Assessment & Remediation of Common Human Errors Leading to Potential Data Loss from an Air-Gapped Network

By

Rizwan Ahmed Shaikh

00000281277

Submitted to the Faculty of Information Security Department, Military College of Signals, National University of Sciences and Technology, Islamabad in partial fulfillment of the requirements for the degree of Masters in Information Security

October 2020

Thesis Acceptance Certificate

Certified that final copy of MS / MPhil thesis, written by **Rizwan Ahmed Shaikh**, Registration No. **00000281277**, of **Military College of Signals**, has been vetted by undersigned, found complete in all respect as per NUST Statutes/Regulations, is free of plagiarism, errors and mistakes and is accepted as partial fulfillment for award of MS / MPhil degree. It is further certified that necessary amendments as pointed out by GEC members of the student have been also incorporated in the said thesis.

Signature: _____

Name of Thesis Supervisor: (**Brig Dr. Imran Rashid, Ph.D.**)

Date: _____

Signature (HOD): _____

Date: _____

Signature (Dean / Principal): _____

Date: _____

Declaration

I hereby declare that no portion of the work presented in this thesis has been submitted in support of another award or qualification either at this institution or elsewhere.

_____

Rizwan Ahmed Shaikh

Dedication

"In the name of Allah, the Most Beneficent, the Most Merciful"
Read in the name of your Lord who created. Created man from a clinging substance.
Read, and your Lord is the Most Generous. Who taught by the pen.
Taught man that which he knew not *(Al- 'Alaq 1:5)*

With immense blessings of Allah, the Almighty, I dedicate this thesis to my parents, siblings, better-half, and especially my teachers whose unflinching trust, help, support and prayers paved the way for me in the timely completion of this work.

Acknowledgements

First and foremost, all praises and gratitude to Allah, the Almighty, for giving me the strength to keep pursuing my research-work despite various challenges and odds.

I would like to express my sincere and deep gratitude to my research supervisor, Brigadier Dr. Imran Rashid, Ph.D., Chief Instructor (Engineering Wing); for giving me the opportunity and providing invaluable guidance throughout this research. His dynamism, vision, sincerity, and motivation were vital for the completion of this tedious task. It was indeed a great privilege and honor to work and study under his noble guidance and persistence help.

I would like to express my earnest reverence to Dr. Haidar Abbas, Ph.D., Head of Department Research Wing, and Major Sohaib Ahmed Khan Niazi; for being an important part of my Research Supervisory Committee. Their scholarly guidance, inspiration, patience, and continuous support have been very meaningful for the successful completion of my research.

I am also thankful to the Military College of Signals and the National University of Sciences and Technology for providing me with a chance to help achieve excellence by being associated with these prestigious institutions.

Finally, I would like to express my appreciation and gratitude to all the people who have provided me valuable support to my study and whose names I couldn't bring to memory.

Abstract

Many organizations process and store classified data within their computer networks. Owing to the value of data that they hold; such organizations are more vulnerable to targets from adversaries. Accordingly, the sensitive organizations resort to an 'air-gap' approach on their networks, to ensure better protection. However, despite the physical and logical isolation, the attackers have successfully manifested their capabilities by compromising such networks; examples of Stuxnet and Agent.btz in view. Such attacks were possible due to the successful manipulation of the human being. It has been observed that to build up such attacks, persistent reconnaissance of the employees, and their data collection often forms the first step. With the rapid integration of social media into our daily lives, the prospects for data-seekers through that platform are higher. The inherent risks and vulnerabilities of social networking sites/apps, such as WhatsApp, Facebook, LinkedIn, and Twitter, etc.; have cultivated a rich environment for foreign adversaries to cherry-pick personal information and carry out successful profiling of employees assigned with sensitive appointments. With further targeted social engineering techniques against the identified employees and their families, attackers extract more and more relevant data to make an intelligent picture. Finally, all the information is fused to design their further sophisticated attacks against the air-gapped facility for data pilferage. In this regard, the success of the adversaries in harvesting personal information of the victims largely depends upon the common errors committed by legitimate users while at workplace, in transit, and after their retreat. Such errors would keep on repeating unless these are aligned and mitigated keeping in view the underlying human behaviours and weaknesses.

Table of Contents

List of Figures

List of Tables

Acronyms

C&C …….	Command & Control
CD ……	Compact Disk
CIA-triad ……..	Confidentiality, Integrity, Availability
EM ……	Electromagnetic
FBI ……...	Federal Board of Investigation
GPS ……..	Global Positioning System
HMDs ……...	Head-Mounted Displays
HR ……	Human Resources
IEEE …….	Institute of Electrical and Electronics Engineers
I/O ……	Input/ Output
IR …….	Infrared
MCD ……	Mobile Computing Devices including Laptop, Smartphone, PDA, tablet, etc.
NADRA ……...	National Database and Registration Authority
OS ……	Operating System
OSN …….	Online Social Networks
PII …….	Personally, Identifiable Information
PDA ……..	Personal Digital Assistant
SIM ……..	Subscriber Identity Module
SMN …….	Social Media Network
SRK ……..	Skill-Rule-Knowledge

Chapter 1

Introduction

1.1 Overview

In today's modern times, data has replaced money as the most valuable asset for an organization or an individual. Financial assets can be redeemed, re-earned, and restored with time, whereas, valuable data once compromised will rarely come back to the owner in its original form with its confidentiality, integrity, and availability intact to its original version. Moreover, in the case of sensitive organizations where leakage of data has national consequences, any slight pilferage is considered as an excruciating loss. In this regard, concrete steps are taken by the national organizations to ensure the safety and security of the data, including the incorporation of air-gapped networks that physically isolates the internal organizational networks from the rest of the world.

1.2 Motivation & Problem Statement

The organizations have been following various security standards, while deploying subsequent technical controls, to mitigate the identified risks. When it comes to an air-gapped network, the existence of the air between the internal and outside networks is considered as the major guarantee for protection of classified data from pilferage. However, news of recent successful attacks and consequent data loss from the air-gapped networks (Natanz nuclear facility of Iran) reveal that technical controls alone do not provide due assurance against a data breach. Moreover, the human being working in the organization is considered as the weakest link in the chain of security. Since they also retain strong footprints online and on social media networks (SMN) in one form or another; any accidental slippage of even slight confidential information can lead to a big security risk, making the very isolation of air-gapped network questionable.

1.3 Research Objectives

The main objectives of this thesis are:

- Study and analyze the human mistakes of legitimate users of an organization that can undermine the air-gapped security and becomes potential for subsequent data loss.

- Propose a way forward to deter identified mistakes, and minimize the chances of a data breach from an air-gapped network.

1.4 Scope

The main focus of this research will be towards identifying and assessing the common mistakes of legitimate users vis-à-vis their weaknesses in psycho-social domains. Moreover, an elaborate study of the associated threats would also be carried out. It will be followed by a proposed way forward and a framework that would be helpful to deter the identified errors. The following limitations and assumptions will be kept in mind while carrying out research:

- Required physical isolation of the organization's internal network has been achieved.
- The required hard-core technical controls to safeguard air-gapped facilities have already been emplaced.
- The employee's mistakes are considered in their day-to-day routine lives besides their workplace / air-gapped facility, during their transit, and their online presence.

1.5 Contribution

The research will contribute in the following ways:

- Assist in formulating a ready-reckoner of common mistakes committed by the legitimate users in an organization vis-à-vis their corresponding security threats.
- Enable the policy-makers to refine their policies, and include the rarely-focused and complex perspective of human errors.
- Helpful for the recruiters and training-organizers to consider various psycho-social inclinations of the human resources (HR) while planning the course of their selection and training.
- Assist civil and military sensitive organizations having air-gapped networks to further enhance their security parameters by reviewing and updating their policies, and HR training procedures, in lines with the identified common mistakes of the legitimate users and their remedial measures.

1.6 Thesis Organization

The thesis is structured as follows:

- **Chapter 1** forms the introduction part of the thesis that highlights the problem statement, research objectives, thesis scope, and its contribution.
- **Chapter 2** highlights threats and attack vectors against an organization. The contents begin from a general threat landscape and proceed on to more specific attacks against the air-gapped networks with various examples.
- **Chapter 3** exclusively covers mobile computing devices including smartphones. It seeks to highlight the various components, their associated threats, and exploitation for data leakage.
- **Chapter 4** ponders some light on psycho-social aspects of human being, their behaviours, errors, and associated exploitation. It tries to touch upon human error classification and their possible mitigation process while highlighting principles of successful social engineering, and its various stages.
- **Chapter 5** is exclusively dedicated to the assessment of common human error of legitimate users. It divides the errors based upon the user's state/ presence – while at workplace, during transit, and after working hours. It also focuses on the errors committed during the use of the internet and Online Social Networks (OSN).
- **Chapter 6** proposes the way forward, keeping in view all the common errors by legitimate users that lead to potential data loss from air-gapped networks. The chapter extends requisite awareness measures for the employees to make use of while at workplace, during transit, and after working hours. The chapter ends by providing an extensive list of guidelines for social networking and online identity and data protection; for the employees, their families, and the organization.
- **Chapter 7** marks the concluding part of the thesis. It proposes a framework that relates the human error with human weaknesses, their associated threats followed by requisite mitigation measures.

Chapter 2

Threats & Attack Vectors Against an Organization

2.1 Introduction

In today's digital economy, the data has been assuming the status of the most valuable asset for an organization. Accordingly, a large amount of data is processed on daily basis at various data centers. The value of the processed data solely depends upon its values in CIA-triad i.e. Confidentiality, Integrity, and Availability. Accordingly, the threat-actor design all their attacks to affect the CIA-triad related to the data. In this regard, the existing threats are capitalized using various attack vectors. The following sections highlight the overall threat landscape while going into certain details to cultivate a baseline understanding of the situation.

2.2 General Threat Landscape

In modern times, the protection of the system and residing data is becoming an excessively challenging task. The development of sophisticated malware coupled with advanced attack techniques has allowed the adversary to design their attacks for their specific targets. Resultantly, an ever-increasing number of fissures in information security of business, government, and citizen's data have been reported by Symantec, FireEye, and Verizon.

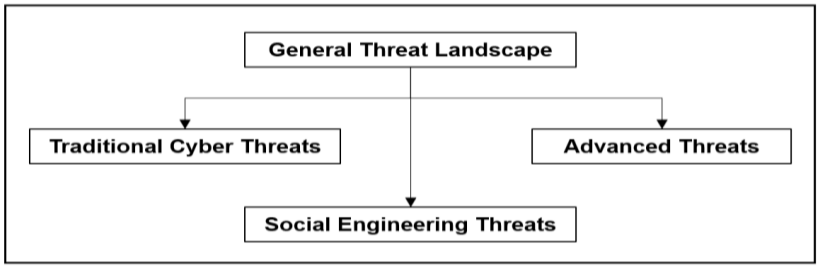

Figure 1: General Threat Landscape

2.2.1 Traditional Cyber Threats. Some of the traditional cyber threats are mentioned below:

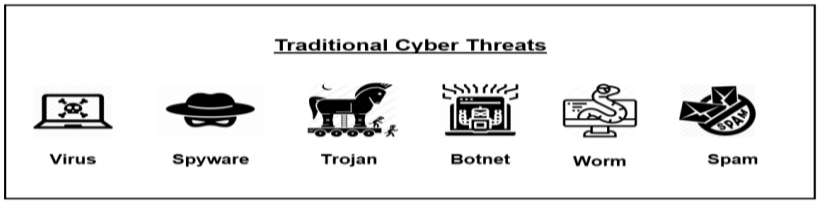

Figure 2: Traditional Cyber Threats

- **Computer Virus**. Primarily, a computer virus is a computer code that is aimed to get embedded with another computer file, such that, when executed it can replicate itself and get propagated on the host computer. There can be various objectives of designing a virus that include but not limited to infecting the host computer by corrupting files, stealing hard disk space, pocketing CPU time, key-logging to steal valuable information, and various other activities performed without the approval of a legitimate computer-user [1, p. 146].
- **Spyware**. It is a malicious program that has a one-point agenda that is to seek and exfiltrate user information without the user's knowledge or consent.
- **Worm**. It is a standalone malware that can replicate itself over the network. It harms the network bandwidth and acts as a lateral attack vector that can be used to exfiltrate data [2, p. 294].
- **Trojan**. It is a malicious program that masquerades itself to be a useful software application. A few of the methods by which it can be installed on a computer system are: by a spam email, social media application, or an online game.
- **Spam**. Spam is an act of spreading unsolicited and unrelated content. Usually, resorted upon for advertisement, it has been observed in several different domains, e.g. email, instant and web messaging, Internet Telephony, etc. [3].
- **Botnets and Cyber Crime Applications**. A botnet is a network of compromised computers that are remotely controlled and coordinated by bad actors to achieve the desired malicious purpose [2, p. 16]. The underlying objective could be the launching of distributed denial-of-service attack (DDoS), click fraud, spam attack, or simply renting out the bot services to other attackers to fit their design of attack. The host components of the bot network are compromised machines that are tricked to install Bot Agents on them and work under the overall control of a Bot Master. The Bot Agents act on the instructions of the Bot Master and executes the malicious tasks as and when communication between the two is established, and instructions are given [4].

2.2.2 Social Engineering Threats

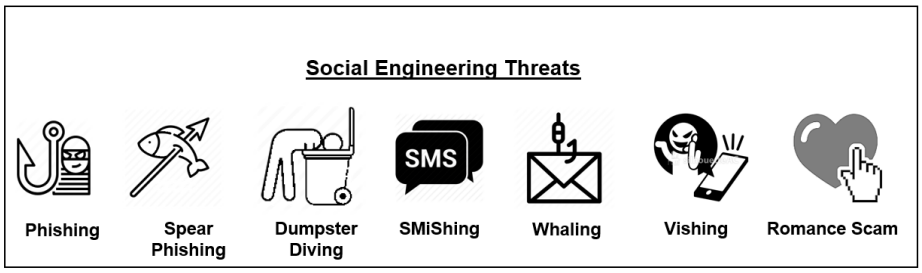

Figure 3: Social Engineering Threats

- **Phishing**. Masquerading as a trustworthy entity, and persuade the victim to willingly share classified information.
- **Spear-Phishing**. It is more focused against a specific individual e.g. an executive-level employee. Such attacks are usually targeted against executive-level employees. This attack technique is very popular among the attackers who hunt to acquire maximum information from government or military personnel.
- **SMiShing**. Tricking a person using messaging services and luring him into downloading a particular software (malware) onto their mobile device.
- **Whaling**. It is a kind of a spear-phishing attack that is directed against senior executives and other high-profile targets.
- **Sex-espionage**. "As long as there is espionage, there will be Romeos seducing unsuspecting Juliets (targets) with access to secrets." Markus Wolf [5]. In the prevailing hostile environment, security agencies often resort to illegal and unethical methods in the name of national security. Some of the methods are based on age-old techniques of emotional abuse to the persons subject to these activities [6]. Sex-espionage is one of them. In this regard, the victim is gradually approached through emotional and physical seduction with the promise of an intimate relationship. In this way, trust is gained followed by cultivating the victim for further espionage.

- **Sextortion**. The Federal Board of Investigation (FBI) defines sextortion as "a serious crime that occurs when someone threatens to distribute your private and sensitive material if you don't provide them with images of a sexual nature, sexual favors, or money" [7]. The sextortion happens when a person is seduced into sexual activities through online contact, while also recording it unknowingly for later use against them for money, goods, or other favours. In most of the cases, the victim caves on a demand to safeguard his repute and rapport in society. An infographic, as released by [8] reveals that an alarming 45 % of perpetrators actually carried out threats. Employees from sensitive organizations are attractive targets for this type of attack [9], because:
  - They often have to serve away from home and keep an online presence.
  - They are deemed to a higher standard of conduct, owing to their services and careers.
  - Their knowledge of the things might be of interest to adversaries.

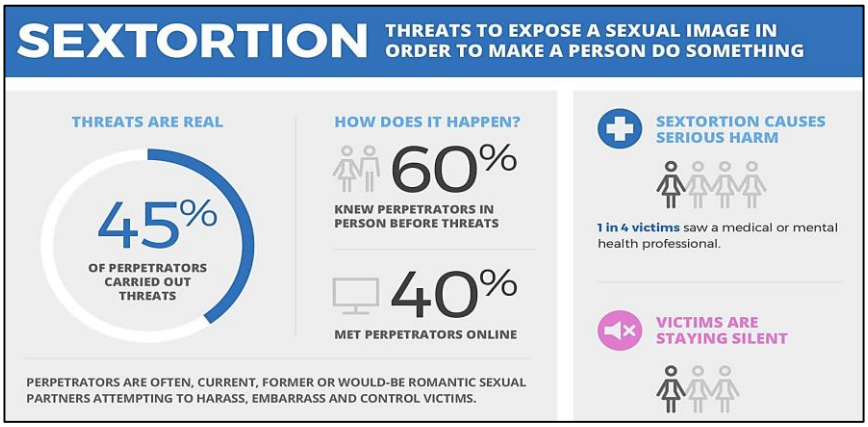

Figure 4: Sextortion - Threats are real

Figure Source: https://www.thorn.org/sextortion/

- **Romance Scam**. A romance scam occurs when a criminal adopts a fake online identity and gains a victim's confidence, affection, and trust. Later on, the scammer uses the illusion of a romantic or close relationship to manipulate and/or steal from the victim. The scam not only leaves a person with a monetary loss but also causes psychological issues [10]. The cybercriminals simply deceive human being by capitalizing upon their weaknesses.

