# ANALYZING CYBER SECURITY: AN ORGANIZATION APPROACH OF IMPLEMENTING CYBER SECURITY POLICIES AND AWARENESS FOR MICRO, SMALL & MEDIUM ENTERPRISES IN INDIA

by

Dinesh Kumar Mohanty, DBA Research Scholar

DISSERTATION

Presented to the Swiss School of Business and Management Geneva

In Partial Fulfillment

Of the Requirements

For the Degree

DOCTOR OF BUSINESS ADMINISTRATION

SWISS SCHOOL OF BUSINESS AND MANAGEMENT GENEVA

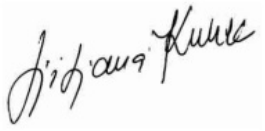
<MONTH OF GRADUATION, YEAR>

ANALYZING CYBER SECURITY: AN ORGANIZATION APPROACH OF IMPLEMENTING CYBER SECURITY POLICIES AND AWARENESS FOR MICRO, SMALL & MEDIUM ENTERPRISES IN INDIA

by

Dinesh Kumar Mohanty

APPROVED BY



__dr.Ljiljana Kukec, Ph.D.
Dissertation chair

RECEIVED/APPROVED BY:

Renee Goldstein Osmic

Admissions Director

## Dedication

I would like to dedicate this research paper journey, to my family members, colleagues & my friends, whose love and support have been my greatest strength. Specifically, I would like to thank my father, the late Rabindra Kumar Mohanty (Ex-Indian Army).

**Acknowledgements**

I would like to express my sincere gratitude to the grace of Almighty God and my family members for inspiring me to undertake this task.

I would humbly submit that my thesis writing is entirely due to support and guidance given by my mentor and guide, Prof. Dragan Perakovic, PhD, Swiss School of Business and Management Geneva.

The long journey of writing this dissertation has been constantly supported by my family and colleagues. My thanks to all of them.

ABSTRACT

ANALYZING CYBER SECURITY: AN ORGANIZATION APPROACH OF IMPLEMENTING CYBER SECURITY POLICIES AND AWARENESS FOR MICRO, SMALL & MEDIUM ENTERPRISES IN INDIA

Dinesh Kumar Mohanty
2025

Dissertation Chair: <Chair's Name>
Co-Chair: <If applicable. Co-Chair's Name>

MSMEs power India's economy. As they move fast in adapting digital tools for sales, daily payments, and operations, cyberattacks are rising and can wipe out years of work. Surveys suggest more than half of MSMEs have faced a cyber incident, and many struggle to recover.

This study looks at how Indian MSMEs adopt basic cyber safety. We used interviews with owners in manufacturing and services, plus public data (MSME Ministry, DSCI, NITI Aayog). We also consider simple impacts of key rules: CERT-In's 2022 directions (incident reporting, log keeping) and the DPDP Act 2023 (personal data protection). The study aims to identify possible gaps and challenges an organization faces in the implementation of cybersecurity policies and procedures and provide effective recommendations for improvement.

According to a study conducted by DSCI (2025), 60% of the Indian market's one-person companies (OPCs) and micro, small, and medium enterprises (MSMEs) have at least faced a cyber incident in the past two years. Whereas, insufficient funding, lack of

technical expertise, and a lack of accessibility to cybersecurity resources create difficulties in the protection of assets within an organization. Hence, cyber risk poses a direct business impact and sustainability challenge rather than a purely technical issue.

Three barriers keep coming up: people (low awareness), budget (limited funds), and skills (lack of affordable experts). Many firms lack basic training, clear roles, and cost-effective support.

We suggest a full-phased, practical roadmap starting with security hygiene like MFA (Multi-Factor Authentication), regular backups, patching, and employee awareness; adding light governance (clear owners, simple policies, vendor checks); then moving to ongoing monitoring (alerts, drills). Policy support should focus on training, easy financing via government subsidies provided by SIDBI/CGTMSE, and simpler compliance. The goal: make cyber safety part of business continuity and build digital trust. The research also contributes to the development of employees by adopting various cybersecurity practices, such as security architecture review, penetration testing (PT), DevSecOps, identity access management (IAM), endpoint security, application security (AppSec), etc., for MSMEs operating in India, helping to protect their digital assets and safeguard against cyberattacks.

TABLE OF CONTENTS

LIST OF TABLES



LIST OF FIGURES

# CHAPTER I:

# INTRODUCTION

## 1.1 Introduction

Cyberspace or the World Wide Web (WWW), represents the way of reaching out to both computerized and simulated environments where individuals may connect whenever and wherever by employing the Internet, computer networks, or other related tools (A. Mishra et al., 2022). The word “cyber security” is widely used as a term for protection against cyber-attacks targeted towards individuals or organizations (Bay, 2016). Security is a vital component for acquiring the work of the data and communication system in an expectable way (Peraković et al., 2015).

Cybersecurity has gain importance in today's digital era, particularly for startups operating in India, because it’s very essential to protect against loss of intellectual property, reputational damage, and financial losses and prevent legal concerns imposed by different governments of different countries for organizations operating in multiple countries, like multinational corporations (MNCs) and micro, small & medium enterprises (MSMEs).

After the COVID-19 epidemic, with WFH (work-from-home) options, India's digital economy is forecasted to extend $1 trillion by 2025-2026, making cybersecurity a national concern to protect the attack surface from malicious actors (S. Kumar & Bansal, 2024). According to telemetry data provided by Seqrite Labs from October 2023 to September 2024, it discloses crucial perception into ongoing threat and risk landscape in India (*Data Security Council of India (DSCI)*, n.d.).

Scale of cyber-Threats: Over 369.01 million security incidents were detected and reported across 8.44 million endpoints. It also says that an average of 702 potential security incidents are happening every minute within the country, or roughly 11 latest cyber threats are appearing every second in India (*Data Security Council of India (DSCI)*, n.d.). A research done by the Data Security Council of India (DSCI) and Nasscom along with Seqrite and Quick Heal Technologies found a shocking 369.01 million malware detections across 8.44 million endpoints in India (Bureau, 2024).

A study shows in financial year 2022–23, around 971 million people used the internet, and digital services made up 11.74% (USD 402 billion) of GDP, which says that India's digital economy is growing exponentially. It is projected to account for one-fifth of the GDP by 2030. In March 2025, India saw 18.3 billion digital payment transactions. This increase was because of the quick adoption of AI, online payments, and more internet-connected smart devices (*Mapping India's Cybersecurity Administration in 2025*, n.d.).

India has a lot of small and medium-sized businesses that work in different areas like technology, finance, insurance, and healthcare. These businesses face special cybersecurity challenges because of the country's big digital environment, different cultural and social rules, and various laws. That is why it is more important for them to have strong cybersecurity plans and make sure their workers understand the risks and its implications.

After reviewing various research papers, I found a clear gap in understanding and implementations of application of security measures among early startups, one-person companies (OPCs), and MSMEs. Despite their financial constraints, they still struggle in implementing effective cybersecurity practices or measures. The emphasis must be on identifying ways that are economical, cost-effective, comply with Indian regulations and global standards, and align with their budget, available resources, and the completion of the project on time (due to the hard deadline).

A significant number of these businesses want to set up and start their own cybersecurity business unit but do not know how to start, run, or manage such teams effectively. An effective security framework helps protect an organization's critical assets, keeps customers' trust, and ensures compliance with legal requirements. These companies can perform better by eliminating security risks, building a good reputation across clients, and keeping their money and operations safe by staying ahead of new security threats and managing risks.

## 1.2 Research Problem

India is quickly adopting digital technology by aligning with global technologies. Companies like one-person companies (OPCs) and micro, small, and medium enterprises (MSMEs) are at a higher risk of cyberattacks because of their technology adoption. Even though different policies and protocols have been put in place, it's still not clear for organizations how well they work. Furthermore, the fact that employees and stakeholders don't know much about cybersecurity is a big risk to these companies' safety.

The prospectus of the study is to recognize the awareness among different stakeholders and employees of existing cybersecurity policies implemented by Micro, Small, and Medium Enterprises (MSMEs) and One-Person Companies (OPCs) operating in India. By identifying an obstacle in their execution and offering the best possible suggestions for enhancing cybersecurity postures within IT/ITES. Additionally, it will also explore different effective strategies for establishing a cybersecurity business unit within these organizations to safeguard their assets and reputation by following different security standards adopted globally and provided by CERT-In (Computer Emergency Response Team) and GoI (Government of India).

Here are the few major challenges an organization (early startup and MSMEs) faces when they do not have adequate policies and procedures for cybersecurity (Crumpler & Lewis, 2019).

- Organizations should focus in building good relationships with local agencies (education institutions) to convey about essential workforce requirements and skills deficiencies. Effective communication between proprietor and training institutions will assist line up the cybersecurity talent with the requirements of the industry (Crumpler & Lewis, 2019).
- Industry should recruit skilled cybersecurity resources with progressive backgrounds or provide enough opportunities for existing employees to up-skill in cybersecurity. (Crumpler & Lewis, 2019).
- Organizations should educate or try to retain resources so that they can have a good pool of resources who can shape and help in protecting assets.
- Organizations should follow various cybersecurity policies and frameworks available within India (Example: Computer Emergency Response Team Indian (CERT-In) regulations for cybersecurity) and global regulations (Example: NIST Frameworks, HIPAA, PCI-DSS, Indian IT Acts, etc.).
- Working with third-party security vendors to assess the security postures of the organizations.
- Organizations (MSMEs) should have a Penetration Testing and Security Operation Center (SOC) team who can help in assessing and defending against cyberattacks.

## 1.3 Purpose of Research

The ambition of the study is to develop a framework for the cybersecurity policies in the IT/ITES industry, mainly those that operate within Micro, Small & Medium Enterprises (MSMEs), with a special focus on cybersecurity. By cyber security policies we mean the processes and procedures of identifying the cyber security risk, mitigation, awareness, employee training, etc., in compliance with the government policies and the strategic framework landscape influencing embracement, and the triad of barriers—people, budget, and expertise.

- Evaluating the current state of cybersecurity policies and procedures implemented by one-person companies (OPCs), early startups and micro, small & medium enterprises (MSMEs) operating in India.
- Assessing the consciousness and perception of cybersecurity risks among team members and stakeholders of one-person company (OPC), early startups and micro, small & medium enterprises (MSMEs) operating in India.
- Identifying the gaps and challenges in the implementation of cybersecurity policies and procedures among one-person company (OPC), early startups and micro, small & medium enterprises (MSMEs) functioning in India.
- Dispensing possible suggestions and security best practices for improving the efficiency of cybersecurity guidelines, strategies development in one-person company (OPC), early startups and micro, small & medium enterprises (MSMEs) operating in India.

- How an organization can set up a cybersecurity business efficiently and effectively by utilizing a limited budget and quality of resources and technology.

## 1.4 Significance of the Study

This research will gather feedback directly from Micro, Small, and Medium Enterprises (MSMEs) in India through a detailed research survey. The participants will include higher management (CEO, managing director, CISO, CTO), directors, senior directors, managers, and proprietors across different business sectors. The objective is to recognize and understanding the gap in the current cybersecurity posture of MSMEs and suggest to them the basic level of maturity required to protect their assets from cyberattacks and threats.

Since one-person companies (OPCs), early startups and micro, small & medium enterprises (MSMEs) play crucial role in nation building, it is important for an organization to have continuous innovation and improvement in cybersecurity practices by maintaining their competitiveness and contributing to the economic growth of the country. This study intends to dispense practical perceptions to help MSMEs magnify their cybersecurity resilience.

- The results of the study will help and provide valuable insights about different security policies formulated by Government of India, discussions and guidance and security best practices for web, mobile and API applications those are developed by one-person companies (OPCs), early startups and micro, small & medium enterprises (MSMEs) govern in India.

- Engage with senior managements of MSMEs, OPCs to acknowledge the ongoing status of cybersecurity controls implemented among their organizations.
- The study will look for security risks by checking where the existing cybersecurity measures are weak.
- Based on the findings, the study will create and share suggestions on effective implementations to fix the issue found.

## 1.5 Research Purpose and Questions

The current research study focuses on identifying various factors influencing the adoption of cybersecurity policies in MSMEs operating in India. It aims to identify and explore the following research questions:

- What is the ongoing state of cybersecurity controls and practices implemented by OPCs, MSMEs operating in India?
- What are the biggest security risks and vulnerabilities identified by OPCs, MSMEs in their products?
- How OPCs and MSMEs currently handeling any security incidents/ attacks and how they should handle it effectively?
- What cost-effective cybersecurity measures can OPCs and MSMEs take to comply with relevant legal and regulatory frameworks in India?
- What are the major diffculities faced by OPCs and MSMEs in adopting and experiencing cybersecurity practices, and how the can be addressed?
- What policy and business recommendations can be formulated to support OPCs and MSMEs in strengthening their cybersecurity readiness?

# CHAPTER II:

# REVIEW OF LITERATURE

## 2.1 Theoretical Framework

(Randori & VentureBeat, 2022) states that 70% (7 out of 10) companies have been compromise due to unknown, unmanaged or poorly managed internet-facing assets. Since the average company takes around 80+ hours to manage and update the inventory of their external attack surface, it becomes hard to repeat the process frequently.

That is why, Randori (2022) claims that 73% of organizations admits they still depend on the spreadsheet to manage their external attack and less than 1 in every 3 organizations could find a potent solution to handle the complexities and chaos of their external attack surface. And investment in external attack has become the number one priority for large businesses in 2022 and around 67% of the nations around the world perceive that the external attack has been getting bigger and bigger.

Sarmah et al. (2017) claims that cybercrimes against organizations include unauthorized data manipulation such as changing or deleting information, unauthorized access to read or copy sensitive data, denial of service (DOS) attacks that overload systems, and mass destruction of inboxes. These include email bomb attacks, and sophisticated salami attacks. No matter how small the amount, it will be fraudulently withdrawn over time.

Developing nations like India, where digital and internet infrastructure is lacking, have experienced a significant number of security incidents that include confidential data and information of an individual, firms, etc. (Bhatia, 2022). Within this evolution of internet usage, people, OPCs, startups, MSMEs, and large organizations must depend on it

to run their daily operations that further leverage the use of cloud computing services, mobile applications, and IoT devices for developing technology (Bhatia, 2022).

Different security methodologies being used by large firms, and some of them are data loss prevention (DLP), identity access management (IAM), penetration testing, threat modelling, architecture review, endpoint security software, virtual private network (VPN), intrusion detection and preventions system (IDS & IPS), log monitoring tools, SIEM tools, digital forensic investigations tools (Bhatia, 2022).

According to Shah (2022), MSMEs do not have IT resources who can adequately protect them because talented resources does not wanted to work for MSMEs, further observed that MSMEs are losing their business continuity due to ransomware attacks.

The goal of the preliminary literature review aims to determine the most economical and successful cybersecurity adoption method that MSMEs can use. This study explores cost-effective cybersecurity approaches tailored to MSMEs, considering their limited financial and technical resources constraints. It will help an organization in understanding how important it is to prioritize risk assessment, employee training, encryption, risk mitigations, access controls, and leveraging affordable or open-source security tools.

In addition, it emphasizes management accounting methods like cost-benefit analysis and risk management to optimize resource allocation for cybersecurity investments. The review emphasizes that practical policies and working with experts are the key to MSMEs for successful cybersecurity adoption. This strategy aims to find a balance between the need for strong cybersecurity defenses and the budgetary constraints that small and medium enterprises often face ensuring that it can help them in defending effectively against growing cyber threats without spending much money.

## 2.2 Types of Attackers

An organization can be attacked either by external/ internal attackers. Some of them are classified as:

**Cybercriminals**: Cybercriminals are people who use computers in illegal activities or other digital technologies, such as the Internet, targeting computer systems, networks, and digital data for malicious purposes (*Cybercriminals - an Overview | ScienceDirect Topics*, n.d.). These actors exploit their experience, human behavior, and a readily available tools developed by different hacking groups and services to commit crimes including hacking, data theft (PII information), digital scams, digital fraud (digital arrest), malware creation and dissemination, and attacks on computer systems and websites (*Cybercriminals - an Overview | ScienceDirect Topics*, n.d.).

**Nation-State Actors**: These sophisticated groups operate on behalf of governments to conduct espionage, sabotage, or influence operations. In education, they often target research data or intellectual property. For instance, Chinese and Russian state-sponsored hackers have been known to infiltrate universities keys (*What Are the Types of Cyber Threat Actors?*, n.d.).

**Hacktivists**: Hacktivists are mostly sponsored by political parties, where they run political agendas or social activities using digital media or social media to support their causes, in which they mostly target the government or different corporate firms to harm their reputation. Sometimes these resources do have direct connections with religious groups, terrorists, drug dealers, etc., (*What Is Hacktivism?*, n.d.).

**Script Kiddies**: These attackers are new to hacking and perform attacks by using tools and exploits that are easy to find online on different security knowledge base websites such as Exploit-DB (a website where exploits for an application are being published by

different attackers). Even though they are not very smart, they can still cause outages or problems by targeting services that are open, using known vulnerabilities within an application, or launching DDoS attacks for fun or to get attention, and they are unpredictable and could get worse over time (Raza, 2025).

**Advanced Persistent Threats (APTs):** APT attacks are mainly executed by different hacking groups in a sophisticated manner targeting a particular organization or government department to extract sensitive information like credit cards, driver's licenses, social security numbers, Aadhar details, and PAN card details. Once extracted or the attack is successful, they either ask for ransom from that attacked organization in the form of Bitcoin, or sometimes they sell it on the dark web (Chen et al., 2014).

**Hackers**: An individual or group of individual hackers who try to obtain unauthorized access to organizations data and networks by exploiting any vulnerabilities/ weakness within organizations' software or by phishing attacks (Levy, 1984).

**Malware Developers**: These are the individuals having coding knowledge who spread malicious software such as (spyware, ransomware, trojans) to employees of an organization to gain unauthorized access (Rieck et al., 2008).

**Insiders**: These are existing employees (individual), contractors who mismanages their privilege within the organization to share confidential data or to attack organizations software/ websites for their personal gain, satisfaction or revenge (N. Saxena et al., 2020).

**DOS Attacks**: The DDoS attack represents one of the severe type of attack that affects the performance of the cloud computing platform, network services, or servers by making it unavailable to its intended users (Gaurav et al., 2021).

In 2001, advancements in intruder automation led to a surge in self-propagating worms, some of which were used for DoS attacks. Windows end-users and Internet routing

technology became more targets, and IRC technology became more prevalent to shut-down the target systems within a network (Long & Thomas, 2001).

Availability of these data with its integrity and confidentiality between sender and receiver a critical parameter in security in information and communication systems (Peraković et al., 2015).

According to (A. Mishra et al., 2021), there are two basic approaches that can be used to prevent DDoS attacks:

1. Safeguarding your network by yourself from these kinds of attacks.
2. Avoiding turning on your network resources from botforces or botnets so that organizations does not get attentions and became unnoticed.

The increasing in number of servers globally poses various concerns in terms of connectivity, security, and its management, by virtue of which these devices became part of a notorious botnet force attacks (A. Mishra et al., 2021).

### 2.3 Outlines different essential security terminology

This discussion outlines essential pillars and processes for organizations, including startup owners, CISOs, ISOs, and the Board of Directors of MSMEs.

**Architecture Review:** Architecture specifications and models structure complex software systems, providing a blueprint for future engineering activities and aiding software engineers in managing the growing complexity of software systems, tells us the importance of the architecture design phase, which considered as one of the most critical and impactful activity in a software engineering project (Aleti et al., 2012).

**Threat Modeling**: Threat modeling is a process of identifying possible vulnerabilities within a product, a system's complex design, and a data flow diagram where

it talks about different components and processes being involved in developing that particular product or hardware system. In this process both security engineers and product team members discuss different frameworks that can be used for the effective development of the solution (Hasan et al., 2005). The process of threat modeling can be:

- It provides an overview of the architecture design of the product or hardware system with its data flow diagrams (DFDs), which are graphical representations of processes between various components like CDNs, third-party applications, database servers, user interactions, etc (Cisco Systems Inc, n.d.).
- Threat modeling further helps in the prioritization of identified risks for businesses, where they can make decisions on addressing these vulnerabilities during the development life cycle (Cisco Systems Inc, n.d.).

**SAST**: Preventive security techniques in source code development can prevent vulnerabilities by preventing developers from making mistakes. However, mistakes are inevitable, so additional security analysis techniques are necessary post-development (Mateo Tudela et al., 2020).

**DAST**: DAST tools are black box tools that analyze a web application by attacking all external source inputs. They crawl the application's attack surface, perform a recursive attack, analyze HTTP responses, and manually revise vulnerability reports. Unlike white box tools, DAST tools don't know the application's source code, resulting less true positives and false negatives than source code analysis tools (Mateo Tudela et al., 2020).

**IAST**: It is mainly adopted by developers because it is integrated within the development tools like VSCode, where developers find it during runtime, eliminating risks for penetration testing. (Mateo Tudela et al., 2020).

**Penetration Testing**: It is a manual process of identifying vulnerabilities based on how the application behaves when accessed by a user; here security engineers follow common practices for assessing the defense mechanism of an asset (infrastructure, web application, or API) by planning and executing all possible attacks to discover and exploit existing vulnerabilities (Ghanem & Chen, 2019).

**SOC**: Security Operations Centers (SOCs) provides an comprehensive solution for an attack which is a mixture of people, processes, technologies, governance and compliance, to identify, detect, and mitigate threats, preferably before any damage occurs (Vielberth et al., 2020).

**IAM**: Identity and Access Management (IAM) is a process of managing users access control and permissions by identifying digital resources and establishing the authorization level assigned for an individual user (Mohammed et al., 2018).

User can create, remove or adjust their permissions by authenticating to an application where combination of username and password and multifactor authentications like smartcards, generated tokens, one time password, and/or biometric data used to make the authentication mechanism more stronger (Mohammed et al., 2018).

**GRC**: The acronym "GRC" (Governance, Risk and Compliance) is a buzz word over few years. As individual issues, governance, risk management and compliance have always been fundamental concerns of business and its leaders (Racz et al., 2010).

It an approach where security engineers establish different rules and structures (governance) to integrate with business requirements and its objectives that align with its integrity for identifying and mitigating threats (risk management) and ensuring regulation, rules, and policies (compliance) are followed, which is used to make proper decisions (Racz et al., 2010).

**Threat Intelligence**: Threat intelligence has gained a boom in the industry, where it may originate from both internal and external sources within an organization, where data feeds are provided by both open-source and commercial vendors specializing in threat intelligence. This information is valuable for identifying new zero-day vulnerabilities and recently discovered threats, detecting stolen data (often from analysis of compromised datasets publicly available on the Internet by anonymous third parties), and for identifying past security breaches (Nikkel, 2014).

**DLP (Data Loss Prevention)**: Data loss prevention helps in identifying, detecting, and preventing security breaches from the exposure of legitimate data. This process helps companies to comply with different regulations such as California Consumer Privacy Act (CCPA), EU General Data Protection Regulation (GDPR), and Health Insurance Portability and Accountability Act (HIPAA), etc (Fortinet, 2023).

**IOT Security:** Realizing the potential of the Internet of Things (IoT) concept resulted in connecting a large number of different devices to provide new services and automation of many processes in the industry, household, transportation and many other sectors, IoT devices has potential of creating of illegitimate traffic with an aim to block the communications network and increasing in such traffic may cause distributed denial of service (DDoS) attacks (Peraković et al., 2015).

## 2.4 CIA-AAA – Core concept for Developers

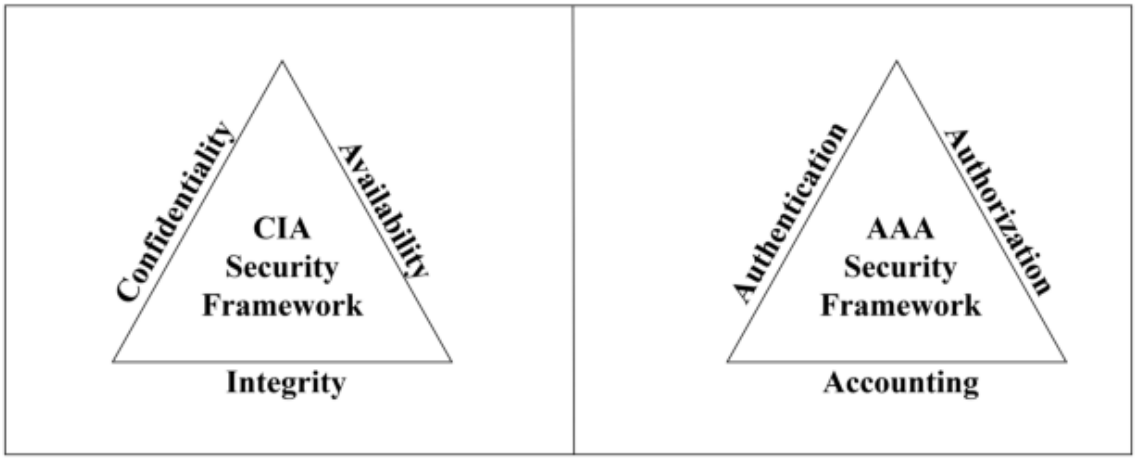



*Figure 2.4.1*
*CIA-AAA*

**Confidentiality**: In confidentiality we make sure that the data being transmitted between source and destination is secured by maintaining its secrecy. To achieve this, data gets encrypted so that if a malicious user is able to get the data by any means, like a man-in-the-middle attack, they cannot decrypt it, as the key that is used here (public and private key) is not with the attacker and is only accessible to the intended user and secure from attackers (Lundgren & Möller, 2019).

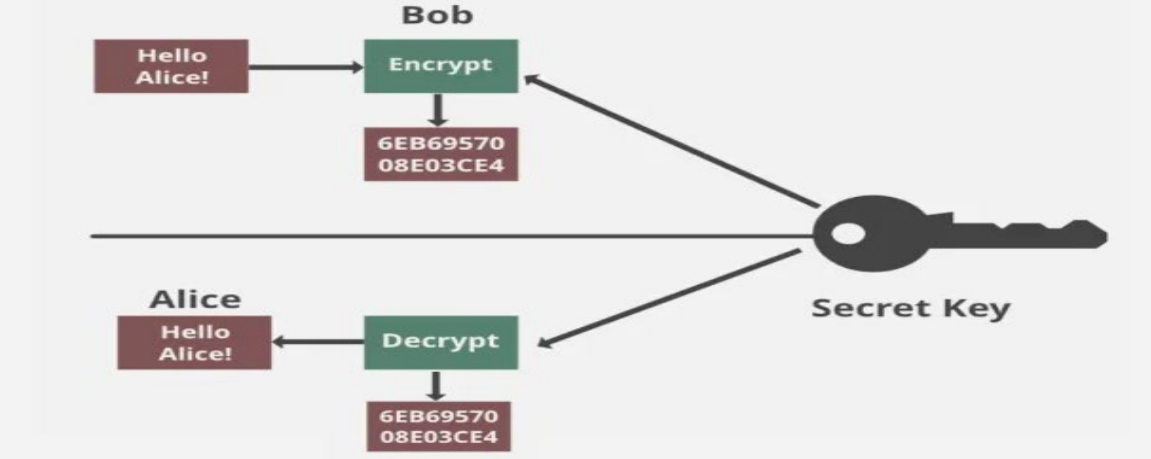



*Figure 2.4.2*
*Confidentiality*

Image Source: *(What Is CIA Triad?, 19:12:09+00:00)*

**Integrity**: It makes sure that when received at the receiver's end, the data is not tampered with or altered by an attacker during transit or at rest (Lundgren & Möller, 2019).

**Availability**: It makes sure that when data is delivered at the receiver's end, the receiver is able to access it whenever required, which is mainly used against threats/attacks like DDOS and ransomware. One example would be when we release a product publicly, we release it with a hash of the file that makes sure that when downloaded by the users, it is not tampered with (*What Is CIA Triad?*).

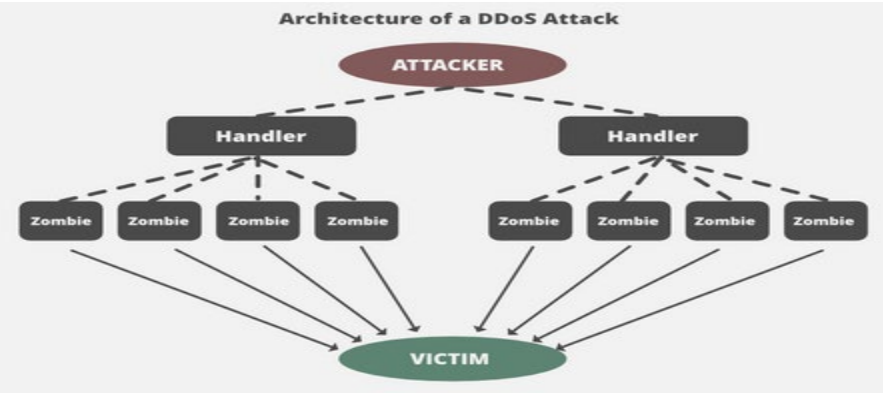


*Figure 2.4.3*
*Availability*

Image Source: *(What Is CIA Triad?, 19:12:09+00:00)*

**Authentication (Access Control):** Verification and identification of the user or server attempting to gain access resources. It's like showing your ID to get into a club. Example: Passwords, Certificates, Biometrics (*Understanding AAA Frameworks in Cybersecurity*, n.d.).

**Authorization:** According to (*Understanding AAA Frameworks in Cybersecurity*, n.d.). Granting permissions or access rights to authenticated users based on policies. It's like getting a special pass to access certain areas.

- Role-Based Access Control (RBAC): This provides an user a access based on mapped roles example, like a student and teacher access on a learning portal.
- Attribute-Based Access Control (ABAC): This decides what actions you can perform when authenticated to a system or application, example teachers can set questions and students and answer based on the question type.
- Rule-Based Access Control: Here, rules set by administrators decide what you can access, usually based on conditions they have set, example an HR management portal where aspirants apply for the job but they cannot post any new jobs like HR can do.
- Least Privilege Principle: This means only giving you access to what you need to do your job, nothing extra privileges.

**Accountability/ Auditing:** Tracking and recording user activities for monitoring, compliance, and forensic purposes. It's like a security camera watching who goes in and out. Example: Logging, Auditing, Reporting, Compliance. (*Understanding AAA Frameworks in Cybersecurity*, n.d.).

CIA is all about protecting the most important parts of information during in-transit or at-rest, whereas AAA is all about making sure that proper authentication, access control (authorization), and accountability (auditing) are implemented within a system or asset. Companies use both models to validate that security systems are well capable of protecting data and to make sure that systems are used responsibly.

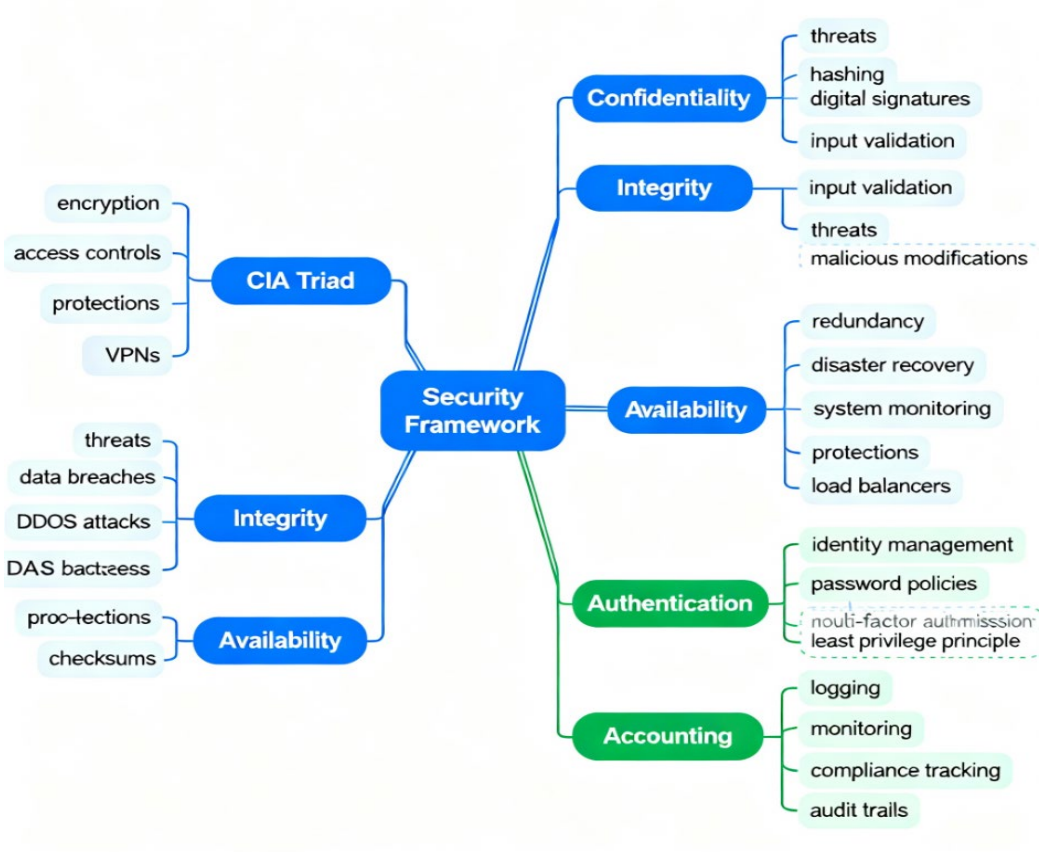



*Figure 2.4.4*
*CIA-AAA Security Framework Examples*

## 2.5 Prioritization of CIA Triad based on different domains

Different domains possess varying priorities aligned with the demand and importance attribution that can be associated with individuals, processes, and technology, that further explains the necessity for physical, logical, or administrative controls, which highlights specific requirements within the confidentiality, integrity, or availability (CIA) triad (Bhattacharjya, 2022).

