audit of the risk assessment plan must be carried out by organizations. The reevaluation process is performed in organizations to ensure that the controls that were put in place are still viable and functional for a given asset and are implemented according to the security policies of the organization.

### Residual Risk

Residual risk refers to a threat that would remain after all attempts and efforts have been made to eliminate the risk. As we already discussed, risk could be dealt with in four ways: avoid it, reduce it, transfer it, or accept it. Because the residual risk is not known, most organizations prefer to either transfer or accept the residual risk (Verma et al., 2016, pp. 157–158)

Summary

In this unit, we thoroughly discussed and explained the overall process of risk management and how it is usually carried out in organizations. The processes of risk assessment, risk mitigation, and continuous reevaluation have been elaborated under the discussion of risk management. The sub-processes that are followed under risk assessment, risk mitigation, and reevaluation processes have been analyzed in detail. Thereafter, we investigated the counter strategies like incident and crisis management that organizations must consider in case even after a robust risk management process, a cyber attack occurs. Finally, we talked about the phenomenon and concept of Black swan events and their impact.

# Unit 7 – Threat Mitigation

**Study Goals**

On completion of this unit, you will be able to …

… understand the different strategies and techniques used to strengthen cyber defense and risk mitigation landscape in an organization.

… recognize how the security controls are assessed and validated in cyber defense.

… identify the concept of security and privacy by design.

… apply threat mitigation strategies in an organization.

# 7. Threat Mitigation

## Introduction

**Digital transformations**

integrating digital technologies into all areas of the business

Continuous evolution in technologies enables businesses to reach their aimed goals, and audiences, collect data, analyze data, and more. But as businesses and organizations are making their **digital transformations** rapidly, the threat of being attacked by cyber criminals is equally growing. According to the Federal Bureau of Investigation’s (FBI) Internet Crime Report 2021, potential losses exceeded 6.9 billion USD in 2021 due to cybercrimes (Acrisure, 2022). Hence, a successful organization must design and implement a strategy that counters these threats and reduces the intensity of a possible data breach resulting from a cyber attack. This strategy is referred to as threat mitigation.

This unit explains in detail the different concepts related to threat mitigation. Different techniques and strategies must be enforced by organizations to enhance their cyber defense landscape. Strengthening the cyber defense is related to risk mitigation, and tactics and technique assist organizations in mitigating the risk.

Additionally, it is imperative to validate the effectiveness of the implemented security controls by auditing them after a fair amount of time. We will go into a detailed explanation about how controls could be validated and audited to ensure that they are up-to-date and compliant. Moreover, it is necessary to embed security at the time of designing the software or any other solution. This brings us to the concept of security and privacy by design, which is one of the main aspects of mitigating threats. Lastly, we will review best practices and techniques for mitigating the threats.

## 7.1 Cyber Defense Tactics and Techniques

Cyber defense is a terminology used in cyber security to refer to the capability to hinder cyber attacks from compromising a network, system, or application. It entails taking proactive steps to anticipate malicious actions from cyber criminals and combat them. All tactics, techniques, or strategies carried out by any organization to strengthen its cyber defense have the goal of preventing, disrupting, and responding to cyber attacks (CyberTalk, n.d.).

Cyber threats continue to target organizations that result in damaged reputations, costly reparations, and compromised information. Cyber criminals can attack several parts of an organization’s network infrastructure by utilizing an extensive variety of tactics and techniques. In a nutshell, our reliance on technology or digital solutions makes us vulnerable to cyber attacks (CyberDefenses, 2019). Hence, an organization that is dependent on technology for their day-to-day operations need to implement a strong cyber defense landscape. The following are some of the most common tactics and techniques to bolster their cyber defense.

### Strong Passwords

One cannot ignore the benefit of using strong passwords in any kind of account. It is human nature that while creating a new password or updating an older one, we prefer to keep it simple so that we can remember it easily or reuse a password for other accounts. According to Verizon’s Investigations Report of the 2019 Data Breach, 80 percent of the breaches and hacked accounts were the result of weak passwords (ADKtechs, 2020).