- **Vishing**. Tricking a person into making a phone call to a particular number and reveal sensitive information.
- **Dumpster Diving**. A very useful technique that supports a social engineering attack. The attacker seeks to access the victim's garbage bins/ trash cans to find some documents or intelligible piece of information. It is a very low-tech way of getting information. However, it is often done in situations when the target is quite a high profile, and every single clue is essential. Examples of documents can be a chit having a password written on it, a routine work document, a copy of utility bills, a Compact Disk (CD), or any other paper containing sensitive information.

2.2.3 Advanced Threats

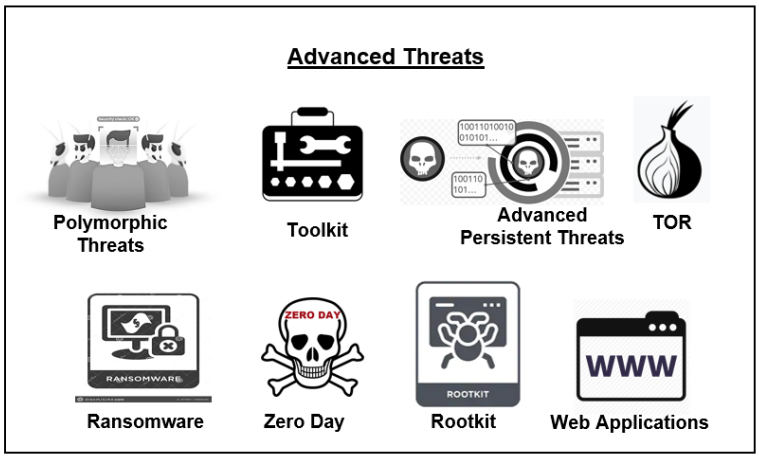

Figure 5: Advanced Threats

- **Polymorphic Threats**. It is a kind of a cyber-attack in which a virus, worm, spyware or Trojan keeps changing its forms (morphs). It allows it to have a unique signature and makes it significantly difficult to detect it using a signature-based defense mechanism.
- **Blended Threats**. The cyber-attack in which multiple types of malware elements are combined employing multiple attack vectors. It is done to achieve a greater degree of damage to the target. Examples include the Nimda virus, Code Red virus, Conficker virus [2, p. 295].

- **Zero-day attacks**. Zero-day vulnerabilities are in-built vulnerabilities that are presented in the hardware and software including Operating System (OS). The attackers invest quite a huge amount of time, in finding it out because, it opens a wide arena for their exploitation, as long as the vulnerability is not identified and patched by the victim. After making the most of the vulnerability, the attackers even sell it out to other cyber-criminals to earn financial benefits.
- **Advanced Persistent Threats (APTs)**. Not primarily designed to cause damage, the APTs are resorted to acquire maximum information or even at times, modify certain data. These are very sophisticated network attacks, in which the unauthorized person seeks to maintain his presence in the networks while staying undetected for a substantial period. In most of the cases, the spear-phishing attacks help the attackers to seek this presence. As an example of APT, in 2012, a famous attack named "Flame" was successfully launched against the Iranian oil terminals to collect the required information and develop cyber-sabotage-programs to hamper Iran's capability to attain nuclear weapons [11, p. 20]. Cole reports that the APT attack is not based on an individual or small hacker cell but a well-structured organization, having a very-well articulated attack methodology and sophisticated tools. The APTs have been using encryption mechanism for data exfiltration via tunneling, thus turning our biggest strength into our weakness, since most of the security devices are not capable of reading encrypted packets.
- **Ransomware**. Just in lines with the APTs, the attackers have been utilizing encryption mechanisms to encrypt and deter legitimate users to access their own data unless the victims pay the extortion fee, and get their data decrypted. It is achieved through the installation of ransomware on the victim's computer. CryptoLocker, a substituted name for Ransomware is one of the few mainstream attacks where the security companies are tested to the limits in their skills and computational resources. However, as Kaspersky Lab in North America reports, no effective cure for the CryptoLocker virus exists [12].

- **Rootkit**. A rootkit is primarily a set of administrator-level tools that allow root access of a computer system to the attacker. Presently, the term root-kit has merged into the term malware that has the root-level permissions on the system. The attackers design very sophisticated root-kit malware which is coded to take complete control of the computer's Operating System and its attached hardware, while hiding its traces in the system. The most successful example of a rootkit in recent times is Stuxnet that permitted the attackers to target Iran's uranium enrichment facility in Natanz, Iran [13].
- **Toolkits**. These are the software programs designed for malicious purposes for onward use by both novice and experienced cyber-criminals. Being fully customizable, the toolkits help them to launch an attack against networked systems. Toolkits are primarily focused on the stealing of banking information to seek financial gains. A prominent example is "Zeus" that reportedly helped cyber-criminals to acquire $70 million from online banking and trading accounts in 18 months. Besides, other prominent prevalent toolkits are MPack, Neosploit, Zeus, Nukesploit, P4ck, Phoenix, etc. [2, p. 14].
- **TOR (The Onion Router) and the Deep Web**. TOR is an internet networking protocol, aimed to conceal its user's identity and their online activity from surveillance and traffic analysis by separating identification and routing information. The involvement of underlying encryption layers and bouncing of the traffic from one node to another makes the user activities significantly anonymous. The concept of the Deep Web also evolved due to the complexity of the TOR protocol in anonymizing internet traffic. The dark side of the Deep Web appears when the users resort to criminal activities, capitalizing on the anonymity it offers. Accordingly, there exist illegal markets that provide a platform for users to sell and purchase illegal drugs, weapons, pornographic material, etc. However, the worst of all appears when a new scale of terrorism vulnerabilities are floated with the sale and distribution of cyber weapons. Thus, TOR provides a suitable place for cybercriminals to engage in illicit deals and exploit the vulnerabilities of the adversary.

- **Web Applications**. Web applications carry along with them several vulnerabilities that need adequate attention. Some of the vulnerabilities include: SQL (Structured Query Language) injection, Cross-site scripting, Information leakage, Improper coding practice and error handling, Lack of suitable cryptographic storage leading to insecure storing of user data. The HP security teams, go on to state: "In fact, the lack of secure programming and IT security best practices only serve as an enabler for the proliferation of the malware" [14]. The claim is made on the grounds of the continuous rise of Internet security threats against web applications with greater sophistication.

2.3 Attacker's Need for Information

The one item absolutely required for the attacker before planning and designing any exploit is the information about the victim. In the case of interconnected computer systems, such information would be extracted through various preliminary probing attacks against the organization networks. The typical method includes reconnaissance for probing of IP addressing schemes, scanning for open network ports, gaining access at the network, OS, and application level, the discovery of vulnerabilities in the networks, carrying out the exploitation while hiding the tracks.

However, the same leverage is not available to the attacker in the case of an air-gapped system, since the network stays isolated, and not connected through the internet. In this scenario, the attacker resorts to the social engineering techniques to draw maximum information about the targeted organization. It is done by reaching out to targeted employees and tricking them to install malicious applications on their personal devices which are connected to the internet.

The attacker seeks to maintain their presence in employee's computer systems to exfiltrate all the relevant information through credible documents that reside on them. The attackers also capitalize on the potentials of social media networks and gather all the publicly available information about the employees of targeted organizations to create a fairly intelligible picture. Thus, fusing all the information, the attacker designs his attacks. Hence, the overarching reality is: "whether you are an individual, small company, a major corporation, government organization, or university, you will be targeted and you will be attacked" [15].

2.4 Possible Attack Methodology against an Organization

By virtue of its disconnection from the rest of the internet, the air-gapped networks are deemed safe from external attacks. Nevertheless, there can still be instances where the air-gap is bridged for some time by the adversary, and the network is compromised with the loss of data. Since the job requires physical access to the facility at least for ones, it is achieved by capitalizing upon the mistakes of innocent employees. The simplest and most straight-forward way to cause infection in the air-gap network is through the connection of the infected USB. The following figure highlights the possible steps that are often used by the attackers to breach data from an air-gap network [16].

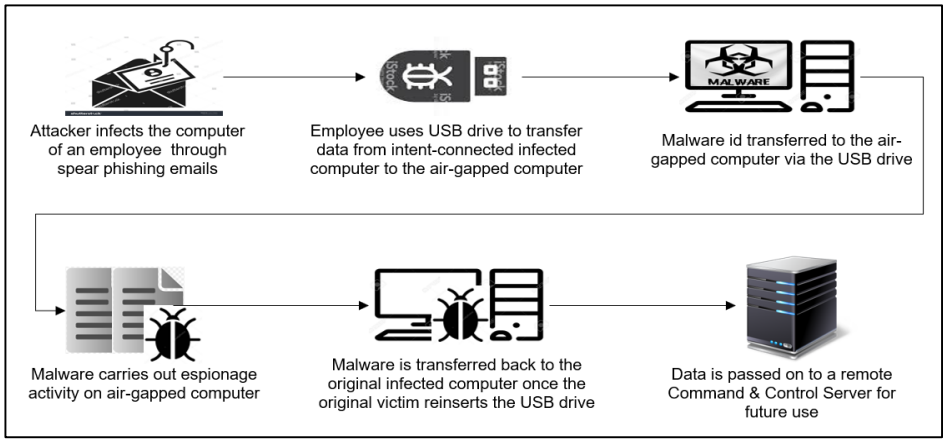

Figure 6: Possible Steps to Breach Air-Gapped Networks

According to Thomas A. Johnson, the general attack methodology against air-gapped systems dictates that it should be carried out in 6x stages [2, p. 292]:

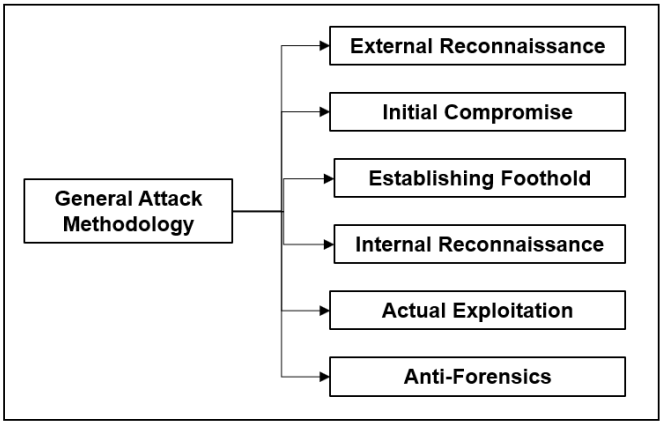

Figure 7: General Attack Methodology

2.4.1 External Reconnaissance. It forms the very first step in general attack methodology. The attacker seeks to collect the maximum possible information of the potential target, making use of all the traditional and advanced attacking tools. In this regard, a very targeted approach is used to hook the employees of the potential target including senior leaders to administrative staff using social engineering techniques. It is done to identify the human resource hierarchy of the target organization with explicit personal information of their employees.

2.4.2 Initial Compromise. In this stage, the attacker gains access to the system. A variety of methods can be used to achieve an initial compromise, including bribing, blackmailing, or otherwise compromising an insider; making him install the malware on the system, and establish a connection to the remote command & control (C&C) server.

2.4.3 Establishing Foothold. In this stage, the attackers seek to attain administrative level access in the compromised system using stealthy malware that stays undetected by host-based and network-based safeguards. It enables them to stay stealthily inside the compromised networks.

2.4.4 Internal Reconnaissance. After establishing a foothold, the attackers try to collect lateral information of the networks of surrounding infrastructure, trust relationships, and the Windows domain structure. In most of the case, the attackers typically cultivate additional backdoors during this phase. This is done to regain network access, should the primary backdoor gets failed.

2.4.5 Actual Exploitation. When the attackers have gained a foothold and preserved valuable information of the network, there comes the time when actual exploitation of the system takes place. This phase typically depends upon the actual objectives of compromising an organization system. Usually, attackers try to locate and extract important confidential data from the system while maintaining their presence [17].

2.4.6 Anti-forensics. This is one of the most important stages of the overall attack methodology. Besides carrying out the actual exploitation of the system, the primary concern of the attacker is to maintain his presence undetected. In this regard, the attackers have to take necessary safeguards as part of anti-forensics measures to cover their tracks and avoid unnecessary alarm and subsequent detection [18].

2.5 Global Data Breaches and Cyber-Espionage Operations

A data breach operation is defined as a confirmed incident in which the data has been accessed and/or disclosed by an unauthorized entity in an unauthorized manner. The data usually contains the information that is sensitive, confidential, and/or protected in nature including personal health information (PHI), personally identifiable information (PII), intellectual property of an individual, and trade secrets of the organization. There are known attacks in the cyber world that have been launched to carry out reconnaissance of the targeted victim, as stated below:

2.5.1 The Red October. The Red October, also known as "Rocra" has inherited its name from Tom Clancy's action/thriller film "Hunt for Red October". According to Kaspersky Lab reports, "a very high-level cyber-espionage campaign has successfully infiltrated computer networks at diplomatic, governmental, trade & commerce, nuclear energy and scientific research, aerospace, and military organizations" [19]. The report further highlights that the number of victim countries is around 69 with their thousands of compromised devices [19]. The primary objective of the attack is to gather data and intelligence from mobile devices, computer systems, and network equipment. The data include files, emails, passwords for devices, key-strokes, screenshots, and user's browsing history from various web browsers. Besides that, the underlying malware takes care of mobile phone data pilferage and seeks to draw contacts, call histories, calendars, text messages, and browsing histories from various smartphones.

What makes Rocra so sophisticated is its multi-functional platform that includes several extensions and malware designed to automatically adjust to different configurations.

2.5.2 Operation Hangover. Operation Hangover has been identified as a persistent effort of cyber-espionage activity originated from India. The primary objectives of this long-running, global Command & Control (C&C) network appear to be surveillance and exfiltration of national security information relevant to India, while also engaging in industrial espionage from the targeted countries. Security researchers at security firm Norman Shark, Norway, established that "major targets of the operation remained government, military, and civilian organizations of Pakistan, Iran, China, and the US" [20].

The analyses and detection process of the underlying malware was started when the analysts investigated Norwegian Telecommunication company "Telenor", operating in Pakistan, for its reported spear-phishing attacks. Later on, it was established that it was an ongoing large-scale cyberespionage operation of Indian origin that had been active for almost three years. The operation was mainly conducted by using remote code execution vulnerabilities in the Windows common controls (CVE-2012-0158), Internet Explorer (CVE-2012-4792), and Java (CVE-2012-0422).

The primary attack vector, as established in the investigation, was highly targeted social engineering tactics making use of spear-phishing against carefully-selected individuals. In this regard, many decoy files and websites were crafted to lure the potential victims to click on their place of choosing, leading to the invocation of the underlying malware.

2.5.3 The Epic Turla operation. "Turla also is known as Snake or Uroburos" [21] is one of the most sophisticated campaigns of cyber espionage. According to a research of Kaspersky Lab "Epic" is the initial stage of the Turla victim infection mechanism. The potential targets of the "Epic" include government agencies, intelligence agencies, military, foreign embassies, education, and research organizations, and pharmaceutical corporations of more than 45 countries of the world. As the G Data's Red Paper highlights in their report that "such kind of sophisticated software is quite expensive to be used just by a group of common hackers". They also point out the strong indicators that suggest the similarities between Agent.btz and Uroburos framework, connecting its ties with a national-level intelligence agency. [22]. The underlying methodology adopted by the attackers is to exploit vulnerabilities in Adobe PDF by using spear-phishing emails, social engineering tricks to make the user install malware that comes with .SCR extension, and watering hole attacks on commonly visited websites by potential victims using Java Exploits. After the initial compromise "Epic", a backdoor immediately connects to the C&C server for onward "Turla" operation. The attacker then delivers and executes pre-configured batch-files on the victim's computer to carry out espionage tasks using keylogging, DNS query, screen-capturing, etc. The sophisticated operation that finds its root well before the year 2014, still exists with its might with some changes in the payload, to avert detection, since the attackers have replaced Skipper with NetFlash for connectivity with the victim [23].

2.6 Attacks examples against Air-gapped Networks

The attack against air-gapped networks is indeed a very complex and challenging task. The key questions, an attacker address, before launching any of the attacks are:

- How would the malware be placed in the air-gapped network?
- How would the malware get commands while being in an air-gapped network?
- How would the attacker get acknowledgments or receive data from the air-gapped network?