*Table 2.1*
*CIA prioritization by different domains*

| Domains | Highest | Second | Third | Justification |
|---|---|---|---|---|
| Financial / Banking Services | I | C | A | The accuracy and trustworthiness of financial data, like transaction records, are crucial to prevent fraud. Protecting confidential customer information is also extremely important. The availability of online banking services is a high priority, but not at the expense of integrity. |
| Healthcare | C | I | A | Regulations like HIPAA protects patients' information which is highly sensitive data. Unauthorized access could lead to severe privacy breaches and legal consequences. Ensuring the |

| | | | | |
|---|---|---|---|---|
| | | | | integrity of medical records is vital for correct patient care, while availability is also critical for timely access by medical staff. |
| Manufacturing | I | A | C | The integrity of operational technology (OT) systems and control data is important for confirming the safety and correct functioning of the physical production process. In order to avoid downtime, it is essential to have system availability. While confidentiality may be important for intellectual data, the physical processes and safety come first. |
| Military / National Security | C | I | A | Protecting highly classified information and intelligence from unauthorized leaking is the top most priority. While availability is also necessary for effective operations, maintaining essential data integrity. |
| E-commerce / Retail | A | I | C | Customers must be able to buy products at online store at all |

| | | | | |
|---|---|---|---|---|
| | | | | time, otherwise organization will lose money. Accurate records also depend on transaction data integrity, and safeguarding private client payment information is crucial for both legal and reputational reasons. |
| Telecommunications / Utilities | A | I | C | For public safety and efficient operation, utilities including communication networks, water, and energy must always be available. The integrity of network data is also critical for proper function, while customer confidentiality is a lower, though still significant, concern compared to public service continuity. |
| IT and Software Development | C | I | A | The confidentiality of intellectual property, such as source code and product roadmaps, is often the highest concern for competitive advantage. The integrity of that code and related data is also critical for functionality, while |

| | | | | |
|---|---|---|---|---|
| | | | | system availability is managed based on development and production needs. |

*I – Integrity, C – Confidentiality, A - Availability*

### 2.6 Defense in Depth (DiD)

Defense-in-depth (DiD) is one type of defense mechanism that protects various components with onion-type layered security, and sometimes it gets a comparison with the eggshell protection layer, where data is at the core of the onion, people are the outer layer, and network, host-based, and application security are the inner layers of the onion (B. Kumar, 2019).

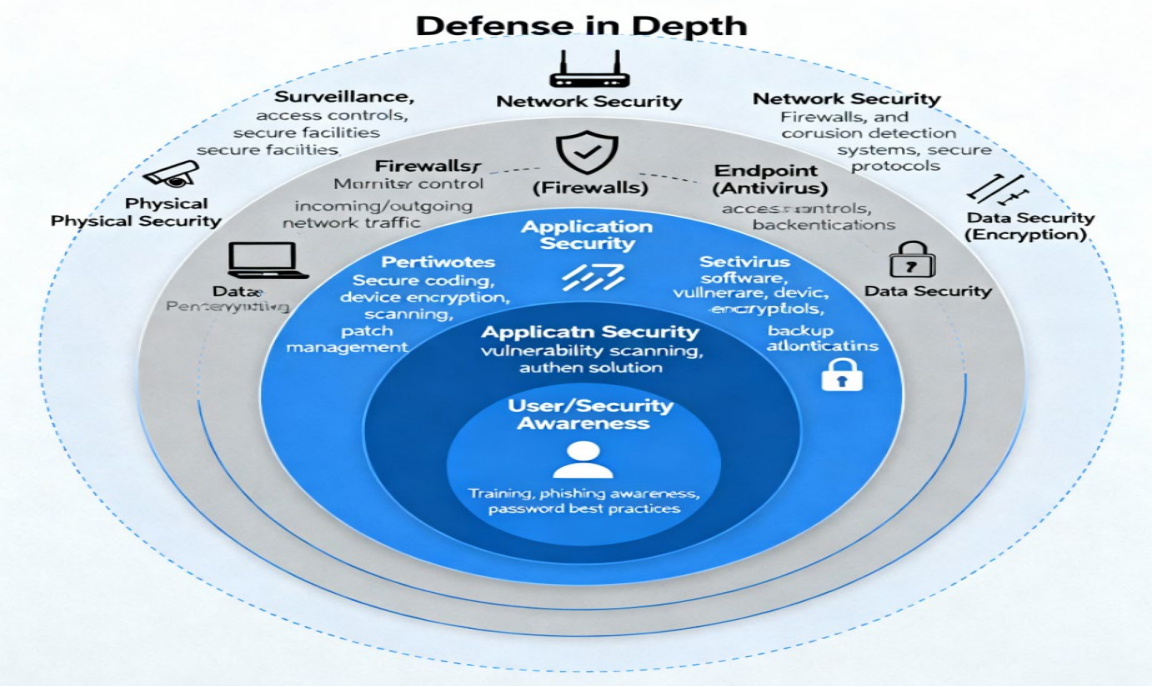



*Figure 2.6.1*
*Defense in Depth (DiD)*

The best defense-in-depth strategy for a software source code and binary file would connect or link with different other application defenses in such a way that each defensive technique protects and supports each other. This action or process of forming interdependent defense mechanisms that would not cause a problem for the development team or the need to maintain best practices for secure software development and software development in general (Stytz, 2004). Each DiD onion layer has its own objective of enhancing data at rest, in transit, and in use for an organizational approach of reducing vulnerabilities that could be exploited by an attacker (Stytz, 2004).

- Physical Security and surveillance layer, focuses on access controls, secure facilities, and protections against physical incursions.
- The next layer represents Network Security, including firewalls, network monitoring, detection systems, and secure protocols to control both incoming and outgoing network traffic.
- The next layer highlights Endpoint Security (antivirus and device protection) and Firewalls for monitoring control and access authentication.
- Application security layer, represents techniques such as secure coding, vulnerability scanning, encryption, patching and maintenance, and device backup strategies are considered.
- Data Security, depicted in the next concentric ring, stresses encryption and protection of sensitive information from penetration and breach.
- The innermost layer focuses on User/Security Awareness, which is foundational—featuring staff training, phishing awareness, and password management best practices.

## 2.7 Threats from Dark Web using Threat Intelligence

If you want to take proactive measures against cyber-attacks within an organization, it's advisable to conduct a detailed analysis of the contents of the Dark Web to understand the nitty-gritty of the criminal minds. If you want to curb the cyber-crimes, the essential step should be either to take a peek into the Dark Web or to take an integrated approach of looking into both the Surface Web and the Dark Web which collects information's from various websites, forums and blog posts (Arunachalam, n.d.).

## 2.8 Attackers approach of Cyber Attack Lifestyle

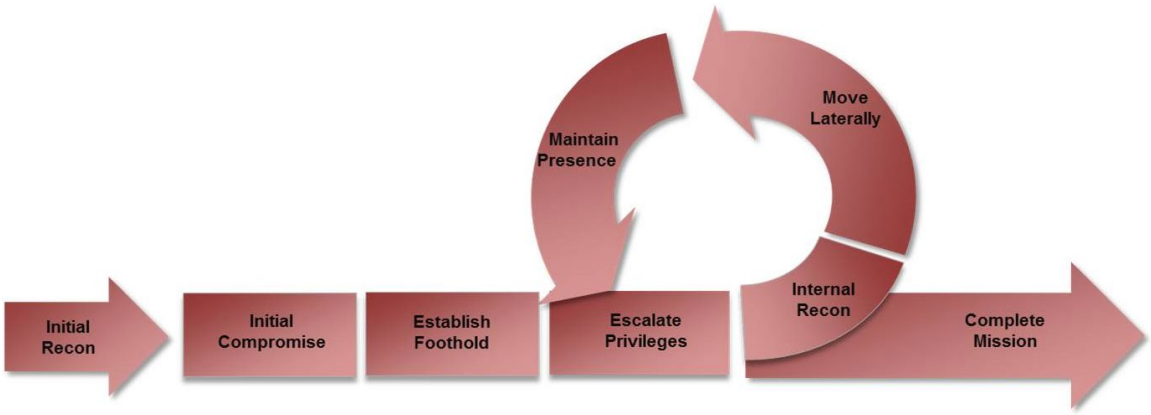



*Figure 2.8.1*
*Cyber Attack Lifestyle*

Image Source: ("Cyber Attack Lifecycle," n.d.-a)

It is mainly devided into two types:

1. ***Passive attack***: In this type of attack, an attacker intercepts the request to observe how a system or application behaves, based on which they formulate the attack. scenario to retrieve the sensitive information where they demand ransom from the victim or the organization (Bhatia, 2022).
2. ***Active Attack***: It's a type of cyber-attack where an attacker directly involves in gaining the system access by altering/ modifying or deleting or by disrupting any services running within system to gain unauthorized access. This attack involves DDOS Attacks or Man-in-the-Middle (MitM) attack or malware-based attack (Zaidan et al., 2023).

Reconnaissance: In this phase the attacker collects initial information about the target (it may be people or a website or a server) and constructs an attack scenario. Attackers collect these data from different sources like internet-facing data (social media, blog posts, or 3rd-party libraries) and internal sources like employee social media harvesting and employee activity observations ("Cyber Attack Lifecycle," n.d.-b).

Initial Compromise: Based on the information gathered, the attacker executes malicious code on the target. It mainly happens via social engineering, phishing, or vishing or by exploiting known vulnerabilities within the internet-facing website/servers ("Cyber Attack Lifecycle," n.d.-b).

Establish Foothold: Once an attacker gains an initial foothold, they want to have persistent access so that whenever they want to access this target, they do not start from scratch; rather, using their uploaded backdoor, they will perform the access. It may include installing backdoors, malware, etc ("Cyber Attack Lifecycle," n.d.-b).

Escalate Privilege: Once low-level access is gained, they try to gain admin-level privilege, followed by cracking the password if they have obtained it in the previous step or by exploiting any persistent vulnerability within an application or service that runs with root or admin-level privilege (“Cyber Attack Lifecycle,” n.d.-b).

Internal Recon: In this phase the attacker tries to search if they would be able to gain access to internal resources that typically run within a DMZ zone (“Cyber Attack Lifecycle,” n.d.-b).

Move Laterally: The attacker uses their internal access to explore the compromised environment by analyzing the Windows tasks, cron jobs, scheduled tasks, and processes running and brute-forcing the remote desktop protocol to gain UI access (“Cyber Attack Lifecycle,” n.d.-b).

Maintain Presence: In this step they again maintain their access so that they are able to gain access whenever they want (“Cyber Attack Lifecycle,” n.d.-b).

Complete Mission: In this phase they dump the database and any sensitive information using which they claim the ransom, or they can even sell it on the dark web to gain some money (“Cyber Attack Lifecycle,” n.d.-b).

### 2.9 Cyber Security Controls

According to IBM (2021), Security controls are the well-established measures, organizations should think of it for their critical infrastructures. By implementing this, one can make sure that they do have proper security countermeasures in place to prevent, identify, mitigate, or reduce the security risks to both their physical and digital assets or other valuable resources (*What Are Security Controls?*, 2021).

*Table 2.2*
*Types of Security Controls*

| | Preventive | Detective | Deterrent | Recovery | Corrective |
|---|---|---|---|---|---|
| PHYSICAL | Fences, Gates, Locks | Cameras | Security offivers, watchman, Dogs | Disaster Recovery, Business continuation plan | Repair physical damage, Re-issue access cards |
| TECHNICAL CONTROLS | Firewall, IDS, MFA, Antivirus, Security Information, And Event Management (SIEM) | IDS, Honeypot | Proxy Server | System restoration, Backups, Server clustering | Vulnerability Patching, Reboot a system, Quarantine a virus |
| ADMINISTRATIVE CONTROL | Hiring & termination policies, Separation of duties, Data Classification | Review access rights, Audit logs and unauthorized changes | A strict security policy stating severe consequences for employees if it is violated | Drills | Implement a business continuity plan, Have an incident response plan |

Endpoint security software like McAfee has built-in antivirus, anti-spyware, DLP systems, remote control, HDD encryption mechanisms, etc., which will satisfy an organization's technical control that can be used to mitigate security risks. If an OPC, startup, or MSMEs is developing a software product, then they are required to perform Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST), Vulnerability Assessment, and Manual Penetration Testing (Manual PT), which act as detective controls to identify vulnerability within an asset or within the application.

When developers remediate these vulnerabilities, it satisfies detective, preventive, and corrective controls for the asset. OPC, startups, and MSMEs are required to dilute at least 20% of their budget with a minimum of physical, technical, and administrative controls to safeguard their reputation.

Preventive controls assist in the mitigation of cyber threats; detective controls assist in the identification of issues or malicious activities; and corrective controls support during the rectification of identified irregularities or issues (Cannon, n.d.). Deterrent mechanisms prevent minute threats are mitigated by deterring assailants through their detectable presence within the system, while recovery controls facilitate return to normal operations following an incident. (CISSP, 2023).

## 2.10 Governance, Risk Management, and Compliance Requirements

"GRC" stands for governance, risk, and compliance, which has had a great rate of business community penetration over the last few years and is now widely being adopted within the software industry (Papazafeiropoulou & Spanaki, 2016).

The Sarbanes-Oxley Act (SOX), Basel II and various other international and regional regulatory requirements have led to the adoption of GRC software systems, given

the regulatory requirements for executives and IT administrators, the software provided by GRC vendors became increasingly important in meeting the new standards (Papazafeiropoulou & Spanaki, 2016). By adopting GRC, organizations make themselves well capable of making better decisions, which helps stakeholders to comply with regulatory requirements (Amazon, 2025).

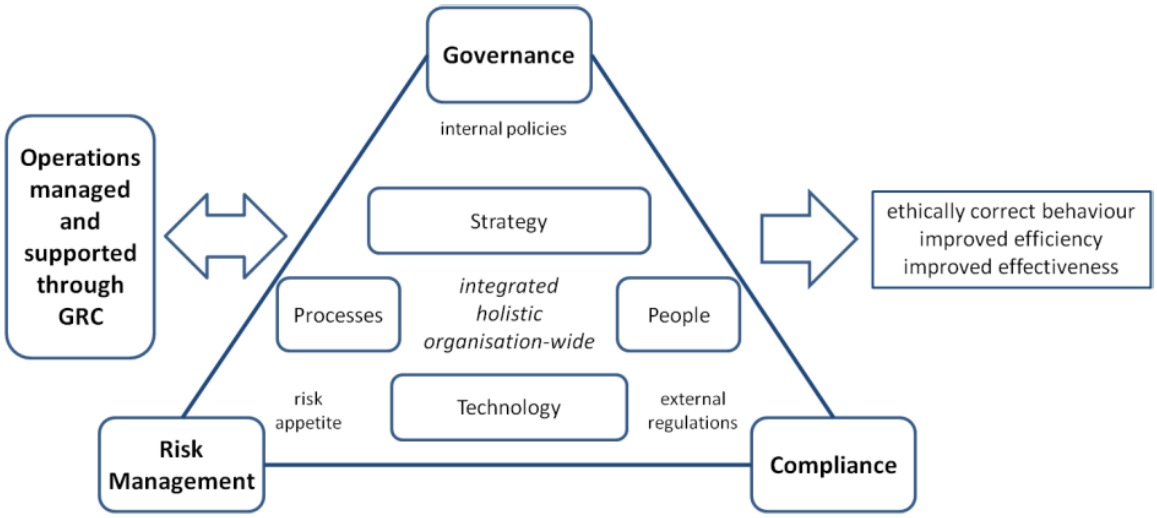



*Figure 2.10.1*
*Frame of Integrated GRC*

Image Source: (Racz et al., 2010)

Each of the subjects consists of the four basic components of GRC: strategy, processes, technology and people, organisation's risk appetite, its internal policies and external regulations constitute the rules of GRC (Racz et al., 2010).

Governance—It is a set of internal policies, rules and regulations, and frameworks that organizations use to accomplish their business requirements. It defines various responsibilities for senior executives and the board of directors. It checks an individual's ethics and accountability, transparency in data sharing, policy acceptance, and resource management (Amazon, 2025).

Risk Management—Organizations sometimes face various risks that include legal, financial, strategic, and security risks, with risk management organizations able to identify a way to fix them by assessing the organization's risk appetite (Amazon, 2025).

Compliance—In this, organizations are bound to follow different laws and regulations enforced by local authorities where they operate, failing which organizations may face penalties and other consequences. For example, if in India you wanted to act as a payment aggregator, then you would need to follow RBI rules as well as PCI-DSS regulation to accept payments (Amazon, 2025).

### 2.11 OWASP compliance guideline for reducing attack surface(s)

OWASP (Open Web Application Security Project) is a community that provides open source tools and security guidelines for application development. According to Fredj (2020), web applications (WAs), use of API services, thick clients, and mobile applications are being used by almost every organization for their daily work; hence, they are more prone to different types of attacks. The biggest challenge organizations face is how to develop secure applications with almost zero vulnerabilities so that, when they go live, attackers won't be able to compromise them. That is where the OWASP Top countermeasures play a vital role in teaching different remediation techniques that one developer can adopt while developing web applications, mobile, thick client, or even backend API services that will guarantee the protection against the most severe attacks and prevention from such attacks (Fredj et al., 2020).

**OWASP Top 10 for Web Applications:**


*Figure 2.11.1*
*OWASP Top 10 for WA(s)*

Image Source: (*What Is OWASP and Why Is It Important?*, n.d.)

Broken Access Control (BAC)—Ranked as the 1st critical vulnerability in OWASP for web applications because of its unfavorable consequence, i.e., privilege escalation that may lead to huge financial loss and reputation damage of the company (Hassan et al., 2018). Broken access control is a kind of privilege escalation methodology or technique in which an attacker tries to gain access to a resource that is not meant for that particular user, meaning gaining access to unauthorized data (Jan et al., 2025). This is not only limited to gaining access; if you were able to perform other actions like UPDATE, MODIFY, or DELETE actions on another resource, that is also considered a BAC issue. This application arises because of developers' misconceptions about developing and allowing resource access or because of input validation and authorization checks to determine whether the requested user is actually authorized to perform that activity or not (Jan et al., 2025).

Cryptographic failures—As the name suggests, when it fails to encrypt sensitive data such as credit card numbers, health information, and passwords securely, we say the application is vulnerable to cryptographic failures (W. A. OWASP, 2025). The reason behind this vulnerability is the use of weak or deprecated algorithms (for example, storing passwords in plain text or MD5 in base64 encoded format that can be easily decrypted), poor key management (if a key is used to encrypt or decrypt the data but that key is exposed in the application; an example would be like the key being hardcoded in the JavaScript), lack of encryption around sensitive data, insecure transmission of data (such as credit card information being transmitted over HTTP protocol when it has to be over HTTPS protocol), and improper implementation of cryptographic protocols (W. A. OWASP, 2025). To fix this vulnerability, one should not use MD5, TLS 1.0-1.2, or SSL 2.0 & 3.0.

Injection attacks—Injection attacks are a broader group that is the combination of different other vulnerabilities like SQL Injection, HTML Injection, Cross-Site Scripting (JavaScript Injection), OS Command Injection, NoSQL Injection, LDAP Injection, Expression Language Injection, XML Injection, etc. A web application is susceptible to these kinds of attacks when an application does not validate user-supplied input or improper sanitization where it gets executed as it is provided. For example, you have a search field where you used to search for some data, but if we put ' (quote) and the application breaks, we can say that the application might be vulnerable to SQL injection (*A03 Injection - OWASP Top 10:2025 RC1*, n.d.).

Insecure Design - Insecure design, sometimes known as business logic flaws, exposes sensitive information in an error message in the form of a stack trace and failure to store these logs in a log server instead of showing them to the end user (*A04 Insecure Design - OWASP Top 10:2025 RC1*, n.d.). Let's say a classic example: in 2025, many of the users were using different mobile applications to make the payments or

cryptocurrencies to do the exchange. Say user 1 is supposed to send 200 rupees to user 2, then user 2 gets credit of 200 rupees. Similarly, if user 2 tries to make a payment of 100 rupees to user 1, instead of a positive value, user 2 sends a negative two hundred (-200), then user 1 gets debited.

Security Misconfiguration – As the name says, this happens when we configure a server but we have not configured it properly, causing a security incident. Some of the examples would be unnecessary features that are enabled by the server administration when they configured the server, like services running with high-privileged user permission or not having a password change policy where the requirement is to change the password at an interval of 90 days, or exposing too much information in HTTP headers (A. S. OWASP, 2025).

Vulnerable and Outdated Components—When a developer develops an application, they rely on some of the 3rd-party libraries or components, such as the jQuery library or frameworks, instead of developing them from scratch, and security researchers sometimes find vulnerabilities within these components that may lead to some injection attacks like XSS or DDOS, etc. (Cloudflare, n.d.).

Identification and Authentication Failures—Sometimes developers did not understand what authentication failure is, and they used to say we have implemented it within our application, whereas we call it authorization failure from broken access control, where it talks about which user has what permissions (*A07 Identification and Authentication Failures - OWASP Top 10:2025 RC1*, n.d.). Whereas in the case of authentication failure, it mainly talks about credential harvesting and brute force attacks by which we gain access to the system, the use of default credentials like admin/admin or admin/password, weak 2-factor or multi-factor or OTP validation, and the last one, improper implementation of user session management. Say we have an application where

the user has the ability to log in and log out and even surf the different pages, and the user did not properly log out from the application and did a system shutdown or closed the web browser, and later when he tries to access that particular application, the application did not ask for credentials and allowed the user to perform further activities (*A07 Identification and Authentication Failures - OWASP Top 10:2025 RC1*, n.d.).

Software and Data Integrity Failures— It is a type of flaw where an application trusts or relies on data generated from an untrusted source or software updates or critical data manipulation or unverified codes. Let's say an application uses a 3rd party vendor for payment processing, and an attacker was able to understand the logic of how that payment processor works, and the attacker is now able to purchase that product by modifying or altering the response of the payment processor without even paying a single rupee. We can see that the application is vulnerable to software and data integrity and that the application fully relied on the response it got without a proper validation. This attack may result in unauthorized data alterations, financial and reputation loss, and other legal implications (*A08 Software and Data Integrity Failures - OWASP Top 10:2025 RC1*, n.d.).

Security Logging and Monitoring Failures—A log is a record of events within an organization's systems and networks, often containing records related to computer security. The increasing number and volume of logs have led to the need for computer security log management (Kent & Souppaya, 2006). This process involves generating, transmitting, storing, analysing, and disposing of log data, and logs are essential for identifying security incidents, policy violations, fraudulent activity, operational problems, auditing, forensic analysis, and compliance with Federal legislation (Kent & Souppaya, 2006). However, balancing limited log management resources with a continuous supply of data is a challenge. Log management helps in protecting confidentiality, integrity, and availability

of logs. Implementing recommendations can help facilitate more efficient log management for federal departments and agencies (Kent & Souppaya, 2006).

Server-side request forgery (SSRF) - Server-side request forgery that allows server-side applications, usually the internal resources that are not externally available, and it is very important to find an endpoint to trigger the SSRF vulnerability (A. S. OWASP, 2025). In this type of attack an attacker tricks the server to make an unauthorized request on its behalf. By exploiting this vulnerability, an attacker can manipulate the server to access internal resources, bypass security controls, and/or attack other systems. This can further lead to accessing internal databases, compromising the server itself, or attacking others within the network (A. S. OWASP, 2025).

**OWASP Top 10 for Mobile Applications:**


*Figure 2.11.2*
*OWASP Top 10 for Mobile*

Image Source: (Mobile Top 10, 2024)

Every researcher talks about web application vulnerabilities, but no one talks about vulnerabilities related to mobile applications. Below are the top 10 mobile vulnerabilities that need to be checked:

Improper Credential Usage - As the name suggests, when developers develop a mobile application, they knowingly or unknowingly hard-code the credentials in the source code in a comment and store them in plain text within the device or transmit them without proper encryption or channel, which allows an attacker to use these credentials to gain unauthorized access to retrieve sensitive information (ZoeniX ), 2025). The reason for this kind of vulnerability is developers develop the application in such a way that they do not want users to log in each time they open the application. Say you have a mobile application that deals with an ecommerce platform where they need login credentials. The user logs in, and the application, instead of storing them in an encrypted format, stores them in plaintext, and when someone is able to gain access to the mobile or they understand the logic of the application, they will be able to extract this data to access the backend services. Sometimes API keys get hardcoded (ZoeniX ), 2025).

Inadequate Supply Chain Security—This vulnerability happens when mobile applications heavily rely on 3rd-party libraries, components, or frameworks to develop their application. If an attacker is able to exploit these vulnerabilities, they would be able to gain access to the actual application that is consuming that library or component. Whenever they distribute the application, the development team needs to make sure that it gets signed properly (Patil, 2025).

Insecure Authentication/Authorization—Authentication says who you are or who the user is, whereas authorization is about what that authenticated user can do when their identity is validated (chamarthi, 2025). Insecure authentication happens when a mobile application does not validate or is not able to verify user identity (login details), and

insecure authorization happens when a user is able to perform the action that they are not supposed to do or are not allowed to do (chamarthi, 2025). In mobile application authentication happens at the client side on their mobile, and authorization checks happen via an API service that communicates with the backend service. Possible attacks are login bypass, admin label actions executed by normal users, access to sensitive data by manipulating ID or tokens, and account takeover to steal PII or financial data (chamarthi, 2025).

Insufficient input/output validation - The application does not validate user-supplied input when processing and the output when rendering within an application, resulting in injection attacks. These vulnerabilities can be used to execute arbitrary code, extract database content, and create backdoors using the application. Classic examples are SQL injection, XSS, and command injection attacks (Getastra, 2024).

Insecure Communication—Insecure communication allows an attacker to intercept the request easily to read the data that is being transmitted over a nonsecure protocol (Getastra, 2024). A common attack is a man-in-the-middle attack. This problem occurs when using an unencrypted protocol, when no proper SSL/TLS is implemented, or when an SSL certificate has expired and validation has failed (Getastra, 2024). Developers can fix these vulnerabilities by doing SSL pinning that establishes communication over a trusted channel, which makes it difficult for an attacker to intercept or tamper with the data (Getastra, 2024).

Inadequate Privacy Controls—Applications are vulnerable when mobile applications collect users' PII information, such as gender, name, email address, age, or credit/debit card information, IP addresses, and information about health, religion, sexuality, and political opinions, but they do not store it securely (Getastra, 2024).

Insufficient Binary Protection—Binary Protection: In a mobile application, "binary" means the compiled code of the application's source code. So, binary protections mean putting security measures in place to keep this compiled code safe from different kinds of attacks and exploitation (*M7*, 2023). Insufficiency Unveiled: When we say that binary protections are insufficient, we mean that enough strong security measures are not in place to protect the binary code of a mobile application. This flaw puts the application at risk of a wide range of problems that could affect the app's and its data's privacy, integrity, and availability (*M7*, 2023). Associated risks are code tampering, reverse engineering, runtime attacks, insecure data storage, and API security risks. Mitigation techniques are like code obfuscation, binary hardening, secure data storage, API security measures, and continuous monitoring and response (*M7*, 2023).

Security Misconfiguration—Improper configuration of security settings, permissions, and controls that can lead to vulnerabilities and unauthorized access for a mobile application. Attackers with physical access can exploit this vulnerability to gain unauthorized access to sensitive data or perform malicious activities (Mobile Top 10, 2024).

Insecure Data Storage—Mobile applications sometimes store data locally, where hackers are able to view these data in plain text by deep diving into internal storage, external storage, content service providers, log files, XML data, binary data, cookies, and SQL databases (SQLite) (Alanda et al., 2020). Developers often use MODE_WORLD_READABLE & MODE_WORLD_WRITABLE for storing data that gives an attacker access and do not use encryption (Alanda et al., 2020).

Insufficient Cryptography—When an application does not use proper cryptographic functions within an application or outdated algorithms are used (Getastra, 2024). Examples are the use of obsolete encryption algorithms with insecure cryptographic

protocols for generating keys. Attackers use these vulnerabilities to decrypt sensitive data extracted from the data storage as well as invalidate the signature (Getastra, 2024). Poor use of cryptography will not be able to protect the data or confidential information, because irresponsible users can easily obtain the data or information (Alanda et al., 2020).

**OWASP Dependency Checks:**

Open-source software (OSS) libraries are extensively used within the industry to expedite the development of products (Ponta et al., 2020). These libraries are susceptible to an increasing number of vulnerabilities that get publicly disclosed by attackers on different websites such as Exploit-DB (Ponta et al., 2020). Therefore, it is important for developers to identify vulnerable dependencies at regular intervals to mitigate any potential risks (Ponta et al., 2020).

## 2.12 Use of AI and ML Model in Cyber Security

Artificial intelligence (AI) is one of the Industry 4.0 technology-based revolutions, which can be used to safeguard Internet-connected systems from cyber threats, attacks, damage, or unauthorized access. To address diversified cybersecurity concerns, widely used AI techniques such as machine learning and deep learning methods, the concept of natural language processing, knowledge representation, reasoning, the Model Context Protocol (MCP) server that enables Retrieval Augmented Generation (RAG), as well as the development of knowledge-based or rule-based expert systems can be adopted (Li, 2018).

The primary advantages and disadvantages of using artificial intelligence (AI) in cyber risk analytics lie in enhancing organizational resilience and better gaining a deeper understanding of cyber risks (Ghillani, 2022).

In the field of computer science, artificial intelligence (AI) is a set of concepts, problems, and methods designed to address specific challenges, which is intended to develop intelligent tools that respond and learn as humans do. On the other hand, this AI can be used to analyze speech, images, and language, and it can transform almost every aspect of life and the economy (Peraković et al., 2021).

In cybersecurity, organizations can take advantage of AI and ML in automated detection, analysis, malware classification, and prevention of phishing attacks with various rule sets and patterns, and it can even learn from the provided data (Merlano, 2024).

Organizations should invest good amount time in validating the models, testing their usability for enhanced understanding of AI/ML in the decision-making process among security engineers and build their trust in the systems and promoting information sharing between information security departments, scientists, and other stakeholders involved in the AI/ML implementation process for better integration (Merlano, 2024).

## 2.13 Implementation of Cyber Security in Various Organizations in India

An organization’s topmost priority should be security when using various types of applications—standalone, web, or mobile. A security incident may lead to various consequences such as reputation damage, data breaches, and financial losses to the organization. It can disrupt organizations’ business operations and cause non-compliance with regulatory requirements and loss of customer trust.

**Security in Railway Industry:**

Kour et al., (2023) states that one of the major considerations in digital transformation of any industry including the railway is the increased exposure to cyberattacks. The railway industry is vulnerable to these attacks because since the number of digital items and also number of interfaces between digital and physical components in the railway systems keep increasing (Kour et al., 2020). Increased number of items and interfaces require new frameworks, concepts and architectures to ensure the railway system's resilience with respect to cybersecurity challenges, such as lack of proactiveness, lack of holistic perspective and obsolescence of safety systems exposed to current and future cyber threats landscape (Kour et al., 2020).

Cyber-attacks are also increasing in railways with an impact on railway stakeholders, e.g. threat to the safety of employees, passengers, or the public in general; loss of sensitive railway information; reputational damage; monetary loss; erroneous decisions; loss of dependability, etc, there is a need to move towards advanced security analytics and automation to identify, respond to, and prevent such security breaches (Kour et al., 2020).

**Security in Marine Industry:**

Ben Farah et al., (2022) states that the vulnerabilities of the Global Navigation Satellite System (GNSS) have been given particular consideration since it is a critical subcategory of many maritime infrastructures and, consequently, a target for cyber-attacks. The dramatic proliferation of cyber-crimes is fueled by increased levels of integration of new enabling technologies, such as IoT and Big Data (Ben Farah et al., 2022). The trend to greater systems integration is, however, compelling, yielding significant business value by facilitating the operation of autonomous vessels, greater exploitation of smart ports, a

reduction in the level of manpower and a marked improvement in fuel consumption and efficiency of services (Ben Farah et al., 2022).

The maritime business uses interconnected cyber network to enable financial transactions, implement contracts, place orders, and perform related business functions over wireless networks compared to other businesses (Kala & Balakrishnan, 2019). The international aspect of maritime transportation means that operators use interconnected cyber systems to provide ship, cargo, passenger, and crew information to customs officials around the world (Kala & Balakrishnan, 2019). While these technologies enable maritime industry to be efficient and reliable, they introduce risks. Exploitation or disruption of the interconnected cyber systems cause disruption of trade and harm the maritime industry (Kala & Balakrishnan, 2019). Vessels use geographic position system for navigation on exclusively networked GPS, while using the same technologies for cargo tracking control. Any disruption, multiple points of failure via a disruption to the GPS signals or malware, controls the way the signal is read, exhibited and used on the vessel or facility (Kala & Balakrishnan, 2019). There are various intentions for organizations and individuals to exploit these vulnerabilities (Kala & Balakrishnan, 2019).

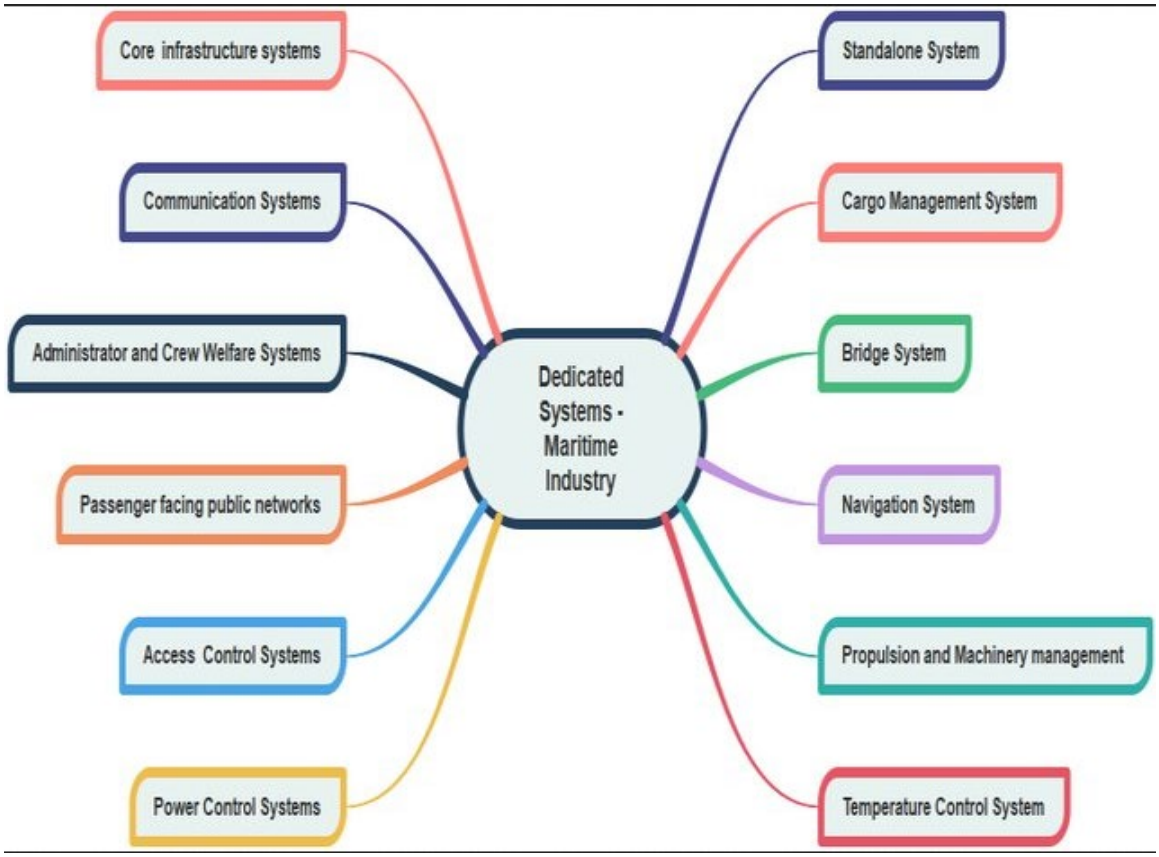



*Figure 2.13.1*
*Dedicated systems associated to maritime industry*

Image Source: (Kala & Balakrishnan, 2019)

**Security in Health-Care Industry:**

In recent days cyber security had been violating in health care systems that stick patients into privacy risk and caused to lost faith in management of health organizations. Although these threats added extra danger to patients health safety and also financial safety to organizations of health system (Bhatia, 2022).