A good and strong password is long, random, and frequently changed. The complexity of a password often comes with the urge to write them down. This may result in further attacks and reduces the use of complex passwords. Hence, a password manager is a good solution; one could utilize it to save all the passwords in the virtual wallet in encrypted form protected with one master password. A long sentences used as a password is called a passphrase, and is also a good alternative. A passphrase is a kind of password that contains a long sentence related to one’s memory and is almost impossible for an attacker to break.

### Multi-Factor Authentication

Multi-factor authentication (MFA) is one of the most robust and easiest techniques used to strengthen the cyber defense of an organization. Multi-factor authentication, also known as two-factor (2FA) authentication, helps add an additional shield of security to a normal password. MFA is the mixture of at least two of the following:

* a standard password, which is also called “something you know.”
* a one-time code or token that is randomly generated via third-party software on your mobile phone, also known as “something you have.”
* biometrics, signature, or voice, also called “something you are.” This technique strengthens the cyber defense in such a way that if somehow one factor is compromised, the attacker will not be able to verify the physical characteristics of the victim.

### Firewalls

A firewall is a physical hardware device or software that is implemented between an internal and external network. A firewall works as an obstacle for the traffic coming from external or outside networks, i.e., the internet toward the organization’s internal network or for the traffic that is going outward from internal toward the external network. It does this by performing some filtering based on some rules that are configured in the firewall. They are crucial shields for small and large businesses and also for home networks.

### Patched Software

It is worth stating here that continuous patching or updating of software is one of the key cyber defense best practices. Every software solution used by a company should be continuously updated to its latest version. Unpatched software is more vulnerable and could lead to massive data breaches if hacked, allowing an attacker to move within the organization’s critical network. Hence, routine patching of software could eliminate one main option that a cybercriminal would have utilized to compromise the complete organization’s network.

### Encryption

Encryption is a technique used to convert readable or plain-text data into a form that cannot be comprehensible by an unauthorized person. Implementation of encryption is imperative for all businesses that make use of the internet for their day-to-day communications. For example, transactions via banking channels take place over the internet, which is an untrusted network. Therefore, banks must enforce this security control to ensure secure credit card payments and transactions. Utilizing encryption in the home network is also suggested and it keeps our stored data more secure when we lost our storage device or are robbed. However, the encryption technique should be up-to-date so that it cannot be cracked with the help of hacking tools. Several organizations regularly publish listings of strong cryptographic algorithms e.g., BSI TR-02102 (Federal Office for Information Security, n.d.).

### Antivirus

One of the basic but imperative security controls to consider in any business is the use of updated antivirus solutions. This software assists in scanning, detecting, preventing, and deleting viruses from a computer. Every organization or even home user must implement the latest antivirus solutions to detect and prevent threats. It is advisable not to download such programs from unknown websites but rather to buy them from a known source and update them regularly.

### VPN

A virtual private network (VPN) is a technique used to communicate securely over a public network such as the internet. For example, employees who work from their homes are sometimes required to communicate securely with their organization over the internet. Hence, a VPN is the best choice because it creates a secure encrypted tunnel over the internet through which both parties may send their data.

### Backups

Taking backups refers to having a copy of all the critical business digital documents regularly. For a stronger defense, organizations must create continuous backups of their digital assets such as spreadsheets, human resource files, databases, and financial files so that if any incident occurs, all data can be restored from the secondary storage. Critical data should be stored at least on two independent devices or media, physically located at different places, which creates a strong redundancy in an organization.

### Employee Security and Awareness Training

No security solution could ever prevent any organization from cyber attacks unless it has a trained and well-aware employee staff who knows the current challenges and threats in the cyber security domain. Cyber criminals always try to fool humans as they are the weakest point of the link. Carrying out security awareness training is easy and inexpensive with an immense outcome. When it comes to strengthening cyber defense, security-aware people are the first point of defense against cyber threats in any organization. Training may include an explanation of the organization’s security policies, letting them know where to inform about any suspicious activity, and teaching them what links are not to be clicked if received through an email, etc.