Although the local presence of the malware in the network is the very first part, the attacker may rely on either of a deceived insider, compromising a malicious insider, or a supply chain attack. A few of the examples are stated in subsequent sections:

2.6.1 Stuxnet. Stuxnet is a classic example of a sophisticated and malicious computer program, targeted against technically highly secure Supervisory Control and Data Acquisition (SCADA) systems that are configured to control and monitor specific industrial processes. Being discovered in June 2010, it successfully targeted and adversely affected Iran's nuclear facility at Natanz. The worm didn't require any internet connection, rather it exploited already existing four zero-day vulnerabilities in Windows Operating System at that time. However, the primary technique of bridging the air-gap was through the connection of a compromised USB to the air-gapped system. In this regard, an insider employee was deceived to connect the infected USB device to the system, and the rest of the job was done by the worm itself. The worm was designed to target only Siemens SCADA systems, that are responsible to control and monitor industrial processes. Stuxnet infected the programmable logic controllers (PLCs) and reprogrammed those to change the rotational speed of the connected motors, causing severe damage to the controllers handling around 1,000 centrifuges at the facility [24].

2.6.2 Brutal Kangaroo. It is a tool suite for Microsoft Windows that is used by the CIA to target closed networks by jumping airgap using thumb-drives, as pointed out in Vault 7 Leaks of WikiLeaks [25]. The leak elaborates working of the Brutal Kangaroo and mentions that it creates a custom covert network within the target closed network that provides functionality for executing surveys, directory listings, and arbitrary executables.

The Brutal Kangaroo begins its infection through an internet-connected computer within the organization (referred to as a *primary host*) and installs malware on it. The infection is transferred to a USB that gets connected to the primary host. In case the thumb-drive is used to transfer data from internet-connected and air-gapped systems, the infection is propagated to the air-gapped network and seeks all the valuable information. The same is stored in USB for onward exfiltration whenever the USB is connected to an internet-connected computer.

2.6.3 **Agent.btz**. This attack finds its traces to the year 2008 when the United States sensitive air-gapped computers were attacked by Agent.btz malware. The attack methodology was simple, wherein the infected flash drives were dropped in the parking area of the Department of Defense facility in their Middle Eastern base. Just when the infected USB flash drive was picked up and attached to the computer networks at United States Central Command, the malware started spreading to other systems. The malware possessed the capabilities to scan computers for the data, open various backdoors, and exfiltrate the data through those backdoors to a remote C&C server. After discovering the existence of worm in their networks, Pentagon spent good about 14 months cleaning it from their military networks. To preclude its further spread, the authorities at Pentagon banned USB flash drives while also disabling the Windows autorun feature.

2.6.4 **Cycldek**. Cycldek (also known as Goblin Panda and Conimes) is considered to be a China-based threat actor that targets aerospace, defense, energy, food, tobacco, government, and marine services of countries in South-East Asia especially Thailand, Vietnam, and Laos. It surfaced in the year 2017 as a first detected case, as blogged by Fortinet [26], according to which the malware can harvest screenshots, user's key-logs, and can also take control of the machine via a remote shell.

The attack begins with the creation of a politically-themed RTF document with an 8.t document builder and sent as a phishing email to the victims. The document is bundled with 1-day exploits that include CVE-2012-0158, CVE-2017-11882, and CVE-2018-0802 [27]. Upon execution, the document acts as a dropper for malicious files, legitimately signed with some AV product application (such as qcConsol, McAfee's QuickClean utility, and Avast's remediation service, etc.) to avoid suspicion and detection.

After the connection between the victim and remote server gets fully established, the final payload known as "NewCore" is pushed onto the victim and run in the memory. However, in the latest mutants of the malware, it is revealed that a new tool "USBCulprit" is being used that relies on USB media. This evolution is suggestive of the fact that attackers intend to exfiltrate important data of the victim through data stealing and lateral movement by jumping the air-gapped networks.

2.6.5 Indian Navy air-gapped computers. According to the reports [28], a sophisticated attack that allegedly used a USB vector breached the computers of the Indian Navy's Eastern Naval Command. Being attributed to Chinese hackers, the attack bridged their air-gapped network, leading to leakage of confidential information abroad.

2.6.6 DTrack RAT attacked Kudankulam (India). In September 2019, India's Kudankulam Nuclear Power Plant (KKNPP), located at Tirunelveli district, Tamil Nadu; came under cyber-attack. The malware, called "DTrack" is allegedly developed by a North Korean hacker group called Lazarus. Primarily designed to extract data such as keylogging, browser history, IP hosts, running processes, and all files on a computer; the malware sought domain controller-level on a server computer [29]. Resultantly, the air-gapped systems at the facility were breached, as also confirmed by the Nuclear Power Corporation of India Limited (NPCIL) – the governing body for nuclear power plants in India [30].

2.7 Research - Compromising Air-Gapped Networks Through Covert Channels

The researchers have been working on covert channels to discover ways and means to jump the air-gap, and get access to the internal networks of the organization or at least extract some information of valuable stature. They have been quite successful in practically manifesting their proofs-of-concept. It adequately sheds away the complacent sense of security in air-gapped systems, forcing the specialists to take suitable measures to maintain the requisite gap. Some of the concepts have been made part of this study:

2.7.1 **MAGNATO**. The study, as done by [31], shows that an attacker can leak data from secluded, air-gapped computers to nearby smartphones through hidden magnetic signals. According to the research, malware would be installed in an air-gapped computer to control the magnetic fields emanating from the computer by regulating workloads on the CPU cores. Moreover, the malware would encode sensitive data including encryption keys, passwords, or keylogging data to transmit it over the magnetic field. On the other hand, the smartphone, located in closer vicinity, would contain another part of the malware which would receive the covert signal with its magnetic sensor.

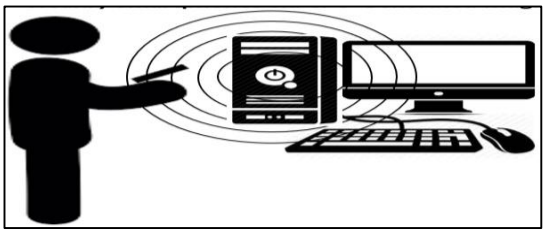

Figure 8: MAGNATO: Covert channel between air-gapped systems and nearby smartphones

2.7.2 **HOTSPOT**. This study shows that the signals generated from an air-gapped computer can be sent covertly to a nearby smartphone and then on to the Internet – in the form of thermal pings [32]. On its core, the malware (transmitter) makes the CPUs and GPUs generate thermal signals by causing heat fluctuations, which are further intercepted by a nearby smartphone (malware app) for onward passing on to the attacker via the internet. The author presents a technical background while describing the thermal sensing capability in modern smartphones. The researchers further recommend the countermeasures to mitigate the threat by using the "Zoning" approach; i.e. to mark defined areas or zones around air-gapped computers where mobile phones and simple devices are prohibited. Moreover, insulation of the partition walls may be helpful to mitigate signal reception distance growth.

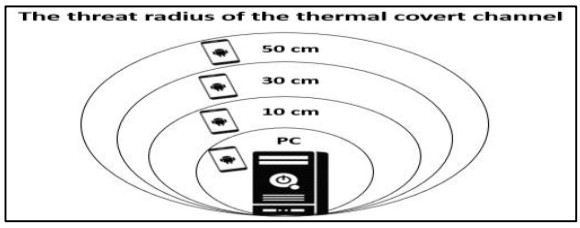

Figure 9: The Threat Radius of the Thermal Covert Channel

2.7.4 **aIR-Jumper**. This research is based on the use of IR light which is invisible to humans, but detectable by cameras due to their optical sensitivity [33]. Researchers reveal the feasibility of establishing bi-directional covert communication between an organization's internal networks and remote attackers using surveillance cameras and IR light. In this regard, two scenarios have been discussed: data exfiltration and data infiltration.

- **Exfiltration**. The exfiltration scenario signifies data leakage out of the network. Malware within the organization network would access the surveillance cameras across the local network and control the IR illumination. Consequently, sensitive data such as passwords, and encryption keys would then be modulated, encoded, and transmitted over the IR signals.
- **Infiltration**. The infiltration scenario signifies sending data into the network. Here, an attacker would use IR LEDs to transmit hidden signals to the surveillance camera(s), even while standing in a public area (e.g., in the street). Binary data such as C&C and beacon messages are encoded on top of the IR signals.

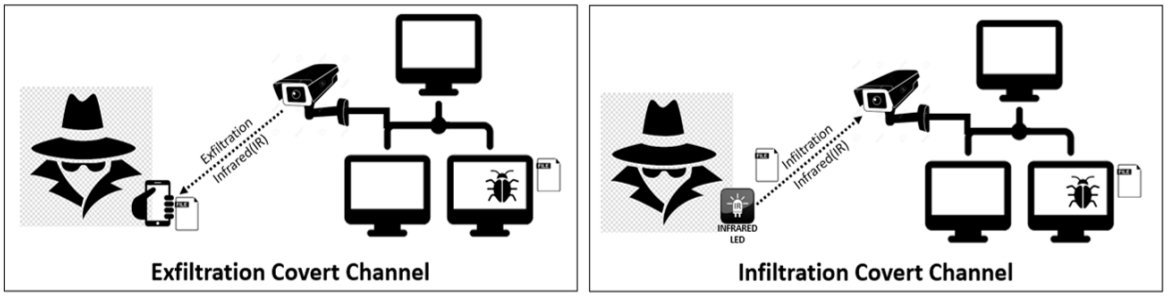

Figure 10: aIR-Jumper: Covert air-gap exfiltration/ infiltration via security cameras & IR

2.7.5 **AirHopper**. It is a technique that is used to bridge the air-gap between isolated networks and mobile phones using radio frequencies [34]. In this attack, the compromised computer is made to produce compatible radio signals by making use of the electromagnetic (EM) radiations associated with the video display adapter (graphics card) through malware. It makes a potential hidden channel that cannot be monitored by ordinary security mechanisms in place.

Once the breach is achieved in the air gap network, harmful code can be triggered and contaminate the systems within the targeted network. In case the suitable connectivity with the attacker is sporadic, the covert program running on the mobile phone may be tuned to store the acquired information, and transmit it to the attacker once the desired connection is available. At the fundamental level the method consists of two essential elements:

- electromagnetic (EM) signals emitted from a computer's monitor cable, along with the data that is intentionally modulated on those signals
- Frequency Modulating (FM) receiver on a mobile phone that can receive, extract, and save the modulated data from transmitted signals.

For the experimentation purposes, measures like the effective transmitting distance, type of cable, the presence of receiver antenna, etc.; have been assumed.

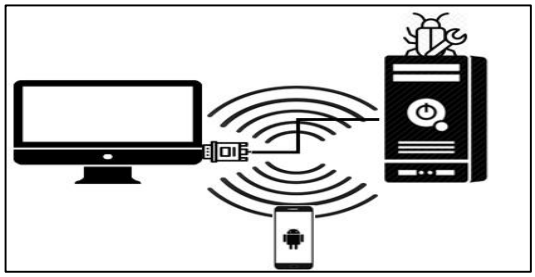

Figure 11: AirHopper: Bridging the air-gap between isolated networks and mobile phones using radio frequencies

2.7.6 PowerHammer. PowerHammer is a malware that uses power lines to extract data from air-gapped computers [35] through Alternating Current (AC) power lines. It requires malware to run on a computer that regulates the power consumption of the system by controlling and channelizing the CPU workload. Binary data is modulated on the changes of the current flow, and then transmitted duly encoded, on top of the current flow fluctuations. It is further conducted and propagated through power lines and intercepted by an attacker who taps the power cables that feed the transmitting computer. The attacker measures the emission conducted on the power cables, by using an unobtrusive tap. The transmitted data is demodulated and decoded back to a binary form, based on the signal received. The receiver measures the current in the power line, processes the modulated signals, decodes the data and if connectivity is established immediately sends it to the attacker, or saves it for later transmission.

The data might contain confidential files, encryption keys, credential tokens, or passwords, etc. Fundamentally, this attack model requires running malicious code in the targeted air-gapped computer which is achievable by *infiltrating the air-gapped networks using social engineering, malicious insiders, or supply chain attacks*.

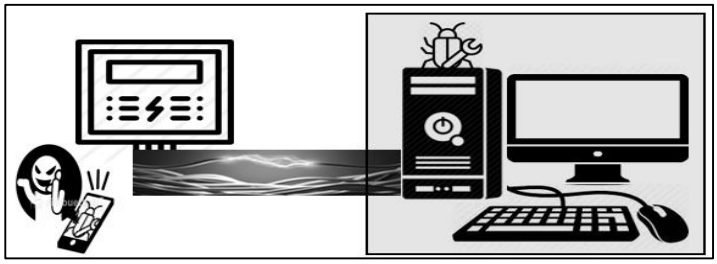

Figure 12: PowerHammer: Exfiltrating data from air-gapped computers through power lines

2.7.7 USBee. Researchers have been working on the use of USB connectors implanted with RF transmitters to exfiltrate data from air-gapped, computers. Primarily, this method requires some modification in USB hardware, embedding a dedicated RF transmitter onto it. However, in this research, the design and implementation details of a software, named "USBee", have been proposed that can utilize an "*unmodified USB*" device connected to a computer as an RF transmitter. The researchers have demonstrated the software's capabilities that can intentionally generate controlled electromagnetic emissions from the data bus of a USB connector [36].

Furthermore, the emitted RF signals can be controlled and modulated with arbitrary binary data. On the receiver end, all that is required is a smartphone or a laptop with an antenna (open to further research) that could cover and receive the range of frequency. The research claims that USBee can be used for transmitting binary data to a nearby receiver at a bandwidth of 20 to 80 BPS (bytes per second).

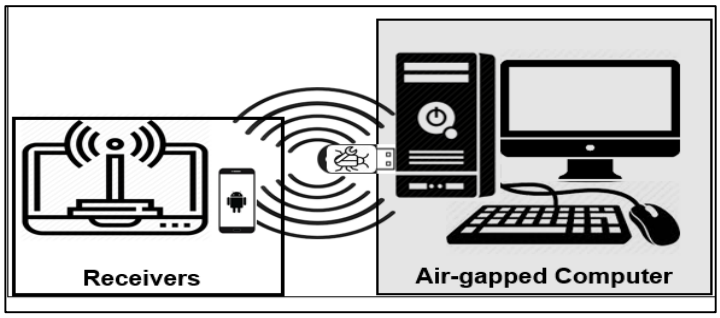

Figure 13: USBee: Air-Gap Covert-Channel via Electromagnetic Emission from USB

2.8 Conclusion

The chapter has highlighted various threats and attack vectors against an organization. It started with a narration of the general threat landscape and further proceeded on to more specific attacks against the air-gapped networks. The content has been augmented with various examples and the latest attack trends for clarity and understanding. The chapter explicitly highlighted the need for information for a potential attacker, which forms the first step of the attack chain. Its exclusive redressal is going to be covered in succeeding chapters.

Chapter 3

Mobile Computing Devices – Threats & Exploitation

3.1 Introduction

Mobile Computing Devices (MCDs) that include laptops, tablets, personal digital assistants (PDAs), smart wearable devices, and smartphones. With the evolution in these devices, the communication among the peers has gone to the next level. Besides that, the persistent mobility, availability, and ease of operation make these devices an absolute must for the users. People have been capitalizing on the potentials and functionalities to make their job a lot easier by accessing the Global Positioning System (GPS), email, and many other applications. Moreover, the smartphone environment comes with a complete package for entertainment and infotainment, so people find it handy to use it when they find some leisure time. Considering the size to performance ratio, smartphones are the most preferred MCD that a user wishes to carry along. But with all the pros in using an MCD, there are inbuilt threats associated with it, that can lead to leakage/ loss of precious information.

3.2 Primary Components of MCD

Every MCD is primarily composed of two main components: hardware and software.

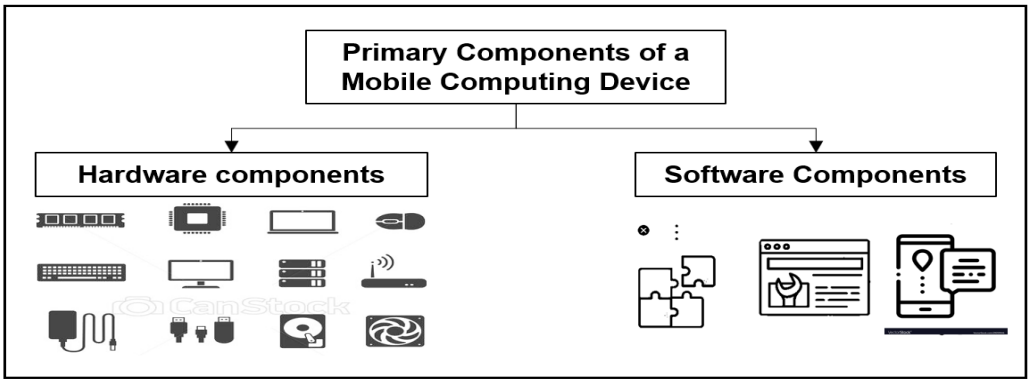

Figure 14: Primary components of a Mobile Computing Device

3.2.1 Hardware components. Hardware components are the physical components that a device requires to function. It encompasses pretty much everything from the circuit board (the motherboard) to CPU (Central Processing Unit), memory, and Input/ Output (I/O) devices [37].