According to Soni et al., (2022), people focus on the intelligent healthcare system expecting sufficient medical facilities even from a remote location. However, to make the healthcare system more trustworthy, secure access control plays a vital role in resisting several cyber-attacks. Security threat on medical data is highly sensitive since it is associated with life risks (Soni et al., 2022). When a user accesses a healthcare system through the Internet, the main concern is preventing unauthorized access to vital healthcare-related data (Soni et al., 2022). Traditional authentication (based on a password, smartcard, and/or biometric) provides a solution to allow such kind of application only to the authorized users, but once a user is authenticated, and he/she is idle for a while, the chances of security threat are reasonably high (Soni et al., 2022). Using latest technology with strong cyber security measures for detecting unauthorized access on devices. Strong firewall network for staff, patients, medical devices. Strict policy for technology procurement (Bhatia, 2022).

**Security in Ed-Tech Industry:**

The growing use of eLearning systems has been documented by numerous studies and with enormous growth; however, little attention has been given to the issue of security of eLearning systems both in research and education (Bandara et al., 2014). Because eLearning systems are open, distributed and interconnected, then security becomes an

impotent challenge in order to insure that interested actors only have access to the right information at the appropriate time (Bandara et al., 2014).

Indian citizens must identify the best techniques in order to protect the information and system, as well as the network in which they work, and the IT industry has been playing catch-up with hackers and cybercriminals for decades (P. Saxena et al., 2012). Thus, there is a need of cyber security curriculum in the near future which will in-build the cyber-security understanding in the current youth and finally the IT sector will get more profound, securely skilled professionals not only in the security sector but also in every sector, thus enhancing the communication, the brain compatibility skills of the employees and the employers (P. Saxena et al., 2012). Effective cyber-security policies, best practices must be planned and most-important must be implemented at all levels and in the future the Government role and education systems participation in the cyber security awareness approach will lead to a strongly secured nation (P. Saxena et al., 2012).

**Security in Financial Sector:**

The Indian banking sector has experienced considerable growth and changes since liberalization of economy in 1991. Though the banking industry is generally well regulated and supervised, the sector suffers from its own set of challenges when it comes to ethical practices, financial distress and corporate governance (Singh et al., 2016). Banks must put cyber risk management plans in place to keep their networks safe and safeguard the safety of their consumers (Singh et al., 2016).. Trust in financial organizations can be eroded by data breaches, which is a big concern for banks. They could lose a large chunk of their consumer base if they have a weak cybersecurity system (S. Mishra, 2023).

Today, bank frauds have taken all possible forms and are prevalent in every facet of banking (Sharma & Sharma, 2018). There is a spirited need for banks to always stay

alive to threat of frauds, build strong systems that can shield, pre-empt frauds, continuously monitor and review the efficiency of such preventive systems (Sharma & Sharma, 2018).

To succeed in controlling frauds, banks need to be proactive and pre-emptive, frauds in banks take place, when either the safeguards or procedural checks are inadequate or not adhered to, leaving the system vulnerable to perpetrators, who can be an insider or an outsider (Sharma & Sharma, 2018).

A fraudster plans to strike the system at its most vulnerable point. An effective defense the bank can have against fraud is to continuously strengthen its operational practices, procedures, and control and review mechanism that fraud prone areas are sanitized against internal and external breaches (Sharma & Sharma, 2018).

**Role of Cyber Security in Retail Industry:**

As the digital retail landscape is rapidly evolving, retailers find themselves to be poorly equipped to handle increasingly sophisticated cyber threats, retailers gave little importance to IT security (Joshi & Akhilesh, 2019). IT security requirements were narrowly framed as ‘checkbox compliance’ given by payment card industry (PCI) for data protection specification and outsourced implementation to individual stores (Joshi & Akhilesh, 2019). As the consumer habits are changing, security should be given a redefined focus and compliance and privacy requirements are making data protection a very essential and critical task (Joshi & Akhilesh, 2019).

Cyber security is a big problem for the retail industry, where the integration of digital technologies has made operations more efficient but also more vulnerable to cyber threats, and retailers must make sure that they are investing in advanced security technologies, fostering a culture of security awareness, and following regulatory standards to protect their business by maintaining customer trust (Vaka, 2025a).

Cyber-attacks in the retail industry can happen in various ways, such as data breaches, payment gateway fraud, malware infections, and ransomware attacks (Vaka, 2025b). These incidents can have major consequences, ranging from immediate financial losses due to theft of funds or data to long-term reputational damage that may lead to loss in customer trust and loyalty (Vaka, 2025b). A data breach reveals users' Personally Identifiable Information (PII), and financial data (including credit card, transaction information, etc.) can cause legal consequences and customers to lose faith in the retailer, affecting the retailer's reputation loss (Vaka, 2025b).

Beyond financial impacts, cyber security incidents can hurt a retailer's reputation, trust plays an important role between consumers and retailers and if an attack happens the customers pays more attention on data privacy issues (Vaka, 2025b). A single cyber security incident can lead to negative publicity, eroding customer trust and loyalty. Rebuilding this trust requires substantial time and resources, and in some cases, may not be entirely achievable (Vaka, 2025b). The reputational damage can also deter potential business partners and investors, limiting the retailer's growth opportunities (Vaka, 2025b).

**Security in Agricultural Industry:**

Globally, India is one of the major players in the agriculture sector which is the primary source of livelihood for about 58% of India’s population. Agriculture is considered as the backbone of the Indian economy (H. C. Verma et al., 2023). It has helped the Indian economy in several ways: providing food, a source of national income, a Source of employment generation, accumulation of the National Capital, provides raw materials for industries (H. C. Verma et al., 2023).

According to the United Nations Food and Agriculture Organization, such a rise in population necessitates an increase in food production of about 70% (H. C. Verma et al.,

2023). Many digital devices such as smartphones, various sensors, global position systems (GPSs), robotics, and drones could be utilised to extract valuable data analysis and make effective decisions to increase food production with less human resources and intervention (H. C. Verma et al., 2023).

For lives and livelihoods, millions of people rely on the food and agriculture industry, just like they do on healthcare, electricity, transportation, and financial services (H. C. Verma et al., 2023). Farmers are using information acquired by GPS, satellite photos, internet-connected gadgets, and other technology to produce more efficiently, which is why precision agriculture is growing in popularity (H. C. Verma et al., 2023). Although the technology underlying these techniques allows hackers and crackers to attack farming machinery to halt food production, these techniques can increase crop yields and cut costs (H. C. Verma et al., 2023). The possibility of a sizable cyber-attack becomes more real as these crucial industries become more and more reliant on digital technologies for corporate operations (H. C. Verma et al., 2023).

It is crucial to implement contemporary cyber defences to safeguard the global food supply chain. Blockchain technology is playing important role in counteracting fraud/duplicity in the food supply chain (H. C. Verma et al., 2023). Additionally, when developing new automation systems, cyber security must be prioritised (H. C. Verma et al., 2023). The entire industry must be safeguarded with the most cutting-edge and efficient instruments and regulations due to the brittle and interconnected character of the food supply because eating is the most vital thing for everyone (H. C. Verma et al., 2023).

## 2.14 Vulnerability Management

Vulnerability prioritization is a fundamental process of vulnerability management. It is a process where precise prioritization enables focused concentration to be concentrated on the most critical vulnerabilities and their timely remediation; otherwise, Organizations may encounter financial loss or damage to their reputations (Walkowski et al., 2021).

During the time between a vulnerability identified and reported to a company or organization it takes time in implementing the fix or workaround, and does not mean that the vulnerability is exploited (Komaragiri & Edward, 2022). With current vulnerability management standards, between 5 and 75% of vulnerabilities remain outstanding, leaving a gaping hole in a company's network security perimeter (Komaragiri & Edward, 2022).

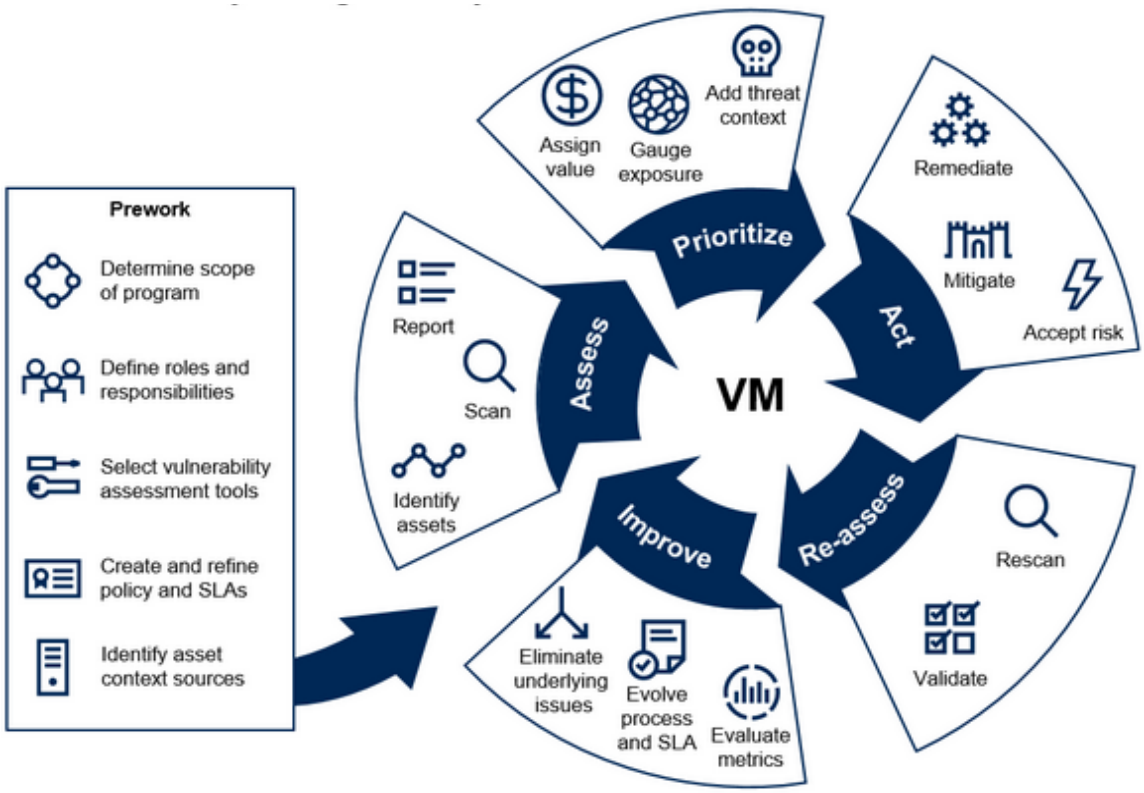


*Figure 2.14.1*
*Vulnerability Management life cycle*

Image Source: (Maués, 2020)

During the prework phase as described in the Figure 2.14.1 it is the responsibility of a security engineer to:

- Determine list of assets and or systems those are in-scope for vulnerability scanning.
- Clearly define the roles and responsibilities to avoid any ambiguity.
- Selection of right software tools for scanning (example: Qualys)
- Create and define policy and SLAs.
- Understand business value and risk profile assessment.

**Assess/Discovery** - In this phase security engineers created a full list of assets (inventory) and prepared a security baseline by identifying vulnerabilities by using vulnerability management tools such as Qualys, Rapid7, etc (Microsoft, 2024).

**Prioritization of assets** - Assign a specific value for each asset group that will help in prioritizing which asset group requires more attention while addressing these vulnerabilities and allocating resources (Microsoft, 2024).

**Assessment/ Act** - In the assessment phase, the security engineer tries to understand the risk profile associated with each asset group, allowing them to determine which vulnerability needs the topmost priority in fixing it so that the attacker won't be able to exploit it on time (Microsoft, 2024).

**Re-Assessment** – In this phase the security engineer performs another scan confirming the remediated vulnerabilities got fixed, which is the final phase of the vulnerability management process, which includes regular auditing and follow-ups to make sure that threats are fixed (Microsoft, 2024).

**Decision flow for Vulnerability Management process:**

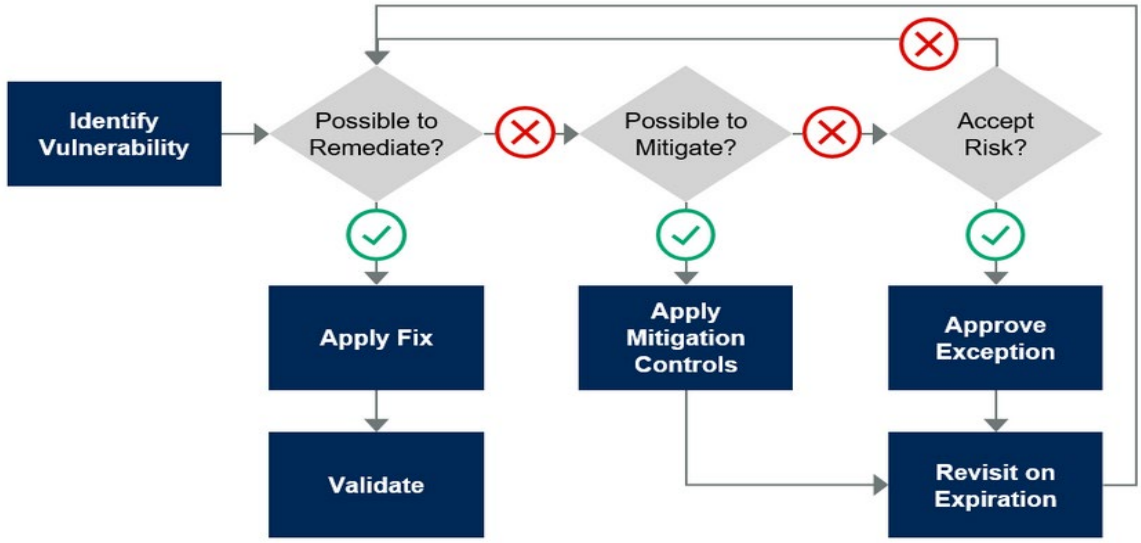



*Figure 2.14.3*
*Vulnerability Management decision flow*

Image Source: (Maués, 2020)

**Identify vulnerabilities** - Vulnerability scanners are the automated scanners that identify weaknesses, threats, and potentially exploitable vulnerabilities within a system or network, where scanning for vulnerabilities and security misconfigurations are the center of attraction (Microsoft, 2024).

**Evaluate vulnerabilities** - Once a vulnerability and its root cause are identified, security engineers must validate its true positive or false positive according to its risk scoring/rating (Microsoft, 2024).

**Address vulnerabilities** - After 2nd phase (evaluation of vulnerabilities) the phase is addressing it where the best options being chosen to remediate either by implementing compensative control and by updating/upgrading the software, if specific vendor has released it (Microsoft, 2024).

**Report vulnerabilities** - Once vulnerabilities are addressed, it is important to document and report known vulnerabilities, that help IT teams to track vulnerability trends across networks and make sure that organizations are compliant with various security standards and regulations (Microsoft, 2024).

### 2.15 OWASP Top 10 API Security Risks

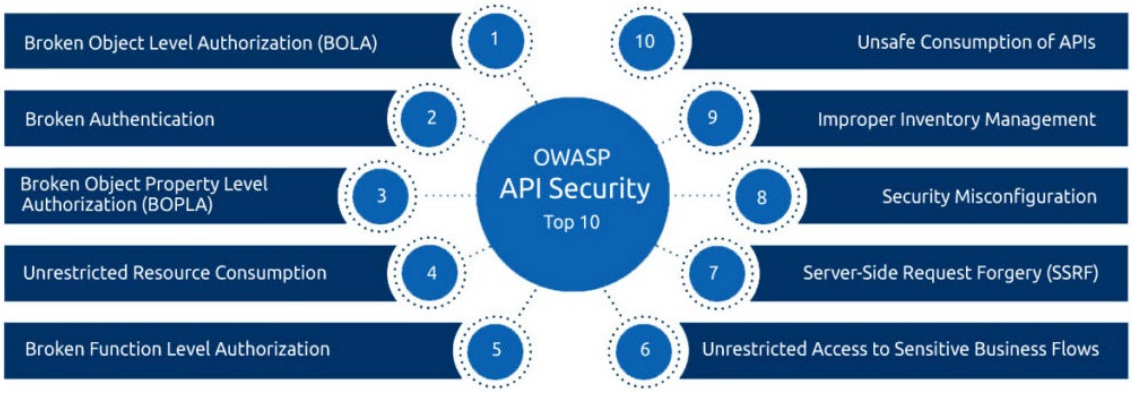



*Figure 2.15.1*
*OWASP API Top 10*

Image Source: (G, 2025)

Broken Object Level Authorization - When an application does not properly restrict access to an object, we say that application is vulnerable to BOLA. Let's say an example, we have been logged in into an web application that usages and API endpoint that returns users profile information based on the user's id says "1234" and this value is being passed in the URL, then you modify this id to say "4321" and you were able to view another users profile information that may contains PII information we can say that application/API endpoint is vulnerable to Broken Object Level Authorization (BOLA), often this is named as IDOR (Pranczk, 2024). This is a classic example of viewing someone's data, but if that

endpoint does have the privilege of deleting or updating data, then as an attacker, we can delete, update or modify all the users' information within that application (Pranczk, 2024).

Broken Authentication - Before understanding broken authentication, we need to understand what authentication is, which allows a user to gain access to the web application based on the user's credentials, where the application verifies the user's identity (A. S. OWASP, 2025). If the provided user credentials are correct, then the application creates a long token that acts as a session token, using which the application does not ask for user credentials each time an application page is refreshed (A. S. OWASP, 2025).

If, as an attacker, we were able to predict the application mechanism of how the session token is being generated, then using this generated token, if we are able to gain access to another user's account, then we can say the application or the underlined API endpoint is vulnerable to broken authentication (A. S. OWASP, 2025). Some of the examples are brute force attacks, where attackers try to perform automated attacks to guess the username and password; another example is the use of weak passwords like "qwertyuiop," and weak session cookies are another example (A. S. OWASP, 2025).

Broken Object Property Level Authorization - RESTful APIs have become the standard for accessing web-oriented resources, enabling users to initiate operational requests through HTTP methods, paths, and parameters. However, the parameters of RESTful APIs are user-controlled, hence, inherently untrusted (Wu et al., 2025). Attackers can exploit this by tampering with the resource ID parameter to access sensitive data of other users without authorization, leading to a Broken Object Level Authorization (BOLA) attack (Wu et al., 2025). Resource ID is the unique identifier of resources in REST API that are used to operate (INSERT, DELETE, UPDATE, READ) resources, that is, BOLA attack injection point. The vulnerability arises from over-reliance on the user-supplied resource ID, without enforcing proper access control mechanisms (Wu et al., 2025). The

BOLA vulnerability is an access control vulnerability, and developers need to perform some security checks before users operate sensitive information to defend against the vulnerability. BOLA vulnerabilities are derived from the lack of object-level authorization checking (Wu et al., 2025).

Unrestricted Resource Consumption - In this type of vulnerability that allows malicious users to launch a brute force attack or DDOS attack against an API endpoint, let's say, for example, a user can continuously send different combinations of username and password until they break the application login (Best, 2025). Another example would be it does a file uploading functionality with a limit, say, of 10MB, but as an attacker, if we upload 1GB of data, then the backend API endpoint will not be able to handle it, resulting in unavailability of the resources (Best, 2025). Another example would be an API endpoint that is used to verify users based on the OTP, where the attacker user constructs different mobile numbers to be sent to the backend service, and the application owner will end up paying a lot of money (Best, 2025).

Broken Function Level Authorization - It is a complex access control policy with different hierarchies or groups and user roles, and an unclear separation between administrative and regular functions tends to lead to authorization flaws (A. S. OWASP, 2025). By exploiting these issues, attackers gain access to the other users' resources and/or administrative functions. Sometimes we can denote it as a vertical insecure direct object reference (IDOR) (A. S. OWASP, 2025). Let's understand with an example: we have an application that has an option to upload a video, and later on stage as a user, we can change the name, so we need to verify its response using proxy tools like Burp Suite, where we need to find the list of OPTIONS that endpoint (the endpoint is /api/user/videos/45) can handle. Now let's say in the application I do not have the delete option, but by changing the OPTION to DELETE, we get an error saying admin can do it, so we modify the URL

from "/api/user/videos/45" to "/api/admin/videos/45." I am able to delete the video. Here we can say that though the user does not have the ability to delete the video, by modifying the API endpoint, he is able to perform the delete action (A. S. OWASP, 2025).

Unrestricted Access to Sensitive Business Flows - API endpoint that does not restrict access to sensitive business flows, allowing excessive usage that can harm the business's reputation (A. S. OWASP, 2025). Let's say within an application on the day of product launch a malicious user can launch a coordinated effort to buy all stocks of the new product to resell at a higher price. Achieved using an automated tool such as web crawlers running on multiple servers globally, we can say the application does not have rate limiting restriction (A. S. OWASP, 2025).

Server-Side Request Forgery (SSRF) - Server-side request forgery that allows server-side applications, usually the internal resources that are not externally available, and it is very important to find an endpoint to trigger the SSRF vulnerability (A. S. OWASP, 2025). In this type of attack an attacker tricks the server to make an unauthorized request on its behalf. By exploiting this vulnerability, an attacker can manipulate the server to access internal resources, bypass security controls, and/or attack other systems. This can further lead to accessing internal databases, compromising the server itself, or attacking others within the network (A. S. OWASP, 2025).

Security Misconfiguration – As the name says, when we configure a server but we have not configured it properly, causing a security incident (A. S. OWASP, 2025).. Some of the examples would be unnecessary features that are enabled by the server administration when they configured the server, like services running with high-privileged user permission or not having a password change policy where the requirement is to change the password at an interval of 90 days, or exposing too much information in HTTP headers (A. S. OWASP, 2025).

Improper Inventory Management - Sometimes it's called improper asset management, where application owners fail to decommission the old version of the API endpoint, or they forget to remove it, and they define v1 or v2 in the API endpoint request. Example We launch a new version of the API with security improvements, and we fail to retire the old version, and a malicious user can leverage the old version to exploit its vulnerabilities that provide access to the application (A. S. OWASP, 2025).

Unsafe Consumption of APIs - Most systems have integrated with third-party APIs, where unsafe consumption of APIs happens when we fail to validate the output from those APIs and leak malicious content into our system that is not intended for that particular user (A. S. OWASP, 2025). Example To set up a user profile, we pull information from a 3rd party application, as a malicious user set their address in the 3rd party app to an SQL injection value like `drop table users;`. When we update the user profile, the SQL query gets executed with potentially damaging different consequences (A. S. OWASP, 2025).

**2.16 Cyber law provisions in India**

In the Indian Penal Code, cybercrimes are sometimes defined as an individual's or organization's involvement in criminal activities, including but not limited to theft, fraud, forgery, defamation, and mischief. Digital fraud, digital arrest and any new era incidents are also included within Indian Information Technology Act, 2000 (Ghate & Agrawal, 2017). Indian IT act application to the whole of India, even other nationalities may come under the law, if the crime happened using a computer or network located in India (Ghate & Agrawal, 2017).

*Table 2.3*
*Indian Information Technology (IT) Act, 2000 and it's Amendment, 2008*

| Section | Offence | Penalty |
|---|---|---|
| 65 | Tampering with computer source documents | Imprisonment up to three years, or/and fine up to ₹2,00,000 |
| 66 | Hacking with computer system | Imprisonment up to three years, or/and fine up to ₹5,00,000 |
| 66B | Receiving stolen computer or communication device | Imprisonment up to three years, or/and fine up to ₹1,00,000 |
| 66C | Using password of another person | Imprisonment up to three years, or/and fine up to ₹1,00,000 |
| 66D | Cheating using computer resource | Imprisonment up to three years, or/and fine up to ₹1,00,000 |
| 66E | Publishing private images of others | Imprisonment up to three years, or/and fine up to ₹2,00,000 |
| 66F | Acts of cyberterrorism | Imprisonment up to life. |
| 67 | Publishing information which is obscene in electronic form. | Imprisonment up to five years, or/and fine up to ₹10,00,000 |
| 67A | Publishing images containing sexual acts | Imprisonment up to seven years, or/and fine up to ₹10,00,000 |
| 67C | Failure to maintain records | Imprisonment up to three years, or/and fine. |
| 68 | Failure/refusal to comply with orders | Imprisonment up to 2 years, or/and fine up to ₹1,00,000 |

| | | |
|---|---|---|
| 69 | Failure/refusal to decrypt data | Imprisonment up to seven years and possible fine. |
| 70 | Securing access or attempting to secure access to a protected system | Imprisonment up to ten years, or/and fine. |
| 71 | Misrepresentation | Imprisonment up to 2 years, or/and fine up to ₹1,00,000 |
| 72 | Breach of confidentiality and privacy | Imprisonment up to 2 years, or/and fine up to ₹1,00,000 |
| 72A | Disclosure of information in breach of lawful contract | Imprisonment up to 3 years, or/and fine up to ₹5,00,000 |
| 73 | Publishing electronic signature certificate false in certain particulars | Imprisonment up to 2 years, or/and fine up to ₹1,00,000 |
| 74 | Publication for fraudulent purpose | Imprisonment up to 2 years, or/and fine up to ₹1,00,000 |

**Table Source:** https://en.wikipedia.org/wiki/Information_*Technology*_Act,_2000

## 2.17 Theory of Reasoned Action

A human psychological model suggests an individual's behavior results from their aim or plan to perform an activity. Mainly it's determined by two factors: their positive or negative feeling of performing an activity and their ability and willingness to perform such activity, or social pressure, surrounding it. It was later expanded as an individual's faith in how easily and effectively they can carry out the task, which accounts for factors that may prevent a person from acting on their intentions.

Within the realm of Cyber Security, the Theory of Reasoned Action (TRA) can offer valuable framework for comprehending and forecasting the acceptance and utilization of cyber security and its applications.

For example, an employee's intention to follow security policies, protocols defined by the organization is influenced by whether they believe those policies and protocols are beneficial (attitude) to them or not, and if they perceive their colleagues and supervisors expect them to follow them. Understanding these two factors, can help organizations to develop more robust effective cybersecurity knowledge base and policies.

### TRA Components in a Cybersecurity Context

**Attitude towards cyber security behaviour**—This shows an individual's (employee's) beliefs and perception about the outcomes of secure behaviours (e.g., avoiding data breaches (phishing, vishing, smishing), protecting company assets) and the value they place on those outcomes (e.g., job security, trustworthiness, efficiency). Example: If an employee believes using an online-based password manager tool or using any random software as a development IDE, regular software update can reduce risk and

values data security and efficiency, their attitude towards the use of these tools will be positive.

**Subjective Norms** - These involve the influences made by peers, managers, and organizational culture. Whether the individual employee believes that important others expect them to behave securely. Example: If an employee perceives that their team and supervisors value secure practices (like locking screens, changing password at regular intervals (at least within 90 days), or reporting phishing emails when they receive them from an external source that they are not aware of), they're more likely to conform.

**Behavioral Intention -** This is the self-motivation or willingness to engage in a cybersecurity behavior, influenced by the two components above. A strong intention increases the likelihood of actual behavior.

**Application of TRA to Cybersecurity Programs**

Through TRA, organizations can develop more effective cybersecurity awareness and training programs by focusing on: Improving attitudes - Present evidence-based accounts of breaches as proof of the consequences. Benefit from effective cyber hygiene (less downtime, fewer incidents). Use interactive simulations to ensure that your actions are safe. Improving Subjective Norms through leadership modeling of secure behaviors. Encourage others to be held accountable (e.g., department security champions). Utilize team-based security metrics to promote shared accountability among staff members. Enhancing Intentions - Employ commitment strategies, such as public pledges to adhere to policy. Enforce distinct directives and facilitate effortless safe behavior.

## 2.18 Human Society Theory

National security in the 21st Century is a compulsory investments in social cybersecurity that requires ground level study and research of the human interaction and understanding of technology and social context and an individual's beliefs and external factors (Beskow & Carley, 2020).

Most of the data breaches happen because of their employee mistakes within an organization. While vulnerability exploits are still employed, the majority of successful attacks begin with manipulation of human behavior rather than malware. It generally points out the main requirements of social structures, including in any industry, be it the software industry or manufacturing industry. Cyber security can be employed to augment these structures, and it has the capability to secure the environment, software, humans, etc.

**Key aspects of human society theory in cybersecurity**

Human Factors and Behavior: This application is the simplest and highlights how human actions and inactions result into breaches. It's easy for people to fall for social engineering attacks when they are stressed, overconfident, or have too much to think about. Using behavioral theory security experts can make better training programs by deep diving into the root cause of for what reason people became victim of attacks. This concept views cybersecurity as a whole system integration that includes people, processes, and technology. It gives special importance of collaboration among team members.

Sociological and Cultural Influences: Management should support and promote a security culture in order to reinforce safe conduct of their employees. It is recommended, to communicate openly but in a culture that does not know how to make people feel unsafe. Using social dynamics can you guess how an attacker's usage people's sentiment and

emotions to bypass technical controls by revealing distinct security challenges faced by different groups, such as those with limited resources or education.

Psychological Factors: Research on personality traits shows that a person's level of conscientiousness affects their intention and willingness to follow security standards. This is one of the psychological factors that are at work. Knowing what users want like productivity could help make security solutions that does not cause too much disruptions.

Interdisciplinary Approach: To create more complete strategy for cybersecurity, it is important to include ideas from psychology sociology and ethics and cybersecurity should not just be a technical problem.

## 2.19 Summary

The idea behind reviewing various research papers, journals, white papers, forums and blogs was to identify an effective, industry-recognized approach that organizations can use to assess and implement strategies for addressing security vulnerabilities and preventing cyber threats. This initiative is intended to support the establishment of a cybersecurity unit within the organization and drive awareness among developers on building secure web, mobile, and desktop applications, ultimately strengthening the company's overall security resilience.

While analyzing the gap, I found that —there is a depth of records available for individual vectors, but no one talks about the organizational approach to defending cyber-attacks within an MSME industry operating in India. In this regard, I am trying to gather data from established companies and trying to put up a framework that MSMEs can use to protect their assets or products from external attackers.

The document also highlights the need to balance organizational and individual aspects of implementing and adopting cyber security policies. To achieve meaningful and sustainable outcomes, continuous collaboration between MSMEs, Government and policymakers is essential to align with cybersecurity requirements and strategies.

# CHAPTER III:

# METHODOLOGY

## 3.1 Overview of the Research Problem

The growth of interconnected technologies has brought about a range of emerging security threats, such as VPNs, external infrastructure, useful marketing platforms, IaaS and SaaS providers, third party vendors, shadow IT practices, or Bring Your Own Device (BYOD) practices. As a result, the size and complexity of the modern attack surface is growing rapidly.

Because of this growth, organizations now need to use proactive external attack surface management in a threat environment. When security measures are not fully implemented, then they can leave low-resistance pathways and uncontrolled "blind spots" that an attacker or a hacker can use to obtain persistent access of the system. Due to this boom in digitalization and the adoption of cutting-edge technologies, cyber threats are more prevalent in both Indian multinational corporations and domestic companies.

Even though there are a lot of rules, regulations, and guidelines in place for cybersecurity, there is a lot of disagreement about the implementation and enforcement of consistency. Inadequate cybersecurity awareness and limited technical proficiency among employees, decision-makers (chief engineers) and stakeholders undermines the security postures of organizations. These factors together shows that India's one-person company, micro, small, and medium enterprise (MSMEs) sector needs a compressive, organizational-wise strategy to establish and implement cybersecurity policies and awareness campaigns.

This is largely due to increased threat detection and containment capabilities. In the United States of America (USA), the cost of breaches reached a record $10.22 million, which was then forced both regulatory fines and slower in incident escalation (Bluefin, 2025).

Despite its role in detecting breaches rapidly, attackers are increasingly dependent on AI for sophisticated phishing schemes, deepfakes, and other attacks. One out of every five breaches were linked to shadow AI, which is illegally produced AI tools that are used without organizational control, and 97% of companies breached had inadequate AI governance and access controls. Due to the oversight flaw, the average cost of breaches is raised by approximately $670,000 and the duration of breach lifetimes is extended by roughly one week (Bluefin, 2025).

This study focused on necessity for the adoption and awareness levels of cybersecurity standards and frameworks among MSMEs, the degree of cybersecurity control implementation, their expertise and readiness of mitigating cybersecurity threats, and the challenges these enterprises faces when they try to effectively implementing cybersecurity controls that helps in protecting businesses and critical assets.

Researches and surveys in the same field show that Indian OPCs, startups, micro, small, and medium enterprises (MSMEs) are open/ prone to cyberattacks because they do not know much about cybersecurity, do not have formal policies in place, have tight budgets to run the business, and do not have enough skilled resources/workers. This survey and analysis will help organizations in implementing better cybersecurity frameworks when developing web applications so that they can protect their digital assets. The survey will also discuss various Indian IT acts that organizations should be aware of to avoid any penalties being imposed if an attack happens.