### Self-Check Questions

1. Please name any two key infrastructures that could be targeted by cybercriminals in an organization.

*Network, System, Application*

## 7.2 Risk Mitigation Strategies

Risk mitigation is the process of taking vital actions to mitigate the probability of a threat exploiting vulnerabilities. To mitigate risk, the implementation of necessary security controls is carried out in organizations. It is usually carried out after risk assessment under the overall process of risk management. The following are the common strategies:

* risk acceptance
* risk transferring
* risk limitation
* risk avoidance

### Risk Acceptance

Risk acceptance, accepting the risk, or risk retention refers to accepting the identified risks without considering any security measures to prevent loss from risk occurring. The decision is carried out by the senior management of the organization, who deem that the cost of implementing necessary security controls is higher than the actual worth of the asset.

### Risk Transfer

Risk transfer is an approach in which the potential loss from a cyber attack confronted by an organization is passed to a third-party company via insurance. These companies, on payment, indemnify the impacted entities for the damage that occurred.

### Risk Limitation

Risk limitation, also known as a risk reduction, is the implementation of security controls. This approach is carried out to reduce the risk by enforcing security controls such as updated firewalls, password policies, incident response planning, multi-factor authentications, and VPN for remote workers.

### Risk Avoidance

Risk avoidance refers to an approach performed to minimize the risk by not carrying out operations that might be deemed risky. One example is an organization confines storing the customer data on its servers if a cyber attack happens, and another is a manufacturing company that does not utilizing harmful chemicals or materials due to the risks of storing and handling them. Monitoring and reviewing the implemented solutions is also one of the ways to avoid risk.

### Self-Check Questions

1. Please list any two strategies carried out under the risk mitigation process.

*Risk acceptance, Risk transferring, Risk limitation, Risk avoidance*

## 7.3 Validation of Defenses

A major requirement for a successful cyber defense program in any organization is assessing and validating the effectiveness of enforced security controls. Organizations should perform this periodically to check whether the security controls are functioning as intended (Bakertilly, 2017). The most common ways that are utilized by organizations to monitor and assess the effectiveness of security controls are through conducting penetration testing, red teaming, vulnerability assessments, and audits.

### Penetration Testing and Vulnerability Assessments

**Security patches**

These are the corrections made in the software code and are released by the software companies to mitigate vulnerabilities.

To verify and assess the effectiveness of the security controls, all organizations must carry out vulnerability assessments and penetration testing. Vulnerability assessments are performed to identify poor security configurations applied by an organization or any **security** **patches** that an organization might have missed. Various vulnerability scanning tools are utilized by the organization to compare the current system’s configurations to the known published list of vulnerabilities (Bakertilly, 2017).

Taking vulnerability scanning one step further leads us to the next step of penetration testing. A skilled and professional **ethical hacker** utilizes those identified vulnerabilities that are found in the vulnerability scanning phase and then simulates real-world attacks to identify if these vulnerabilities could be exploited by an actual cyber criminal that might lead to a real breach. Organizations then use these results of vulnerability scanning and penetration testing to determine security gaps along with considering the key reason for what allowed these vulnerabilities to be introduced to the organization (Bakertilly, 2017).

**Ethical hacker**

A skilled professional who simulates real-world attacks with the permission in order to identify the vulnerabilities in the network, system, and applications.

### Cyber Security Audits

An audit in cyber security is an extensive assessment of an organization’s information systems to assess compliance and determine the gaps in the implementation of security policy. Auditing involves carefully reviewing the organization’s security controls and digital assets to ensure they meet compliance requirements. Cyber security audits are categorized as either internal or external (Sengupta, 2022).

#### Internal auditing

**Cyber security processes**

Methodologies or strategies within an organization

designed to guide cyber security experts.

An in-house dedicated team of an organization carries out internal audits to assess the **cyber security processes**. Strong internal auditing helps an organization and the audit team to understand the flaws in the security implementation. This also enables the organizations to fill the gaps, i.e., which security controls should have been in place that are not enforced.

#### External auditing

In external audits, third-party cyber security experts scrutinize the regulatory compliance, security controls, and gaps in security within an organization’s enterprise network. Since external auditors are highly qualified and trained in identifying sensitive data, network assets, and vulnerabilities, they make sure that the audit process assists an organization to meet its objective by more thoroughly performing the **gap analysis**. A strong audit evaluates five key facets of security (Sengupta, 2022).