- **Central Processing Unit (CPU)**. The device's central processing unit (CPU) is often simply referred to as the processor [38]. It is the portion that is responsible to retrieve and execute all the instructions. Besides that, it manages all the operations of the other connected hardware.
- **Memory**. Memory is composed of two sub-components, i.e. Random-Access Memory (RAM) which is accessible as long as the device is powered on; and Read-Only Memory (ROM) that comprises the storage of the device. The storage is available in both static components (hard disk) and removable components (external storage card).
- **Connectivity Modules**
  - **Subscriber Identity Module (SIM)**. SIM is an important component of the mobile device which is essentially a smart card that stores data for the subscriber of GSM-based cellular phones [39]. GSM is Global System for Mobile communication, that enables the subscriber to have a valid SIM to communicate with other GSM-based devices the world over. SIM card holds the subscriber's information including his unique identity as a phone number. It authorizes him to use its features such as placing a call or sending a text message.
  - **Wireless Network Adopter**. Wireless Network Adopter relies on Wi-Fi protocol for wireless communication and uses the radio waves to provide cordless high-speed Internet and network connections [40]. Wi-Fi radios use 802.11 networking standards of the Institute of Electrical and Electronics Engineers (IEEE) for carrying out their interconnectivity.
  - **Bluetooth Adopter**. Bluetooth adopter utilizes a wireless technology that allows the exchange of data between different devices [41]. Bluetooth makes use of wavelengths to transmit information, however for the devices to stay connected, it generally works within a short distance. Bluetooth is mainly used for connecting a mobile device with another one at a shorter range.

- **Power Batteries**. Mobile devices are equipped with adequate rechargeable power batteries, to meet up their power requirements. Battery stores electrical energy in a chemical reaction and then discharges it. Batteries rely on multiple electrochemical cells, to produce electricity by chemical means [42].
- **Input/ Output (I/O) Devices including sensors**. In computer terminology, I/O can be defined as any set of programs, operations, and/or devices that transmit data between computer systems or other I/O devices [43]. The main I/O functions performed on a mobile device is through the display screen, touch screen, keyboard (for laptops), speakers, and microphones. Besides that, all MCDs in general, and smartphones in particular, are packed with various sensors that are used for real-time data collection about everything [44]. The data not only includes a device's movement but its overall environment as well. Almost all the MCDs are equipped with many or all of the following sensors:
  - **Cameras**. MCDs are equipped with multiple cameras that enable them to capture still snapshots and record videos.
  - **Barometer**. Used to gauge the altitude of the device according to ambient pressure.
  - **Motion Sensors**. These include a gyroscope, accelerometer, and digital compass, and are used to ascertain the device's motion, including acceleration, rotation, and direction.
  - **Proximity sensor**. Used to find the distance of an object from the device's touchscreen, e.g. a user's ear during a phone call.
  - **NFC**. This sensor chip enables contactless payment from the mobile device. The underlying NFC-chip stays in an "always-on" state, so it can be exploited by the cyber-criminals to get in communication with the device without making active close physical contact with it.
  - **3D Touch**. The sensor is used in pressure-sensitive displays. It enables a user with options of applying varying degrees of touchscreen force according to its sensitivity.
  - **Ambient light sensor**. Used to ascertain the level of light in the device's environment to adjust the brightness of the screen.

- **Microphones**. Modern-day smartphones are equipped with 3-4 microphones, which are used to make phone calls, record audio, or even instruct software-based personal assistants on mobile devices like Siri, Alexa, Cortana, Bixby.
- **GPS**. This sensor is responsible for calculating the device's location, which is used in real-time location services like maps. GPS location service makes use of the GPS hardware available with almost every modern mobile device. It keeps a track of the device where-so-ever the user takes it along. Researchers go on pointing that the user location is consistently preserved and stays trackable to the mobile device/software manufacturers even when the location service is turned off.
- **Fingerprint Sensor**. It helps the user in the authentication process. It works based on comparing the biometric sample against a known template [45], which is securely acquisitioned from the user when he or she enrolled in the system initially.

3.2.2 Software components

The software components of MCD can be primarily categorized into the Operating System (OS) and applications. OS is responsible for interfacing between the user and the device hardware, whereas the applications help the user to accomplish specific tasks. The most notable OS on the device are: Microsoft Windows, Linux-based Android OS, and Macintosh-based iOS. Certain pre-installed applications provide basic features/ functionalities to the user. However, there are tens of thousands of applications available online for downloading and installing on the devices, by granting them special hardware permissions for them to work.

3.3 Common Threats Associated with all MCDs

MCDs include smartphones, tablets, laptops, and PDAs. According to a survey [46], there are 3.5 billion smartphone users in the world, that signifies almost one in every three persons worldwide owns a smartphone. Modern smartphones, laptops, and PDAs work just like personal computers, albeit they have an added advantage of mobility and portability. Hence, all these devices share common security threats, which can be classified as:

3.3.1 Physical threats due to theft or accidental loss. MCDs are small, portable, and lightweight devices, and form a good companion during travel. However, these characters often become their cause of theft or accidental loss, which not only leads to financial loss but also the data residing on the device. Since our MCDs host a large amount of data on them, any theft or accidental loss can lead to one or all of the following:

- **Identity theft**. Identity theft involves when the cyber-criminals get access to and exploit the information stored on a mobile device. Stolen information is often used for further social engineering attacks like spamming, blackmailing, and trapping contacts into sending money. In case the device contains a SIM card that stores phone numbers, the criminals can gain access to user's social media or even bank accounts; since the phone number is usually linked with those accounts [39].
- **Fraudulent purchases**. In case the MCD possesses online shopping apps while also storing certain payment information, the cyber-criminals may enjoy the leverage of online shopping on the user's behalf [47]. It can be easily accomplished on the compromised phone through various malware.
- **Personal safety issues due to the leakage of sensitive information**. When it comes to circumventing a password or lock, it is just a trivial task for a seasoned attacker. Hence, with too much information exposed that includes official/ personal photographs, contacts, and conversation-messages; even the personal safety of the user comes at stake. That can even lead to physical attacks against the user such as kidnapping for ransom or robbery etc.
- **Permanent loss of data**. In case the user did not keep regular backups of his data, everything stored on the MCD gets slipped from his hands forever.

3.3.2 Web-based threats. The users prefer accessing the web onto their devices while letting the associated threats go quite unnoticed. There are a large number of compromised websites on the internet, which appear quite harmless on the front-end, yet automatically download malicious content on the device upon access [48]. A few of the prominent threats are:

- **HTTP-based websites**. The HTTP-based (and not https-based) websites don't rely on any encryption mechanism to cipher the ongoing traffic. Therefore, any confidential information including usernames, passwords, etc., sent over such websites is always susceptible to hacking.
- **Websites with shortened links**. Various internet-surfing platforms offer URLs shortening services e.g. bit.ly and TinyURL etc., that replace the long internet address into something briefer for ease of sharing. It provides a perfect opportunity for scammers to hide malware behind shortened URLs.
- **Torrents sites**. Torrent sites (such as uTorrent) are often used for sharing pirated content including music, videos, or software. Since they only work on a peer-to-peer sharing basis, so there's practically no authority that could vet and validate the files. Hence, it can be safely assumed that the downloaded file would contain some form of malware.
- **Websites with vulgar and profane content**. As a general reputation, the sites hosting profane, vulgar, and obscene contents are considered to be less secure than other mainstream sites. "There is no doubt that visiting Websites of ill-repute is deadly dangerous. If you make a habit of it, it's a given that you'll be attacked at some point," says Roger Thompson, a chief research officer with security firm AVG. It can even lead to drive-by downloads, that install malware just upon visiting the site.

3.3.3 In-built virtual personal assistants

Almost all the modern-day device's operating systems are equipped with in-built virtual personal assistants that are programmed to work on voice and facial recognition technology using complex algorithms of Artificial Intelligence (AI). Examples include: Siri (iOS), Cortana (Windows), Bixby (Samsung), etc. They bring a lot of comfort to the user by keeping track of calendar and meeting reminders, scheduled tasks automation, natural conversation, and recommendations. But to do all this, these assistants require greater access to the entire device's hardware, including microphones, and cameras. In case, the bad actors compromised the security of the device, the user's privacy gets fully compromised.

3.3.4 Charging at public places. Researchers have revealed that bad actors tend to tamper with publicly available charging cables and attach them back to the public USB charging stations [49]. When any passer-by plugs his MCD into these hacked cables, his device gets compromised, thus granting access to the cybercriminals, who can in turn steal sensitive information or even plant a malware. This attack is broadly known as *'Juice Jacking'*.

3.3.5 Threats associated with wearable devices. The wearable devices are typically mobile devices that are designed to be worn by an individual, e.g. smartwatches, smart jewelry, smart glasses, fitness trackers, head-mounted displays (HMDs), and medical implantable. These devices not only perform many basic computing functions, akin to laptops and smartphones but can also perform unique health-tracking services as a result of being in contact with the user's body. Few of the threats are [50]:

- **Lack of in-built security controls**. Being a low-powered device, there's no PIN, password, or biometric protection. If fallen in the wrong hands, entire data would be accessible to the holder.
- **Ability to capture photos, videos, and audio**. These abilities are further augmented with their surreptitious conduct. Hence, anybody can covertly capture confidential information, videos, and images of sensitive places.
- **Insecure wireless connectivity**. The device needs a persistent wireless connection with smartphones using Bluetooth, NFC, and Wi-Fi protocols, for full functionality.

3.3.6 Threats associated with the use of social media platforms. Almost every smartphone user keeps his signature in at least one of the social media platforms, for better connectivity with friends and family. However, the public availability of the personal data of every user, makes it quite a challenging media for the users affiliated with critical organizations, including governmental agencies and the military. In this regard, the user's slight mistake can very rapidly get circulated to an enormous number of people around the globe. Some of the social media platforms with greater user-base are: Facebook, YouTube, Twitter, LinkedIn, Vimeo, Flickr, TikTok, and Instagram, etc. A few of the prominent threats are:

- User profiling through readily available user habits and inclinations on their social media accounts.

- Pilferage of confidential information, while circumventing the device security settings by malicious apps.
- Susceptibility of an employee in falling to social engineering techniques on this platform.
- Revealing personal identity leading to the disclosure of personally identifiable information (PII) and onward identity theft.
- Character defamation, in case the user's data is stolen and the campaign is launched.
- Damage to organizational reputation in case of data leakage.
- Reduced productivity of employees.

3.3.7 Communication interception – public Wi-Fi. Free of cost Wi-Fi connections available at places like a coffee shop, an airport terminal, or a public library are the heavens for attackers. They exploit the open Wi-Fi connections without any security or even create rogue Wireless Access Points (WAPs) to let the users connect and route their internet traffic through them. Thus, the attackers get away with successful man-in-the-middle (MITM) attacks.

3.4 Specific Threats Associated with Smart Phones

The unbelievable rise in the use of smartphones has created a landscape vulnerability of immense proportion. Since the ownership of the smartphone is globally increasing, it offers an attractive attack surface to the bad actors to target the unwary or unprotected users [51]. Besides that, the lack of any meaningful security on the devices has provided a suitable platform for the attackers to fully exploit it to their interests. This is one of the reasons that mobile devices are becoming an attractive target for cyber-criminals. Certain threat vectors dissuade adequate security of the device and may compromise the user's data. These include: "the mobile device itself, the installed apps with lots of permissions, access to compromised websites, wireless data connections, other users/ organizations, and the service provider" [52].

3.4.1 Riskware apps. People often make use of cracked/ pirated apps. Although "there's an ethical aspect that discourages downloading and installing pirated software" [53]; bad actors do modify certain files in the pirated software, thus enabling them to create loopholes in the user devices for later exploitation. Such apps are usually downloaded and installed from unofficial platforms, and usually become a greater source of data leakage. They force the users to grant them broader permissions on the device hardware. "The apps usually perform their tasks as advertised, yet they collect personal – and potentially corporate – data and upload it to a remote server, where it is mined for advertisements, and can also be used for malicious purposes" [54].

3.4.2 Precarious permission-model for mobile apps. This model exhorts the users to extend their consent on the use of certain sensors, before the installation of an app. However, generally, "the common users are conditioned to approve and give away all the requested permissions to the apps, to access it regardless of the consequences" [44]. Since the users tend to carry mobile devices wherever they go including their most private of the places, therefore, sensor-sniffing malicious apps tend to have more chances to compromise the privacy of mobile device owners.

3.4.3 Mobile app's reliance on mobile sensors. Mobile applications (apps) extensively rely on sensor data to carry out their intended operations. In the case of malicious apps, it may access the sensors for spying on users. At times, the routine apps access our mobile device's hardware so aggressively that these could even lead to ascertaining our heart rate, gait pattern, can estimate weight and height, and even the gender of the user; one such example is *Fitbit*.

3.4.4 Mobile sensors can give away user security PINs. Newcastle University researchers have found [55] that the attackers can crack mobile PIN codes from the motion and orientation sensor of the device. Since mobile apps and websites do not require any permission to access most of the sensors, it helps the malware to listen to and collect the data. In their experiments, they claimed to have "cracked four-digit PINs with 70 % accuracy on the first attempt". Researchers further point out that unless the app or the website with malicious code is completely closed down, "there's a possibility of getting spied even when the device is locked" [56].

3.4.5 Mobile sensors with 'Always-On' state. Most of the sensors in modern-day mobile devices, with some degree of variation, tend to remain at an always-on' state. The malicious actors can make use of these "always-on" sensors to jeopardize our security by carrying out audio and visual recordings or even extracting our location information.

3.4.6 Little to no security in default settings. According to the default configurations of the modern-day mobile devices, the emphasis is laid on usability and user-friendliness rather than security. Therefore, using the devices just at their factory default settings offer greater vulnerabilities to exploit. This holds equally for all the mobile devices irrespective of their baseline OS.

3.4.7 Legitimate apps with inherent privacy and security issues. A recent study [57] reveals that on average every smartphone user keeps around 26 apps on his smartphone, and most of them fall short of addressing privacy and security issues. It even includes those apps that are downloaded from trusted app stores. For example, almost all mobile phone apps have access to information such as your contacts and email account. Certain apps access the device's core functions, and potentially influence the way information is shared between devices.

3.4.8 Prone to malware attacks. The bad actors often design their attacks based on two factors: the victim device, and victim habits. As discussed earlier, the devices at default settings offer a good platform to infect them. When it gets augmented with user's casual practices, the chances of success for the attacker get even higher. Some of the capabilities of the malware are:

- Listening to live phone calls, and covertly sniffing call logs, and SMS texts.
- Controlling all the phone functions and features from a remote location.
- Hiding traces and avert detection during operation.
- Getting access to saved passwords and sensitive email correspondence.

3.4.9 Storage of unencrypted data. By default, the smartphones only offer an unencrypted storage facility; and the user has personally look for the encryption options and perform it manually. Therefore, all the residing data is susceptible to be compromised for its CIA values, or even permanently lost.

3.4.10 Contacts information. Mobile phones being primarily a communication device, allows the user to make up a complete directory of the private contacts, the user wants to get contacts into. And this leads to greater security risks in the event when the mobile is compromised physically or through software; and the contacts are exfiltrated by malicious attackers.

3.5 Conclusion

The chapter has focused upon the MCDs that include laptops, tablets, personal digital assistants (PDAs), smart wearable devices, and smartphones. However, the exclusive emphasis has been laid upon smartphones owing to their vast utilization for both communication and data processing purposes. In this regard, various components of the MCDs have been identified. Besides that, various threats have also been highlighted for better assimilation with the subject. This chapter has provided a baseline understanding of MCDs and threats which is essential to proceed ahead towards succeeding chapters, that mention human errors vis-à-vis MCDs.

Chapter 4

Psycho-Social Aspects of Human Errors & Their Exploitations

4.1 Introduction

Humans make mistakes, and in no case are exempt from falling. This particular trait makes them the weakest link in the chain of cybersecurity. Their mistakes could have both the normal and the grim consequences. Considering the case of cybersecurity and air-gapped systems, there are many incidents (as discussed in chapter 2 ante) that suggest that human failings are one of the key factors that lead to pilferage of precious data, despite all the measures taken. It has been established by researchers that human errors directly depend upon their psycho-social aspects. In this regard, it is essential to have a fair idea of human behaviours in their psycho-social domains.