### 3.2 Operationalization of Theoretical Constructs

According to Snyder (2019), an approach that may be defined as qualitative, quantitative, or have a mixed design depending on the phase of the review.

Quantitative research is a method in which research focuses on collection and analysis of quantifying, statistical or numerical data for its trends and relationships and to verify the measurements made, therefore, quantitative research involves measurement and assumes that the phenomena under study can be measured (Watson, 2015).

Qualitative research is a method used to analyze human experiences by understanding individuals point of view on different questions, its actions and aspects like an interview where we evaluate individuals knowledge on the topic/ subjects (Fossey et al., 2002).

A mixed-method approch in which researcher usage both qualitative and quantitative methods of data collection and analysis in a single study, which helps researcher to understand complex phenomena qualitatively as well as to explain the phenomena through numbers, charts, and basic statistical analyses (Creswell, 1999).

In this research paper, I utilized both quantitative and qualitative research methods. Participants were asked different types of questions to determine the internal cybersecurity posture of an organization and selected participants as top management, directors, managers and other key personnel who may not have much knowledge about it. All MSMEs' input will be scrutinized to find any gaps in the on-going implementation of cybersecurity controls or existing standards/frameworks to meet required security posture. Additionally, The new proposed solution will aim to bridge any gaps discovered. Out of those, only 55 MSMEs (150 participants) were sought for research studies. This survey

yielded useful information, as MSME provided valuable input on the implementation of cybersecurity, which is considered a critical and sensitive aspect of any business. The qualitative method was chosen again to ensure that SMEs received appropriate recommendations. Additionally, which is called as research interviews, in which, interviews were conducted with 45 senior executives (with designations like Manager, Senior Manager, Director, Senior Director, CISO) from OPCs, startups, MSMEs across different BU (business units). It helped us to understand their thoughts on the business priorities and assets they are concerned with protecting.

### 3.3 Research Purpose and Questions

Only personal feedback from one-person company (OPC), micro, small, and medium enterprises (MSMEs) leaders is being sought for this study. There are other additional considerations for the identification of loop-holes; moreover, it is about suggesting security policies and methodology implementation, approaches for identifying and remediating vulnerabilities within their products during the development life cycle, and readiness to tackle any security incidents.

- What is the current state of cybersecurity controls and practices implemented by MSMEs operates in India?
- What are the biggest cybersecurity risks and vulnerabilities faced by MSMEs?
- What gaps exist between the current and the desired maturity levels needed to effectively mitigate cyber threats for OPCs, startups, and MSMEs?
- How can MSMEs implement cost-effective cybersecurity measures that comply with relevant legal and regulatory frameworks?

- What are the major challenges, problems faced by MSMEs when try to adopt and keep cybersecurity practices?
- How can policies and business suggestions be made to help MSMEs in strengthening their cybersecurity readiness?

**When Surveryed (using google form):**

- Do you know what is your organization's cybersecurity policies (rules and regulations) and best practices?
- Do you think that your organization's cybersecurity rules and regulations are good enough in protecting assets against cyber threats and attacks?
- Does your organization aware of in industry standards or frameworks?
- Have you ever been a victim of a cyber threat or attack while employed for an organization?
- How often do you change the passwords and update security patches on your devices?
- How would you rate your knowledge and skills of cyber security?
- Do you think that your colleagues and supervisors take cybersecurity seriously?
- Have you ever seen your colleague violating cybersecurity policies or engaging in unsafe practices?
- What do you do to protect any sensitive informations from an incident?
- Have you ever reported an incident to your organization's security team?
- How can the company support you in implementing safe cybersecurity practices in your day-to-day work?

### 3.4 Research Design

To address the proposed research topics, the study will use a mixed approch (both quantitative and qualitative) method. The research study can be more diverse and examine different perspectives on the 360-degree adoption of cybersecurity processes that includes IAM policies, SDLC lifecycle, vulnerability management, assets identification and management, application security, SAST, DAST, OSS, etc., with comprehensive understanding of the issue being examined. It will suggest possible recommended solutions for the identified problems, using basic cybersecurity ideas already in place. The main goal of this study is to determine the factors contributing to the rise of cyber threats in OPCs, startups, micro, small and medium sized enterprises, it also explores the general viewpoints of MSMEs on cybersecurity.

In the research survey (quantitative) method, participants who are the employees of the organization as well as Managing Director, Director, Senior Director, Security Manager, AVP, Director of Products, Chief Information Security Officer, Chief Technical Officer, are taken into consideration.

**Q1. Do you know what is your organization's cybersecurity policies (rules and regulations) and best practices?**

Whether an employee is aware of any set of rules, guidelines, and procedures their organization has established to protect its computers, networks, data, and digital assets, codes, from cyber threats and attacks. They have been given an option to select either YES or NO.

**Q2. Do you think that your organization's cybersecurity rules and regulations are good enough in protecting assets against cyber threats and attacks?**

Irrespective of the answers provided in Q1, the survey asked whether employees are aware of current cyber security policies and practices that safeguard their assets from potential threats. They have been given an option to select either YES or NO.

**Q3. Does your organization aware of in industry standards or frameworks?**

This question checks whether organization follows industry suggested security frameworks that define cybersecurity standards and systems. Common examples include: a framework commonly used to identification, protection, detection, response, and recovery from cyber incidents is the NIST Cybersecurity Framework. It provides guidelines for this approach. ISMS is based on ISO/IEC 27001, which is an international standard that emphasizes the importance of risk management and continuous security improvement. It is a set of best practices designed to help organizations protect their IT environments with prioritized actionable controls, known as CIS benchmarks. The OWASP Framework is the ideal choice for developing Mobile, API, and Web applications. The protection of sensitive health data, personally identifiable information (PII), banking information such as encrypting and securely storing credit/debit card, etc., are the primary goal of HIPAA, GDPR, and PCI DSS regulatory frameworks.

**Q4. Have you ever been a victim of a cyber threat or attack while employed for an organization?**

This question will check on individuals awareness on phishing, ransomware, malware, vishing, unauthorized access, and other cyber-related incidents that their

organization affected during their tenure. They have been given an option to select either YES or NO.

**Q5. How often do you change the passwords and update security patches on your devices?**

This question checks individuals or organizations policy on regular updates to system security patches beeing provided by vendors and how often organizations encouraged in cyber hygiene practices to minimize exposure to vulnerabilities (whether they get notified by the organization on regular interval or they do change the password proactively). They have been provided with an option to write their answers.

**Q6. How would you rate your knowledge and skills of cyber security?**

This question does a Self-assessment of individual understanding of cybersecurity principles, threats, vulnerabilities, CVE, attack-surface and safe behaviors in the workplace. Options are provided with a scale of 1 to 5 where 1 is low, 3 is medium and 5 is high.

**Q7. Do you think that your colleagues and supervisors take cybersecurity seriously?**

Evaluates organizational culture and leadership attitudes towards cybersecurity adherence and prioritization. Three options were provided and they are: Yes, No, and Maybe.

**Q8. Have you ever seen your colleague breaks cybersecurity policies or engaging in unsafe practices?**

Seeks to identify of any non-compliance or risky behaviors exist within the workplace by any employee which could lead to exploitation of internal system or applications. Three options were provided and they are: Yes, No, and Maybe.

**Q9. What do you do to protect any sensitive informations from an incident?**

By asking this questions, we tries to evaluate how often employees are changing their password or if they are changing, then what is the minimum length of the password, whether they are updating softwares regularly when released by vendor or using any pirated softwares, checks their proactiveness of avoiding clicking on malicious/suspicious links when they recevies an email from an unknown source, encrypting sensitive files when transfering, and reporting suspicious activity (if the clicked). They have been provided with an option to write their answers.

**Q10. Have you ever reported an incident to your organization's security team?**

Use of well know reporting channels like PhishPond PhishMe inbuilt security incident reporting tools within different email providers like Microsoft and Google workspace. Two options were provided and they are: Yes and No.

**Q11. How can the company support you in implementing safe cybersecurity practices in your day-to-day work?**

Support can be provided through regular training, enhanced security equipment, awareness raising, the appointment of dedicated security officers and better policy communication. They have been given the chance to write their own answers.

**Q12. What are the major vulnerabilities that were reported externally in your product or identified internally?**

By asking this survey question, the aim was to determine the vulnerabilities that an organizations employees are aware of, which causes the reputational loss when exploited. For these questions, options were provided based on the OWASP Top 10 for web application, mobile and APIs (backend communication services). This survey question further helps in analyzing whether the organizations are aware of any external websites (bug bounty program websites like HackerOne, Bugcroud, Synack, Intigriti) where hackers lawfully report vulnerabilities to the organization via an external website.

**Q13**. **How often do you receive cybersecurity training or awareness programs?**

By asking this question tries to analyze if employees are getting an opportunity to up-skill or not and the options we provided are like Monthly, Quarterly, Never, Yearly or Bi-annually.

### 3.5 Population and Sample

Individuals got selected from different units of an organization, such as banking, finance, insurance, farming, e-commerce, the IT, education, manufacturing, government agencies that perform day-to-day operations, pharmaceuticals, and few other micro industry based organizations. The data was collected from 55 MSMEs (150 respondents ) out of which 45 senior executives were interviewed.

### 3.6 Participant Selection

Participants of the study were carefully selected from various designations such as senior management including owner of the organization, C-level executives (such as CISO, CTS, Senior Director, Director etc.), business unit heads working in MSME and multinational corporations operates in India. These individuals considered the most appropriate and legitimate sources to share the insights for this research. Additionally, employees with varying level of security knowledge from diverse business domain with MSME were taken into consideration.

### 3.7 Instrumentation

Participants, such as CISO, CTS, Senior Director, Director etc., were contacted via social media messaging, colleagues from different industry, messages (SMS), emails, direct visiting to their offices etc. Questions and corresponding answers were noted down in a digital format. In conclusion the in-depth discussions were conducted via in-person visiting different MSMEs within State of Odisha (India), via zoom and MS Team's call.

### 3.8 Data Collection Procedures

The survey was structures to allow participants be able to complete it within 20 minutes. The structures of the questions kept simple and easy for the participants. Responses were collected once the participants submitted the form and used for further analysis and study.

### 3.9 Data Analysis

Extracted data from Goole form, and used MS excel and Anaconda (Jupyter Notebook) were used, for analysis, then transformed it into a visualized format for ease of understanding of the treasures input provided by participants.

### 3.10 Research Design Limitations

This research design was to facilitiate the understanding of problems and huddles organizations faces. Due to the collection sensitive information, management resources requested not to disclose their organization name as they were running a small business within the state (Odisha) India, and any incident may raise a security concern and financial losses.

### 3.11 Conclusion

To sum up this chapter, research would like to hightlight the existing literature, which explains many cyber vulnerabilities, that OPCs, startups, MSMEs needs to address. This research gathered various input from various designated peoples including CISO, CTS, Senior Director, Director and employees through research survey to understand their issues, they are facing in implementing cybersecurity policies, following and practicing secure development while developing products.

CHAPTER IV:

RESULTS

## 4.1 Result Analysis

The results from the survey helped in identifying the gaps and pain-points organizations and employees faces.

### 4.1.1 Do you know what is your organization's cybersecurity policies (rules and regulations) and best practices?

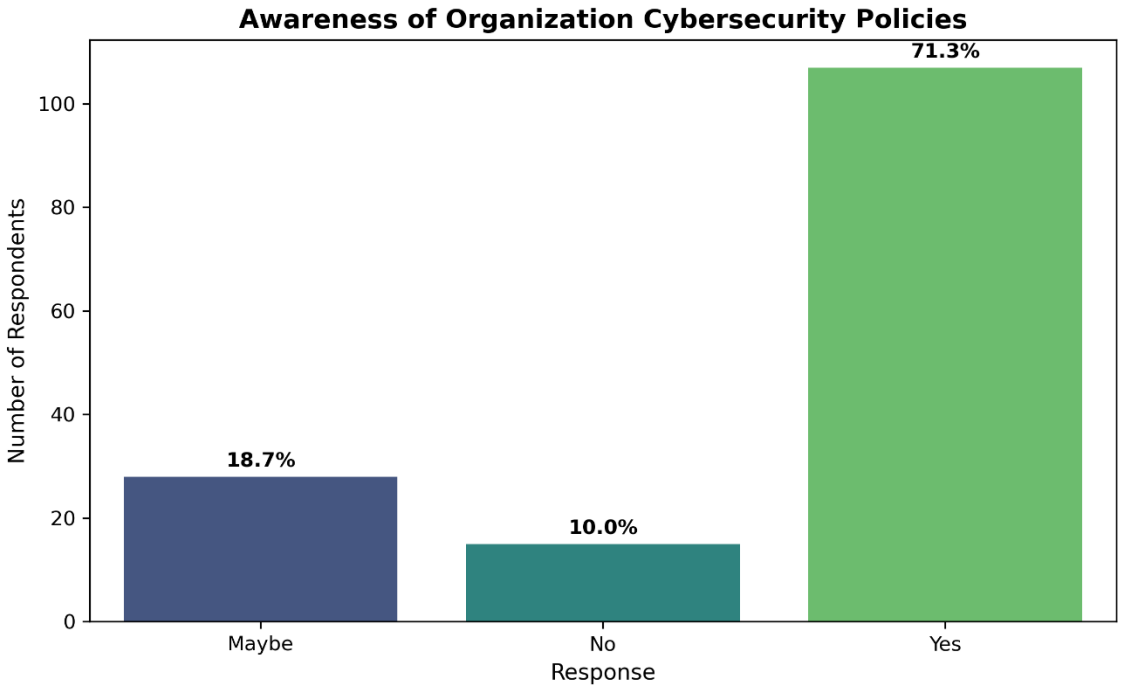



*Figure 4.1.1*
*Cybersecurity policy awareness*

Based on the responses, analysis of the data is as follows:

- 18.7% responded that they may not aware of organization cyber security policies.

- 10% responded that they are not aware of organization cyber security policies.
- 71.3% responded that they are aware of organization cyber security policies.

### 4.1.2 Does your organization aware of in industry standards or frameworks?

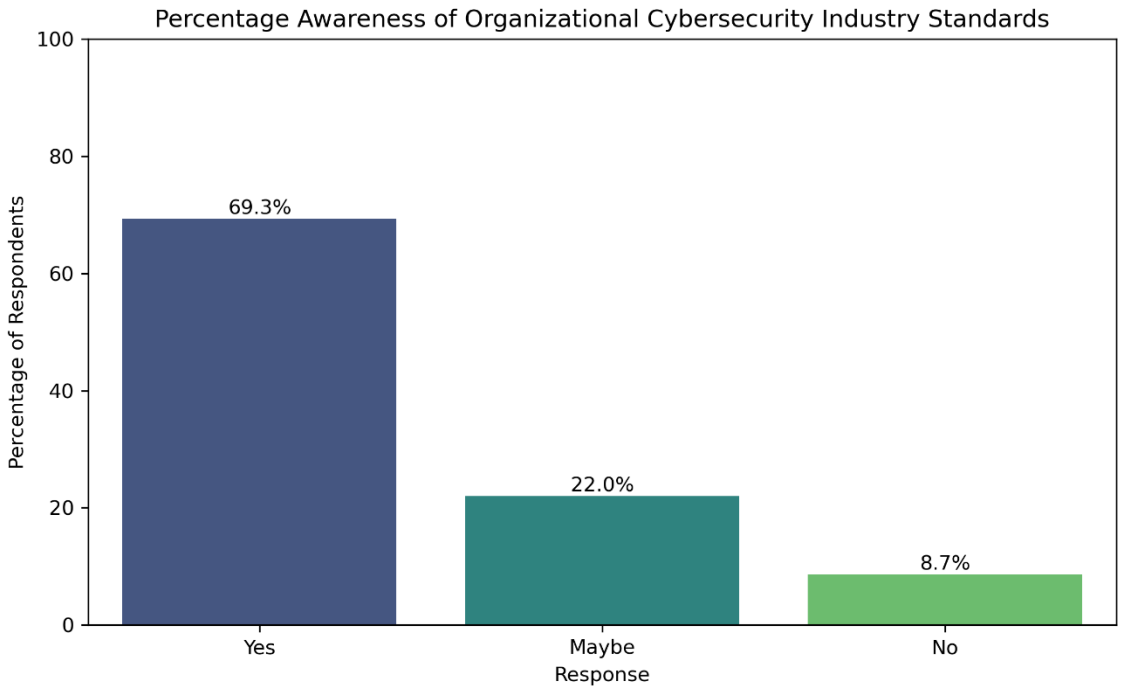



*Figure 4.1.2*
*Cybersecurity standard awareness*

Based on the responses, analysis of the data is as follows:

- 22% responded that they may know any security standard or frameworks used in their organization.
- 8.7% responded that they do not know any security standard or frameworks used in their organization.
- 69.3% responded that they know about security standard or frameworks being followed in their organization.

### 4.1.3 Do you believe that your organization's cybersecurity policies and practices are effective in protecting against cyber threats?

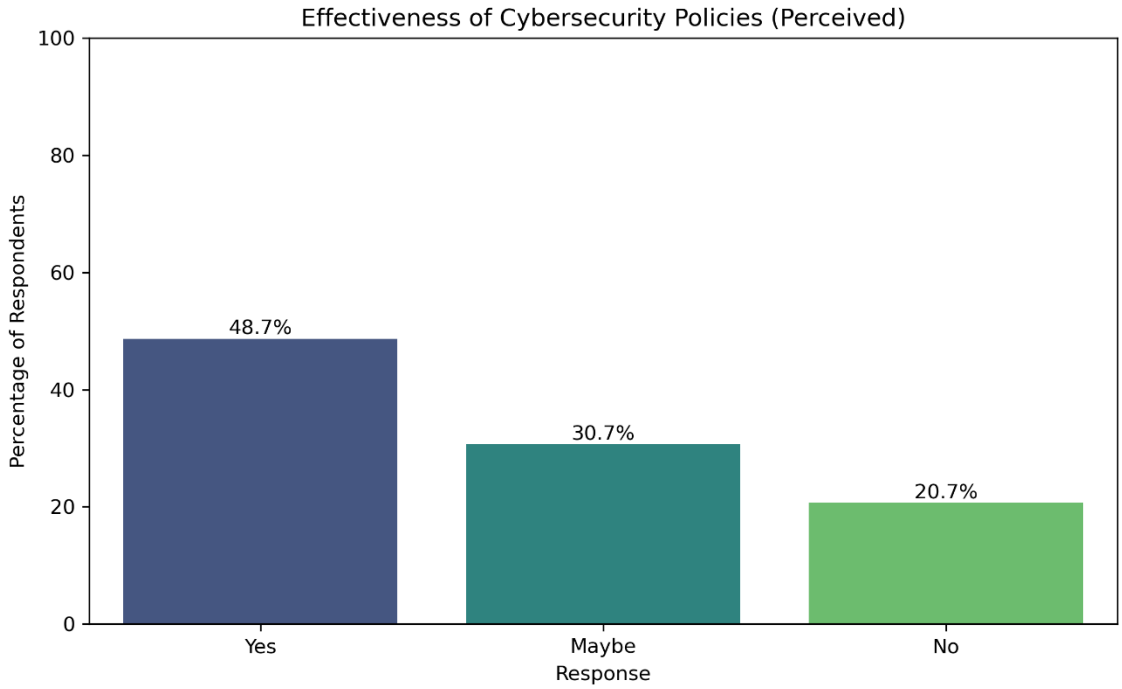



*Figure 4.1.3*
*Effectiveness of Cybersecurity policy*

follows Based on the responses, analysis of the data is as follows:

- 20.7% responded that they do not have effective cyber security policy in-place.
- 30.7% responded that may be the policy they do have is somewhat effective.
- 48.7% responded the policy they do have in their organization is effective and robust in protecting organizational assets from any cyber-attacks.

### 4.1.4 How often do you receive cybersecurity training or awareness programs?

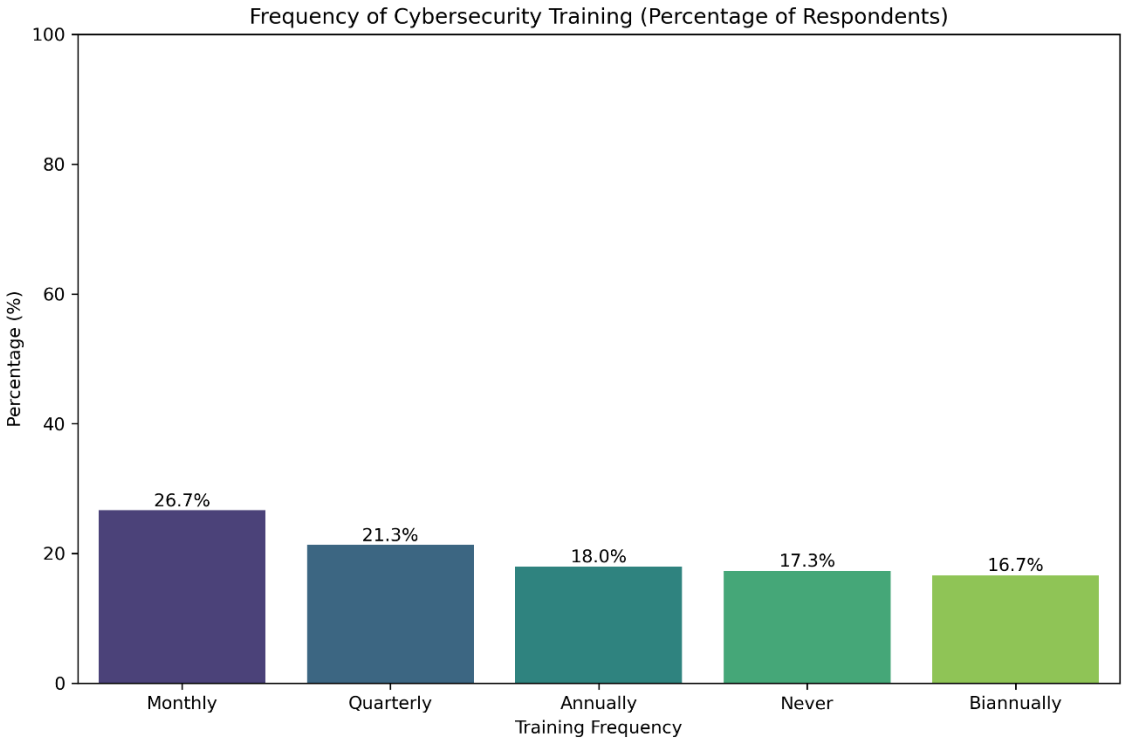



*Figure 4.1.4*
*Cybersecurity training frequency*

Based on the responses, analysis of the data is as follows:

- Monthly, Percentage: 26.7%
- Quarterly, Percentage: 21.3%
- Annually, Percentage: 18.0%
- Never, Percentage: 17.3%
- Biannually, Percentage: 16.7%

Most respondents receive cybersecurity training either quarterly or monthly, reflecting a proactive approach to maintaining awareness. Whereas a smaller portion attend training annually or biannually, which might correspond to roles with less exposure or

lower risk. The minority who reported never receiving training indicates gaps where organizations should focus on improving compliance and education.

### 4.1.5 Have you ever been a victim of a cyber threat or attack while employed for an organization?

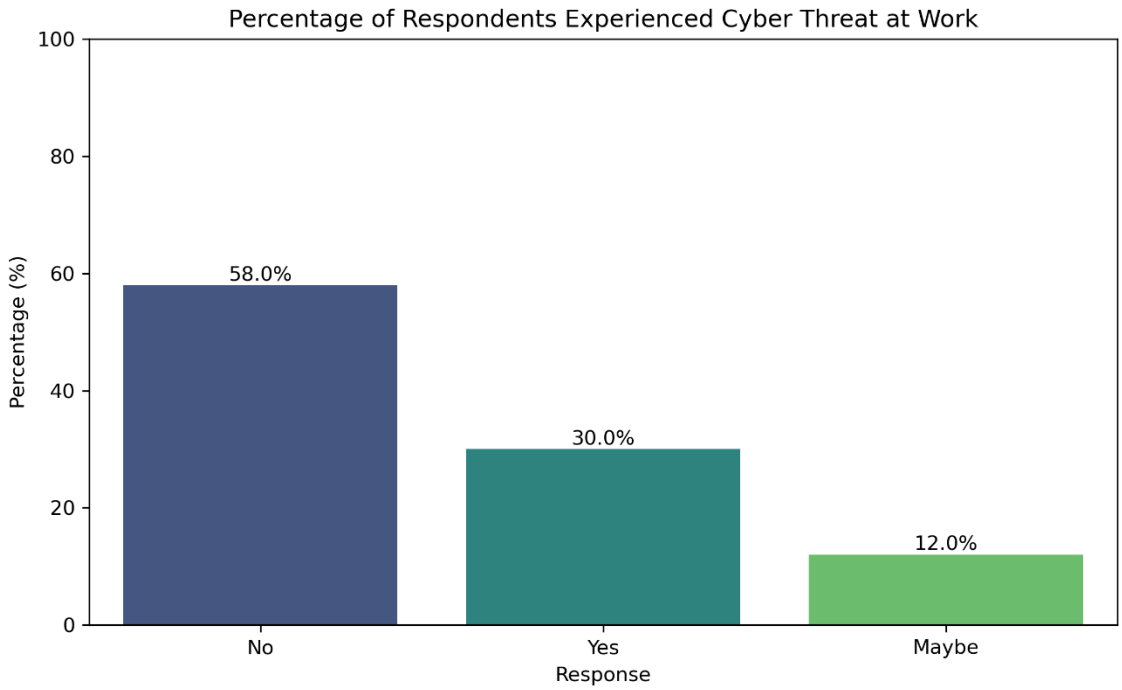



*Figure 4.1.5*
*Experienced Cybersecurity threats at work*

Based on the responses, analysis of the data is as follows:

- 58% respondedthat they did not face any security incidents while working meaning these are the individuals they are well versed with security norms.
- 30% responded that they encountered security incidents.
- 12% respondedthat maybe they faced security incidents but they do not want to express it or they are afraid of the job security if they express it as Yes.

### 4.1.6 How frequently do you change your passwords and update security patches on your work devices?

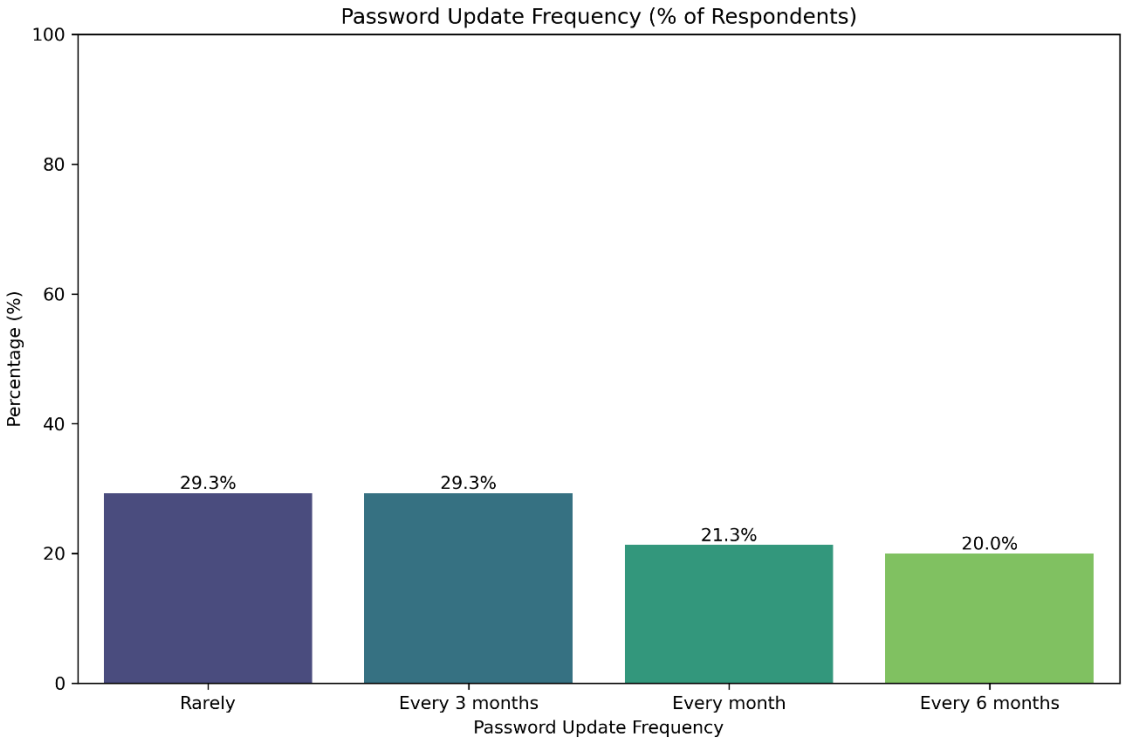



*Figure 4.1.6*
*Password change policy*

Based on the responses, analysis of the data is as follows:

- Rarely, Percentage: 29.3%
- Every 3 months, Percentage: 29.3%
- Every month, Percentage: 21.3%
- Every 6 months, Percentage: 20.0%

Majority of respondents update passwords every 3 to 6 months, which aligns with common security policies. Some updates are regular interval, showing a higher security

vigilance. A smaller percentage update rarely or never, indicating potential security risk areas for the organization. Looks like in their organization they do have adequate security policies that may lead to various security breaches.

### 4.1.7 How would you rank your expertise and knowledge of cyber security?

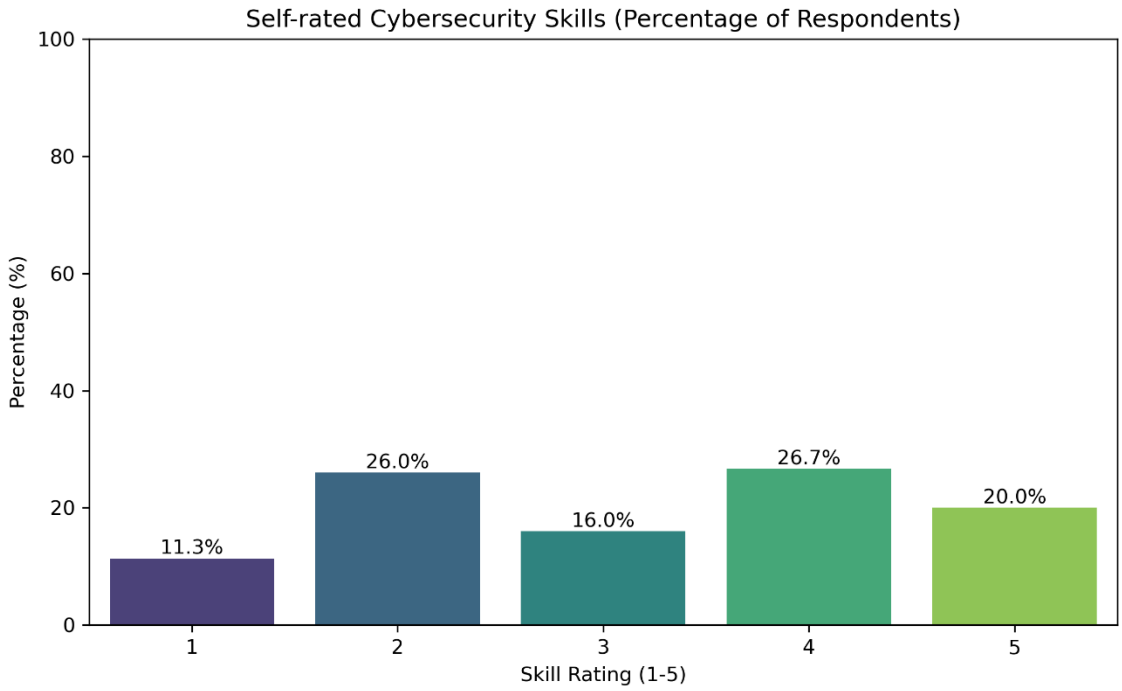



*Figure 4.1.7*
*Self-skill-rating for Cybersecurity skills*

Based on the responses, analysis of the data is as follows:

- Skill Rating: 1, Percentage: 11.3%
- Skill Rating: 2, Percentage: 26.0%
- Skill Rating: 3, Percentage: 16.0%
- Skill Rating: 4, Percentage: 26.7%
- Skill Rating: 5, Percentage: 20.0%

Most of the peoples have rated their cybersecurity skills between 3 and 5, which means they are vigilant. On the other hand, 37% of people rated their skills as low, which means there is a chance to improve their cybersecrutiy skills. It also shows the need for continuous training and awareness programs among employees.

### 4.1.8 Do you think that your colleague and supervisors take cybersecurity seriously?

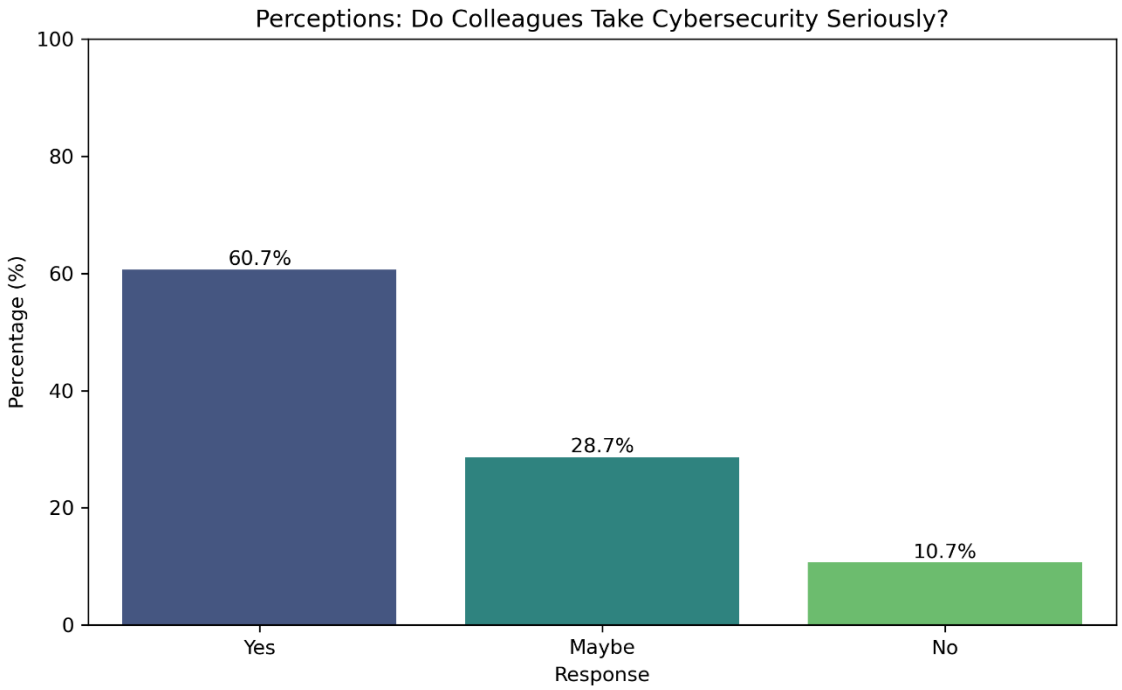



*Figure 4.1.8*
*Individual perception about seriousness of cybersecurity*

Based on the responses, analysis of the data is as follows:

- Most respondents (60.7%) perceive that their colleagues take cybersecurity seriously, highlighting a positive security culture.
- 28.7% individuals reported uncertainty and 10.7% reported negativity, indicating area of improvements in awareness.