**Gap analysis**

This detailed review assists organizations in identifying the difference between their existing information security state to industry requirements.

#### Operational security

Operational security is comprised of the organization’s cyber security policies, security controls, and best security practices. Operational security comprises providing extensive safeguards on different infrastructure assets’ administrative functions.

#### Network security

A network security audit is the evaluation of the security posture of network systems and resources that can be accessed through the internet. A comprehensive audit of network security examines the availability of the network and the entire operations of network devices such as firewalls, switches, and routers.

#### Data security

Data security includes controls enforced in safeguarding the data’s confidentiality, integrity, and availability within the organization. Security controls that are usually implemented for data security include authentication, authorization, encryption, and best security practices to protect vital business data in **rest and transit**.

**Rest and transit**

Data in rest data are in storage, e.g, data stored on hard disk; data in transit are moving, e.g., when entering the user account credentials on a website.

#### System security

The implementation of security controls on hardware and operating systems refers to system security. Auditing the system security includes reviewing the administration of **elevated permissions**, device access management, patching process, etc.

**Elevated permissions**

This refers to the concept of a normal user being able to access the administrative account rights to execute commands.

#### Physical security

Preventive controls are implemented to control physical access to software assets, hardware assets, and application data. Physical security controls also safeguard the organization’s workers from potential dangers of threats that can lead to the compromise of critical business systems. A cyber security audit evaluates several physical security aspects, such as access control, physical disk drive backups, and surveillance procedures.

### Self-Check Questions

1. Please name a method that could be used to check the validity of security controls within an organization.

*vulnerability assessment, penetration testing, internal audits, external audits, building security metrics*

## 7.4 Security and Privacy by Design

In this section, we will discuss the concepts of both security and privacy. Although closely associated, they are not similar. Information security ensures the protection of assets and activities of both the organizations and the public, while privacy aims to protect and respect personally identifiable information by enabling individuals to keep control and check over its use, collection, and disclosure (Cavoukian & Dixon, 2013).

### Privacy by Design

Even though privacy demands the protection of personally identifiable information from unauthorized access, and strong security controls are vital to achieving such a level of protection, it is imperative to discern that privacy addresses much more than just ensuring secure and authorized access to the data. In a nutshell, privacy refers to control which means it would enable individuals to keep personal control over the collection, utilization, and disclosure of their personally identifiable information. This notion of privacy is best stated as “information self-determination,” terminology initially used in the ruling of the German constitution regarding the collection of personal information in Germany’s 1983 census (Cavoukian & Dixon, 2013).

With the expansion of interconnected digital systems, challenges to desired privacy are also growing. Privacy laws are striving to align with the ever-changing digital landscape that is caused by swift technological changes. However, despite the rising challenges caused by cloud computing, social media, and mobile, achieving privacy is still not only doable but extremely desirable for organizations who want to keep the trust of their clients (Cavoukian & Dixon, 2013).

The concept of privacy by design offers a holistic approach in this ever-evolving era of digital transformation. It addresses the whole end-to-end structure of an organization or a business, including its network infrastructure, business practices, and information technology. This allows an organization to take full benefit of the technology by implementing privacy in each of its entities (Cavoukian & Dixon, 2013).

Privacy by design addresses the seven basic principles:

1. Proactive and not reactive – preventive not remedial
2. Privacy as a default setting
3. Privacy embedded into design
4. Full functionality – positive sum
5. End-to-end security – complete lifecycle protection
6. Transparency and visibility
7. Respect for user privacy

### Security by Design

As mentioned above, information security refers to the protection of the assets and activities of both enterprises and people. The NIST defines “Information Security” under its Glossary of Key Information Security Terms as protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide:

* **confidentiality** – which refers to keeping authorized restrictions on disclosure and access.
* **integrity** – which is the protection given against unauthorized information destruction or modification.
* **availability** – which means guaranteeing reliable and timely access to information.