4.2 Skill-Rule-Knowledge (SRK) – Based Model for Human Behaviours and Consequent Errors

Skill-Rule-Knowledge (SRK) – based model of human behaviours, as proposed by Dr. [58], ponders individually upon three different terms of human behaviours. According to the scholar, "these are the performance level of human beings, and are essential to understand to comprehend the associated types of human errors". Moreover, these terms refer to the degree of conscious control exercised by the actor over his activities.

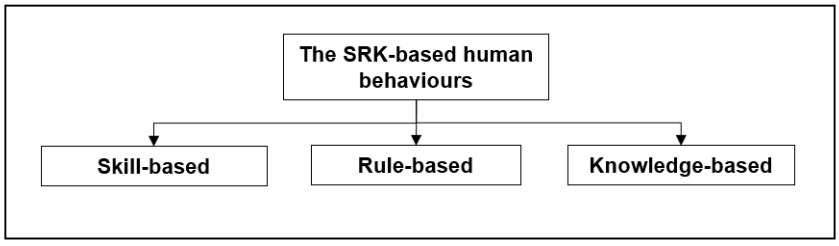

Figure 15: The SRK-based human behaviours

4.2.1 Skill-based behaviours. The skill-based behaviours represent the execution of adequately practiced routine actions in which cognitive commitment is quite low. Skill-based responses are generally triggered by some event, and the human actor performs an action related to a procedure well interiorized. e.g. instantaneously carrying out fire-suppression drills in case of a fire-alarm. The primary causes of errors in this mode are:

- Frequent intrusions due to the actor's own habits.
- Inappropriate use of the invoked rule.
- Unwarranted situational changes that do not trigger the need to change the habits.

4.2.2 **Rule-based behaviours**. These are the human behaviours, that adequately rely on the set of rules, that may have been learnt as a result of some formal training or interaction with the systems, or by working with other experienced staff. In this mode, the human actor identifies the situation and does the right action to carry out a task, which is followed by a series of actions based upon the rules. In this mode, the level of cognitive engagement is higher with the incorporation of certain reasoning in the form of if-than-else statements. The primary cause of error in this mode is:

- Misapplication of a good rule.
- Application of a bad rule.

4.2.3 **Knowledge-based behaviours**. In this mode, the actor is exposed to a novel situation, that is not essentially catered for already, and thus makes use of his knowledge, judgment, and available information while reacting to the situation creatively. Here, the level of cognitive engagement is very high, and actions are done very consciously. The actor's response is deliberate and based upon the previously acquired knowledge, with a successive evaluation of every action vis-à-vis its outcome. The primary causes of errors in this mode are:

- Physical or mental overloading/pressure in the situation.
- Out of sight, out of mind.
- Lack of knowledge to put up an effective response.
- Lack of awareness of the consequences of performed actions.

4.3 Forms of Human Failure

Broadly, there are two main forms of human failure, as classified by [59] i.e. ‘errors’ and ‘violations, as discussed below:

4.3.1 Violations. Violations are intentional (in)actions, which violate established rules, regulations, procedures, or norms. These are deliberate and utterly based upon the decisions of the actor made consciously. However, with all the deliberate intentions that cause violations, it is usually believed that it would generally be bona fide, with intention of at least keeping the things under control. There are 3x kinds of violations: routine, situational, and exceptional.

4.3.2 Errors. Errors are intentional (in)actions, which fail to achieve their intended outcomes. This leads us to believe that a clear intention to achieve a specific intended outcome remains as a baseline in the event when the error occurs due to any reason. Hence, the uncontrolled movements, e.g. reflexes are not considered as errors. Here, the originally planned action of the actor has to be intentional, whereas, the error itself is not supposed to be intentional. Moreover, it can be assumed that the outcome is not determined by factors outside the control of the actor.

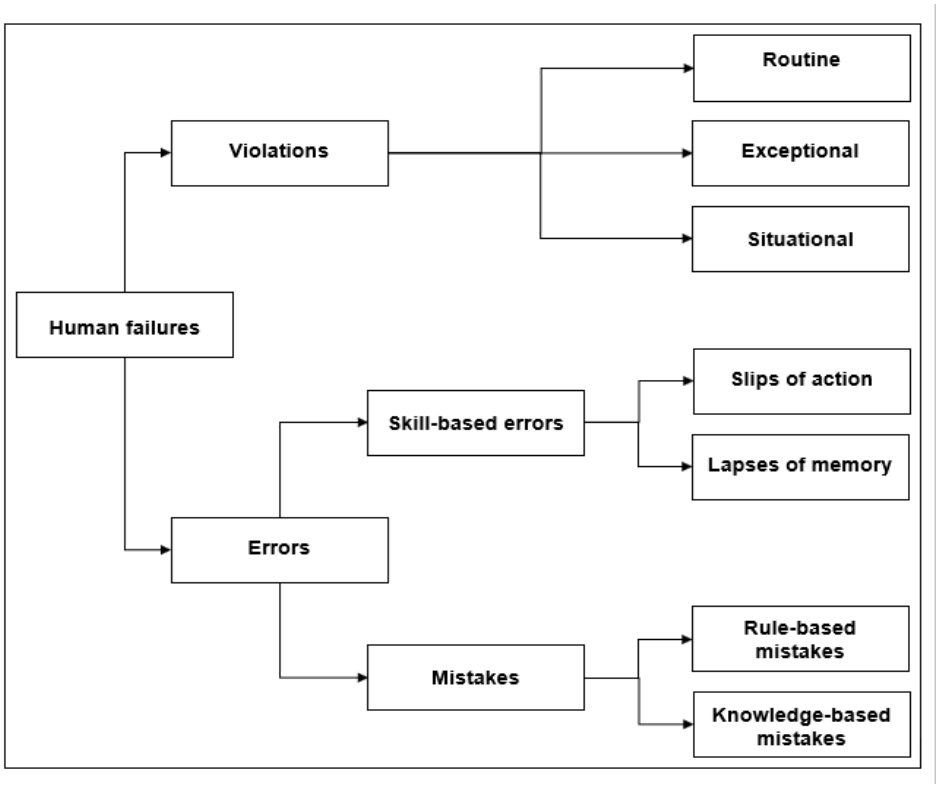

Figure 16: Forms of Human Failure

4.4 Human Errors – Elaboration and Further Classification

Human errors are usually a product of very complex and complicated events that occur in a sequence. A generic dictum about human and error relationships often goes as: to err (i.e. making mistakes) is human. Nevertheless, James Reason of the Risoe Laboratory in Denmark has defined “human error” as: "Error will be taken as a generic term to encompass all those occasions in which a planned sequence of mental or physical activities fails to achieve its intended outcome, and when these failures cannot be attributed to the intervention of some chance agency” [59]. Considering the very nature of the human being, it can be safely assumed that human errors cannot be eliminated. However, if the typical mistakes are identified in time and accordingly addressed, most of them can also be prevented from recurrence.

4.4.1 Classification of human errors. Errors can further be classified into three categories: slips, lapses, and mistakes. The distinction between these classes of errors was first coined by Norman [60]. Following human errors classifications are based on the Generic Error Model System, as advanced by [59], and the following paragraphs helps in differentiating all the three categories:

4.4.1.1 Slips of action. Slips fall into *execution failures*, where the planning and actor’s intention is correct; however, the things don’t go as per the plan owing to the actor’s attention deficit, lack of skills, or involuntary mistake. Here, the actor exactly knows how to perform a certain task but erroneously executes it incorrectly. This type of error is *directly observable*. e.g. slip occurs when an employee knows that he has to check computer logs on alternative days, but misses out to check on a particular day when the computer was hacked. More examples of slips can be: intrusion, omission, and reversal, and mistiming, etc.

4.4.1.2 Lapses of memory. Lapses also fall into *execution failures*, where the planning and actor’s intention is correct. Lapses are attributed to failures in human memory. These are usually the run-time errors in which one or more (scheduled) steps are skipped out of omission or forgetfulness during performing a planned action. This type of error is *not directly observable*. e.g. while carrying out updates of the antivirus programs, one computer was omitted, which was then targeted by the bad actors. More examples of lapses of memory can be: omissions, repetitions, and reduced intentionality, etc.

4.4.1.3 **Mistakes**. Mistakes signify *the wrong things done by the actor*. Mistakes fall into planning failures, where the planning is outrightly incorrect. Therefore, although the execution of the plan may be flawless, it would not lead to the achievement of the intended outcome. An example here would be if an employee on a night duty, wrongly assumed that the server room had caught fire, and so initiated a fire alarm and suppression scheme; thereby performing correct fire drills. Incorrect assumptions involved in the committing of mistakes may arise from a *lack of knowledge* or *inappropriate diagnosis*. For this type of error, we can have *rule-based mistakes* (e.g. misapplication of a good rule, application of a bad rule) and *knowledge-based mistakes* (e.g. confirmation bias, selectivity, vagabonding).

4.5 Heading Towards Mitigation Process of Human Errors

Other than compromised insiders, it has generally been observed that people intend not to make errors deliberately. Considering the human psychology, humans are often 'set up to fail' by the way their brain processes information, by their training processes, through the design of equipment and procedures, and even though the culture of the organization they work for. Besides, people can make catastrophic decisions even when they are aware of the underlying risks. Often, humans can also misinterpret a situation and as a result act inappropriately. Both of these can lead to the escalation of an incident. It can be rightly stated that it is not sufficient just to divide and classify human errors; rather it provides a further lead to understand and address the shortcomings. Hence, this forms the first step that paves the way to introduce requisite amendments in overall organizational culture through human ingenuity and resourcefulness.

4.5.1 **Addressing mistakes**. In case the mistakes are the frequent happenings in an organization, that means, the action plans that we activate in the situations have flaws and loopholes. Moreover, there's a probability that the manpower lacks the right skills to perform well in the tasks and achieve the set goal, or their skills are not detailed and developed enough, or even their knowledge is incorrect. In this regard, the existing Standard Operating Procedures (SOPs) and plans need to be thoroughly reviewed with due diligence. Moreover, *the skill-based training* with thoughtful sessions of rules-assimilation becomes mandatory to be conducted for every stakeholder. With adequate knowledge and training, the mistakes can considerably be reduced.

4.5.2 Addressing slips and lapses. Slips and lapses are often caused by excessive distractions, fatigue, haste, disproportionate workload, stress, and lack of focus and orientation. If the organization is experiencing frequent slips of actions and lapses of memory, that signifies, that human resource does not lack the requisite knowledge to carry out the task. However, efforts would be required to induce the elements of being focused, while avoiding distractions and increase attention and rest.

4.6 Exploitable Weaknesses of Human Personality

The main cause of the data infringement from the organizations with strong security measures is the failure at the end of the human resources. As discussed in the above sections, the human being is prone to making errors and mistakes in the conduct of actions. A smart adversary would bank upon the exploitation of human resources than wasting efforts on technological infringements against firewalls. There are certain human traits, which are usually exploited by a smart adversary to cause a data breach. A few of those traits are discussed below:

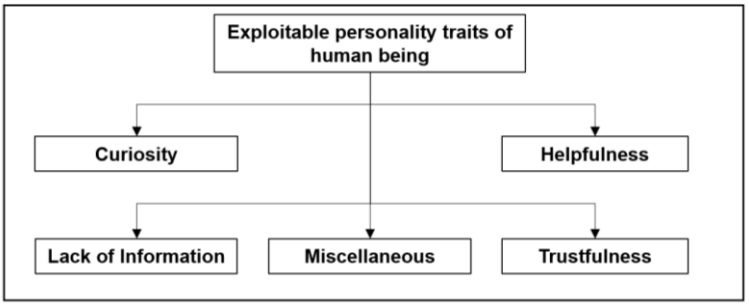

Figure 17: Exploitable human traits of human being

4.6.1 Human curiosity. The primary characteristic of humans that make it susceptible to cybersecurity attacks is "curiosity". On the positive side, it has fueled the advancements in technology, besides introducing astounding developments in healthcare that even allow humans to have a healthier and longer life. But on the other hand, it becomes the very reason to ignore that omen that forbids us to click on a malicious link or open a file. Hackers have been exploiting human curiosity over the years through many successful attacks. This very trait of human being outshines all the technical cybersecurity controls in place to safeguard an organization. For example, if a victim finds a USB flash drive lying on the floor near the entrance of an office, his curiosity won't let him be at ease before he checks it by plugging into his computer.

4.6.2 Trustfulness. Many social scientists believe that "trust forms a very important component for almost all of the workable human interactions that vary from friendship and love to the economic prosperity and development of organizations" [61] [62]. According to Karen S. Cook, "trust infuses public good and finds its basis in social intelligence. This allows the human to appreciate the level of risk that they face in social situations when socializing with strangers who could lead to a beneficial outcome" [63]. Trust is indeed a risky endeavor given the context of uncertainty that pervades while interacting with others.

4.6.3 Helpfulness. In human psychology, "helping behaviours are actions intended to provide support to another person with a problem, or to address their state of being distressed" [64]. Graziano and his colleagues [65] explore how *agreeableness* plays a key role in shaping up of helping behavior. Agreeableness tends to achieve harmonious social relations and friendliness through sympathy, generosity, and forgiveness. All these very instincts of human nature are virtuous at their core, and allow humanity to witness and extend kindness. However, the same very traits can be exploited by malicious attackers to draw human attention for fulfilling their nefarious designs.

4.6.4 Lack of information. People often take for granted the information on the things they otherwise do as a matter of their routine. It ultimately exposes them to certain threats. A good example of this phenomenon would be computer passwords, which is designed to allow access to an authorized and legitimate user to the computer and data. However, most people view passwords as a hindrance, rather than strategic protection, and accordingly keep easy-to-remember passwords. Hence the most preferred avenues for the attackers to bypass all the security measures of the company are to get a valid username and password and get access to the network.

4.6.5 Miscellaneous Weaknesses. Beside above-mentioned human weaknesses, there are many others that actually incite him to fall for errors. Some of those are listed below:

- Helpfulness / Kindness
- Naiveté / Ingenuousness
- Candidness / Honesty
- Complacence / Boastfulness
- Insouciance / Carelessness / Marry-go-lucky

- Undue Precautions
- Conceitedness /
- Excitement / Enthusiasm
- Appeal to costless items or services / Financial advantage
- Social stimulation
- Enticement
- Reciprocity
- Liking
- Audaciousness
- Carnality / Arousal
- Lustfulness / Impulsion / Amusement
- Commitment / Dedication
- Acquisitiveness / Greed / Covetousness
- Intimacy
- Opportunism
- Insensitivity to the value of held data/lack of security knowledge
- Reposefulness
- Negligence
- Inattentiveness
- Contentment
- Frustrations

4.7 Social Engineering

The term social engineering, also known as brain-hacking among the researcher's community, is the emotional and psychological manipulation of human beings that persuade them to perform certain actions as per the social engineer's desire. At its core level, social engineering itself is not necessarily malicious. It is the building of some influence upon other humans, to get the desired job done.

4.7.1 Principles for successful social engineering. Certain scientifically validated principles of persuasion provide for small, practical, and often costless changes that could lead to a big difference in the ability to influence others in an entirely ethical way. Social engineers rely on human traits and errors; and influence their targets using one or many of the following principles, as per the dictates of the situation:

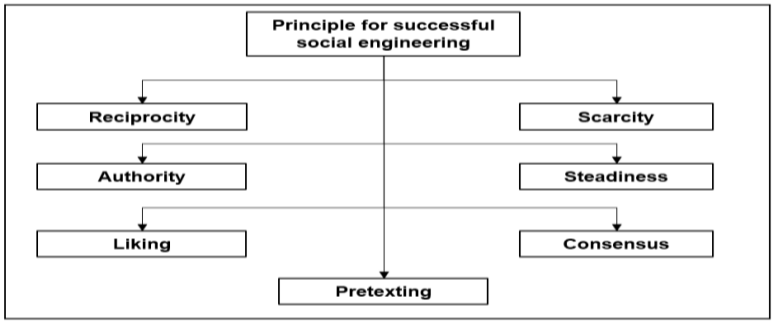

Figure 18: Principles for successful social engineering

4.7.1.1 **Reciprocity**. It is the feeling of social obligation that persuades a person who receives something (a gift or service) from somebody to return the favour. In this regard, the social engineer would create an environment where he would extend a gift or service to the potential victim to win his confidence, and crave in him a feeling of returning the favour [66].

4.7.1.2 **Scarcity**. According to human psychology, people tend to have a natural craving for things that are scarce and rare [66]. Accordingly, the victim surely gets inclined to the bait, that he is fully convinced about is not unique but also beneficial for him. Besides that, the feeling of what the victim stands to lose may act as just the right catalyst to accept the proposal.

4.7.1.3 **Authority**. People don't like being ambiguous about a thing, and so they naturally look for and follow the authority figures. For example, if someone appears in a white coat at a hospital, the patient would tend to give more weight to their medical opinion, considering them to be an authority. In a similar context, the social engineer proves himself to be an authority on a matter and influences his target victim to accord him due attention. This implies that the illusion of information can be far more dangerous than ignorance.