### 4.1.9 Have you ever seen your colleague violating cybersecurity policies or engaging in unsafe practices?

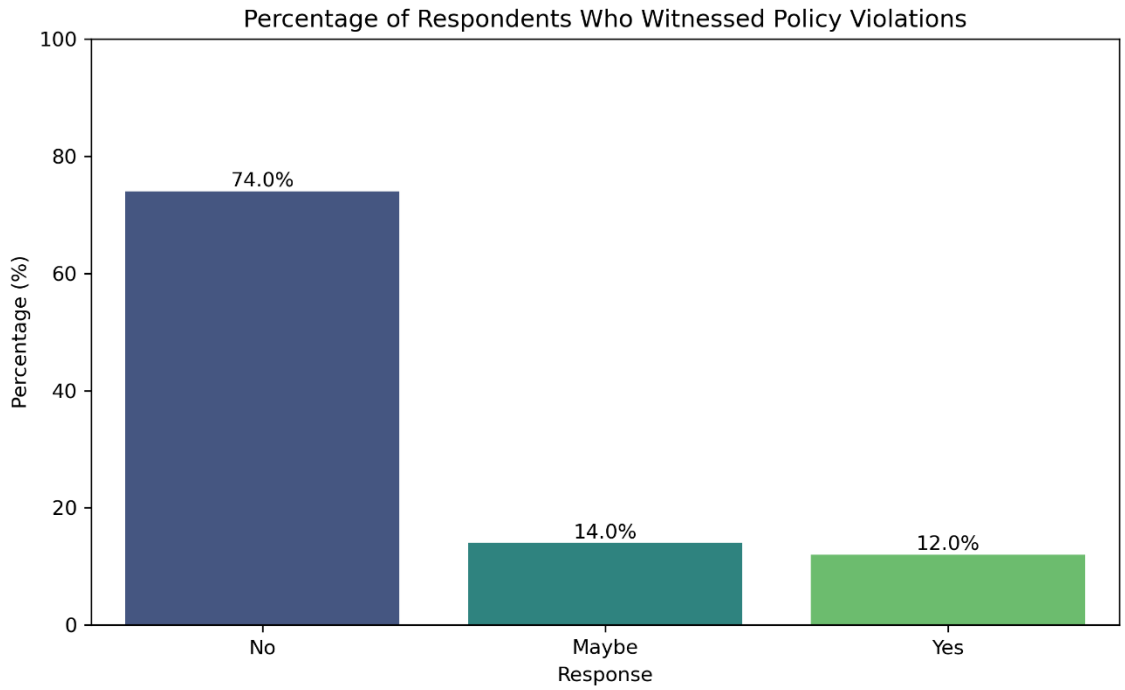



*Figure 4.1.9*
*Witnessed cybersecurity policy violations*

Based on the responses, analysis of the data is as follows:

- 74% individuals responded that they have not witnessed policy violations, indicating good compliance culture or possible under reporting.

- Out of 100%, 26% (14% selected maybe 12% selected yes) have witnessed violations, suggesting areas for increased monitoring and enforcement by the organization.

### 4.1.10 What steps do you individually take to protect sensitive information?

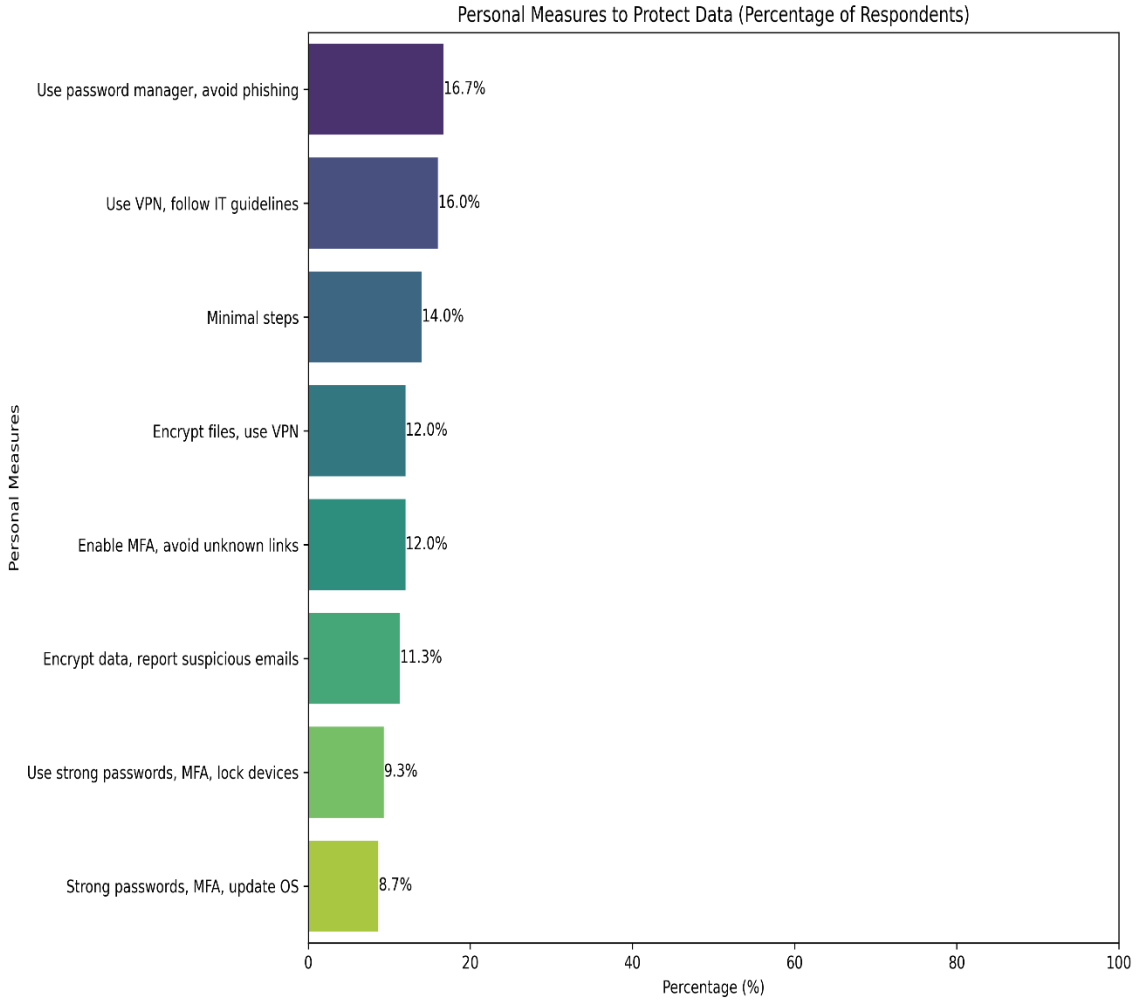



*Figure 4.1.10*
*Personal measures to protect individual data*

Based on the responses, analysis of the data is as follows:

**Personal Measures Taken by Respondents:**

- Use of password manager and avoiding phishing: 16.7%
- Follow IT guidelines by using VPNs: 16.0%
- Bare Minimal own steps: 14.0%
- Use VPN to encrypt files: 12.0%
- Enable Multi Factor Authentication: 12.0%
- Reporting suspicious/ phishing emails: 11.3%
- Use strong passwords (minimum 12 characters), MFA, lock devices when not in desk: 9.3%
- Use strong passwords and regularly update OS security patches: 8.7%

The survey shows individuals are protective to protect their data, such as using VPNs, strong passwords, encryption, and avoiding phishing. The varying responses shows that the participants who responded had different levels of knowledge and experience in cyber security. This information can help an organization with effectively running awareness training and internal policies that encourage people to do things that are less common to protect themselves.

### 4.1.11 Have you ever reported a suspected incident to your organization's security team?

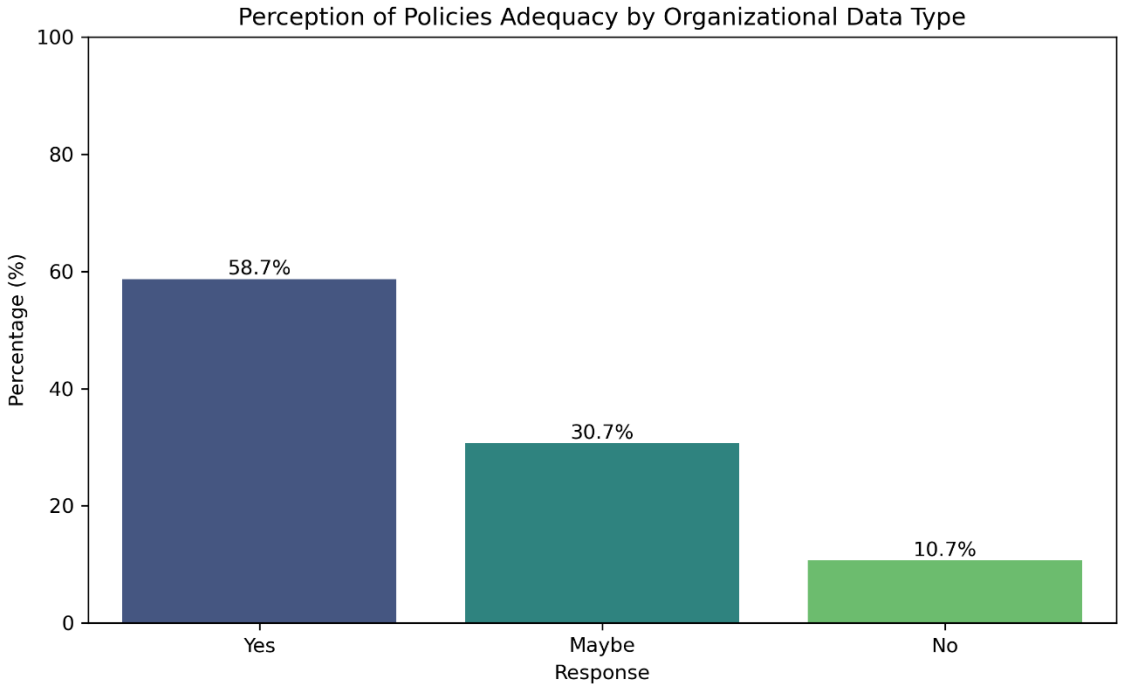



*Figure 4.1.11*
*Perception of policy adequacy*

Most people who answered said that the cybersecurity policies were good enough for the type of data that organizations have, which shows that they trust the current controls. Some participants who answered the survey says they are unsure or feel inadequate, which suggests areas that could be looked at and improved. These insights help businesses figure out where to make policy frameworks that are more in line with how sensitive the data is.

### 4.1.12 How can the company support you in implementing safe cybersecurity practices in your day-to-day work?

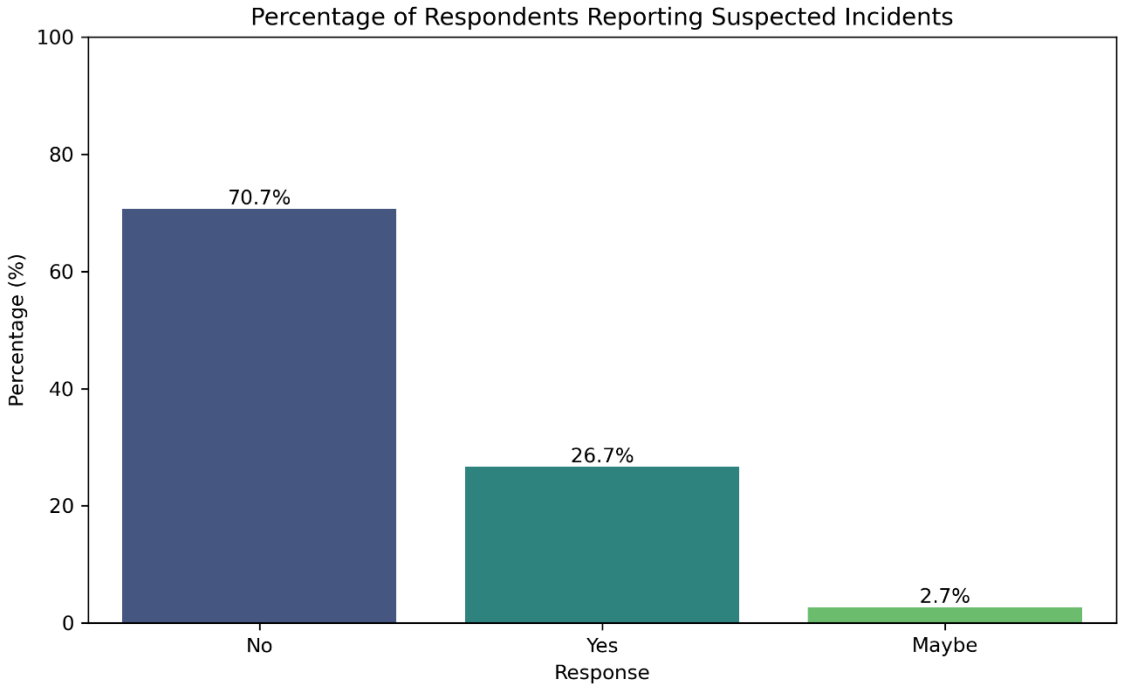



*Figure 4.1.12*
*Reported suspected incidents*

Based on the responses, analysis of the data is as follows:

- 27% of the respondents indicated that they actively reported any incidents happened within their organization.
- 71% of the respondents indicated that they do not report any incident.
- 3% they are not aware of any such activity.

**Q13. What are the major vulnerabilities that were reported externally in your product or identified internally?**

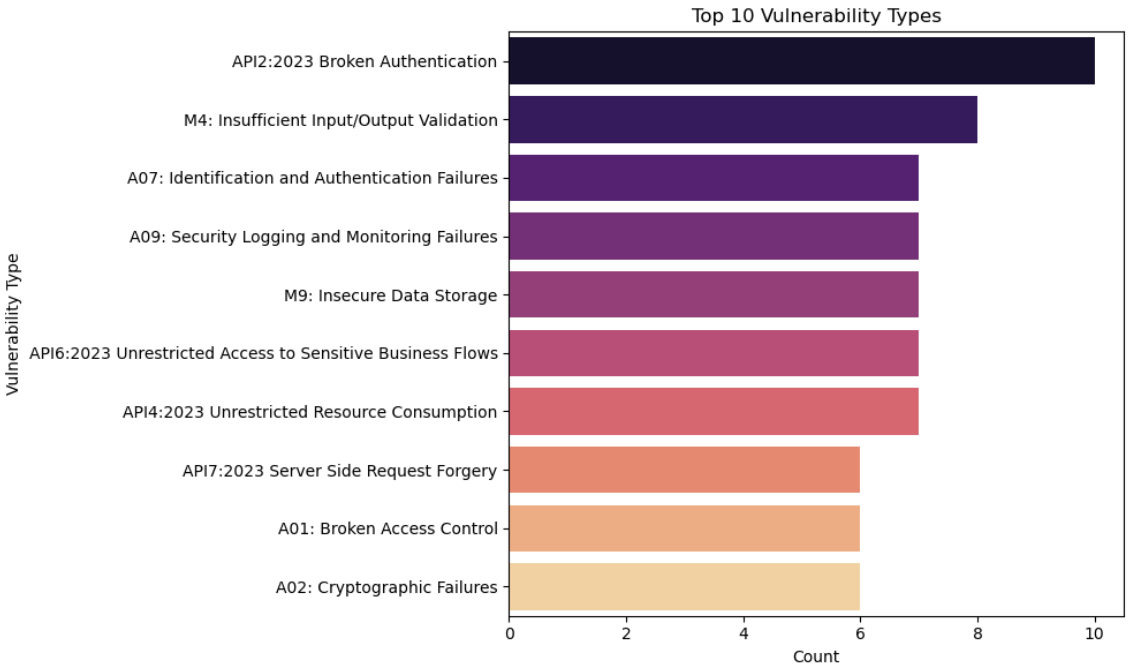



*Figure 4.1.13*
*Overall Top 10 Vulnerabilities awareness*

Based on the responses, analysis of the data is as follows:

- 10% responded that, they know about Broken Authentication vulnerability.
- 8% responded that, they know about Insufficient Input/Output Validation.
- 6% of them know about Server-Side Request Forgery (SSRF), Broken Access Control and Cryptographic Failures.
- 7% responded that, they know Identification and Authentication failure, Security logging and monitoring failures, Insecure Data storage,

Unrestricted Access to sensitive business flows and Unrestricted resource consumption vulnerabilities.

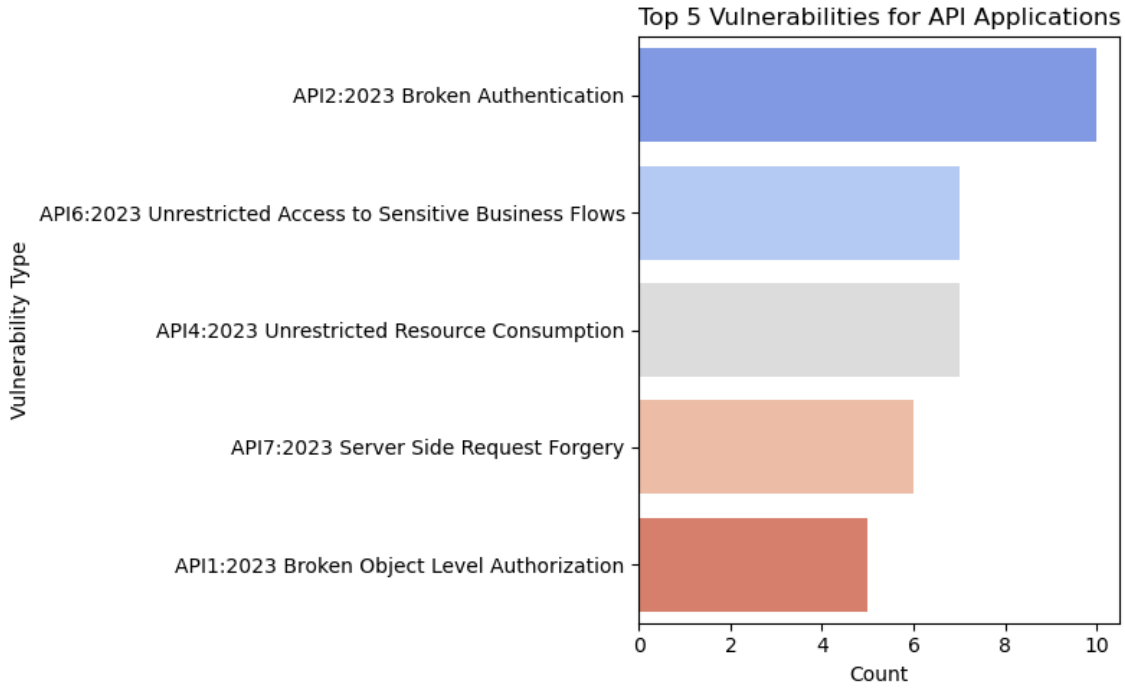



*Figure 4.1.14*
*API vulnerabilities*

According to the responses received Top 5 vulnerabilities for API applications are Broken Authentication, Unrestricted Access to sensitive business flows, Unrestricted resource consumption, Server-Side Request Forgery (SSRF) and Broken Object Level Authorization.

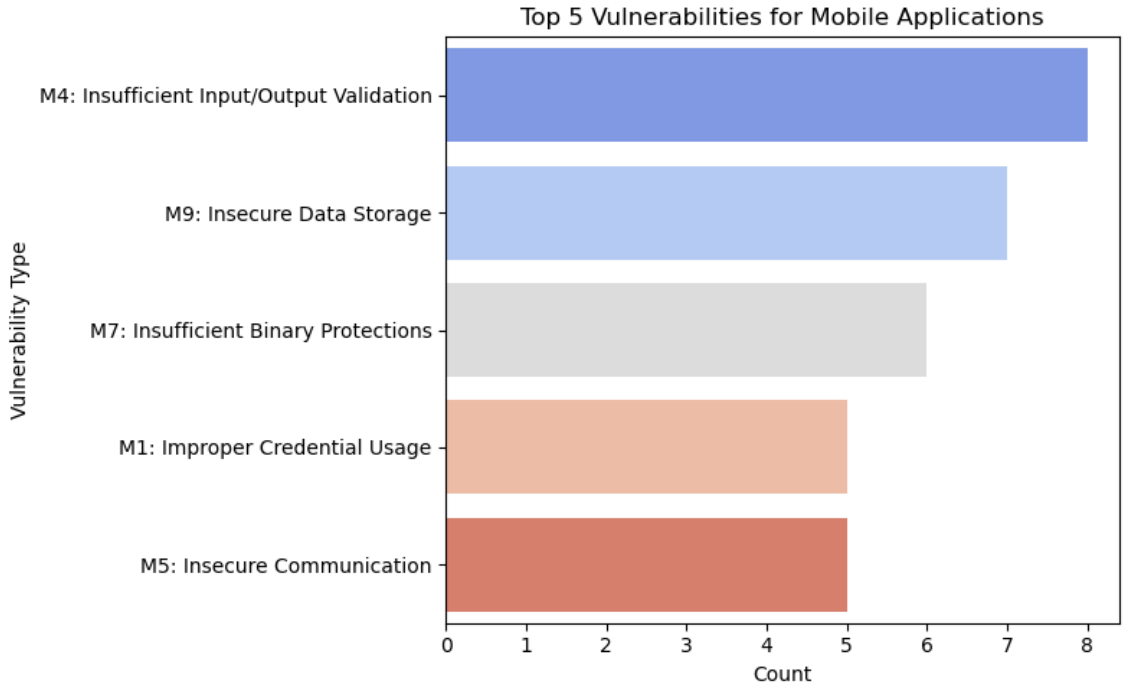



*Figure 4.1.15*
*Mobile Vulnerabilities*

According to the responses received Top 5 vulnerabilities for mobile applications are Insufficient Input/Output Validations, Insecure Data Storage, Insufficient Binary Protections, Improper Credential Usage and Insecure Communication.

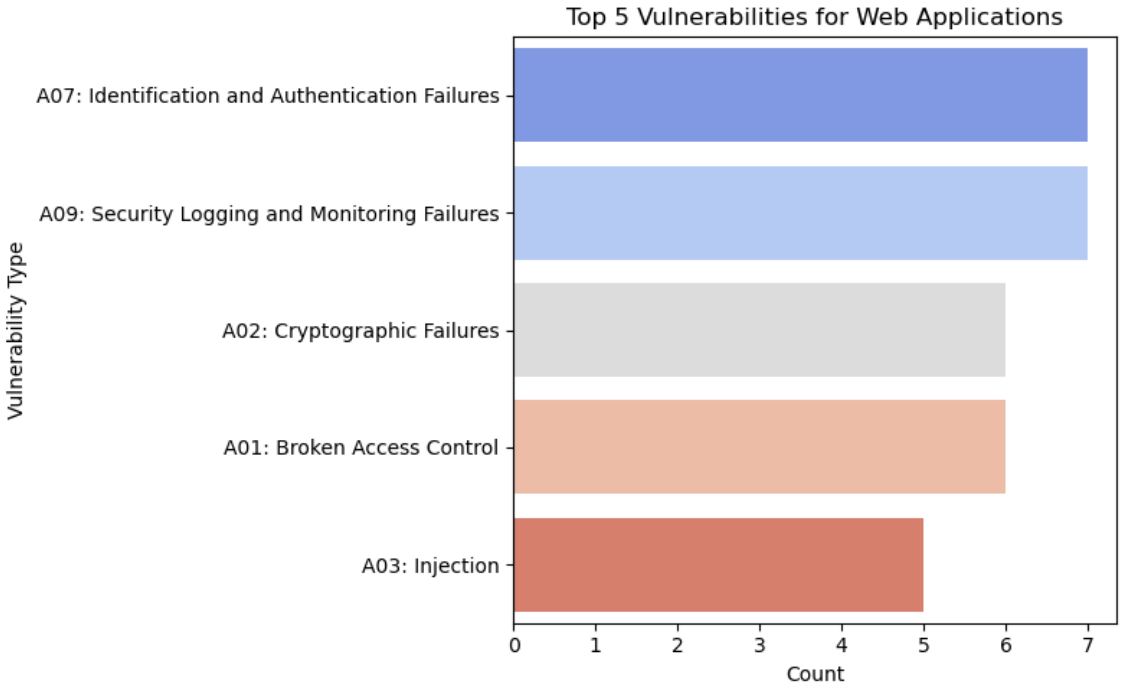



*Figure 4.1.16*
*Web Application Vulnerabilities*

According to the responses received Top 5 vulnerabilities for web applications are Identification and Authentication Failures, Security Logging and Monitoring Failures, Cryptographic Failures, Broken Access Control and Injection flaws.

### 4.2 Research Question One

Are individual's are ready to upskill in cyber security to protect themselves and their organization, and the customers who purchases their products?

### 4.3 Research Question Two

The current research focuses on identifying the factors that impacts, OPCs, startups, micro, small, and medium enterprises (MSMEs) to adopt cybersecurity and its implementation at an early stage before any real incident happens. It aims to address the following research questions in this context, How can an OPCs, startups, micro, small, and medium enterprises (MSMEs) have their own cyber security business unit, or at least train an internal employees to ensure the organization is cyber-ready ?

### 4.4 Summary of Findings

I have accomplished some quantitative research on the responses, that came from people from different sectors. The fact was acquired via a study of the current status of MSME's, the way of their function, and the types of protection and guidelines are being pursued. The research analysis reflects the different features collected from the soles, like key industry, what type of principles and structure are executed, and what type of policies and framework are implemented, and whether the individuals are actually following security best practices or they simply are on paper.

Along with that, I have also confirmed whether there exists any mechanical and managerial oversight that has been executed or not. The information also acknowledges to us the occurrence of security perception training supervised for personnel by the institution. In conclusion, I have collected some data on the issues are being encountered while designing or executing policies. After that I questioned if the firm has encountered any attacks or not, if yes then, what kind of attack happened. I supervised an experimental data

survey on this information for the purpose of gaining some perception into the information and establishing what kind of assumptions can be illustrated from it.

**Descriptive Statistics Analysis**

*Table 4.4.1*
*Frequency of Cybersecurity Training*

| Training Frequency | % |
|---|---|
| Monthly | 26.67 |
| Quarterly | 21.33 |
| Annually | 18.00 |
| Never | 17.33 |
| Biannually | 16.67 |

*Table 4.4.2*
*For self-related cybersecurity skills (1-5)*

| Statistic | Value |
|---|---|
| Count | 150. 000000 |
| Mean | 3.180000 |
| Std | 1.326397 |
| Min | 1. 000000 |
| 25% | 2. 000000 |
| 50% | 3. 000000 |
| 75% | 4. 000000 |
| Max | 5. 000000 |

"Frequency of cybersecurity training" tells you how often an employee gets cybersecurity training to up-skill or re-skill themselves. The percentages of each frequency show how often companies train their employees to be compitent as per industry requirements.

Report for self-rated security skills includes:

- **Count**: Number of Individual respondents participated in the survey.
- **Mean**: Shows the average skill level, showing the confidence level an individual have in cybersecurity capabilities.
- **Standard Deviation (Std)**: It suggest the diversification of competence.
- **Minimum and Maximum**: It shows the overal skill ratings of an individual, with a range of lowest and highest self ability.
- **25th, 50th (Median), and 75th Percentiles**: It shows the concentrations of scores.

Mean skill rating of 3.5 on a 5-point scale reflects moderate confidence among individual respondents. Standard deviation tells about the consistency in skills, while a wide range indicates polarized experience levels in the organization.

**Logistic Regression Analysis: Impact of Training Frequency on Reporting Suspected Incidents**

```
         Current function value: 0.586242
         Iterations 5
                           Logit Regression Results
==============================================================================
Dep. Variable:        Reported_binary   No. Observations:                  146
Model:                          Logit   Df Residuals:                      144
Method:                           MLE   Df Model:                            1
Date:                Thu, 23 Oct 2025   Pseudo R-squ.:                0.001582
Time:                        16:42:50   Log-Likelihood:                -85.591
converged:                       True   LL-Null:                       -85.727
Covariance Type:            nonrobust   LLR p-value:                    0.6026
==============================================================================
                     coef    std err          z      P>|z|      [0.025      0.975]
------------------------------------------------------------------------------
const             -0.8285      0.333     -2.486      0.013      -1.482      -0.175
Training_encoded  -0.0707      0.136     -0.520      0.603      -0.337       0.196
==============================================================================
```

*Figure 4.4.17*
*Logit Regression Analysis*

It is a statistical model that used to draw the relationship between qualitative dependent variable and independent variable (Nick & Campbell, 2007). The analysis was done using Python code which is in Appendix.

Model Overview:

- Count of observations: 146
- Model convergence was achieved successfully.
- The model's Pseudo R-squared was 0.0016, indicating the training frequency alone explains a very small portion of the variability in incident reporting.
- The likelihood ratio test p-value (0.6026) suggests that the model as a whole is not significantly better than a null model without predictors.

The intercept is statistically significant, which means there is a baseline chance of reporting incidents. The coefficient for the encoded training frequency is negative (-ve) but not statistically meaningful (p=0.603), which means there is not significant evidence to say that training frequency affects how many suspected incidents are reported.

### 4.5 Conclusion

These findings underscore the significance of employee hands-on education of cybersecurity, as well as identifying proper security control and policies that could help OPCs, startups, and MSMEs in mitigating the security risks. With limited manpower, skill, and controls, it is challenging for an organization to defend individuals, procedures, merchandise, and mechanisms from cyberattacks. In the following research chapter we will be discussing what has been seen as an alarming security concern for an organization that is a bare minimum requirement to safeguard in detail. It is recommended that website owners and administrators take proactive measures to regularly assess and address vulnerabilities in their systems and applications.

# CHAPTER V:

# DISCUSSION

## 5.1 Discussion of Results

When a one-person company (OPC), startups, or MSMEs is adopting cybersecurity measures, they should plan it properly so that they meet the needs of their business requirements. If cybersecurity measures offer a benefit for the business domain, they will attract more MSMEs to invest in and use their product. A lot of times most effective security standards and frameworks do have a complete set of controls in place that enforces businesses to adopt them, and sometimes most of them do not apply to their line of business. Depending on their line of business, organizations should derive their own set of controls that can protect assets based on company needs for running and executing operations.

During the interview with various stakeholders, it is found that:

- Due to the hard deadline for completion of the project, they do not pay attention to security.
- If at all they are considering secure development of the project/application, then the cost of the development will increase, and customers won't be able to agree on paying the high cost for the development.
- If some customers agree to include security during the development or secure application development, then maintenance becomes another hiccup, as with the evolution in security approaches, they won't be able to accommodate the maintenance cost. Even if customers do not pay the development maintenance cost, they request to do it for free, as they have

given the project to that organization when other organizations were in line to do the work at a lesser cost.

- Resource layoff/exit is another major concern. A reason was provided, like we will invest in resource grooming, be it development training or security training. After getting training, resources are not loyal to the organization; they switch to another organization by showing they do have the skill sets.
- Security tool cost sometimes plays a major concern where they have to pay millions of dollars for different tools and where they end up using open-source tools, whereas proprietary tools identify more issues or are being developed with more features.
- Regulatory penalties play another vital role where the organizations have to follow different countries' different rules.
- Operational challenges occur where sometimes 24/7 monitoring is required for an application, and its 3rd-party component is used to address any vulnerabilities, and sometimes due to non-payment of maintenance costs, they do not update the same.
- We are in 2025, some users are still using default passwords, and when asked the reason, they commented with a smile that they are easy to understand, and with frequent usage, they need simple passwords, which sometimes are exposed in the code as a comment.

### 5.2 Threat Modeling – A developer's approach

Threat modeling is a hypothetical approach to system design that aligns with the secure development life cycle (SDLC) using which developers developed a secure application; it is sometimes called the proactive approach of securing an application from different types of vulnerabilities, which can be adopted at different stages, like during the design phase, incremental developments, or even after development is completed (Xiong & Lagerström, 2019).

Security engineers proactively work with the development team to identify threats and vulnerabilities in an application, system, and networks during the architecture design phase, and it can be accomplished at various stages, like the initial phase, during feature releases, or incremental stages, etc. During threat modeling the questions usually asked is:

1. What are we building? (Understanding product architecture, its components, and data flow between components.)
2. What can go wrong? (This is the phase where we Identify threats and vulnerabilities based on the design.)
3. What are we doing to protect it? (Define various security controls that can prevent attacks.)
4. Did we do a good job? (One done validate mitigations via Penetration testing process and reassess as an when needed.)

Threat modeling helps prioritize risks based on it's likelihood and impact, reduces costly rework by addressing vulnerabilities at early stage in development, ensures compliance with regulations (e.g., GDPR, PCI-DSS, HIPPA etc.,) and enhances team

awareness of security best practices (Nagori, n.d.). There are 13 main threat modeling methods present for identifying vulnerabilities, and they are:

1. PASTA stands for Process for Attack Simulation and Threat Analysis is a risk analysis based approach of identifying vulnerabilities that involves a 7 stages (objectives of the assesment, scope of the assesment, application decomposition, threat identification, vulnerability analysis, attack simulation and risk analysis) (Imperva, 2025) .
2. DREAD full form is Damage Potential, Reproducibility, Exploitability, Affected users and Discoverability is a framework that focuses on threat prioritization on these 5 criteria (Hussain et al., 2014).
3. TRIKE (It is a risk-based approach that mainly focuses on business, operational, and technical aspects and the data flow of assets).
4. VAST (Visual, Agile, and Simple Threat) used techniques for identification and assessment of threats.
5. LINDDUN—It is a privacy-focused threat modeling frameworkthat stands for Linkability, Identification, Non-repudiation, Detection, Disclosure of Information, Unawareness, and Non-compliance (Naila, 2024).
6. CVSS (Common Vulnerability Scoring System) is used to identify vulnerability with attributes like attack vector, complexity, privileges required, user interaction, scope, confidentiality, integrity, and availability; by selecting the values for these attributes, a score is generated based on which vulnerability's severity is defined (Naila, 2024).
7. OCTAVE stands for Operationally for Critical Threats, Asset, and Vulnerability Evaluation, which is a risk management framework that mostly aligned with security and organizational goals (Bridges, 2023).