Apart from providing a strong defense landscape in an organization, a thorough and robust information security program could enable organizations to achieve their business goals. For instance, if the increase in revenue by enhancing customer satisfaction is the ultimate objective of a business, then offering a secure environment to manage and receive customer information along with giving access to that information could improve customer trust and confidence in the organization, leading to high revenues. The same would also be true while dealing with vendors or business partners (Cavoukian & Dixon, 2013).

In information security, security by design is an approach that is robust, holistic, and embedded into the systems or products at their inception. It would be worth noting here that the concept of security by design stands in contrast to “security through obscurity” in which security is approached from the perspective of complexity, secrecy, and incomprehensibility (Cavoukian & Dixon, 2013).

### Aligning Privacy by Design with Security by Design

The table below explains how privacy by design principles can be aligned to model security by design principles.

|  |  |  |
| --- | --- | --- |
| Privacy by Design and Security by Design | | |
| **Privacy by design’s basic principles** | **Privacy** | **Security** |
| Protect and respect personal information | Protect assets and activities of both enterprises and people |
| Proactive not reactive | Predict and stop privacy-intrusive incidents before they occur | Implement preventive controls such as IPS and firewalls |
| Default setting | Build privacy controls direct into business practice or ICT systems | Implement “secure by default” policies such as need-to-know, least privilege, and separation of duties |
| Embedded into the design | Implement privacy into the architecture and design of business processes and ICT systems | Utilization of hardware security solutions, e.g., trusted platform module (TPM) |
| Positive-sum | Adjust all valid objectives and interests in a positive-sum “win-win situation” fashion, not using the zero-sum technique involving useless trade-offs | Accommodate stakeholders and resolve disputes for a win-win situation |
| End-to-end security | Ensure life-long secure management of information | Ensure the protection of confidentiality, integrity, and availability of information |
| Transparency and visibility | Keep parts of ICT systems and day-to-day business activities transparent and visible to users | Intensify the security of an organization by leveraging the industry standards and robust auditing |
| Respect for User | Protect and respect individual’s interest, above all and keep it individual-centric | Protect and respect all information owners’ interests; Security must address both organizational and individual interests |

Source: Cavoukian & Dixon (2013).

#### Proactive not reactive

Preparing before something happens requires a change in the “state of mind” of the leadership and the entire organization’s culture. This is a strategic approach rather than a tactical approach in which the threats are addressed once they occur (Cavoukian & Dixon, 2013). As listed in the table above, controls such as firewalls and IPS are examples of proactive or strategic approaches in which unauthorized or malicious traffic is blocked from entering the network of the organization. This is in contrast with the reactive approach in which the malicious traffic is tackled when it enters an enterprise network.

#### Secure by default

This principle refers to enforcing the policies for the implementation of the security controls and special ways for configuring and installing the software. The main objective of this principle is to ensure secure configurations of information systems by default, instead of users doing it separately or, in the worst case, tightening down the security after the compromise (Cavoukian & Dixon, 2013).

#### Embedded into the design

To create secure systems, it is essential to implant security into the design of such systems. This could be achieved through software or hardware. TPM, as mentioned in the table above, is an example of embedding security into the design through hardware. TPMs give support in key management through the hardware. They are microcontrollers (computer chips) with limited storage to securely store certificates and key material on a motherboard. Embedding certificated and key material within the system’s hardware allows the signing and hashing of the data without even the encryption key going out of the TMP. This guards a key from being stolen or changed by malware, thereby incorporating an additional cover of security to the authentication and **cryptographic services** of the system (Cavoukian & Dixon, 2013).

**Cryptographic services**

the process of encryption and decryption

#### Positive-sum

In this approach, respect is given to each stakeholder to accommodate them so that all of them could come to a single objective that drives the design, and implementation of technologies and business initiatives that would lead to a strategic boost to attain sustainability and effectiveness.

#### End-to-end security

The main goal of the organization’s information security is to preserve confidentiality, integrity, and availability. In such an approach, vulnerabilities throughout the enterprise are addressed rather than just protecting the perimeter of the organization. Database security, network security, identity access management, and privilege access management are some of the examples that are considered while implementing end-to-end security in an enterprise (Cavoukian & Dixon, 2013).