4.7.1.4 **Steadiness**. People like to be consistent with the things they have previously said or done. It is activated by looking for and asking for small initial commitments that can be made. It is mostly justified by people's conviction about a certain job, event, or happening. The social engineer seeks to discover or in certain cases cultivates the voluntary active or public commitments in his potential victim, and tries to get those in writing.

4.7.1.5 **Liking**. People prefer to fall for the things or other people that they have developed a liking about. According to human psychology, the researchers point out [67] three important factors for developing a sense of liking someone:

- People who are similar
- People who pay compliments
- People who cooperate towards a mutual goal.

These factors hint towards making up of a certain ground by the social engineer, wherein he impersonates to be similar while paying genuine compliments, and extending due cooperation to the victim. It enables him to win his heart; before fully getting down to the business.

4.7.1.6 **Consensus**. People tend to imitate particularly in situations when they are unsure of what to do in the first place. For example, if someone enters a crowded room where everyone is staring at the ceiling; the new entrant would unwittingly follow them. For this principle to be more effective, a social engineer creates a scenario wherein he convinces the victim to do a certain thing by making him believe that many other similar people also do it. In this way, a requisite consensus is established in performing actions.

4.7.1.7 **Pretexting**. It is related to the decision-making process of the human, wherein the human responds to the stimulus and capitalize his judgement skills. However, when the victim is offered with a very limited time window by creating a sense of urgency, he may unwittingly fall for the misjudgment and perform actions he would never perform in otherwise ordinary scenarios. For example, the social engineer impersonates as victim's boss on a spoofed email or a phone call, and encourage him to reveal some personal/ confidential information.

4.7.2 **General stages of a social engineering attack**. There are 4x well-established stages of social engineering attack: research and information gathering, rapport and relation-building, relation exploitation, and attack culmination [68]. Depending upon the nature of the target, these stages can be self-repeating as an inner loop or can repeat one after the other in an attack cycle.

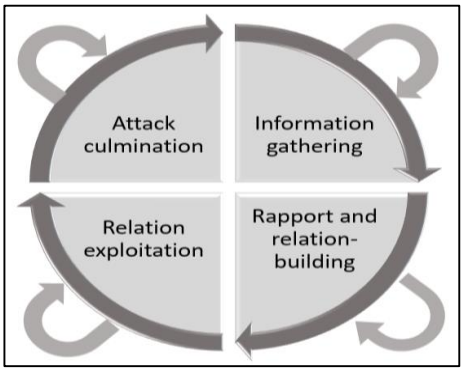

Figure 19: General Stages of Social Engineering

4.7.2.1 **Information gathering**. It forms the first stage of almost every social engineering attack, after target identification, and setting up the goals. Since the likelihood of success of the entire attack depends primarily upon this stage, it calls for investing the majority of the time, resources, and attention here. There are various ways and means to gain information about an individual or organization. Some of these options require technical skills while others require just "soft skill" i.e. to make use of principles of successful social engineering as mentioned above, and hack the humans. It is pertinent to highlight that no method, whatsoever, provides complete information about the target. It is the job of the social engineer to arrange the acquired pieces like a puzzle, connect all the dots, and make an intelligible picture. Primarily there are two methods of information gathering, as stated below:

- **Physical methods**. These methods require the physical presence of the attacker on-site and in-person. This means the attacker needs to have a sound understanding of the human weaknesses vis-à-vis their exploitation measures, to maintain an adequate cover while gathering the required information. The common techniques used in this method are: *dumpster diving, impersonation, tailgating, shoulder surfing, accessing disgruntled employees, or even carrying out reverse social engineering for later exploitation.*

- **Technical methods**. These methods don't necessarily require the physical presence of the attacker. However, he has to rely on technical equipment ranging from as low as a simple telephone and going up to higher ones including actually attacking the victim's system remotely to plant malware and gain information. The common techniques used in this method are: *Seeking information through fake calls, carrying out online searches, learning through photos/ videos of employees (uniformed) and building, accessing social networking sites and employees' profiles, fingerprinting the servers for their operating system, applications, and network protocols, and utilizing other paid computer-based tools, etc.*

4.7.2.2 **Rapport and relation-building**. This stage signifies the establishment of a working relationship with the target. After the spadework is done in the first stage, the quality of the relationship and consequent trust determines the level of cooperation that an attacker can get from the victim. In this regard, the attacker might make use of fabricated stories showing family pictures and sharing stories with the victim, to capture their trust and emotional attentions. It could also be as sophisticated as building an online relationship with the victim through an extensively created fake profile on a dating or social networking site, that may even lead to a physical relationship. The greater the trust is established in the relationship, the better would be the prospects of getting the job done.

4.7.2.3 **Relation exploitation**. This is the stage when the attacker is eager to have his fruits of hard work done in the previous two stages. Here, the attacker uses both information and relationship to actively penetrate the target. Moreover, "the attacker has to be quite focused on upholding the unquestionable trust that was established in stage 2" [69]. The exploitation can take place through the revealing of seemingly unimportant information or access granted/ transferred to the attacker. Examples of successful exploitation include:

- The act of holding the door open or otherwise allowing the attacker to get inside the facility.
- Unveiling username, password, or other confidential information over the phone.

- Introducing malicious payload into the company's computer system by just complying with inserting a USB flash drive into it.
- Get enthused to opening an infected email attachment.
- Revealing trade secrets in a discussion with an imaginary "peer" in a quest to help them.

4.7.2.4 **Attack culmination**. This is often the last stage of the attack that calls for the successful accomplishment of the mission. Here, the attacker tries to conciliate the victim as if they did something really good for someone while disengaging on a happy and positive note, leaving space for possible future interactions. Moreover, the attacker addresses all the loose ends such as erasing digital footprints and ensuring that no information or items are left behind for the target to carry out any backtracking or realize if something malicious had happened. A deliberately planned, thoroughly practiced, and meticulously executed exit strategy marks the final goal of the attacker, and indeed his final act in the attack.

4.8 Conclusion

This chapter has touched upon the psycho-social aspects of the human being. In this regard, various behaviours of the human have brought under discussion that mold their personality. While touching upon the forms of human failure, i.e. violations and errors; specific emphasis has been laid on human errors and their classification. Further, the exploitable personality traits of human beings revealed some of the traits that are essentially targeted by a potential attacker. The chapter concluded with the identification of general principles and stages of a successful social engineering attack, which paved a way for understanding the importance of social engineering concepts.

Chapter 5

Common Human Errors of Legitimate Users

5.1 Introduction

Making mistakes is a core part of human experiences – enabling him to learn and grow in life. But every error does have certain repercussions associated with it, which may lead to its cost in terms of reputation, time, or finances. When it comes to cybersecurity, "the human error means any inadvertent action, or inaction – by its employees and users that invokes, spreads or allows a security breach to take place" [70]. This ranges from failing to use a strong password to even downloading a malicious file by falling prey to social engineering attacks. Certain interesting statistics highlight the gravity of the issue, as identified jointly by Ponemon Institute, USA, and IBM Security's report on the global cost of a Data Breach in 2020 [71].

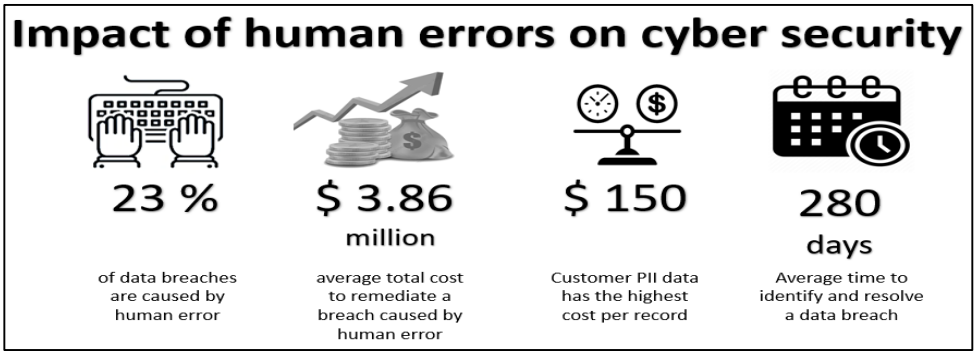

Figure 20: Cost of a Data Breach in 2020

"There is no universally-agreed classification of human error" [72]; and therefore, there doesn't exist any single scheme that may fully address all the needs. In this regard, a taxonomy is usually developed based on achieving a specific objective. For this research, we focus on human as a subject, and categorize the errors as per their scenarios, place, and state of conduct; as discussed in the following sections:

5.2 Common Errors at Workplace

"Human makes mistakes even at the places he's highly trained to work at, in the organization" [73]. It is imperative to know the common mistakes, that do not necessarily receive the highest emphasis, can be more damaging than any other sophisticated attack.

5.2.1 Casually discussing classified matters in the physical world. Man becomes the slave of his spoken words, and the master of those that remain unspoken [74]. The resource proprietors and resource custodians have a great responsibility for controlling access to information including system and data. However, in the physical world, information is casually shared among the peers, during office breaks or leisure times, even in public places without realizing the underlying sensitivity of the issue. This common human error can feed the potential attacker with very valuable information, that he may receive as a passive listener at some public place. Moreover, when more people possess valuable information than required, the attacker would have multiple options to phish any of the employees, as per his choice.

5.2.2 Negligently disposing-off documents / CDs in Wastebin. The attackers essentially carry out dumpster diving to collect maximum possible information about the organization/ person, as part of stage one of their attack. This type of negligence in the organizations, especially done by clerical staff is sheer negligence and a felonious mistake. In case any classified information that includes access codes, passwords written on the chits, rough diagrams of the network, phone list, organizational charts, and calendars, etc.; ends up in a dumpster, it can further reach the potential persistent attacker.

5.2.3 Inability to report an error. Often the employees bear witness to an untoward happening, incident, or a security lapse in the organization. However, lack of any error-reporting mechanism, lack of job security, and fear of getting embarrassed in front of co-workers; deters the employees to report any such errors, leaving more room for their recurrence.

5.2.4 The disinclination towards cybersecurity practices. Employees tend to focus solely upon their job role, while not inclining towards the requisite security procedures. As per the general tendency, cybersecurity is considered the job of designated personnel. In this regard, the common employees tend to get relax and stay aloof of the latest cybersecurity trends. It is “capitalized by the attackers, who finds them to be an easy target, and holds them off-guarded to steal credentials, get access to critical data, and introduce malware to a system” [75].

5.2.5 Physical security lapse. The data breaches are commonly attributed to cyber-attacks while overshadowing the importance of the physical security of the organizations. This negligence can cause loss of valuable confidential information, that can even help bad actors to design a greater cyber-attack against the organization if they gain access to the secured premises. There can be many forms of physical security errors, e.g.

- Allowing unauthorized visitors in sensitive areas along with all their electronic gadgets. This may happen even after the working hours, or when the guests themselves belong to some senior executive in the organization.
- Leaving the documents with sensitive information unattended on the desks, in meeting rooms, or even on output trays of printers.
- Allowing *tail-gaiting* in sensitive areas – where an unauthorized person follows an authorized one through a secure door or barrier, while walking close behind them.

5.2.6 Unsecured way of data transfer. The use of unsecured USBs to copy data from an internet-connected system to air-gapped computers is a major security lapse. It also includes the transfer of snapshots from a directly official digital camera to an air-gapped system. This practice can compromise the entire notion of air-gap security.

5.2.7 Bringing compromised electronic devices to the workplace. The user/ employee could inadvertently bring along their personal, already compromised devices. In other cases, if the insider himself is compromised due to some threat or blackmail, he might be forced to unwillingly bring, and use, malicious devices in the organization given by the attackers. If plugged into the system, the rogue device could trigger the underlying malware and compromise the network security.

5.2.8 Use of personal MCDs in office. Many sensitive organizations especially the ones maintaining an air-gap, deter the bringing and use of personal mobile computing devices in the office premises, keeping in view the threats as highlighted in chapter 3. However, as a matter of general practice, the implementation of the policy remains quite questionable due to human lapses, especially in the night hours of the duty. Ben Gurion university's researchers have demonstrated how the compromised mobile phones could form an attack vector in an air-gapped network, using radio frequencies [34].

5.2.9 Use of smart wearable devices inside the facility. Security researchers have found that a gyroscope, "a sensor that is used to measure angular velocity in smart wearable devices, can also be used for eavesdrop on the conversation" [76]. According to them, the MEMS (microelectromechanical systems) gyroscope is sensitive enough to recognize the sounds and can pick up some sound waves and turn them into crude microphone signals. Since iOS and Android do not require any special permission from users to access the gyroscope; therefore, any conversation could easily have eavesdropped on without the user's consent. Besides that, wearable devices are equipped with dedicated microphones and cameras, as discussed in the threats section of chapter 3, which can be used by bad actors for espionage activities.

5.2.10 Imprudent security culture in the organization. It is often the case that the end-users know about the right course of action to preserve security, but do not adopt it because they find an easier way to do the things or simply deem the security guidelines just as an overhead. In an environment where security is trivially neglected and pushed to the back-burner, the errors of the grave nature are bound to occur.

5.2.11 Delays in software updating / patching. At times, the user shows dereliction towards the software updating / patching process, considering it as an unimportant activity for already an air-gapped environment. This complacency doesn't last longer, as the malicious actors find some way to exploit it to their interest. The examples of 2017 WannaCry [77], and the Equifax data breach [78] that caused millions of users to compromise their data were the product of such sluggishness. In both the cases, the vulnerabilities had been already identified, and patches were released. However, end-users/ organizations didn't turn up seriously, until it was all over.

5.2.12 Poor password practices. With so many different platforms to access, it is indeed quite challenging for the human being to maintain a unique yet strong password for every single platform. This leads them to go for the shortcuts like choosing a short password and re-using it. According to the National Centre for Cyber Security's report of 2019, "123456" remained the most popular password for the year" [79]. The report further elaborates, almost 45% of the people use the same password for multiple platforms. The untrained users go one step ahead in making mistakes by writing the passwords near their work-desk or even sharing it with their colleagues.

5.3 Common Human Errors During Transit

During their service, the employees often find themselves in transit due to daily commutation (to and from workplace), a deliberate business trip, training activity, or even a private tour during the casual leave. Generally, the most preferred and economical method of travel is through public transport, especially when long routes are involved. The public-interaction is barely avoidable when there is quite a free time in longer hours of journey. It is, when employees, working with sensitive organizations make errors that may lead to the risk against their organizations and even themselves. The following are some aspects of common errors:

5.3.1 Disclosure of classified information to travel mates. Mutual-interaction is considered a good time pass. However, a naïve employee working in a sensitive organization may go on to revealing confidential information about their job. This way, a great deal of important information may flow to the adversary, who may deliberately adopt the same travel route by design as that of the employee.

5.3.2 Negligence towards luggage items during travel. The employees, being extra confident of the protocols and security measures offered in foreign countries, may lower their defenses. In that case, they may casually leave their devices at the airport (even turned on) and engage in other activities like attending nearby washrooms, buying snacks, etc. The sheer complacency in the security measures could end up losing their precious information to the adversary, if not the device.

5.3.3 Considering hotels, a safe place. The hotels are generally considered as a safe place to keep one's belongings. Accordingly, the visitors/ guests utilize the password-based safes to keep their important belongings including data containing electronic devices. Since almost all the safes are programmed to have a master password, it's a big mistake to rely on their security. Any determined attacker can design an attack, using a room-service, etc., and access the room, where knowing the master password, he may extract data from electronic devices in the occupant's absence.

5.3.4 Falling into social engineering techniques

Falling to Honeytraps. Business/ official conferences offer a great environment for social interactions besides formal learning. In the process, the participants informally exchange considerable information through their conversation, uniforms (if applicable), and ID badges containing biodata, company/ organization details, and job position, etc. The chances of compromise become even greater when the span of the conference/ activity is prolonged for more than a day. In that, a determined adversary would have plenty of time to win the victim's trust and have a congenial environment (may be through a 1 x night stand) to arrange honey traps for their target and extract classified information.

- **The disappearance of an Army Officer**. In April 2017, Lieutenant Colonel Habib Zahir retired from Pakistan Army, went missing in Lumbini town Nepal, some 5 kilometers from the Indian border [80]. Pakistan foreign office maintains, "there are strong reasons to believe that the former army officer was trapped and kidnapped by a hostile intelligence agency". Similarly, a person can be kidnapped by other non-state actors in a foreign country for their technical needs.
- **The kidnapping of Engineers**. Mexican notorious Zeta drug cartel lured and kidnapped several communication engineers/ technicians and enslaved them to build their Radio Zeta [81].
- **"Can I borrow your device"**? It is a very common scam in airports – when some stranger approaches a traveler to seek access to his device for making emergency contact with someone. Upon getting the phone, the stranger often sends SMS to subscribe to some harmful service or even send emails using the traveler's email account for later compromise.

5.3.5 Lapses on social media

- **Oversharing of information**. Frequent status updates and photographs (in uniforms etc.) out of sheer excitement, and let the loved ones know about it, is what causes a person to inadvertently feed more information to the receiver, than necessary. It may help unwanted people to keep a track of the traveler activities and have ample of information to exploit.