8. Attack Trees - Formal, methodological way of describing the security of system, based on various attacks. It is representation of attacks against a system in a tree structure.
9. Security cards – It uses a deck of 42 cards to facilitate threat discovery activities: Human Impact (9 cards), Adversary's Motivations (13 cards), Adversary Resources (11 cards), and Adversary's Methods (9 cards) (Shevchenko et al., 2018).
10. hTMM - The Hybrid Threat Modeling Method (hTMM), developed by the Software Engineering Institute in 2018, it consists of a combination of SQUARE (Security Quality Requirements Engineering Method), Security Cards, and PnG activities (Shevchenko et al., 2018). The targeted characteristics of the method include no false positives, no overlooked threats, a consistent result regardless of who is doing the threat mod-eling, and cost-effectiveness (Shevchenko et al., 2018).
11. Quantitative Threat Modeling Method - This method usages quantitative data to identify potential security threats, that involves gathering data on the assets, risks, threats, and vulnerabilities associated with a system or application (Thevarmannil, 2023). This information is then analyzed, and a quantitative risk score is assigned to each potential threat that helps to prioritize potential threats based on their risk level and allocate resources accordingly (Thevarmannil, 2023).
12. Persona Non Grata (PnG) - PnGs represent archetypal users who behave in unwanted, possibly nefarious ways (Mead et al., 2018a). However, like ordinary personas, PnGs have specific goals that they wish to achieve and specific actions that they may take to achieve their goals. Modeling PnGs can therefore help us to think about the ways in which a system might be vulnerable to abuse and use this information to specify appropriate mitigating requirements (Mead et al., 2018b). The PnG approach makes threat modeling more tractable by asking users to focus

on attackers, their motivations, and abilities. Once this step is completed, users are asked to brainstorm ideas about targets and likely attack mechanisms that the attackers would deploy (Mead et al., 2018b). The theory behind this approach is that if engineers can understand what capabilities an attacker may have and what types of mechanisms they may use to compromise a system, the engineers will gain a better un-derstanding of targets or weaknesses within their own systems and the degree to which they can be compromised (Mead et al., 2018b).

13. STRIDE is a threat modeling framework developed by Microsoft, which is our main focus in this paper, and sometimes security engineers call it the developer-centric approach of CIA-AAA for threat modeling.

*Table 5.2.1*
*Stride Framework*

| Type of Threat | CIA-AAA Mapping | Explanation | *Real-World Example* |
|---|---|---|---|
| Spoofing | Authentication | Impersonating to be another user to gain system access | A fake login page of an original page to capture user credentials. |
| Tampering | Integrity | Un-AuthZ alternation of data or a system behavior. | Altering a database entry to change prices of a product in an E-Commerce application. |
| Repudiation | Non-Repudiation | Denying any responsibility of an action due to lack of accountability | A user deleted a critical file and when asked denies that he did not perform the action, because of audit logs are missing. |
| Information Disclosure | Confidentiality | Exposing of sensitive information (data) to unauthorized parties (say guest user) | An unsecured API endpoint exposing sensitive information without authorization. |
| Deniel of Service | Availability | Overloading a system to make it unavailable when required | Botnets attack on a website with N no. of requests making it inaccessible to |

| | | | |
|---|---|---|---|
| Elevation of Privilege | Authorization | Gaining unauthorized high-level user access by exploiting a new or existing vulnerability | legitimate users (down). Exploiting a security misconfiguration vulnerability within an application to access admin or any higher user functionalities |

**Threat Modeling with an example:**

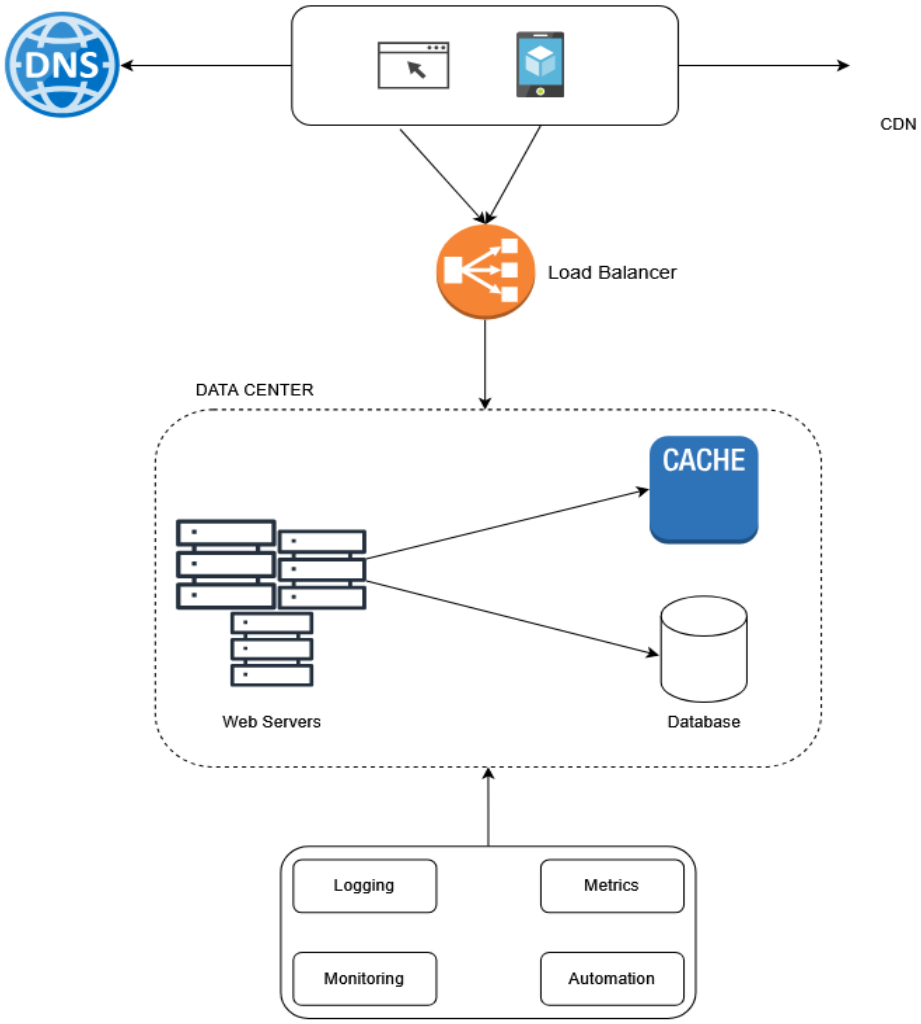



*Figure 5.2.1*
*Application Architecture Diagram*

This is the basic architecture diagram that explains how users connect to an application from a web or mobile application and the backend assets being used to set it up. In this Flow Diagram we need to identify Assets, Controls and Threats or Threat Mapping.

Assets—These are the core components that an organization strives to protect. Componets are both physical and digital assets. The more critical the asset ia, the higher probability of protecting it against potential threats.

Controls – Security mechanisms and policies implemented to protect the assets from various possible threats. These controls can be categorized into three primary types:

Administrative controls: These include policies, procedures, and governance frameworks e.g., access management policies, security training, and risk assesments (Cochran & Reis, 2025).

Technical controls: Used to protect digital assets such as firewalls, encryption, intrusion detection systems, and multi-factor authentication (Cochran & Reis, 2025).

Physical controls: Used to protect physical assets and facilities like locks, surveillance systems, security personnel, and perimeter defenses, fences (Cochran & Reis, 2025).

Threat mapping – It is the process of finding potential threats/ vulnerbailities in the assets and controls in place**,** it also helps in assessing the likelihood of each threat occurance and the potential impact it would have on the organization's operations. By mapping threats to assets, it helps security teams to prioritization if fixing of a vulnerability (Cochran & Reis, 2025)**.**

Trust Boundary—It is a logical perimeter within which components of a system are present that either store data or execute the process across the boundaries of a given network, system, or application (and services) (Cochran & Reis, 2025).

Mapping of Assets: As per their names the mapping happens meaning Assets are mapped as A1, A2, …A(N), Controls are mapped like C1, C2, … C(N) , similarly Threats are mapped as T1, T2….T(N).

*Table 5.2.2*
*Asset Identification from Architecture Diagram*

| Asset ID | Asset | *Description* |
|---|---|---|
| A1 | DNS Server | Resolves domain names to IP address |
| A2 | Load Balancer | Distributes incoming traffics across multiple servers |
| A3 | Web Application | Provides applications core functionalities over Web |
| A4 | Mobile Application | Allows users to access applications via mobile |
| A5 | CDN (Content Delivery Network) | Caches static contents such as (JS, CSS codes) close to users' area. |
| A6 | Web Servers | Hosts web application, API services and processes user requests |
| A7 | Cache Server | Speed up responses |
| A8 | Database | Used to store user data such as login credentials, user PII information etc |
| A9 | Datacenter | Physical infrastructure providers for housing servers, cache, CDNS |
| A10 | Logging and Monitoring Tools | Uses to track metrics, storing user logs. |

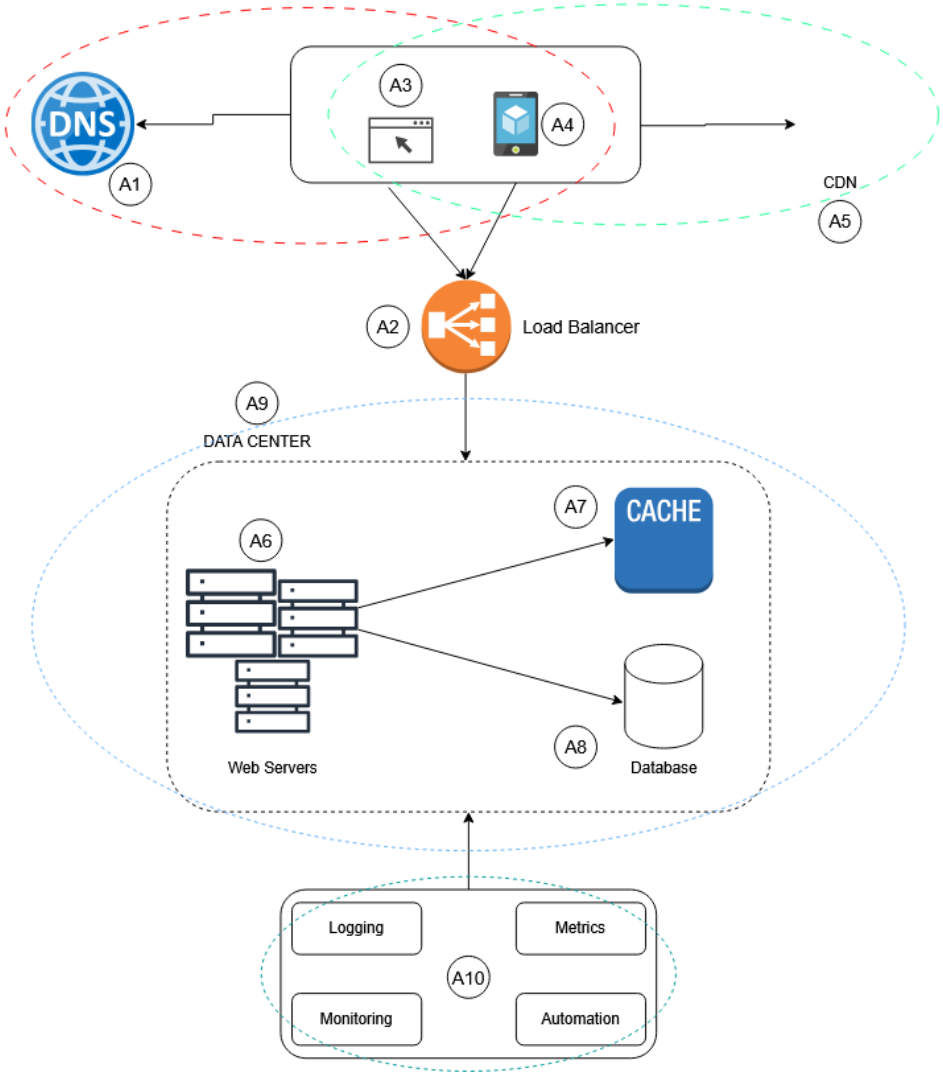



*Figure 5.2.2*
*Application Architecture Diagram with Assets and trust Boundaries*

*Table 5.2.3*
*Controls Identification from Architecture Diagram*

| Asset ID | Asset | *Description* |
|---|---|---|
| C1 | DNSSEC | Cryptographic authentication to DNS responses which ensures integrity and authenticity of DNS data to prevent spoofing, MITM attacks. |
| C2 | DNS Filtering | Blocks access to malicious or unauthorized domains |
| C3 | DNS Rate limiting | Limits no of requests made to DNS servers by an IP address, which further usages to prevent DDOS attacks |
| C4 | SSL/TLS Encryption | This ensures that sensitive information's are transmitted is secure (encrypted during transit) preventing eavesdropping, data tampering and MITM attacks. |
| C5 | Authentication | Validating authenticity of the servers interactive with CDN, which prevents DNS hijacking and spoofing. |
| C6 | Access control policies | Defines and enforces access control policies, who can access cached content on edge servers. Policies can be user roles, country-based access etc. |
| C7 | Content Security Policies | Implementing CSP header can mitigate web application vulnerabilities like XSS, data injection attack etc. |
| C8 | Access Control | This ensures secure access to critical components like web servers, cache, database etc. |
| C9 | Network Segmentations | Segmentation of network into smaller, isolated environment preventing lateral movements |
| C10 | Encryption | Encrypting sensitive data during in transit and at rest. Example AES encryption. |
| C11 | Patching and Updates | Ensures that security vulnerabilities were patched on regular interval both on 3rd party libraries and on Operating systems |
| C12 | Data backup and recovery | Backup ensure if any disaster happens then we can store data from a backup server for availability. |
| C13 | Monitoring and Logging | Ensures real time detection and anomalies through log analysis and monitoring, which improves security incidents and incident response time |

| Asset | Spoofing (T1) | Tampering (T2) | Repudiation (T3) | Information Disclosure (T4) | Denial of Service (T5) | Elevation of Privilege (T6) |
|---|---|---|---|---|---|---|
| **DNS (A1)** | DNS cache poisoning (T1) - **C1, C2** | Malicious redirection (T2) - **C1, C2** | Lack of DNS logging (T3) - **C3** | Exposure of DNS queries (T4) - **C3** | DNS amplification attacks (T5) - **C3** | Not applicable |
| **Load Balancer (A2)** | IP spoofing (T1) - **C4** | Forged traffic routing (T2) - **C4** | Insufficient logging (T3) - **C11** | Intercepting traffic (T4) - **C4, C5** | Flooding attack (T5) - **C4** | Misconfigured access control (T6) - **C8** |
| **Web App (A3)** | Session hijacking (T1) - **C6** | Parameter tampering (T2) - **C6, C7** | Poor audit trails (T3) - **C11** | XSS, CSRF attacks (T4) - **C7** | Application layer DDoS (T5) - **C11** | Exploiting insecure APIs (T6) - **C8** |
| **Mobile App (A4)** | API key theft (T1) - **C6** | Altering mobile traffic (T2) - **C6** | Denied app usage logging (T3) - **C11** | Leaking app data (T4) - **C6** | Overloading requests (T5) - **C4, C5** | Exploiting outdated app versions (T6) - **C11** |
| **CDN (A5)** | Fake CDN nodes (T1) - **C5** | Modified cached content (T2) - **C5** | Insufficient logging (T3) - **C7** | Exposure of cached data (T4) - **C5** | CDN exhaustion attack (T5) - **C5** | Not applicable |
| **Web Servers (A6)** | Credential theft (T1) - **C8** | File upload tampering (T2) - **C8** | Weak access logging (T3) - **C11** | Server misconfigurations (T4) - **C9** | Volumetric DDoS (T5) - **C4** | Privilege escalation via vulnerabilities (T6) - **C8** |
| **Cache (A7)** | Fake cache poisoning (T1) - **C10** | Cache invalidation (T2) - **C10** | Cache operations logging (T3) - **C11** | Sensitive data leakage (T4) - **C10** | Cache overflow attacks (T5) - **C10** | Misconfigured permissions (T6) - **C8** |
| **Database (A8)** | Unauthorized connections (T1) - **C8** | Data injection (T2) - **C9** | Poor access tracking (T3) - **C11** | SQL injection attacks (T4) - **C9** | Overloading connections (T5) - **C4** | Exploiting weak database roles (T6) - **C8** |
| **Data Center (A9)** | Rogue devices (T1) - **C8** | Physical tampering (T2) - **C8** | Lack of physical audit logs (T3) - **C11** | Data exposure via backups (T4) - **C10** | Physical sabotage (T5) - **C8** | Unauthorized admin access (T6) - **C8** |
| **Monitoring (A10)** | Fake logs (T1) - **C11** | Log tampering (T2) - **C11** | Disabling audit mechanisms (T3) - **C11** | Sensitive log leaks (T4) - **C11** | Overloading telemetry systems (T5) - **C11** | Exploiting monitoring tool vulnerabilities (T6) - **C11** |

*Figure 5.2.3*
*Threat Mapping for the Diagram with Controls*

Explanation of Controls:

- C1, C2: DNSSEC, DNS Filtering & Blacklisting – Protects DNS traffic by stopping DNS spoofing, cache poisoning attacks etc.
- C3: DNS Rate Limiting – Helps protect against DDOS attacks targeting DNS services running in the servers.
- C4: SSL/TLS Encryption – Data integrity of sensitive data.
- C5: Origin Authentication – Checks the source of the traffic reaches CDN or web application by verifying it source of origin.

- C6: Access Control Policies – Limits and enforce role-based access to resources from unauthorized access.
- C7: Content Security Policies (CSP) – Protections against content injection, such as XSS and CSRF, data injections (images, CSS, JavaScript).
- C8: Access Control (Physical & Logical) – This limit who can access to data centres, servers, databases, and enforces principle of least privilege access to sensitive assets.
- C9: Network Segmentation – Stop lateral movement by isolating network components and reducing the attack surface.
- C10: Data Encryption – Make sure data is encrypted during transit and at rest to prevent unauthorized access or leaks (Andersen, 2024).
- C11: Regular Patching, Monitoring, & Logging – Make sure systems are up to date with security patches, and activities are logged and monitored for signs of abnormal behaviour (Mehta, 2023a).
- C12: Data Backup & Recovery – Daily, weekly and monthly backs up critical data to an offshore location ensures its availability and integrity in case of data loss or system failure during natural disasters (DSCI, 2025b).

### 5.3 Major Vulnerabilities, it's Impact and Remediations

Based on the responses, major organizations should also focus and train employees on software vulnerabilities, their impact, likelihood and mitigation techniques and tools (open-source) used to identify these vulnerabilities by aiming to suggest the use of free to use software's.

**SQL Injection**

Type of vulnerability within an application not in the Database that occurs when untrusted user provided input is not properly validated and sanitized by the web application when it tries to process (insert, update, fetch) the SQL queries. This helps hackers to manipulate SQL query potentially leading to unauthorized access to the database.

*Table 5.3.1*
*SQL Injection Types*

| SQLi Types | Description |
|---|---|
| In-band SQLi (Classic SQLi) - Error-based & Union-based SQLi | According to (Acunetix, n.d.), these are the most common and easy to exploit vulnerability and it occurs when an attacker provided malicious SQL query into input fields (such as login forms or search fields). It is of two types.<br>1. Error Based—In this SQLi based on the error message thrown by the database server, attackers obtain information about the structure of the database (e.g., you have an error in your MySQL query). Error reporting is good when developing the application but not advised in |

the case of a production server and should be disabled (Acunetix, n.d.).

2. Union-based SQLi, in this, attackers leverage the UNION SQL operator to joins multiple SELECT statements into a single statement, which is then returned as part of the HTTP response, based on this, they are able to identify which column is vulnerable to SQLi and then they do the lateral action on that particular column (Acunetix, n.d.).

Inferential / Blind SQLi - Boolean-based (content-based) Blind SQLi & Time-based Blind SQLi

According to (Acunetix, n.d.), Boolean-based (Content-based) Blind SQLi - Attackers keeps sending a SQL payloads to the backend database server which forces the application to return results in the form of TRUE or FALSE result.

Time-Based Blind SQLi - Attackers keeps sending SQL payloads to the database with some time delay that forces database to wait that much of time (in seconds) before it returns an actual response (Acunetix, n.d.).

Based on the returned result, the content of HTTP response gets changed or remain the same, by reviewing the responses, attacker crafted the payload that returns true or false or even though no data from the database (Acunetix, n.d.).

| | |
|---|---|
| Out-of-Band SQLi | When an attacker is unable to use the same channel to launch the attack and based on the results an attacker use an inferential time-based techniques, and in this case server responses are not very stable (making an inferential time-based attack unreliable) (Acunetix, n.d.). It relies on the database server's ability to make DNS or HTTP requests to deliver data to an attacker, example of Microsoft SQL Server's xp_dirtree command, which can be used to make DNS requests to a server an attacker controls (Acunetix, n.d.). |
| Second-Order SQL Injection | When a user provided malicious SQL payload is stored or saved in the database and later used or retrieved in an SQL query without proper validation (e.g., in an input field, a user supplies a malicious SQLi query that is stored in the database and executed when that particular function or page is called), resulting in an 2nd Order SQL injection (Acunetix, n.d.). |

---

Impact – Disclosure of sensitive information that may contain users PII information, Organizations financial information or any confidential business Data. Data alternation by the attacker or deletion of the data. Server and application compromission.

Tools Used – SQLMap, SQLNinja

Mitigation Techniques - Use of prepared statements or parameterized queries (use prepared statements or parameterized queries with placeholder values to separate SQL code

from user input; this treats user-supplied input as data but not the SQL query), Input validation and sanitization (filter or escape special characters that could be used in SQLi)(Senapati, 2024).

Principle of lease privilege (make sure the database user has the required permission set in the database and not set with ALL permissions), web application firewalls, and regular security testing (A. Verma et al., n.d.).

**Insecure Deserialization**

Before we proceed, we need to understand what serialization is. In serialization, we convert user-supplied input data into an object format that is stored in a file or memory or transmitted over the network and used when required (Malik, 2025). On the other hand, this serialized data is recreated with attackers supplied malicious data and is used to brute force or abuse the behavior of an application's deserialization process, allowing an attacker to execute it at the backend. That further manipulates objects or performs an injection attack is called Insecure Deserialization (Malik, 2025).

The impact of insecure deserialization could be dangerous, as it provides an entry point for an attacker to execute remote code executions, gaining persistent access, or sometimes it may lead to privilege escalation or arbitrary file access or a DDOS attack.

Tool used: Ysoserial, Java Deserialization Scanner (Bursuite), ZAP Proxy, SerialKiller

Mitigation Techniques: Integrity Checks of supplied data (such as digital signature usage), Strict Type constraints, Isolate Code (running code in isolated or sandbox environment), Log Deserialization Exception, Use alternate data formats like JSON for serialization if required, User input validation, Limiting access to the code.

**Insecure Direct Object References**

The insecure direct object reference (IDOR) is a type of design flaw in which a web application tries to provide direct access to the data without proper validation of the user-supplied input. On successful exploitation of this vulnerability, an attacker may gain sensitive PII information or even get privileged users' information; sometimes it is also considered an authorization bypass vulnerability (KumarShrestha et al., 2015).

Say an example “https://vuln-website.com/student_account?studentID=132” It is executed in the backend and returns the student with the information within the application. As an attacker, if we modify **studentID** from **132** to **133**, if no control is in place, it will return student data for the user **133**. This is a classic example of an IDOR vulnerability leading to horizontal privilege escalation.

Impact: Sensitive data exposure leading to penalties for violating compliance breaches like GDPR and HIPAA. Account takeover, privilege escalation, and legal issues.

Mitigation: Never rely solely on obfuscation for access control, validate whether the querying user is authorized to view the data or not based on which user should be able to view the data (Gordon, 2015).

Instead of a static number, use UUIDs, which make it hard for an attacker to guess the next number. Implementing role-based or attribute-based access control mechanism, and use session tokens to validate/re-validate all requests using the user's authenticated identity (Gordon, 2015).

**XML Injection**

An application or web service that deals with Extensible Markup Language (XML) data where the user-provided data is stored in XML format at the backend, where an attacker injects malicious XML tags as an input parameter that gets executed by the application, causing an application or server crash. It can further be used to carry out nested attacks like SQL injection or cross-site scripting (XSS) (Jan et al., 2017). By exploiting this kind of vulnerability, attackers try to gain unauthorized access to the backend database, resulting in the exposure of confidential data in the form of XML output (Jan et al., 2017). Tool Used: Burp Suite, ZAP proxy, SoapUI

Remediation: Input validation for user-supplied data, use of a secure XML parser and disabling features like external entity resolution, use of parameterized queries, application of least privilege to XML processing, logging, and error handling.

**XML external entity injection (XXE)**

XML external entity injection (also known as XXE) when an application tries to execute without improper input validation of user supplied XML data containing a reference to an external entity by the XML parser, leading to an unauthorized access (Mehta, 2023b). The XML parser further allows the external entity to gain access to internal resources to conduct network attacks and DDOS attack.

Impact: It can lead to sensitive data exposure, DOS attack, Server-Side-Request Forgery (SSRF), remote code execution (RCE) once gained access, reputation and financial losses.

Tool Used: Burp Suite, ZAP proxy, SoapUI

Remediation: Input validation for user-supplied data, use of a secure XML parser and disabling features like external entity resolution, use of parameterized queries, application of least privilege to XML processing, logging, and error handling.

**Cross Site Scripting Attacks**

XSS stands for cross-site scripting, in which an attacker tries to inject malicious JavaScript into the application, which the browser tries to execute on the client-side instead of in a web application, types of XSS are reflected (non-persistent), stored (persistent), DOM-based, blind stored, and self-XSS (A. Verma et al., n.d.).

In case of reflected XSS, the attacker's malicious code is executed by the browser without interaction with the backend application, and these are mainly crafted in the URL, and when the victim opens it or clicks, the alert pops up, whereas, in stored XSS attack, the script is stored in the backend database, and when a user tries to call that specific page (say, the profile page), the code is then executed, and we call it stored XSS (A. Verma et al., n.d.). DOM-based XSS is a client-side vulnerability where the attacker takes advantage of the DOM (Document Object Model, like document.URL, location.href, location.search, etc.). Blind XSS happens when an application processes the user-supplied data and stores it in the database that is executed at a different application (A. Verma et al., n.d.).

Impact: Information theft, session hijacking, malware delivery and redirection, web application/ website defacement.

Remediation: Input validation, CSP header implementation, HTTPOnly attribute in header, Sanitize user data in API

Tool Used: Burp Suite, ZAP

**LLM Attacks and Prompt Injection**

Organizations are rushing to have their own LLM model in order to have a better user experience. This exposes to web LLM attacks that take advantage of backend services such as APIs to retrieve data that the LLM model has access to (this could be any sensitive information). The attacker could use the LLM model to perform an SQL injection attack based on the API endpoint access. LLM attacks mainly rely on a technique called prompt injection. This is the attack where the attacker uses crafted prompts to manipulate an LLM's output. As a result, AI can call backend APIs to return sensitive information to the attacker (Portswigger, n.d.).

**Server-Side Template Injection**

Templates such as Smarty tags, etc., are being widely used by an application to show dynamic content within a web page or in an email body, and if the application does not validate user-supplied unvalidated syntax that looks similar to the original template and renders these data in the UI, it causes a server-side template injection attack (Mamtora et al., 2021a). Though these vulnerabilities do not have that much significance, if an application uses these (for example, WHMCS uses smarty tags), it may impact remote code execution by giving full access to the hosted server (Mamtora et al., 2021b). Applications like Smarty, twig, jinja2 are vulnerable to SSTI injection attacks.

Remediation: Input validation, Does not trust on user supplied inputs and do not allow users to add template-based input such as {8*8}.

Tool Used: Burp Suite, ZAP

**Other types of Vulnerabilities that Developers and Organization should focus on but not limited to:**

*Table 5.3.2.*
*Different Vulnerabilities organization should focus on*

| Name of the Vulnerability | Description |
|---|---|
| OAuth 2.0 | The OAuth 2.0 protocol is among the most commonly used authorization/single sign-on (SSO) protocols by organizations, which serves as the foundation for the new SSO standard OpenID Connect (Fett et al., 2016). |
| Password reset poisoning | When an application uses the Host header of an HTTP request to reset or create the password reset links, which allows an attacker to change user's password and take control of the account (Kosh, 2025). |
| Directory Listing | This is a web server vulnerability that shows list of directory or images, CSS etc. within a folder which helps in gathering basic information on application or website. |
| JSON Injection | In JSON injection hackers injects malicious data into the JSON streams to modify application behavior. This of 2 types Server-Side (data from untrusted source is written by the server into the JSON stream) and Client-Side (happens because of JavaScript eval function) (*JSON Injection*, n.d.). |
| NoSQL Injection | NoSQL (Not Only SQL) vulnerability happens when an attacker injects malicious code into database and these queries executed by the NoSQL databases like MongoDB, |

| | |
|---|---|
| | CouchDB, Amazon DynamoDB, Neo4j, Azure CosmosDB (*NoSQL Injection*, n.d.). |
| CRLF Injection | CRLF stands for Carriage return (CR) and Linefeed (LF) is a type of attack where an attacker inserted malicious input with \r and \n characters into application header that further executed by the application giving access to the system. |
| LFI & RFI | Local file inclusion and Remote file inclusion are the vulnerability where application allow to include local or remote files in the URL as parameters (example: index.php?file=index.php (LFI) or index.php?file=https://x/a.php) (Orlando, 2021). |
| OS Command Injection | An attacker tries to trick the application to execute the OS command, giving system information like OS version, installed applications etc. |
| Unvalidated redirects and forwards | Used in phishing attempts where attacker tries to redirect the user from one application to other application. Sometime we call it as Open redirect vulnerability. |
| Clickjacking | In this type of attack, an attacker embedded original application within an iframe showing its legitimation and when user supplies the inputs it first executed within attacker's website and then redirected to actual website, by which user collect victims' credentials etc. |
| CSV Injection | This happens when user supplied malicious input which with excel sheet and application ties to execute it, |

| | |
|---|---|
| | giving access to external source via RCE or opening calculator |
| Default Password | This is a type of attack where application allows default credentials such as admin as username and password giving admin portal access (this is a human error that developers kept using default password always) and they do not remove it from product server. |

## 5.4 Recent Security Incidents – A case study

**MGM Cyber Attack:**

In the year 2023, MGM Resorts posted in their X post that they have been attacked by a security group named Scattered Spider and ALPHV. As a result of this attack, MGM Resorts estimated they made a loss of $100 million (Schrader, n.d.).

Initially attackers gained access via IT helpdesk based on the employees' information available on social media like LinkedIn. Using information provided by the helpdesk, attackers gained administrative access into their OKTA (OAuth provider) and Azure tenant environments, and then ransomware was deployed to encrypt virtual servers (Schrader, n.d.). The data of 37 million individual persons was compromised. Restoration from such an incident took 10 days for the organization to be fully operational (Schrader, n.d.).

**Ticketmaster Data Breach**

In the year June 2024, an American ticket sales and distribution company named Ticketmaster has been attacked by a hackers group named ShinyHunters, who take this responsibility on the 28th of May, 2024 (TraceSecurity, 2025). With this incident, the hacking group was able to gain access to 560 million users' data and further threatened that if the ransom was not paid, they would sell these data on the dark web at a cost of $50000 for 1.3TB of data that includes customers' addresses, mobile numbers, and credit card details (TraceSecurity, 2025). Whereas Ticketmaster claims the group was able to gain access that is limited to the U.S., Canada, and Mexico, and they may include email, mobile number, and encrypted credit card information, the company has informed that they have informed the attacked users to take appropriate action (Ticketmaster, 2025).

**Deloitte's AI Fallout - The $440,000 Report That Backfired**

According to the report by (NDTV World, 2025), Deloitte AI report controversy involves consultancy failure in Australia as a result the Big4 has agreed to refund part $440000 to Australia Government. Deloitte used Azure OpenAI GPT-4o with various errors in the report. The report, commissioned by the Department of Employment and Workplace Relations (DEWR) to assess the "Future Made in Australia" compliance framework and associated IT system, was published in July 2025. Subsequent scrutiny revealed fabricated academic citations, false references and a quote wrongly attributed to a Federal Court judgment(NDTV World, 2025).

Sydney-based welfare law academic Christopher Rudge, who first flagged the issues, called them AI "hallucinations" - where generative models fill gaps, misinterpret, or invent plausible but incorrect details. Similarly In September 2023, Deloitte's Colombian affiliate, Deloitte & Touche SAS, was penalized $900,000 by Public Company

Accounting Oversight Board (PCAOB) for audit quality control failures. In Canada, Deloitte admitted to violating ethical and audit conduct rules in Ontario, paying over CAD 1.5 million in 2024 for the "deliberate backdating" of audit workpapers (NDTV World, 2025).

**DISA Global Reach – Data Breach**

In the year April 22, 2024, a 3rd-party employment screening services provider named DISA Global Solutions, Inc., had a data breach where 3.3 million users' data related to drug and alcohol and background checks was exposed, and the company in their press release (on their website) said that they became a victim of a cyberattack where attackers were able to gain access to individuals' PII information between Feb 9, 2024, and April 22, 2024 (Christ, 2025).

The company further added that they did an investigation of the incident and found that the data that got leaked contains individuals' names, SSNs (social security numbers), driver's license and government ID numbers, banking information, and other sensitive data (Christ, 2025).