#### Transparency and visibility

Transparency and visibility are eminent security principles that enhance vendor and customer confidence in the information security that is implemented in an organization. Organizations could achieve this by following international information security standards such as ISO 27001 for implementing information security. When implemented correctly, this well-known international standard allows organizations to be ISO 27001 certified after proper external auditing, which assures customers and vendors that the information that the organization is maintaining is secured (Cavoukian & Dixon, 2013).

#### Respect for user

A basic rule of privacy by design is to respect individuals and their privacy rights. Security, though, addresses a wider aspect. It must protect and respect the concerns of information owners, which entails both enterprise assets and individuals. For instance, in cyber attacks where the main target is to steal intellectual property and not personally identifiable information, it is also essential to protect the enterprise data (Cavoukian & Dixon, 2013).

### Self-Check Questions

1. Please complete the following sentence.

Both security and privacy are *dissimilar* concepts.

## 7.5 Implementing Threat Mitigation in an Organization

The average cost of a data breach by 2022 was $4.35 million, with a rise of 2.6 percent from 2021 (Tunggal, 2022). Can organizations afford this? Of course not. Cyber security is crucial for any organization today, especially in this digital era where data is the new oil. But implementing protection is not cheap. Effective implementation of threat mitigation includes tools and solutions, as well as the strategies carried out in the organization’s operations (Usiagwu, 2021). Some of the most common threat mitigation tactics in cyber security are discussed below.

### Risk Assessment

Risk assessment is the first step in threat mitigation. Organizations must take a complete inventory of the assets they have and document vulnerabilities related to each one of them. To address this, a risk assessment process is carried out. To understand the risk assessment process in brief, a few main vital questions that are asked in this process are listed below (Usiagwu, 2021).

* What kind of information and data are we collecting and storing?
* What is the criticality and importance of this data? Organizations must define their scope to tailor their strategies to address threats and risks. For example, health and financial organizations handle more sensitive data and therefore more rigorous protection must be given.
* How are we storing the data?
* Who has access to these data?

### Creating a Robust Cyber Security Culture

Humans are the weakest link and the most vulnerable entity in any organization. The best cyber security solutions will fail if humans are not trained on the best cyber security practices and current threat landscape. An organization cannot achieve a stringent cyber security culture if it is not rooted in its employees. Hence, nurturing consistent cyber security best practices with periodic user awareness training is paramount (Usiagwu, 2021).

### Incident Response

Incident response is essential for threat mitigation as when an incident happens in an organization, the impact of a cyber attack could be limited by detecting it early and subsequently taking necessary steps immediately. The organization must have a policy for incident response. Guidelines must also be in place that dictate what should be done in case of a cyber attack. What would be the point where cyber security team acquires employees’ devices? What attacks require a complete network shutdown? All these questions are crucial. Organizations must also consider taking continuous backups in case of a data breach (Usiagwu, 2021).

### Network Monitoring

Organizations must implement network monitoring to hunt the threats. An organization or specifically, a network, might remain compromised for several days or even months, remaining totally hidden from information security teams. So, here, the importance of monitoring comes in. Network traffic of an organization should be continuously monitored by the information security teams, detecting and flagging down unusual and suspicious activities, especially activities performed by the employees that might expose endpoints. This could be achieved by leveraging security information and event monitoring (SIEM) having artificial intelligence and machine learning capabilities to monitor real-time network traffic (Usiagwu, 2021).

### Self-Check Questions

1. Please complete the following sentence.

The average cost of a data breach is *increasing* every year.

Summary

In this unit, we explained and discussed in detail the different strategies and techniques that could be leveraged to strengthen the cyber defense of an organization. Since cyber defense cannot be strengthened without understanding and addressing risk mitigation, we also looked at how could we follow different risk mitigation techniques that would eventually enable organizations to a stronger cyber defense landscape. Additionally, we reviewed how to ensure the effectiveness of security controls. For that, we discussed the concept of auditing in cyber security and how and when it should be carried out by organizations for the validation of their implemented security controls. Moreover, we understood how security could be embedded in each aspect of an organization or a product by addressing the topic of security by privacy and security by design. Lastly, we talked about the different strategies to be followed to mitigate a threat.