- **Putting the location online**. Besides sharing the latest happenings through status updates, the travelers often go to the next level of the slip by sharing their pin-point locations. There are glaring underlying risks involved like "anyone (including bad actors) can precisely locate him for causing any kind of harm to the person" [82].

5.3.6 Inadvertently misplacing personal laptop/ electronic devices. Personal laptop/ digital devices including wearable ones carry a lot of private information, useful to a potential attacker. During travel, a little slip of action in the form of misplacing it can cost the employee with loss of precious data, besides the device.

5.3.7 Inappropriate device charging measures during travel. There are occasions, especially on longer journeys, when travelers exhaust their electronic devices and require them to recharge. In such quest, they get their devices connected with public charging places and ultimately fall prey to *juice-jacking* while charging their electronic devices. The incidents of juice-jacking are on the rise because of the higher gains with little to no complexity in the implementation.

5.3.8 Use of public Wi-Fi. As already highlighted in chapter 3, free internet access granted in public places is always a lucrative target for the attackers, who find a great deal of opportunity in compromising so many victims in one place. In this regard, if an employee is accessing any online platform that requires an authentication mechanism, the same information is likely to fall into the attacker's computer, due to a man-in-the-middle attack.

5.3.9 Apathy towards shoulder surfing. Few employees consider the free time, as the best opportunity to finish up their pending official work. Few others try to pass the time by accessing social media platforms or even browsing various sites. In the quest, they pay little to no attention to the shoulder surfing done by the nearby passengers (potential attackers). In this way, they end up in inadvertently revealing their confidential information, their job nature, their interests, and much more precious information.

5.3.10 Carrying-along excessive data during travel abroad. Some countries make travelers pass through certain checks to go away with electronic data devices. At some places, the pre-requisite to seek clearance would be to unlock devices for them and have them peep into the data. It carries-along an immense risk of leaking confidential data including all the stored passwords for online platforms. It may even lead to the installation of a fully undetectable remote access tool (RAT) on the device.

5.3.11 Curious to use a potentially infected USB drive. The human curiosity often drives him to experience certain sensational episodes in life; e.g., he is deluded to plug in a USB drive he finds in the parking lot, hotel lobby, gifted in some official conference or finding one in a shopping mall. As soon as he complies with the attacker's design in using an infected USB, he contaminates his system, allowing greater access to a remote hacker. After all, it had to be seen in the broader context of being a traveler.

5.3.12 Oblivion to policies and procedures of a foreign country. Often, a traveler is oblivious of the visited country's policies and procedures, especially at the border crossings. Moreover, many countries possess and run deliberate surveillance programs for its people. For example, in Russia, they have a system for operational-investigative surveillance/ activities (SORM), which enables them to check telephone, internet, fax, and email communication. Another example is FinFisher spyware, which was bought by over 32 different countries to monitor the online activities of its citizens.

5.4 Common Errors by an Employee After Working-Hours

5.4.1 Sharing confidential information with family and friends. The most common error employees make is to share official/classified matters with their family and friends. It has gross implications in the form of inadvertent slips by their family members and friends, who become the cause of further propagating it to the other people.

5.4.2 Falling to phishing/ransomware attacks. While surfing online, the employee may inadvertently click a legitimate, yet malicious link. It may render their computers/ MCDs compromised. Moreover, the adversary could make use of the employee's known contacts to launch phishing attacks through their spoofed ID. At times, the thing that was initiated with just a phishing attack could eventually lead to ransomware [83]. It can bring the employee into a compromising position, and forcing him to even give away some malicious favour to the attacker, as a means of ransom.

5.4.3 Falling to romance scam/ sextortion/ sex-espionage. The adversary may resort to any means of extracting classified information, and entrap the unguarded employee. In such moves, one of the common mistakes that force a person to submit to the adversary's designs is falling to a romance scam, sextortion, or even land into sex-espionage. In all three different methods, the common thing is the exploitation of human emotions, as discussed in chapter 3. History is witness to the fact that even other family members of the employees in sensitive positions were lured in to extract valuable information from them during world war – II [84].

5.4.4 Doing official work at home on internet-connected devices. The obedient employees, with good intentions, try to burn their midnight oil for doing well according to their job position in the organization. In this regard, they may inadvertently process some classified information on their (potentially compromised) devices. The examples include making of official presentations, editing or processing of official photographs for official portals, etc.

5.4.5 Storing confidential data on internet-connected devices. MCDs, especially the ones with an internet connection, is always susceptible to get compromised. Since, they contain valuable information including visited locations-maps, contact lists, personal photographs, and files; they form a lucrative target for potential adversaries. The most common mistakes often done by employees is to save and process confidential data onto their devices. This lapse is sufficient to compromise an organization's security if a determined adversary compromised the device.

5.4.6 Falling for gifts (electronic gadgets) from less known sources. "The gifts have often been one of the best ways to show someone the reverence and intimacy" [85]. The common mistake that may lead an employee to leakage of confidential information is accepting gifts from unverified sources, especially some electronic ones with data processing capabilities, and start bringing them into their personal use. It may vary from a small USB drive, offered at some conference, to an expensive mobile computing device. A slight slip may jeopardize the entire security of the organization.

5.4.7 Inadvertently revealing classified information to others. "Often the adversary comes up with the tricks to mask the bribery as a rightful payment for research, lecture, and assistance of a scholar in scientific work" [86]. In a recent example, a former CIA officer was held on charges of involuntarily sharing confidential material with an agent in an adversary country, when he was offered a fully-funded lecture-delivery in another country's university [87]. In yet another example, an employee from Tesla was approached with offers of $500,00, in case they only insert a USB drive into the air-gapped networks [88]. However, the loyal employee reported the matter to their company, who further reported it to the FBI.

5.4.8 Inappropriately disposing-off data-containing/ processing devices. The electronic computing devices such as computers, smartphones, tablets, and digital camera, create and process a large amount of digital data during their lifetime. The data may be personal or classified in nature. Not realizing the sensitivity of the matter, people often dispose-off the legacy devices, and replace them with newer ones. One very common mistake done by employees is to get repairs or even dispose it off in the local market or through some online selling platforms like *OLX*. At times, even the employees tag online selling posts with their distinguished ranks or affiliated organizations to attract better offers. An adversary, looking for information, may find it as a golden opportunity to buy that used gadget and extract information.

5.4.9 Negligence towards mobile connections. The user, while using a mobile device, connect to different other devices including Wi-Fi routers, Bluetooth earphone/ car audio device, and NFC for payment, etc. However, a common user usually doesn't bother to revoke all the connections after their fair use; thus, opening the ways for malicious actors to exploit.

5.4.10 Relinquished password protection on MCDs. Kaspersky Lab finds "over half of the consumers don't password-protect their mobile devices" [89]. This mistake of employees turns out to be good news for malicious actors, for they would have easy access to all the information stored on the phone without many efforts. Some employees, if at all bother, prefer to keep easy to remember 4x digits PIN code type of password, e.g. 1234 or 0000, which is just a few tries away from hackers.

5.4.11 Relying on default settings of MCD. The default settings of mobile devices do not provide an adequate level of security. As discussed in chapter 3, different settings are manually turned on, to make the device relatively secured. However, a common, not conversant with it, keep using the device at their default settings.

5.4.12 Installing riskware apps on mobile devices with broad permissions. [90] says: "riskware mobile apps are often the cause of unintentional data leakage, and pose a serious challenge for mobile users who don't always check their security". e.g. a variety of innocent-looking apps like keyboard-enhancing apps are typically available for free and found in official app stores, asking for broad permissions. The permissions enable the apps to access the device's sensors, hardware features, and file directory. However, most of the users are just tuned to agree with all the asked permissions without deliberately considering them at all. Hence, other than performing the promised task, many of them also send personal - and potentially corporate - data to a remote server, where it is mined by advertisers, and at times, by cybercriminals.

5.4.13 Naiveté's attitude towards unusual happenings on MCD. The users often remain focused on running the apps, disregarding the proper functionality of the mobile device. They often let go of the glaring indicators which are suggestive of some malicious activity on a mobile device. The indicators usually include a decline in battery health, greater lag observed in the starting of various apps, and greater time taken by the device to restarts. Making peace with such indicators let the potential malware to stay on a mobile device forever.

5.4.14 Keeping the camera's lenses uncovered. On MCDs, there is no default way to cover the in-built camera lenses. However, few third-party companies offer certain options for covering the lenses. However, users remain oblivious of it and leave it uncovered even while using it at very private places, e.g. while responding to natural calls. Any potential malware/ riskware can access the device and make use of the on-phone sensors including cameras; thus, causing greater infringement to the user's privacy.

5.4.15 Visiting unsafe websites. With the storage of much of the personal information on home computers, it has never been more important to get on guard against internet predators looking to gain access to personal files. One of the many ways, an adversary can do this is by infecting the user's computer, enticing him to click at places of his interest, and then extracting information from an infected computer. In this regard, unsafe websites prove extremely harmful. A few of the potential hazards are:

- **Use of HTTP-based websites**. As highlighted in the web-based threats section of chapter 3, any confidential information is always susceptible to hacking on an HTTP-based website. Common users, often, let it go unnoticed while surfing online.
- **Accessing websites with shortened links**. Shortened links can host a hidden malware into them, as discussed in earlier sections. Common user hardly thinks about it before clicking on the shortened links, and eventually end up executing the malware on their device.
- **Use of torrent sites**. A common user finds it a better option to download free content from torrent sites. However, as highlighted in web-based threats of chapter 3, anything downloaded from torrent sites may contain malware, and upon execution may infect the device.
- **Accessing websites with vulgar contents**. Often moved emotionally, a common user may access the websites with, vulgar and obscene contents; and end up compromising their device with malware.

5.4.16 Abstinence from the security-related conversation. In the fast-paced life, there's hardly any time spent on a security-related conversation among friends and family, which could bring the latest trends into the limelight. It is indeed an overall cultural lapse that leads to sheer unpreparedness from the imminent and obvious threat.

5.4.17 Common errors in Online Social Networks (OSNs).

- **Keeping personal data as "public"**. A critical error, in which the user inadvertently keeps all his personal information as "public".
- **Revealing personal/ official information**. Common users hardly consider the underlying threat and therefore don't mind in sharing personal or even official information including the snapshots in official uniform etc.

- **Furnishing detailed personal information on social media platforms**. Social media platforms are designed to connect people with common backgrounds including birthplace, schooling, and interests, etc. In this regard, the users tend to furnish a lot of personal information on the platforms, to have better connectivity. Such lapses provide a free-of-cost ready-reckoner to the bad actors since it can further be mined and used to design more sophisticated attacks.
- **The auto-download option enabled for social media apps**. Social media apps, by default, are designed to offer full functionality and features, leaving few options to the user for desired settings. e.g. WhatsApp is by-default set to auto-download every single file including audio, video, and images. It poses a great hazard if a malicious file gets downloaded by itself on the mobile device. An unintentional execution of it would trigger the malware, thus compromising the device.
- **Frequent status updates of various happenings**. As already discussed in the section of 'common errors during transit', every single status update provides an essential dot of information that defines a user's personality. In their leisure time, users keep providing this information to the public.
- **Getting into unnecessary arguments on public social groups**. An employee, with a clear identity on social media, when to indulge in any hot arguments, he is associated with the organization. Common users, often, go for unnecessary arguments, revealing their inclinations and ideas.
- **Responding to unacquainted friendship requests/ phone calls**. Many of the scams begin with fake friendship requests/ anonymous phone calls. Common users, often fall for such requests, allowing the impersonators to have better access to the user's profile and data.

5.4.18 Default administrative password for internet-device at home. Generally, the user makes use of internet connections offered through Fiber-To-The-Home (FTTH) technology, or even CAT-6 cable; that end up at routers/ access points placed inside homes. Users may be smart enough to set a good Wi-Fi password. However, the administrator password on the access points is often the neglected subject. Any adversary, on the same network, may be able to compromise the device and tap or even redirect the internet traffic.

5.4.19 Errors committed by an employee's family. "Our biggest violators are our family members that include our parents, siblings, spouses, and children" Mr. Vihn Cayton [91]. The most common errors by family members are:

- **Slip of actions by young children**. The children are innocent and unable to comprehend and resist the heinous motives of the adversary. Owing to their online presence, they are easily approachable by impersonators with their all-time-tested social engineering tricks. The children may succumb to the tricks, and reveal much of the information about their parents, they are not supposed to tell. Moreover, the children may inadvertently disclose information in their social circle/ school/ friends.
- **Casually sharing personal information**.
  - **In the physical world**. The family members, often share personal information with the public, without realizing the underlying threats. e.g., while traveling in public transport, they may open up to co-passenger/ ladies, revealing much of the classified information.
  - **On social media**. Family members are the greatest contributor to revealing information on social media. e.g. Excitement of posting to a certain station, boasting about promotion, sharing happiness while traveling via check-ins, and status updates.

5.5 Conclusion

The chapter precisely touched upon the common errors of a human being, dividing them into three scenarios / states based upon human presence i.e. at workplace, during transit, and after working hours. The chapter also had a section for the common errors committed by the employee's family. All the common errors have been stated concerning their potential threats.

Chapter 6

Way Forward

6.1 Introduction

Human error would occur whenever there is an opportunity, in the light of incognizance and oblivion to the subject. This calls for taking requisite measures to eliminate the opportunities for error; while at the same time, it is essential to approach human error from the perspective of human awareness and education. The very first thing that needs emphasis is to make an employee know and realize that something, he may deem casual, is not necessarily to be casual. After all, the claim of a person to be infallible is not that hard to disprove when he is contested with valid arguments and proofs. Therefore, the organizations, specially air-gapped ones, have to have a way forward to curb the common human errors of their employees to the maximum possible level, or at least, control the damage at early stages after something wrong has erroneously been done.

6.2 Safety measures at Workplace

Besides taking care and full implementation of existing organizational policies, the following remedial measures are proffered against the identified common human errors (as mentioned in chapter 5):

6.2.1 Exercise restrain from information sharing. The information should only be shared based on the need-to-know principle. This principle signifies that the users should only be granted access to information only when it is necessary for their job function, and it is immediately revoked when the job is over. Besides that, the employees must exercise restrain over-sharing or discussing classified matters among colleagues (from other departments). The information about specific assignments/ projects should be considered as confidential.

6.2.2 Implementation of document's shredding/ burning policy. It is very important to get rid of extra printed documents, especially when they contain classified information by physical shredding. In this regard, a proper shredding/ burning policy be fully implemented. Moreover, as a safe practice, even the soft copies of the documents, no longer required, should be shredded using any reliable software, rather than just performing an ordinary deletion process.

6.2.3 **The error-reporting mechanism in the organization**.

Organizations often lack a requisite platform where suspicious activity could be reported in a straight forward manner without undue adverse consequences to the reporter. The platform needs to be devised in a manner that protects the reporter's identity, while also encouraging employees to report any lapse witnessed or done; so that early remedial action could be taken in the better interest of the organization.

6.2.4 **Deliberate sessions of cyber-security training and awareness**.

It is a known fact that regular training instills better habits. When people adopt something as a habit, it's more likely to get turned into their second nature. The formal sessions of cyber-security training and awareness programs should be suitably augmented with other measures like posters, quotes of the day, monthly periodicals in the native language, centralized lectures, quiz competitions, etc. The active participation of employees should be encouraged, allowing them to share the ideas, encountered various security threats in their lives, and thus promote learning through collective experiences and efforts. In this regard, "Employee-reported phishing attempts and other hacking schemes are valuable data" [92].

6.2.5 **Effective access control mechanism including physical security**

- There's a need to implement the *zoning* concept by dividing the facility into various zones. The zones that contain sensitive equipment, data processing, and storage devices are termed as 'Red Zone', which must be put under strict checking and scrutiny.
- No unauthorized person, whatsoever, be given access to a sensitive area.
- Making of only one entrance and exit point, so that the exact presence of the individuals could be conveniently ascertained.
- A dedicated staff is placed to physically check every individual and deter tail-gaiting.
- A strict ban must be imposed on carrying personal MCDs to the red zone.
- A requisite surveillance system, besides motion detection arrangements, and enforcement of multi-factor authentication on entry point would add into the layers of defense mechanism.

6.2.6 Secured way of data transfer. The secure USBs that use hardware encryption and decryption mechanism is a preferred option to be employed for data transfer at the air-gapped facility. However, in no case, the same USB should be used for data transfer from an internet-connected device to an air-gapped device. In this regard, an adequate colour-coding scheme is also useful for better identification and usage.

6.2.7 Discourage the bringing of a personal electronic device. The electronic devices bear some inherent threats with regards to information leakage, as already discussed in chapter 5. The employees should therefore be discouraged to bring any electronic device including mobile computing devices and smart wearable devices at the workplace. In this regard, the alternative means of communication (such as landline numbers) are necessary to be provided to them for tackling emergencies.