**Finastra Secure File Transfer**

In November 2024, a UK-based company named Finastra, which provides banking services for 8100+ financial institutions and 800000 insurance customers worldwide, has experienced a cyberattack (Jain, n.d.). The attacker was able to gain access to their internally hosted File Transfer application using already stolen and available credentials (username and password) that were used to exchange sensitive information between clients using this SFTP application (Jain, n.d.).

The hacker group "abyss0" claimed this attack and posted 400 GB of data in a hacking forum. This is not the first time Finastra has been hacked; the incident happened in 2020, when the company made their system shut down for a long time to investigate this incident (Hill, 2025).

**Checkout.com Data Breach:**

In November 2025, Checkout.com, a payment processor company, was impacted by a security incident where the hacking group “ShinyHunters” claimed they had obtained Checkout.com's internal server access, and they demanded ransom (Albera, 2025). The company has investigated the case and found that the hacking group was able to gain access to a legacy 3rd-party file storage server that they decommissioned in the year 2020 (Albera, 2025). In an estimation, the company mentioned in their website (blog post) that this would affect less than 25% of the merchant base, whereas the affected server was used for internal purposes, where they used it for onboarding merchants, and the incident did not affect their payment processing platform and Checkout.com admitted this was their mistake, and they took full responsibility for this incident (Albera, 2025).

**Security Incidents in Farming Industry:**

The Government of India and the Government of Odisha are providing financial assistance/subsidies to farmers by different public schemes, by which many of these farmers have recently become victims of cyber security attacks. Attackers are embedding or forging malicious APK files within links sent via SMS or WhatsApp messages to the farmers, or sometimes they call the victims directly and tell them about the scheme and then send malicious links. These messages often appear to come from the government, and farmers click the links knowingly by trusting the source as the pretend to be government

agencies, allowing malicious software to be installed in the background on their mobile devices. This malware operates in the background, sending one-time passwords (OTPs) to the attackers, which they then use to empty the farmers' bank accounts.

**Digital Arrest & Bank account fraud cases**

In the digital arrest scam, individuals are getting international calls and calls from local numbers via WhatsApp calls, where fraudsters pretend to say that they are from law enforcement agencies like the police or customs department and your near & dear ones sent you a parcel in which we found some suspicious things, and they demand money, or else they won't release the parcel or the person who they have arrested.

By doing this, they play with the emotional factor of an individual, and persons fall into this trap, and they pay the money. Sometimes hackers call with the name of customer care from the bank to do the Aadhar KYC of their bank account, and by virtue of this, hackers get the photocopy of the Aadhar, PAN, etc., using which they do the transaction on their own by emptying the victim's bank balance.

With the rise of this kind of incident, the government and bankers have started educating the people of India not to fall for this kind of activity, and if they feel they have become victims of such frauds, they can call the government-provided number 1930 to report such suspicious activity, by virtue of which the Cyber Crime cell holds such balance with the chain of accounts where the transactions have happened. By this, even legitimate customers' accounts get put on hold, and they are not able to operate their accounts.

## 5.5 India's Cybersecurity Laws and Regulations

Among the primary problems with India's guideline in the cybersecurity eco-space is that the government still litigates under ambiguous or antiquated states, which can obstruct development and the execution of satisfactory cybersecurity legislation. Firms have struggled to obtain genuine guidelines and assistance from obscure laws and a shattered legislative route in data solitude and cybersecurity (Chin, 2025).

To carry on broadly accepted cybersecurity principles, India must approve more extensive and enlightening cybersecurity regulations and simplified rules and amendments to grow a finer cybersecurity structure and data shield legislation (Chin, 2025).

If these regulations are not implemented, the Indian government, its regulatory bodies, and assigned authorities remain obliged to ancient laws, which feasibly result in unsuitable addressed and unsettled cybersecurity matters (Chin, 2025).

### The Information Technology Act, 2000

The IT Act of 2000 was validated by the Parliament of India and managed by the Indian Computer Emergency Response Team (CERT-In) to instruct Indian cybersecurity regulations, install data protection policies, and manage cybercrime (Chin, 2025). Similarly, it defends e-governance, e-banking, e-commerce, and the commercial sector, among others (Chin, 2025).

Whilst India lacks unique, integrated cybersecurity regulations. It employs the IT Act and numerous sector-specific rules to encourage cybersecurity excellence; it also furnishes a lawful structure for essential information networks in India (Chin, 2025).

For example, Sections 43A & 72A of the IT Act say Indian organizations are required to have "reasonable security practices and procedures" to protect sensitive

information against compromise, damage, exposure, or misuse. Similalry any intermediaries or individuals who disclose personal data without written consent of the actual owner, then they (organizations) will be behind bars up to three years and finedup to Rs 500,000, or both (Chin, 2025).

**Information Technology (Amendment) Act 2008**

The IT Act of 2008 applies to individuals, firm, or institution (mediator) that utilizes computer assets, the computer web, or additional facts. Automation in India also incorporates service operators of web hosting, cyberspace, and networks. Telecommunication and global institutions that have an authoritative presence in India and trade exterior to the nation, which has been functioning in India (Chin, 2025).

It is significant to observe the biggest issue in the IT Act 2008 (Subsection 69), where the Indian government reserves to right to intercept, monitor, decrypt, block, and remove data and content at its own preferences, which may raise signifiant privacy concerns (Chin, 2025).

By violating this IT Act, individual, firms may face penalties ranging from $1,250 to three year imprisonment, while penalties for more substantial offenses and cybercrimes may result in imprisonment of up to 10 years (Chin, 2025).

**Information Technology Rules, 2011**

Under the IT Act, a crucial component of the cybersecurity law is the Information Technology (Appropriate Security Measures and Techniques and Personally Identifiable Data or Information) Rules 2011 (Confidential Rules) (Chin, 2025).

The most crucial alterations incorporate amenities for the rule of intercessors, improvised retributions, and defying fees for cybercrime, fraud, defamation, and unauthorized publication of personal pictures, as well as suppression of specific articulation (Chin, 2025).

Each Information Technology Act (ITA) and the IT Rules are significant for supervise how the Indian system and institutions handle confidential info, data security, data preservation, and the assembly of confidential data and other private information (Chin, 2025).

Other Indian sectors, like finance, insurance, telecommunication, and health services, also involve information security allocations partly for their sculptures (Chin, 2025).

**Indian SPDI Rules, 2011 for Reasonable Security Practices**

The IS/ISO/IEC 27001 regulations are identified by the Indian SPDI Rules, 2011, as international standards. As such, Indian companies aren't obligated—but are highly advised—to implement these standards, which can help meet the "reasonable security practices" under Indian jurisdiction (Chin, 2025). The rules can also provide individuals the right to correct their information and impose restrictions on disclosure, data transfer, and security measures (Chin, 2025). They only apply to corporate entities, but they aren't responsible for the authenticity of sensitive personal data (SPD), like sexual orientation, medical records and history, biometric information, and passwords (Chin, 2025).

**National Cyber Security Policy, 2013**

In 2013, the Department of Electronics and Information Technology (DeitY) announced the National Cyber Security Policy 2013 as a security framework for public and private institutions with an aim to create and develop more robust policies to improve and defend themselves from cyber attacks (Chin, 2025).

The NSCP's alternate targets include:

- Producing a strong and protected cyberspace for individuals, organizations, and the government employees and entities (Chin, 2025).
- Observing, defending cyber infrastructure and data, by mitigating vulnerabilities, and enhancing defensive mechanisms against cyber attacks (Chin, 2025).
- Developing indiginious security frameworks, capabilities, and vulnerability management and mitigation strategies, for reducing, forestalling, or reacting to cyber events, cyber risks, cyber incidents and threats (Chin, 2025).
- Stimulates institutions to emerge cybersecurity rules that corresponds with crucial objectives, business procedures, and common practices (Chin, 2025).
- Immediately building organizational framework, methods, technology, and collaboration to lessen the damage induced by cybercrime (Chin, 2025).

**IT Rules, 2021**

IT Rules, 2021 also differentiates among minor and crucial social media grounded on subscribers and localities a massive load on great social network negotiator respecting private data protection (Chin, 2025).

Moreover, there are substitute to the privacy and visibility needs of mediators, such as:

- Making mandatory for intermediaries to disclose to users about the applicable rules and regulations, privacy policies, and terms and conditions governing the use of their services (Chin, 2025).
- Making mandatory intermediaries to appoint a grievance officer responsible for addressing and resolving user complaints concerning violations of IT Rules, 2021 (Chin, 2025).

**National Cyber Security Strategy 2020**

The National Cyber Security Strategy of 2020 was the anticipated action plan by the Indian government to additionally upgrade cybersecurity efforts, while the proposal is yet undergoing expansion and uncertain appraisal by the National Security Council Secretariat, the idea's main aim is to assist as the official instruction for contributors, and executives to block cyber occurrence, cyber violence, and surveillance in cyberspace (Chin, 2025).

The approach aims to enhance cybersecurity audit integrity so institutions may show positive appraisals of their cybersecurity planning and proficiency; the expectation is certain that, when the strategy is executed, the cyber referee will enhance their security measures, eventually promising institutions to place their security agendas (Chin, 2025).

**KYC (Know Your Customer)**

KYC (Know Your Customer) operations are guidelines used globally and requested by the RBI (Reserve Bank of India). KYC is the supervision of data protection for enhanced protection against scams and payment fraud which involves banks, insurance firms, and remaining e-payment firms that execute payments to authenticate and ascertain their clientele (Chin, 2025).

For genuine KYC obedience and to encounter financial compliance, commercials require adding the successive cybersecurity steps:

- Having a knowledge-based questionnaire test for verifying customer identities (Chin, 2025).
- Implementing pre-screening KYC verification methods like email verification, phone verification, Device ID intelligence, and reputational data, among others (Chin, 2025).
- Using AI-based technology and machine learning for verifying documents and government-issued IDs (Chin, 2025).
- Using biometrics like fingerprinting and facial recognition to verify a user's identity (Chin, 2025).
- Maintaining a database of customers for verification purposes (Chin, 2025).

Businesses with KYC policies assure customers they have the relevant compliance management and anti-fraud solutions to protect their digital identities and payment transaction data (Chin, 2025). With KYC Compliance, Indian merchants can have peace of mind with safe and secure payment processing, complying with regulations from SEBI, as well as establishing trust with customers (Chin, 2025).

Failing to adhere to the KYC directions, banks, businesses, and corporations may face a monetary penalty of ₹2 lakh (₹200,000) (Chin, 2025).

**Reserve Bank of India Act 2018**

The RBI Act of 2018 aims to:

- Create standards that equalize security frameworks of banks and payment operators according to how they adapt to new technologies and digitalization (Chin, 2025).
- Mandate banks to create and present their cyber crisis management plans (Chin, 2025).
- Mandate banks to implement corporate-approved (board-approved) information security policies which will successfully outline cybersecurity preparedness (Chin, 2025).
- Require banks to implement mandatory breach notifications, in which UCBs must promptly detect and report cybersecurity incidents to RBI within 2-6 hours of discovery to better respond to the attacks (Chin, 2025).
- Encourage banks to regularly schedule threat assessment audits (Chin, 2025).
- Help banks implement their own email domains with anti-phishing and anti-malware technology, as well as enforce DMARC security controls (Chin, 2025).

All Indian banks must follow these guidelines to standardize frameworks for payment processing cybersecurity and combat the ever-increasing business complications in a digital environment (Chin, 2025).

The RBI Act of 2018 imposes fines on banks and the financial sector in cases of non-compliance with their cybersecurity requirements and the penalties can be up to ₹10 lakh (₹1,000,000) (Chin, 2025).

**The Digital Personal Data Protection Act of 2023 (DPDP)**

On August 11, 2023, the Indian Central Government passed its long-awaited Digital Personal Data Protection Act (DPDP). The act borrows its broad definition of personal data from the EU's General Data Protection Regulation (GDPR) and aims to protect data principals and restrict the activities of data fiduciaries (Chin, 2025)..

The DPDP obligates data fiduciaries to:

- Only appoint or involve third-party data processors who are obligated to follow DPDP procedures by a legal contract (Chin, 2025).
- Ensure personal data is complete and accurate before using the data to make a decision that affects the data principal or before participating in the transfer of personal data (Chin, 2025).
- Implement necessary organizational measures and technical protocols to ensure ongoing compliance (Chin, 2025).
- Implement reasonable security safeguards and audits to protect personal data and prevent personal data breaches (Chin, 2025).
- Notify all affected data principals and the Data Protection Board of any and all known data breaches (Chin, 2025).
- Safely erase and destroy all personal data upon a data principal withdrawing their consent (unless retention of such data is required by law) (Chin, 2025).

In addition, the DPDP established the Data Protection Board of India and outlined a new class of data fiduciaries. Significant data fiduciaries are organizations determined to pose increased risk based on a government assessment (Chin, 2025). Organizations determined to be significant data fiduciaries must comply with additional requirements (Chin, 2025).

**Computer Emergency Response Team (CERT-In)**

Made official in 2004, the Computer Emergency Response Team (CERT-In) is the national nodal agency for collecting, analyzing, forecasting, and disseminating non-critical cybersecurity incidents (Chin, 2025). In addition to cybersecurity incident reporting and notifying, the CERT-In cybersecurity directive helps with issuing guidelines for Indian organizations guidelines as well, offering the best information security practices for managing and preventing cybersecurity incidents (Chin, 2025). The Jurisdiction of Information Technology Rules, 2013 is responsible for mandating all Indian data centers, service providers, and their intermediates (Chin, 2025). All intermediaries are required to report any cybersecurity incidents to CERT-In (Chin, 2025).

**National Critical Information Infrastructure Protection Center (NCIIPC)**

The Indian Parliament divides cybersecurity into two segments: "Non-Critical Infrastructure (NCI)," which CERT-In is responsible for, and "Critical Information Infrastructure (CII)," which NCIIPIC is responsible for. CII is defined by the Indian Parliament as "facilities, systems or functions whose incapacity or destruction would cause a debilitating impact on national security, governance, economy and social well-being of a nation." (Chin, 2025).

NCIIPC successfully implemented several guidelines for policy guidance, knowledge sharing, and cybersecurity awareness for organizations to conduct preemptive measures of these important sectors, especially in power and energy (Chin, 2025).. The guidelines represent the first means for regulating such sectors and requiring "mandatory compliance by all responsible entities." (Chin, 2025).

Additionally, the Indian government approved the Revamped Distribution Sector Scheme in August 2021, and the main goal of this regulation is to improve the operations of DISCOMs (distribution companies) by enhancing the cyber infrastructure with AI-based solutions (Chin, 2025).. This will ultimately aid organizations and companies in meeting the framework's goals (Chin, 2025).

**Cyber Regulations Appellate Tribunal (CRAT)**

Under the IT Act, 2000, Section 62, the Central Government of India created the Cyber Regulations Appellate Tribunal (CRAT) as a chief governing body and authority for fact-finding, receiving cyber evidence, and examining witnesses (Chin, 2025). While CRAT doesn't have as much jurisdiction for cybersecurity notification as CERT-In, the government also serves to respond to and act on related cybersecurity incidents and breaches (Chin, 2025)

According to the Civil Court and Code of Civil Procedure, 1908, CRAT has the power to:

- Receive evidence on affidavits (Chin, 2025)
- Ensure that all electronic and cyber evidence and records are presented for court (Chin, 2025)
- Enforce, summon, and issue regular commissions for examining witnesses, documents, and people under oath (Chin, 2025)
- Review final decisions of the court to resolve incidents and cases (Chin, 2025)
- Approve, dismiss, or declare the defaulter's applications as ex-parte (Chin, 2025)

**Insurance Regulatory and Development Authority (IRDAI)**

The insurance sector of India is regulated by IRDAI, which issues information security guidelines for insurers and addresses the importance of maintaining data integrity and confidentiality (Chin, 2025).

The insurance sector of India mainly focuses on areas of higher risk, including ransomware attacks, transaction frauds, data leaks, and risks of violating intellectual property rights (Chin, 2025). According to a report by Sophos, 68% of Indian organizations were affected by ransomware and resorted to paying ransom to recover their data (Chin, 2025).

On October 9, 2022, IRDAI introduced an improved cybersecurity framework focused on the insurers' main security concerns (Chin, 2025). It aims to encourage insurance firms to establish and maintain a robust risk assessment plan, improve mitigation methods of internal and external threats, prevent ransomware attacks and other types of fraud, and implement a strong and robust business continuity (Chin, 2025).

Depending on the seriousness of the violation, insurers and businesses may be penalized upward of ₹1 lakh (₹100,000), if insurers fail to protect data they may be fined up to ₹5 crores per affected person (Chin, 2025). The IRDAI Guidelines for Information and Cyber Security for Insurers apply to all insurers regulated by Insurance Regulatory (Chin, 2025).

**Telecom Regulatory Authority of India (TRAI) & Department of Telecommunications (DoT)**

TRAI is a regulatory body, and DoT is a separate executive department of the Ministry of Communications in India. Although TRAI has been granted more regulatory powers, both work together to govern and regulate telephone operators and service providers (Chin, 2025).

On June 16, 2018, TRAI released recommendations for telecom providers on "Privacy, Security and Ownership of the Data in the Telecom Sector." In the newest guidelines, TRAI addresses newer responsibilities governing consumer data because most digital transactions in India are done via cell phones (Chin, 2025).

The DoT has collaborated with the Indian IT ministry to impose layered data consent rules that safeguard personal data processing (Chin, 2025). This gives users the freedom to decide whether or not they will consent to the usage of their personal data and the right to withdraw consent at any time (Chin, 2025).

The new rules state that organizations and companies will only have to collect the necessary user details and that the data may be retained only for as long as required. Additionally, Indian telecommunications service providers comply with common standards like ISO 27000, 3GPP and 3GPP2, and ISO/IEC 15408 (Chin, 2025).

### 5.6 Discussion of Research Question One

Following the valuable responses received from the participants regarding the awareness program and proactiveness, the majority of the respondents are aware of cyber security. It demonstrates that they do have a keen interest in knowing more about the adoption of cybersecurity in their day-to-day life. We will also discuss the different vulnerabilities that mostly MSMEs face and the different approaches that can be used to fix them or develop a training awareness module within an organization that will educate the employees. One can find that, the value of the input factors contributing to the delay in the implementation of cybersecurity policies and procedures for OPCs, early startups and MSMEs.

Organizations are well aware of different security standards and frameworks, but they do lack in implementing them within an organization because of various constraints like resource constraints and budget constraints, and if they approach any well-known organization to do the implementation, then they charge a huge amount for the implementation. If attackers are able to exploit these vulnerabilities by taking advantage of weaknesses present in the product or environment, resulting a financial loss or even damage to their reputation in the market, lowering their brand value of the OPCs, early startups, and MSMEs. 60% of OPCs, early startups, and MSMEs do not have proper cybersecurity frameworks or standards in place that will help them in tackling these kinds of security risks.

### 5.7 Discussion of Research Question Two

**What are the major vulnerabilities that were reported externally in your product or identified internally?**

10% of the individuals replied that they are aware of the broken authentication vulnerability. 8% of the individuals replied that they are aware of insufficient input/output validation. 6% of them know about Server-Side Request Forgery (SSRF), Broken Access Control, and Cryptographic Failures. 7% of the individuals replied that they know about identification and authentication failure, security logging and monitoring failures, insecure data storage, unrestricted access to sensitive business flows, and unrestricted resource consumption vulnerabilities.

According to the responses received, the top 5 vulnerabilities for API applications are broken authentication, unrestricted access to sensitive business flows, unrestricted resource consumption, server-side request forgery, and broken object-level authorization. According to the responses received, the top 5 vulnerabilities for mobile applications are insufficient input/output validations, insecure data storage, insufficient binary protections, improper credential usage, and insecure communication. According to the responses received, the top 5 vulnerabilities for web applications are identification and authentication failures, security logging and monitoring failures, Cryptographic failures, broken access control, and injection flaws.

# CHAPTER VI:

# SUMMARY, IMPLICATIONS, AND RECOMMENDATIONS

## 6.1 Summary

This research helps on analyzing the organizational approach of implementing cybersecurity policies and awareness from micro, small, and medium enterprises operating in India aimed to create awareness of different security vulnerabilities and guideline policies for organizations to protect assets. The research answered the understanding of different vulnerabilities organizations face and their mitigation techniques and their consequences if exploited. By addressing different vulnerabilities such as SQL injection, security misconfiguration, IDOR, input validation, and privilege escalation, and focusing on OWASP Top 10 for web applications, mobile, and APIs during the development life cycle, they will better fight against external attacks. Organizations should be proactive in adopting technological solutions and regular risk assessments as well as a measuring tool like KPI (Key Performance Index) to check how they are performing. Employees should be aware and make sure they are strictly following it, regularly monitoring and updating their security guidelines to adapt to the evolving security landscape.

## 6.2 Implications

"All's well that ends well, my friend. Enjoy your meal!" - Instate of no security policies and aware program among employees its better to have a bare minimum security policies and train the developers with security guidelines of secure development life cycle to safe guard assets within an organization by dedicating 5% of the budget in Cybersecurity. A huge penalties may be imposed if organization fail to follow different IT

acts imposed by the Government of India for their respective businesses that we discussed in Indian Cyber Security laws and regulations section.

### 6.3 Recommendations for Future Research

The survey results provide multiple suggestions for future research in application security.

- Assessing best proprietary tools for manual penetration testing with AI capabilities.
- In-depth study on the, GRC, Security Operations Center and its implications and applications.
- Deep dive into specific vulnerabilities, their attack scenarios, and mitigation techniques for different applications like Java, PHP, .Net, and other programming languages.
- Focusing on identifying and detecting design flaws from a threat modeling perspective to address vulnerabilities during the early phase of the software development life cycle (SDLC).
- How CI/CD pipeline and DevSecOps can play vital role in vulnerability remediations and automation.

## 6.4 Conclusion

This research provides a comprehensive understanding of different attacks that MSMEs should focus on when developing their products. It also identified various gaps and concerns about how MSMEs address cybersecurity, ensuring their ability to establish an effective cybersecurity posture. To prevent attacks, MSMEs must adhere to fundamental and incremental cybersecurity measures by following country specific regulations provided by CERT-In and state specific regulations provided by CERT-O.

For any MSMEs this research can help them in having secure product and security within the organization. With CERT-In's clear plan and basic steps like training and awareness between staffs, following secure development life cycle, and backing up data regularly, MSMEs can protect themselves and build trust among their customers. Cybersecurity should be seen as smart business, not extra cost. Policymakers must help smaller firms with simple tools and support. Securing MSMEs strengthens India's economy — when small businesses stay safe, the nation's digital growth stays strong.

As per Digital Personal Data Protection Rules (*2025*) released by Ministry of Electronics and Information Technology (MietY), Government of India (GoI) in the month of November 2025, has published updated rules, that talks more about bringing clarity on consent, notices, breach reporting, children's data, and additional duties for Significant Data Fiduciaries. For organizations, this means implementation and review your data flows, update consent journeys, re-check and validate vendor contracts, refresh your breach-response plan and timelines, and prepare for heavier accountability and avoidance of penalties.

APPENDIX A

SURVEY COVER LETTER

# Cyber Security Survey

Sign in to Google to save your progress. Learn more

* Indicates required question

Are you aware of your organization's cybersecurity policies and practices? *

- Yes
- No
- Maybe

Do you believe that your organization's cybersecurity policies and practices are effective in protecting against cyber threats? *

- Yes
- No
- Maybe

Does your organization aware of in industry standards or frameworks? *

- Yes
- No
- Maybe

How often do you receive cybersecurity training or awareness programs? *

- ◯ Monthly
- ◯ Quarterly
- ◯ Annually
- ◯ Biannually
- ◯ Never

Have you ever been a victim of a cyber threat or attack while employed for your organization? *

- ◯ Yes
- ◯ No
- ◯ Maybe

How frequently do you change your passwords and update security patches on your work devices? *

- ◯ Rarely
- ◯ Every 3 months
- ◯ Every 6 months
- ◯ Every month

How would you rank your expertise and knowledge of cyber security? *

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Low | ○ | ○ | ○ | ○ | ○ | High |

Do you think that your colleagues and supervisors take cybersecurity seriously? *

- ○ Yes
- ○ No
- ○ Maybe

Have you ever seen your colleague violating cybersecurity policies or engaging in unsafe practices? *

- ○ Yes
- ○ No
- ○ Maybe

What steps do you individually take to protect sensitive information? *

Your answer

Have you ever reported a suspected incident to your organization's security team? *

- ◯ Yes
- ◯ No
- ◯ Maybe

How can the company support you in implementing safe cybersecurity practices in your day-to-day work? *

- ◯ Yes
- ◯ No
- ◯ Maybe

Application Type *

Choose

Based on type selected in Application Type, What are the major vulnerabilities that were reported externally in your product or identified internally? (A series for Web, M series for Mobile and API for API) *

Based on type selected in Application Type, What are the major vulnerabilities that were reported externally in your product or identified internally? (A series for Web, M series for Mobile and API for API) *

- ○ A01: Broken Access Control
- ○ A02: Cryptographic Failures
- ○ A03: Injection
- ○ A04: Insecure Design
- ○ A05: Security Misconfiguration
- ○ A06: Vulnerable and Outdated Components
- ○ A07: Identification and Authentication Failures
- ○ A08: Software and Data Integrity Failures
- ○ A09: Security Logging and Monitoring Failures
- ○ A10: Server-Side Request Forgery (SSRF)
- ○ M1: Improper Credential Usage
- ○ M2: Inadequate Supply Chain Security
- ○ M3: Insecure Authentication/Authorization
- ○ M4: Insufficient Input/Output Validation
- ○ M5: Insecure Communication
- ○ M6: Inadequate Privacy Controls
- ○ M7: Insufficient Binary Protections
- ○ M8: Security Misconfiguration
- ○ M9: Insecure Data Storage
- ○ M10: Insufficient Cryptography

- ◯ M1: Improper Credential Usage
- ◯ M2: Inadequate Supply Chain Security
- ◯ M3: Insecure Authentication/Authorization
- ◯ M4: Insufficient Input/Output Validation
- ◯ M5: Insecure Communication
- ◯ M6: Inadequate Privacy Controls
- ◯ M7: Insufficient Binary Protections
- ◯ M8: Security Misconfiguration
- ◯ M9: Insecure Data Storage
- ◯ M10: Insufficient Cryptography
- ◯ API1:2023 Broken Object Level Authorization
- ◯ API2:2023 Broken Authentication
- ◯ API3:2023 Broken Object Property Level Authorization
- ◯ API4:2023 Unrestricted Resource Consumption
- ◯ API5:2023 Broken Function Level Authorization
- ◯ API6:2023 Unrestricted Access to Sensitive Business Flows
- ◯ API7:2023 Server Side Request Forgery
- ◯ API8:2023 Security Misconfiguration
- ◯ API9:2023 Improper Inventory Management
- ◯ API10:2023 Unsafe Consumption of APIs

Submit Clear form

APPENDIX B

CODE BASE

```python
import pandas as pd
import matplotlib.pyplot as plt
import seaborn as sns

# Load Excel data
data = pd.read_excel('Cybersecurity_Survey_Responses.xlsx')

# Select the first question column
column = 'Aware of org cybersecurity policies?'

# Count frequency of each response
response_counts = data[column].value_counts().sort_index()

# Compute percentages
total_responses = response_counts.sum()
percentages = (response_counts / total_responses * 100).round(2)

# Plot bar graph
plt.figure(figsize=(8, 5))
ax = sns.barplot(
    x=response_counts.index,
    y=response_counts.values,
    hue=response_counts.index,
    palette='viridis',
    legend=False
)

# Add percentage labels on bars
for i, p in enumerate(ax.patches):
    value = response_counts.values[i]
    percent = percentages.values[i]
    ax.text(
        p.get_x() + p.get_width() / 2,
        p.get_height() + 1,   # Slightly above the bar
        f"{percent:.1f}%",
        ha='center',
        va='bottom',
        fontsize=10,
        fontweight='bold'
    )

# Chart titles and labels
plt.title('Awareness of Organization Cybersecurity Policies', fontsize=13, fontweight='bold')
plt.xlabel('Response', fontsize=11)
plt.ylabel('Number of Respondents', fontsize=11)
plt.tight_layout()

# Save chart
plt.savefig('column1_cyber_awareness.png', dpi=300)

# Display observations
dominant_response = response_counts.idxmax()
dominant_percent = round((response_counts.max() / total_responses) * 100, 2)

print("Total Responses:", total_responses)
print("Most Common Response:", dominant_response, f"({dominant_percent}%)")
print(f"Observation: The majority of respondents ({dominant_percent}%) indicated '{dominant_response}', "
      "suggesting a strong awareness of cybersecurity policies within the organization.")
```

```python
import pandas as pd
import matplotlib.pyplot as plt
import seaborn as sns

# Load the data
data = pd.read_excel('Cybersecurity_Survey_Responses.xlsx')

# Select the column for analysis
column = 'Org aware of industry standards?'

# Get counts and calculate percentage of each response
response_counts = data[column].value_counts()
response_percent = (response_counts / response_counts.sum()) * 100

# Prepare the plot
plt.figure(figsize=(8, 5))
bars = sns.barplot(x=response_percent.index, y=response_percent.values,
                   hue=response_percent.index, palette='viridis', legend=False)

# Add percentage labels on top of bars
for bar, percent in zip(bars.patches, response_percent):
    height = bar.get_height()
    bars.annotate(f'{percent:.1f}%',
                  (bar.get_x() + bar.get_width() / 2, height),
                  ha='center', va='bottom')

# Titles and labels
plt.title('Percentage Awareness of Organizational Cybersecurity Industry Standards')
plt.xlabel('Response')
plt.ylabel('Percentage of Respondents')
plt.ylim(0, 100)
plt.tight_layout()

# Save the plot
plt.savefig('column2_org_standards_percent.png', dpi=300)
plt.show()

# Print observations
total_responses = response_counts.sum()
dominant_response = response_percent.idxmax()
dominant_value = response_percent.max()
```

```python
import pandas as pd
import matplotlib.pyplot as plt
import seaborn as sns

# Load the data
data = pd.read_excel('Cybersecurity_Survey_Responses.xlsx')

# Use exact column name as it appears in DataFrame
column = "Policies effective against threats?"

# Calculate counts and percentages
response_counts = data[column].value_counts()
response_percent = (response_counts / response_counts.sum()) * 100

# Plot
plt.figure(figsize=(8, 5))
bars = sns.barplot(x=response_percent.index, y=response_percent.values,
                   hue=response_percent.index, palette='viridis', legend=False)

# Annotate percentages on bars
for bar, percent in zip(bars.patches, response_percent):
    height = bar.get_height()
    bars.annotate(f'{percent:.1f}%',
                  (bar.get_x() + bar.get_width() / 2, height),
                  ha='center', va='bottom')

plt.title("Effectiveness of Cybersecurity Policies (Perceived)")
plt.xlabel("Response")
plt.ylabel("Percentage of Respondents")
plt.ylim(0, 100)
plt.tight_layout()

plt.savefig('column3_policy_effectiveness_percent.png', dpi=300)
plt.show()

# Output observations
total_responses = response_counts.sum()
dominant_response = response_percent.idxmax()
dominant_value = response_percent.max()

print(f"Total responses: {total_responses}")
print(f"Most common response: '{dominant_response}' ({dominant_value:.1f}%)")
print(f"Observation: Most respondents ({dominant_value:.1f}%) believe their organization's cybersecurity policies are effective against cyber threats.")
```

```python
import pandas as pd
import matplotlib.pyplot as plt
import seaborn as sns

# Load the data
data = pd.read_excel('Cybersecurity_Survey_Responses.xlsx')

# Column to analyze
column = 'Frequency of cybersecurity training'

# Calculate counts and percentages
response_counts = data[column].value_counts()
response_percent = (response_counts / response_counts.sum()) * 100

# Plotting
plt.figure(figsize=(9, 6))
bars = sns.barplot(x=response_percent.index, y=response_percent.values,
                   hue=response_percent.index, palette='viridis', legend=False)

# Annotate bars with percentage labels
for bar, percent in zip(bars.patches, response_percent):
    height = bar.get_height()
    bars.annotate(f'{percent:.1f}%',
                  (bar.get_x() + bar.get_width() / 2, height),
                  ha='center', va='bottom')

# Title and Labels
plt.title('Frequency of Cybersecurity Training (Percentage of Respondents)')
plt.xlabel('Training Frequency')
plt.ylabel('Percentage (%)')
plt.ylim(0, 100)
plt.tight_layout()

# Save the figure
plt.savefig('column4_training_frequency_percent.png', dpi=300)
plt.show()

# Observations
print(f"Total responses: {response_counts.sum()}")
for response, percent in response_percent.items():
    print(f"Response: {response}, Percentage: {percent:.1f}%")

print("\nResearch Observations:")
print("- Most respondents receive cybersecurity training either quarterly or monthly, reflecting a proactive approach to maintaining awareness.")
print("- A smaller portion attend training annually or biannually, which might correspond to roles with less exposure or lower risk.")
print("- The minority who reported never receiving training indicates gaps where organizations should focus on improving compliance and education.")
```

```python
import pandas as pd
import matplotlib.pyplot as plt
import seaborn as sns

# Load data
data = pd.read_excel('Cybersecurity_Survey_Responses.xlsx')

# Select the column
column = 'Experienced cyber threat at work?'

# Calculate counts and percentages
response_counts = data[column].value_counts()
response_percent = (response_counts / response_counts.sum()) * 100

# Plot
plt.figure(figsize=(8, 5))
bars = sns.barplot(x=response_percent.index, y=response_percent.values,
                   hue=response_percent.index, palette='viridis', legend=False)

# Annotate bars with percentage labels
for bar, percent in zip(bars.patches, response_percent):
    height = bar.get_height()
    bars.annotate(f'{percent:.1f}%',
                  (bar.get_x() + bar.get_width() / 2, height),
                  ha='center', va='bottom')

plt.title('Percentage of Respondents Experienced Cyber Threat at Work')
plt.xlabel('Response')
plt.ylabel('Percentage (%)')
plt.ylim(0, 100)
plt.tight_layout()

# Save plot
plt.savefig('column5_experienced_threat_percent.png', dpi=300)
plt.show()

# Observations
print(f"Total responses: {response_counts.sum()}")
for response, percent in response_percent.items():
    print(f"Response: {response}, Percentage: {percent:.1f}%")
```

```python
import pandas as pd
import matplotlib.pyplot as plt
import seaborn as sns

# Load data
data = pd.read_excel('Cybersecurity_Survey_Responses.xlsx')

# Select column
column = 'Password update frequency'

# Calculate counts and percentages
response_counts = data[column].value_counts()
response_percent = (response_counts / response_counts.sum()) * 100

# Plot
plt.figure(figsize=(9, 6))
bars = sns.barplot(x=response_percent.index, y=response_percent.values,
                   hue=response_percent.index, palette='viridis', legend=False)

# Annotate percentages on bars
for bar, percent in zip(bars.patches, response_percent):
    height = bar.get_height()
    bars.annotate(f'{percent:.1f}%',
                  (bar.get_x() + bar.get_width() / 2, height),
                  ha='center', va='bottom')

plt.title('Password Update Frequency (% of Respondents)')
plt.xlabel('Password Update Frequency')
plt.ylabel('Percentage (%)')
plt.ylim(0, 100)
plt.tight_layout()

# Save the plot
plt.savefig('column6_password_update_frequency_percent.png', dpi=300)
plt.show()

# Observations
print(f"Total responses: {response_counts.sum()}")
for response, percent in response_percent.items():
    print(f"Response: {response}, Percentage: {percent:.1f}%")
```

```python
import pandas as pd
import matplotlib.pyplot as plt
import seaborn as sns

# Load data
data = pd.read_excel('Cybersecurity_Survey_Responses.xlsx')

# Select column
column = 'Self-rated cybersecurity skills (1-5)'

# Calculate counts and percentages
response_counts = data[column].value_counts().sort_index()
response_percent = (response_counts / response_counts.sum()) * 100

# Plot
plt.figure(figsize=(8, 5))
bars = sns.barplot(x=response_percent.index.astype(str), y=response_percent.values,
                   hue=response_percent.index.astype(str), palette='viridis', legend=False)

# Annotate percentages on bars
for bar, percent in zip(bars.patches, response_percent):
    height = bar.get_height()
    bars.annotate(f'{percent:.1f}%',
                  (bar.get_x() + bar.get_width() / 2, height),
                  ha='center', va='bottom')

plt.title('Self-rated Cybersecurity Skills (Percentage of Respondents)')
plt.xlabel('Skill Rating (1-5)')
plt.ylabel('Percentage (%)')
plt.ylim(0, 100)
plt.tight_layout()

# Save plot
plt.savefig('column7_self_rated_skills_percent.png', dpi=300)
plt.show()

# Research observations
print(f"Total responses: {response_counts.sum()}")
for response, percent in response_percent.items():
    print(f"Skill Rating: {response}, Percentage: {percent:.1f}%")
```

```python
import pandas as pd
import matplotlib.pyplot as plt
import seaborn as sns

# Load data
data = pd.read_excel('Cybersecurity_Survey_Responses.xlsx')

# Select column
column = 'Colleagues take cybersecurity seriously?'

# Calculate counts and percentages
response_counts = data[column].value_counts()
response_percent = (response_counts / response_counts.sum()) * 100

# Plot
plt.figure(figsize=(8, 5))
bars = sns.barplot(x=response_percent.index, y=response_percent.values,
                   hue=response_percent.index, palette='viridis', legend=False)

# Annotate bars with percentage labels
for bar, percent in zip(bars.patches, response_percent):
    height = bar.get_height()
    bars.annotate(f'{percent:.1f}%',
                  (bar.get_x() + bar.get_width() / 2, height),
                  ha='center', va='bottom')

plt.title('Perceptions: Do Colleagues Take Cybersecurity Seriously?')
plt.xlabel('Response')
plt.ylabel('Percentage (%)')
plt.ylim(0, 100)
plt.tight_layout()

# Save plot
plt.savefig('column8_colleagues_cybersecurity_serious_percent.png', dpi=300)
plt.show()

# Observations
print(f"Total responses: {response_counts.sum()}")
for response, percent in response_percent.items():
    print(f"Response: {response}, Percentage: {percent:.1f}%")
```

```python
import pandas as pd
import matplotlib.pyplot as plt
import seaborn as sns

# Load the data
data = pd.read_excel('Cybersecurity_Survey_Responses.xlsx')

# Select the column
column = 'Witnessed policy violations?'

# Calculate counts and percentages
response_counts = data[column].value_counts()
response_percent = (response_counts / response_counts.sum()) * 100

# Plot the percentage bar chart
plt.figure(figsize=(8, 5))
bars = sns.barplot(x=response_percent.index, y=response_percent.values,
                   hue=response_percent.index, palette='viridis', legend=False)

# Annotate percentage labels on top of bars
for bar, percent in zip(bars.patches, response_percent):
    height = bar.get_height()
    bars.annotate(f'{percent:.1f}%',
                  (bar.get_x() + bar.get_width() / 2, height),
                  ha='center', va='bottom')

plt.title('Percentage of Respondents Who Witnessed Policy Violations')
plt.xlabel('Response')
plt.ylabel('Percentage (%)')
plt.ylim(0, 100)
plt.tight_layout()

# Save and show the plot
plt.savefig('column9_witnessed_policy_violations_percent.png', dpi=300)
plt.show()

# Print observations
print(f"Total responses: {response_counts.sum()}")
for response, percent in response_percent.items():
    print(f"Response: {response}, Percentage: {percent:.1f}%")
```

```python
import pandas as pd
import statsmodels.api as sm

data = pd.read_excel('Cybersecurity_Survey_Responses.xlsx')

# Encode binary outcome
data['Reported_binary'] = data['Reported suspected incident?'].map({'Yes':1, 'No':0})

# Encode categorical predictors as numeric categories
data['Training_encoded'] = data['Frequency of cybersecurity training'].astype('category').cat.codes
data['Policy_aware_encoded'] = data['Org aware of industry standards?'].astype('category').cat.codes

# Select predictors and add constant for intercept
X = data[['Training_encoded', 'Policy_aware_encoded']]
X = sm.add_constant(X)

# Outcome variable
y = data['Reported_binary']

# Fit logistic regression model
logit_model = sm.Logit(y, X, missing='drop')
result = logit_model.fit()

print(result.summary())
```

```
Optimization terminated successfully.
         Current function value: 0.584544
         Iterations 5
                           Logit Regression Results
==============================================================================
Dep. Variable:        Reported_binary   No. Observations:                  146
Model:                          Logit   Df Residuals:                      143
Method:                           MLE   Df Model:                            2
Date:                Thu, 23 Oct 2025   Pseudo R-squ.:                0.004473
Time:                        17:04:37   Log-Likelihood:                -85.343
converged:                       True   LL-Null:                       -85.727
Covariance Type:            nonrobust   LLR p-value:                    0.6815
=========================================================================================
                            coef    std err          z      P>|z|      [0.025      0.975]
-----------------------------------------------------------------------------------------
const                    -0.5805      0.481     -1.208      0.227      -1.523       0.362
Training_encoded         -0.0811      0.137     -0.593      0.553      -0.349       0.187
Policy_aware_encoded     -0.1561      0.220     -0.709      0.478      -0.588       0.275
=========================================================================================
```

# APPENDIX C

## INTERVIEW GUIDE

Ethical aspects will be taken into account when collecting data from various stakeholders during this process. Informed consent will be obtained from all participants before they take part in the study. The data collected will be kept confidential and anonymous, and the participants' privacy will be protected throughout the study.

REFERENCES

*A03 Injection—OWASP Top 10:2025 RC1*. (n.d.). Retrieved November 21, 2025, from https://owasp.org/Top10/A03_2021-Injection/

*A04 Insecure Design—OWASP Top 10:2025 RC1*. (n.d.). Retrieved November 21, 2025, from https://owasp.org/Top10/A04_2021-Insecure_Design/

*A07 Identification and Authentication Failures—OWASP Top 10:2025 RC1*. (n.d.). Retrieved November 21, 2025, from https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/

*A08 Software and Data Integrity Failures—OWASP Top 10:2025 RC1*. (n.d.). Retrieved November 21, 2025, from https://owasp.org/Top10/A08_2021-Software_and_Data_Integrity_Failures/

Acunetix. (n.d.). *Types of SQL Injection?* Retrieved October 24, 2025, from https://www.acunetix.com/websitesecurity/sql-injection2/

Alanda, A., Satria, D., Mooduto, H., & Kurniawan, B. (2020). *Mobile application security penetration testing based on OWASP*. *846*(1), 012036.

Albera, M. (2025, December 11). *Protecting our Merchants: Standing up to Extortion*. https://www.checkout.com/blog/protecting-our-merchants-standing-up-to-extortion

Aleti, A., Buhnova, B., Grunske, L., Koziolek, A., & Meedeniya, I. (2012). Software architecture optimization methods: A systematic literature review. *IEEE Transactions on Software Engineering*, *39*(5), 658–683.

Amazon. (2025, November 21). *What is GRC? - Governance, Risk, and Compliance Explained - AWS*. Amazon Web Services, Inc. https://aws.amazon.com/what-is/grc/

Andersen, G. (2024, February 2). *The Role of System Security Engineering in Advancing Sports Technology*. https://moldstud.com/articles/p-the-role-of-system-security-engineering-in-sports-technology

Arunachalam, C. (n.d.). *MINIMUM VIABLE CYBERSECURITY FRAMEWORK FOR PROTECTING CYBER ATTACKS FROM EXTERNAL THREAT VECTORS*.

Bandara, I., Ioras, F., & Maher, K. (2014). *Cyber security concerns in e-learning education*. 728–734.

Bay, M. (2016). What is cybersecurity. *French Journal for Media Research*, *6*, 1–28.

Ben Farah, M. A., Ukwandu, E., Hindy, H., Brosset, D., Bures, M., Andonovic, I., & Bellekens, X. (2022). Cyber security in the maritime industry: A systematic survey of recent advances and future trends. *Information*, *13*(1), 22.

Beskow, D. M., & Carley, K. M. (2020). Social Cybersecurity Chapter 13: Casestudy with COVID-19 Pandemic. *arXiv Preprint arXiv:2008.10102*.

Best, S. (2025). *Unrestricted Resource Consumption—API4—OWASP API Top 10*. https://salt.security/blog/api4-2023-unrestricted-resource-consumption

Bhatia, D. (2022). A Comprehensive Review on the Cyber Security Methods in Indian Organisation. *International Journal of Advances in Soft Computing & Its Applications*, *14*(1).

Bhattacharjya, A. (2022). A holistic study on the use of blockchain technology in CPS and IoT architectures maintaining the CIA triad in data communication. *International Journal of Applied Mathematics and Computer Science*, *32*(3), 403–413.

Bluefin. (2025, August 12). IBM's 2025 Data Breach Report: Key Findings and the Year's Biggest Attacks. *Bluefin*. https://www.bluefin.com/bluefin-news/ibms-2025-data-breach-report-key-findings-and-the-years-biggest-attacks/

Bridges, J. (2023, October 19). *IT Risk Management Process, Frameworks & Templates*. ProjectManager. https://www.projectmanager.com/training/it-risk-management-strategies

Bureau, T. H. (2024, December 4). DSCI study identifies 369.01 mn malware detections across installation base of 8.44 million endpoints in India. *The Hindu*. https://www.thehindu.com/business/dsci-study-identifies-36901-mn-malware-detections-across-installation-base-of-844-million-endpoints-in-india/article68947434.ece

Cannon, D. L. (n.d.). *CISA Certified Information Systems Auditor Study Guide, 4th Edition | Wiley*. Wiley.Com. Retrieved October 17, 2025, from https://www.wiley.com/en-us/CISA+Certified+Information+Systems+Auditor+Study+Guide%2C+4th+Edition-p-9781119419211

chamarthi, M. (2025, May 3). M3: Insecure Authentication / Authorization — OWASP Mobile Top 10–2024. *Medium*. https://medium.com/@madhuhack01/m3-insecure-authentication-authorization-owasp-mobile-top-10-2024-510a2d0f419e

Chen, P., Desmet, L., & Huygens, C. (2014). *A study on advanced persistent threats*. 63–72.

Chin, K. (2025). *Top Cybersecurity Regulations in India [Updated 2025] | UpGuard*. https://www.upguard.com/blog/cybersecurity-regulations-india

Christ, G. (2025). *Employment screening provider data breach affects 3.3M people | Cybersecurity Dive*. https://www.hrdive.com/news/DISA-data-breach-affects-33m-people/740982/

Cisco Systems Inc. (n.d.). *What Is Threat Modeling?* Cisco. Retrieved October 17, 2025, from https://www.cisco.com/site/us/en/learn/topics/security/what-is-threat-modeling.html

CISSP, M. S. (2023, December 8). The 3 Types Of Security Controls (Expert Explains). *PurpleSec*. https://purplesec.us/learn/security-controls/

Cloudflare. (n.d.). *What is OWASP?* Retrieved October 21, 2025, from https://www.cloudflare.com/learning/security/threats/owasp-top-10/

Cochran, K. A., & Reis, K. (2025). Core Concepts in Cybersecurity. In K. A. Cochran & K. Reis (Eds.), *CompTIA Security+ (SY0-701) Certification Companion: Hands-on Preparation and Practice Guide* (pp. 13–72). Apress. https://doi.org/10.1007/979-8-8688-1498-3_2

Creswell, J. W. (1999). Mixed-method research: Introduction and application. In *Handbook of educational policy* (pp. 455–472). Elsevier.

Crumpler, W., & Lewis, J. A. (2019). *The cybersecurity workforce gap*. JSTOR.

Cyber Attack Lifecycle. (n.d.-a). *Law Enforcement Center Cyber*. Retrieved November 17, 2025, from https://www.iacpcybercenter.org/resource-center/what-is-cyber-crime/cyber-attack-lifecycle/

Cyber Attack Lifecycle. (n.d.-b). *Law Enforcement Center Cyber*. Retrieved November 20, 2025, from https://www.iacpcybercenter.org/resource-center/what-is-cyber-crime/cyber-attack-lifecycle/

*Cybercriminals—An overview | ScienceDirect Topics*. (n.d.). Retrieved October 23, 2025, from https://www.sciencedirect.com/topics/computer-science/cybercriminals

*Data Security Council of India (DSCI)*. (n.d.). Data Security Council of India (DSCI). Retrieved October 13, 2025, from https://www.dsci.in

*Digital Personal Data Protection Rules 2025 | Ministry of Electronics and Information Technology*. (n.d.). Retrieved November 17, 2025, from https://www.meity.gov.in/documents/act-and-policies/digital-personal-data-protection-rules-2025-gDOxUjMtQWa?pageTitle=Digital-Personal-Data-Protection-Rules-2025

DSCI. (2025a). *DSCI Annual Report*. DSCI. https://www.dsci.in/files/content/knowledge-centre/2023/DSCI-Annual%20Report%202021-22.pdf

DSCI. (2025b, November 19). *India Cyber Threat Report*. DSCI. https://www.dsci.in/files/content/knowledge-centre/2024/India-Cyber-Threat-Report-2025.pdf

Fett, D., Küsters, R., & Schmitz, G. (2016). *A comprehensive formal security analysis of OAuth 2.0*. 1204–1215.

Fortinet. (2023, December 8). What Is Data Loss Prevention (DLP)? *What Is Data Loss Prevention (DLP)?* https://www.fortinet.com/resources/cyberglossary/dlp

Fossey, E., Harvey, C., McDermott, F., & Davidson, L. (2002). Understanding and evaluating qualitative research. *Australian and New Zealand Journal of Psychiatry*, *36*(6), 717–732.

Fredj, O. B., Cheikhrouhou, O., Krichen, M., Hamam, H., & Derhab, A. (2020). *An OWASP top ten driven survey on web application protection methods*. 235–252.

G, P. (2025, March 17). 10 Must-Know Updates in the OWASP API Security Top 10 | Prophaze Blog. *Prophaze*. https://prophaze.com/blog/10-must-know-updates-in-the-owasp-api-security-top-10/

Gaurav, A., Gupta, B. B., Hsu, C.-H., Peraković, D., & Penalvo, F. J. G. (2021). *Filtering of distributed denial of services (DDoS) attacks in cloud computing environment*. 1–6.

Getastra. (2024, August 15). *OWASP Mobile Top 10 2025: A Security Guide*. https://www.getastra.com/blog/mobile/owasp-mobile-top-10-2024-a-security-guide/

Ghanem, M. C., & Chen, T. M. (2019). Reinforcement learning for efficient network penetration testing. *Information*, *11*(1), 6.

Ghate, S., & Agrawal, P. K. (2017). A literature review on cyber security in indian context. *J. Comput. Inf. Technol*, *8*(5), 30–36.

Ghillani, D. (2022). Deep learning and artificial intelligence framework to improve the cyber security. *Authorea Preprints*.

Gordon, A. (2015). *Official (ISC)2 Guide to the CISSP CBK* (4th edition). https://doi.org/10.1201/b18257

Hasan, R., Myagmar, S., Lee, A. J., & Yurcik, W. (2005). *Toward a threat model for storage systems*. 94–102.

Hassan, M., Ali, M. A., Bhuiyan, T., Sharif, M., & Biswas, S. (2018). Quantitative assessment on broken access control vulnerability in web applications. *Okt*.

Hill, E. (2025, July 11). Alleged Data Leak Hits Finastra, Provider to World's Largest Banks. *The National CIO Review*. https://nationalcioreview.com/articles-insights/extra-bytes/alleged-data-leak-hits-finastra-provider-to-worlds-largest-banks/

Hussain, S., Kamal, A., Ahmad, S., Rasool, G., & Iqbal, S. (2014). Threat modelling methodologies: A survey. *Sci. Int.(Lahore)*, *26*(4), 1607–1609.

Imperva. (2025, November 19). What is Threat Modeling | Guide to Security Risk Management | Imperva. *Learning Center*. https://www.imperva.com/learn/application-security/threat-modeling/

Jain, R. (n.d.). *Finastra Data Breach: Lessons from the 400GB Data Exposure Attack*. Retrieved October 25, 2025, from https://www.letsbloom.io/blog/finastra-data-breach-key-lessons-from-the-400gb-data-exposure-attack/

Jan, S., Khan, S. U., & Wahab, A. (2025). Access Restricted: A Study of Broken Access Control Vulnerabilities. *Archives of Advanced Engineering Science*, 1–6.

Jan, S., Panichella, A., Arcuri, A., & Briand, L. (2017). Automatic generation of tests to exploit XML injection vulnerabilities in web applications. *IEEE Transactions on Software Engineering*, *45*(4), 335–362.

Joshi, K., & Akhilesh, K. (2019). Role of cyber security in retail. In *Smart Technologies: Scope and Applications* (pp. 233–247). Springer.

*JSON Injection*. (n.d.). Retrieved October 25, 2025, from https://www.invicti.com/learn/json-injection

Kala, N., & Balakrishnan, M. (2019). Cyber preparedness in maritime industry. *International Journal of Scientific and Technical Advancements*, *5*(2), 19–28.

Kent, K., & Souppaya, M. (2006). Guide to computer security log management. *NIST Special Publication*, *92*, 1–72.

Komaragiri, V. B., & Edward, A. (2022). AI-Driven Vulnerability Management and Automated Threat Mitigation. *International Journal of Scientific Research and Management (IJSRM)*, *10*(10), 981–998.

Kosh. (2025). *Password Reset Poisoning*. https://www.invicti.com/learn/password-reset-poisoning

Kour, R., Karim, R., & Thaduri, A. (2020). Cybersecurity for railways–A maturity model. *Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit*, *234*(10), 1129–1148.

Kour, R., Patwardhan, A., Thaduri, A., & Karim, R. (2023). A review on cybersecurity in railways. *Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit*, *237*(1), 3–20.

Kumar, B. (2019). Effective Approach Toward Intrusion Detection and Pretention Systems in Implementing Defense in Depth. *INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) CICTAB*, *7*(04).

Kumar, S., & Bansal, G. (2024). DIGITAL VULNERABILITIES: CYBERSECURITY THREATS IN INDIA'S DIGITAL TRANSFORMATION JOURNEY. *ShodhKosh: Journal of Visual and Performing Arts*, *5*(1), 704–710. https://doi.org/10.29121/shodhkosh.v5.i1.2024.3726

KumarShrestha, A., Singh Maharjan, P., & Paudel, S. (2015). Identification and illustration of insecure direct object references and their countermeasures. *International Journal of Computer Applications*, *114*(18), 39–44.

Levy, S. (1984). *Hackers: Heroes of the computer revolution* (Vol. 14). Anchor Press/Doubleday Garden City, NY.

Li, J. (2018). Cyber security meets artificial intelligence: A survey. *Frontiers of Information Technology & Electronic Engineering*, *19*(12), 1462–1474.

Long, N., & Thomas, R. (2001). Trends in denial of service attack technology. *CERT Coordination Center*, *648*(651), 569.

Lundgren, B., & Möller, N. (2019). Defining Information Security. *Science and Engineering Ethics*, *25*(2), 419–441. https://doi.org/10.1007/s11948-017-9992-1

*M7: Insufficient Binary Protections - OWASP Mobile Top 10 - Best Practices - ASPIA InfoTech*. (2023, December 8). https://aspiainfotech.com/2023/12/08/6373-insufficient-binary-protections/

Malik, V. (2025). *Insecure Deserialization | OWASP Foundation*. https://owasp.org/www-community/vulnerabilities/Insecure_Deserialization

Mamtora, R., Sharma, D., & Patel, J. (2021a). Server-Side Template Injection with Custom Exploit. *International Journal of Scientific Research in Science, Engineering and Technology*.

Mamtora, R., Sharma, D., & Patel, J. (2021b). Server-Side Template Injection with Custom Exploit. *International Journal of Scientific Research in Science, Engineering and Technology*.

*Mapping India's Cybersecurity Administration in 2025*. (n.d.). Carnegie Endowment for International Peace. Retrieved October 13, 2025, from https://carnegieendowment.org/research/2025/09/mapping-indias-cybersecurity-administration-in-2025?lang=en

Mateo Tudela, F., Bermejo Higuera, J.-R., Bermejo Higuera, J., Sicilia Montalvo, J.-A., & Argyros, M. I. (2020). On Combining Static, Dynamic and Interactive Analysis Security Testing Tools to Improve OWASP Top Ten Security Vulnerability Detection in Web Applications. *Applied Sciences*, *10*(24), 9119.

Maués, R. (2020, January 28). *Vulnerability Management Process, what is it?* Conviso AppSec. https://blog.convisoappsec.com/en/vulnerability-management-process-what-is-it/

Mead, N. R., Shull, F., Vemuru, K., & Villadsen, O. (2018a). A hybrid threat modeling method. *Carnegie MellonUniversity-Software Engineering Institute-Technical Report-CMU/SEI-2018-TN-002*.

Mead, N. R., Shull, F., Vemuru, K., & Villadsen, O. (2018b). A hybrid threat modeling method. *Carnegie MellonUniversity-Software Engineering Institute-Technical Report-CMU/SEI-2018-TN-002*.

Mehta, J. (2023a, February 8). Top Software Vulnerabilities in 2024—How to Identify and Prevent the? *SignMyCode - Blog*. https://signmycode.com/blog/how-to-identify-and-prevent-the-top-software-vulnerabilities-in-2023

Mehta, J. (2023b, February 8). Top Software Vulnerabilities in 2024—How to Identify and Prevent the? *SignMyCode - Blog*. https://signmycode.com/blog/how-to-identify-and-prevent-the-top-software-vulnerabilities-in-2023

Merlano, C. (2024). Enhancing cyber security through artificial intelligence and machine learning: A literature review. *Journal of Cybersecurity*, *6*, 89.

Microsoft. (2024). *What Is Vulnerability Management? | Microsoft Security*. https://www.microsoft.com/en-us/security/business/security-101/what-is-vulnerability-management

Mishra, A., Alzoubi, Y. I., Gill, A. Q., & Anwar, M. J. (2022). Cybersecurity enterprises policies: A comparative study. *Sensors*, *22*(2), 538.

Mishra, A., Gupta, B. B., Perakovic, D., & Zhou, Z. (2021). *Defensive approach using blockchain technology against distributed denial of service attacks*. International Conference on Smart Systems and Advanced Computing (Syscom-2021).

Mishra, S. (2023). Exploring the impact of AI-based cyber security financial sector management. *Applied Sciences*, *13*(10), 5875.

Mobile Top 10, O. (2024). *OWASP Mobile Top 10 | OWASP Foundation*. https://owasp.org/www-project-mobile-top-10/

Mohammed, K. H., Hassan, A., & Yusuf Mohammed, D. (2018). *Identity and Access Management System: A Web-Based Approach for an Enterprise*.

Nagori, R. (n.d.). *Threat Modeling*. Retrieved October 24, 2025, from https://interview.rajanagori.in/threatmodel/

Naila, N. (2024). *Threat modelling technique for GDPR compliance based on logical reasoning*.

NDTV World. (2025). *Deloitte's AI Fallout Explained: The $440,000 Report That Backfired*. NDTV. https://www.ndtv.com/world-news/deloittes-ai-fallout-explained-the-440-000-report-that-backfired-9417098

Nick, T. G., & Campbell, K. M. (2007). Logistic regression. *Methods in Molecular Biology (Clifton, N.J.)*, *404*, 273–301. https://doi.org/10.1007/978-1-59745-530-5_14

Nikkel, B. J. (2014). Fostering incident response and digital forensics research. *Digital Investigation*, *11*(4), 249–251.

*NoSQL Injection*. (n.d.). Retrieved November 19, 2025, from https://www.invicti.com/learn/nosql-injection

Orlando, K. R. (2021). *Automating Virtual Patching via Application Security Testing Tools*.

OWASP, A. S. (2025). *OWASP Top 10 API Security Risks – 2023—OWASP API Security Top 10*. https://owasp.org/API-Security/editions/2023/en/0x11-t10/

OWASP, W. A. (2025). *A02 Cryptographic Failures—OWASP Top 10:2025 RC1*. https://owasp.org/Top10/A02_2021-Cryptographic_Failures/

Papazafeiropoulou, A., & Spanaki, K. (2016). Understanding governance, risk and compliance information systems (GRC IS): The experts view. *Information Systems Frontiers*, *18*(6), 1251–1263.

Patil, shubham. (2025, June 17). OWASP M2: Inadequate Supply Chain Security Explained. *SecureLayer7 - Offensive Security, API Scanner & Attack Surface*

*Management*. https://blog.securelayer7.net/owasp-m2-inadequate-supply-chain-security/

Peraković, D., Periša, M., & Cvitić, I. (2015). Analysis of the IoT impact on volume of DDoS attacks. *XXXIII Simpozijum o Novim Tehnologijama u Poštanskom i Telekomunikacionom Saobraćaju–PosTel*, *2015*, 295–304.

Peraković, D., Periša, M., Cvitić, I., & Zorić, P. (2021). Artificial intelligence application in different scenarios of the networked society 5.0 environment. *Zbornik Radova Trideset Devetog Simpozijuma O Novim Tehnologijama U Poštanskom I Telekomunikacionom Saobraćaju–Postel 2021*.

Ponta, S. E., Plate, H., & Sabetta, A. (2020). Detection, assessment and mitigation of vulnerabilities in open source dependencies. *Empirical Software Engineering*, *25*(5), 3175–3215.

Portswigger. (n.d.). *Web LLM attacks | Web Security Academy*. Retrieved October 25, 2025, from https://portswigger.net

Pranczk, K. (2024, April 17). Web API Security Champion: Broken Object Level Authorization (OWASP TOP 10). *DevSec Blog*. https://devsec-blog.com/2024/04/web-api-security-champion-broken-object-level-authorization-owasp-top-10/

Racz, N., Weippl, E., & Seufert, A. (2010). *A frame of reference for research of integrated governance, risk and compliance (GRC)*. 106–117.

Randori. (2022, February 10). The State of Attack Surface Management 2022 [Https://info.randori.com/hubfs/State%20of%20ASM%20Report.pdf]. *The State of Attack Surface Management 2022*. https://info.randori.com/hubfs/State%20of%20ASM%20Report.pdf

Raza, M. (2025). *Threat Actors: Common Types & Best Defenses Against Them*. Splunk. https://www.splunk.com/en_us/blog/learn/threat-actors.html

Rieck, K., Holz, T., Willems, C., Düssel, P., & Laskov, P. (2008). *Learning and classification of malware behavior*. 108–125.

Sarmah, A., Sarmah, R., & Baruah, A. J. (2017). A brief study on cyber crime and cyber laws of India. *International Research Journal of Engineering and Technology (IRJET)*, *4*(6), 1633–1640.

Saxena, N., Hayes, E., Bertino, E., Ojo, P., Choo, K.-K. R., & Burnap, P. (2020). Impact and key challenges of insider threats on organizations and critical businesses. *Electronics*, *9*(9), 1460.

Saxena, P., Kotiyal, B., & Goudar, R. (2012). A cyber era approach for building awareness in cyber security for educational system in India. *International Journal of Information and Education Technology*, *2*(2), 167.

Schrader, D. (n.d.). *An Overview of the MGM Cyber Attack*. Retrieved October 25, 2025, from https://netwrix.com/

Senapati, M. (2024, October 5). Understanding Injection: A Critical Vulnerability in Web Security. *Medium*. https://medium.com/@mrutunjayasenapati0/understanding-injection-a-critical-vulnerability-in-web-security-7c5c5b692958

Shah, V. (2022, August 16). *Why SMEs need to make cybersecurity their top priority*. https://yourstory.com/smbstory/why-smes-need-to-make-cybersecurity-priority

Sharma, N., & Sharma, D. (2018). Rising toll of frauds in banking: A threat for the Indian Economy. *Journal of Technology Management for Growing Economies*, *9*(1), 71–88.

Shevchenko, N., Chick, T. A., O'riordan, P., Scanlon, T. P., & Woody, C. (2018). *Threat modeling: A summary of available methods*.

Singh, C., Pattanayak, D., Dixit, D. S., Antony, K., Agarwala, M., Kant, R., Mukunda, S., Nayak, S., Makked, S., & Singh, T. (2016). *Frauds in the Indian banking industry*.

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, *104*, 333–339.

Soni, P., Pradhan, J., Pal, A. K., & Islam, S. H. (2022). Cybersecurity attack-resilience authentication mechanism for intelligent healthcare system. *IEEE Transactions on Industrial Informatics*, *19*(1), 830–840.

Stytz, M. R. (2004). Considering defense in depth for software applications. *IEEE Security & Privacy*, *2*(1), 72–75.

Thevarmannil, M. (2023, February 6). 10 Types of Threat Modeling Methodology To Use in 2025. *Practical DevSecOps*. https://www.practical-devsecops.com/types-of-threat-modeling-methodology/

Ticketmaster. (2025). *Ticketmaster Data Security Incident*. Ticketmaster Help. https://help.ticketmaster.com/hc/en-us/articles/26110487861137-Ticketmaster-Data-Security-Incident

TraceSecurity. (2025). *The Ticketmaster Databreach: Explained*. TraceSecurity. https://www.tracesecurity.com/blog/news/the-ticketmaster-databreach-explained

*Understanding AAA Frameworks in Cybersecurity: Authentication, Authorization, and Accounting*. (n.d.). Retrieved October 16, 2025, from https://www.linkedin.com/pulse/understanding-aaa-frameworks-cybersecurity-accounting-sohail-%D1%85%D0%B0%D0%BA%D0%B5%D1%80--llxic

Vaka, P. R. (2025a). CYBER SECURITY IN THE RETAIL INDUSTRY. *International Research Journal Of Modernization In Engineering Technology And Science*, *7*(2), 939–946.

Vaka, P. R. (2025b). CYBER SECURITY IN THE RETAIL INDUSTRY. *International Research Journal Of Modernization In Engineering Technology And Science*, *7*(2), 939–946.

VentureBeat. (2022, April 25). Trend Micro launches new attack surface management platform [Https://venturebeat.com/business/trend-micro-launches-new-attack-surface-management-platform/]. *Trend Micro Launches New Attack Surface Management Platform*. https://venturebeat.com/business/trend-micro-launches-new-attack-surface-management-platform/

Verma, A., Singh, A. K., Shukla, D., Sharma, R., & Laroiya, S. (n.d.). Xploitguard: Automated Vulnerability Scanning Tool. *Available at SSRN 5230287*.

Verma, H. C., Srivastava, S., Ahmed, T., & Usmani, N. A. (2023). Cyber threats in agriculture and the food industry: An Indian perspective. In *Advances in cyberology and the advent of the next-gen information revolution* (pp. 109–122). IGI Global.

Vielberth, M., Böhm, F., Fichtinger, I., & Pernul, G. (2020). Security operations center: A systematic study and open challenges. *IEEE Access*, *8*, 227756–227779.

Walkowski, M., Oko, J., & Sujecki, S. (2021). Vulnerability management models using a common vulnerability scoring system. *Applied Sciences*, *11*(18), 8735.

Watson, R. (2015). Quantitative research. *Nursing Standard (2014+)*, *29*(31), 44.

*What are Security Controls? | IBM*. (2021, October 15). https://www.ibm.com/think/topics/security-controls

*What are the Types of Cyber Threat Actors?* (n.d.). Retrieved October 16, 2025, from https://www.sophos.com/en-us/cybersecurity-explained/threat-actors

*What is CIA Triad?* (19:12:09+00:00). GeeksforGeeks. https://www.geeksforgeeks.org/computer-networks/the-cia-triad-in-cryptography/

*What Is Hacktivism? Meaning, Types, and More*. (n.d.). Fortinet. Retrieved October 23, 2025, from https://www.fortinet.com/resources/cyberglossary/what-is-hacktivism

*What is OWASP and why is it important?* (n.d.). Retrieved November 17, 2025, from https://humanize.security/blog/cyber-awareness/what-is-owasp-of-2022

Wu, A., Feng, Z., Feng, R., Xing, Z., & Liu, Y. (2025). Rethinking Broken Object Level Authorization Attacks Under Zero Trust Principle. *arXiv Preprint arXiv:2507.02309*.

Xiong, W., & Lagerström, R. (2019). Threat modeling–A systematic literature review. *Computers & Security*, *84*, 53–69.

Zaidan, M., Noeraini, F., Sari, Z., & Akbi, D. R. (2023). Website vulnerability analysis of AB and XY office in East Java. *JITEKI: Jurnal Ilmiah Teknik Elektro Komputer Dan Informatika*, *9*(2), 455–492.

ZoeniX ), M. H. | (. (2025, February 26). OWASP Mobile Top 10 | M1: Improper Credential Usage 🔓. *Medium*. https://z0enix.medium.com/owasp-mobile-top-10-m1-improper-credential-usage-bf6ee99eed69