6.2.8 Inculcation of sense of security as organizational culture. The ideal information security culture is identified with the workforce that is aware and knowledgeable, manifest conscientious, and caring behaviour while fully comply with policies of the management. "Organizations that have a strong information security culture achieve a supreme level of trust and integrity through the protection of their information" [93]. This calls for the integration of security in the overall organizational ambit starting from the mission statement down to the implementation of the lowest level policy. Accordingly, the workforce would be trained to observe security procedures in every single prospect of their work.

6.2.9 Emphasizing on-time software patching. The devices usually get software updates from their manufacturers that contain patching up of known vulnerabilities that arise with due course of time and usage. Hence, whenever the updates are offered from a trusted source, they should be installed without delay.

6.2.10 Good password practices in the workplace

- Keep a good pass-phrase.
- Never reuse a password for multiple accounts.
- Do not share passwords among peers and co-workers.
- Do not write down the passwords, PINs, or combinations of the office safe.

6.2.11 Miscellaneous measures

- Do not leave an unattended computer, duly logged in especially on Namaz, lunch, or washroom breaks.
- Never insert an unknown CD/ DVD /USB drive in any computer, even for checking purposes, since it may contain malware [73].
- Always be mindful that fool-proof security can only be accomplished if everyone assumes his responsibility and stays vigilant.
- **Conducting simulation exercises**. Simulation exercises should be planned and conduct with due diligence, keeping in view the common human errors, and the latest exploitation trends on the subject. In this way, the employees could be well-prepared to take them on when encountered in real-world situations.

6.3 Safety Measures During Transit

6.3.1 Cautious interactions with co-passengers in travel. An employee working with a sensitive organization bears a lot of confidential information that he knows by virtue of his experiences. The strangers / co-passengers that happen to involve in chitchat just to pass the time often begin with questions like the workplace. There, the employee has to show the presence of the mind and must be cautious in revealing any information that may leak out confidential information. In this regard, the employee must get conversant with social engineering tricks, the adversary is likely to resort upon, to extract valuable information. Moreover, it is better to get abreast of the subject through various case studies of the already held incidents.

6.3.2 Exercise conscientiousness about luggage items. Never leave items especially data storage ones, without due supervision. If the destination's laws and regulations require physical inspection of the goods; it is a wise idea to put commercially sold anti-tamper seals over the travel laptop's hard drive covers and some screws. It would deter any impersonator/ strangers from examining your device to copy hard disk data by removing it.

6.3.3 **Safety measures at hotels/residences**

. Hotels are not safe, even the most reputed ones. It is the general procedure that room-service staff visits in the guest's absence, primarily for cleaning/ services. But the theft of a device or even just the data from it cannot be ruled out. Therefore, it is better not to leave any data-carrying device back in the room, even in the safes.

6.3.4 Safety measures against social engineering techniques

- **Vigilance against honeytraps**. The conference attendee must be aware of the fact that not everybody around in the conference is a friend. Therefore, he should limit the display of ID badges only to the places where he has to prove his ID, else keep it upside down; because it easily gives away, company name, country, and person's specialty. The attendee should also limit the amount of information sharing with other participants. Finally, exercise restraint upon human emotions and don't get carried away. Use a sense of proportion and judgment against any inappropriate and indecent advancement by any other participant. The bottom line he must understand is: *there is no free meal*; and so, the cost of impromptu physical intimacy should not be the precious data held with the attendee in any form.
- **Verification and validation of foreign offers**. The baits extended by social engineers can easily be validated and verified through various online sources. Therefore, before getting carried away with certain offers specially for foreign jobs, all pros and cons must be evaluated.
- **Defeating the misuse of the personal device**. The employee should not let anyone use their personal device, in any case, whatsoever. It would considerably save them from scams like "Can I borrow your device". Moreover, it is not a safe practice to use anyone else's devices for personal communications, unless in cases of extreme emergencies.

6.3.5 Precautionary measures for social media usage

- **Avoiding undue sharing of travel information**. The traveler should avoid posting sensitive information, while adjust their settings to make profiles more private. The best practice signifies that while in travel, hold off sharing pics on social media since it indiscriminately reveals personal information that is not safe to share with everyone. In this regard, the option of personal messages can be used for explicitly sharing with the intended audience.
- **Sensible use of geotagging/ location services**. It is the equivalent of adding a 10-digit grid coordinate to everything posted on the Internet. Any employee exposing his or her location can jeopardize entire organizational security. Most of the modern applications are designed to automatically embed geotags into pictures, and videos in default settings. Accordingly, the user must look into the settings on their device to disable the location-based social networking services.

6.3.6 Physical safety of laptop/ electronic devices. It is not possible to force an employee to refrain from using his mobile computing devices [47]. However, he can be inspired to keep and process minimal data onto it, while completely disregarding the storage of sensitive data onto it. Furthermore, the following preventive measures are recommended to be adopted to considerably mitigate the identified physical risks arising due to theft or loss of the device.

- **Data encryption**. Data encryption with a strong encryption mechanism would keep the stored data safe from falling into criminal's hands, in case the device gets stolen. In this regard, many software solutions are available, that can be incorporated, including propriety and open-source ones.
- **Blocking of the communication device**. Just in the case of stolen mobile phones, the already noted model number, serial number, and International Mobile Equipment Identity (IMEI number) of the device would be very helpful to get the devices blocked through the local communication authority; PTA in the case of Pakistan. In this regard, all the requisite information must be preserved to be utilized for the said purpose.

- **Configure the auto-erase feature for data**. Some applications allow setting security features of auto-wiping of the data in case of several incorrect password attempts. The device should, therefore, be configured to erase all data. However, it is recommended to keep a backup of important data at a safer place.
- **Configure remote data wiping features**. Modern mobile phones offer the facility to locate the lost device and even go on to the extent of wiping of entire data. The in-built feature "Find My Device" can be configured to locate and wipe the device.
- **Mobile Data Backup**. It must be made as a matter of routine to keep a backup of mobile data including contacts at a safer system. Although, online sources including do offer such features. But it is a safe practice to make a manual backup on your own computer and keep it encrypted.

6.3.7 Requisite arrangements for charging of the devices. To avoid juice-jacking at public charging points, own arrangements for charging of mobile devices be catered for. In this regard, a portable power bank can be a better option to carry along.

6.3.8 Relinquish the use of public Wi-Fi hotspots. As identified in the above chapters, the free internet offered at public Wi-Fi hotspots carry a lot of vulnerabilities with them. Therefore, it is strongly suggested to limit the use of public Wi-Fi for only the most essential job that too by using virtual private networks (VPNs).

6.3.9 Anti-shoulder surfing measures. By putting on a privacy cover on the screen, we can minimize the risk of exposing valuable information from undesirable viewers. Privacy cover is especially useful for data protection against the prying eyes from the sides when the user has to access his device during travel [94].

6.3.10 Intelligent selection of personal belongings for traveling abroad. Employee travelers should be educated to choose the best items for themselves before proceeding on any official visit abroad. Besides, all the other items of personal use, the major concern is electronic devices that they may carry along. In order, to safeguard personal and official data, employees must not carry along any data storage devices having classified data. Should there be any essential requirement of carrying data, it must be adequately enciphered using well-established cryptographic standards.

As a safe practice, it is advisable to use a new/ reimaged mobile computing device with "throw-away" accounts.

6.3.11 Adequate disposal of gifted / found data devices and electronic items. The gifted data devices or found ones must not be used straight away on personal computers. If possible, found devices should be reported and submitted to the near lost & found service, if available. Else it should only be accessed through an internet café or a virtual machine to find its owner. The gifted data devices, if not in need, should be kept separately for elaborate sanitization before use.

6.3.12 Getting abreast of the destination country's security law and policies. It is a better idea to have a fair knowledge of the laws, customs, culture, and traditions of the visited country, especially with regards to their cyber-security policies. Certain countries discourage data encryption and the use of VPN services. Having a beforehand knowledge can save the traveler from a lot of trouble at airports.

6.4 Safety Measures after Working Hours

6.4.1 Restrain the sharing of classified information with the family. The friends and family are usually not trained to keep confidential information restricted. So, it is highly unwise to share it with them. As a best practice, the employee must not share any information that he deems is of a classified nature. Moreover, efforts should be made for the training and awareness sessions of family and friends.

6.4.2 Anti-phishing and anti-ransomware measures. The user must avoid clicking on the suspected links including those embedded in emails even if it is sent from a trusted source. A safer approach is to always type the link contents into your browser. Moreover, the phishers set up websites almost identical to the spellings of the intended website. So, any accidental mistype could lead you to a fraudulent version of the site. Another important consideration to get alert is when the website offers a product or service at an unheard-of price, or maybe they are promising a significant return on investment. In this regard, some research can be done to find reviews or warnings from other users. Besides that, right-clicking a hyperlink and selecting "Properties" will reveal the true destination of the link, and therefore, can be verified. Moreover, the installation of antivirus is a safety measure that helps in the detection of many malware before they could successfully get executed on the device.

6.4.3 **Safety measures against romance scam/ sextortion/ sex-espionage**.

Besides exercising strong control over human emotions during online interactions, the user should be careful in his overall online conduct. The following measures are proffered:

- Double-check through other platforms (physical and online) to verify the legitimacy of the other person engaged in a cyber-relationship.
- Never post, demand, or exchange any indecent or compromising photos or videos with ANYONE online.
- Double-check privacy settings that could restrict the information from outsiders.
- User should trust their basic instincts while communicating with anyone not personally known. In case of a slight suspicion, all communications must be stopped immediately.
- The user should promptly get suspicious, in case he's asked to send money to a person, have an only cyber-based acquaintance [95].
- DOD officials said, "sextortion often goes unreported because many victims are embarrassed that they fell for it. But it happens worldwide and across all ranks and services". In the case of the lapse, the following may be done:
  - Stop communicating with the scammer.
  - Report the matter in the chain of command for requisite legal assistance.
  - Save all communications you had with that person.
  - Do NOT pay the perpetrator.

6.4.4 **Restricting official work to office premises only**.

Home should be a place to relax and regain energies while spending quality time in the social circle. Presently, the race to staying one step ahead of other peers in the job is leading to errors when employees start doing official work at home, using internet-connected devices. Employees must get abreast of the underlying threats associated with this practice. Besides that, they must not host any official data onto their personal devices.

6.4.5 Segregated devices for internet access having no any classified data. One must not store and process anything on the internet-connected device if that is intended to be protected. And in case, when it's necessary, always use standard encryption mechanisms to keep personal/ confidential information on the device safe, in case the device gets lost.

6.4.6 Discouraging gifts from less known sources. Gifts from unknown sources have the potential to bring along the vulnerabilities that may compromise personal or even organizational security. The employees to understand the situation and motives behind the party extending any gifts. In the slightest doubt, the employee should believe in their instincts, and smartly turn down any such offer. It would surely save them from potential problems.

6.4.7 Smartly dealing with any request for information sharing. There are incidents as highlighted in chapter 5 above, where the employees are socially engineered to reveal classified information, such as, through the conduct of paid lectures, etc. In such an event, the best practice is to seek a written request from the party interested in the lecture. It should be followed by seeking written approval from own organization before promising to participate in any such adventure.

6.4.8 Proper disposal of data containing / processing devices. Proper disposal of the legacy digital devices. The devices should only be disposed-off, after removing the data containers (HDD/ SSD) from them, and physically destroying them. In case, it's not possible, the data sanitization becomes extremely important, which is achieved through these steps performed in sequence [96]: complete data encryption, secure deletion, disk wiping, exposing the device to magnetic media degaussers.

6.4.9 Revoking/ turning off all the mobile connections when no more in use. The persistent availability and discovery of device connections including Bluetooth invite unwanted attacks based on this channel of communication, including bluejack and bluesnarf. Moreover, for wireless connections, disable the auto-connect feature on mobile devices especially when connecting through an unsecured network (in emergencies only). The same holds good for all Bluetooth connections. This practice deters bad actors to get connected to the device covertly.

6.4.10 Strong password implementation. Never leave a mobile computing device without a suitable password, pattern, or gesture to unlock it. It acts as the first line of defence, helps to secure the device from straightforward unauthorized access in the event of a loss. Instead of a simple password, use a strong pass-phrase having a combination of letters, symbols, and numbers. Moreover, it is a safe practice to regularly change PINs and passwords of the device so that malicious websites may not start to identify a pattern.

6.4.11 Revisit the security features of MCD to make it more secure. The default settings of mobile phones are primarily based upon providing the ease of access to its user. This signifies that by-default there's little-to-no security. However, mobile phones offer a good package of security settings, that can be implemented by the concerned user. In this regard, the user must refer to user-manual or online resources to learn about all the security settings, and implement them one-by-one on his device. Besides that, the protection measures for mobile computing devices also incorporate the timely patching and updating of the mobile computing devices, while also removing the unused software, apps, services, etc.

6.4.12 The cautious approach in the installation of various mobile apps. It is always a good idea to keep the applications thoroughly sifted, and keep the minimum ones, essentially required. Besides that, it is always recommended to download and install apps from trusted sources only. It is very important to be cautious about the permissions acquired by the app before getting installed on the device. Should there be any skepticism about an app seeking irrational permission, it should not be installed at all. When in doubt, look for alternative apps with more rational permissions. Moreover, it is a safe practice to completely close down the apps running in the background, and uninstall the ones that are no longer needed.

6.4.13 Being watchful of any unusual happening on the mobile device. The employees should develop a sense of skepticism in using their electronic gadgets. The frequent user gets conversant with his device over time. In this regard, any sudden sluggishness in performance, with relatively faster draining of battery power should incite the alarm. The employees must consult for a piece of expert advice, if there's any setup in the organization, or else learn to backup entire data, and perform a factory-restart to kill the potentially malicious activity, that might be running in the background.

6.4.14 Covering camera lenses when not being used. In the case of the device compromise, it is not very challenging for the adversary to access the device's hardware and sensors including cameras, and invoke it at any time he wants. In this regard, the safe practice is to apply a physical cover on the device (mobile and laptop, etc.) that would allow the opening of the lens, only when the camera feature is required. It would help employees deterring malicious actors from remotely carrying out any privacy infringement through this medium.

6.4.15 Safe use of internet services including email and websites

- **Accessing only validated websites**. It's very important to verify and validate all the links and file downloads well before executing them. e.g., if the link says www.faceb00k.com be sure that it is actually Facebook's link.
- **Use only secure URLs**. Reputable sites begin with https://. The "s" is key. Besides that, the padlock icon must be clearly visible in the browser's address bar, when executing the website. This is especially important when entering credit card or other personal information.
- **The shortened-link website**. As highlighted in chapter 5 above, the shortened link websites often enable malicious actors to mask their malicious code into them. It is therefore recommended not to click on any such links. Rather, a best practice is to hover over the link, without clicking it and notice the full URL of the link's destination in a lower corner of the browser, which is often available. In case it shows any URL other than the intended one, better not to click it. Moreover, the user can securely copy the URL and scan it through URL scanners like "URLVoid", and "VirusTotal" etc.
- **Avoid the use of torrent sites**. Torrent sites must be avoided especially on the computer that hosts personal data, as these are considered to be unsafe, with the availability of pirated versions of various copyrighted programs; and no security check.
- **Avoid accessing websites with explicitly vulgar and profane content**. Accessing such websites on the personal computer with a substantial amount of private data is highly risky, and can lead to data loss; and therefore, must be avoided.

- **Miscellaneous safety measures**
  - Avoid clicking and opening up of spontaneous messages or pop-up windows.
  - Stay safe from re-direction links. e.g., if the writing on the web link says www.gmail.com but it gets changed while placing mouse and hovering on it, it's a clear indication that the link is redirecting to somewhere else. Therefore, it's a safe practice not to click it.
  - Ensure mandatory logging out of every single website or application accessed from the device.
  - It is always advisable not to make use of the option "Remember Login Information / Password".
  - Use specific-purpose email accounts for catering to the unimportant information and controlling the spam.
  - Delete and block any spamming email that claims to fix your device or social media accounts.
  - Avoid downloading or opening any attachments, as long as it is proven to be safe.
  - Avoid using the same password for more than one email accounts.
  - INSCOM OPSEC program manager in the USA, Mr. Connie Moore says, "It's best to make yourself a hard target, make it as hard as possible for the enemy to find your information" [97].

6.4.16 Suitable passwords for all the internet devices at home. The internet devices including routers at home must be secured with a long and suitable password, and must not be relied upon the default password.

6.4.17 Deliberate sessions of security-related conversations with family. In the present times, when the security threats are all around, the employee shoulders a very heavy responsibility of not only get conversant with the situation themselves, but also extend the word of wisdom to their family, and even friends. Unless an adequate level of awareness exists, it is not possible to expect our dear ones to be suitably in a position to stay safe. In this regard, the subject of security (in its entirety including physical and cybersecurity) can be broadly discussed during informal sessions on meals, etc. Later on, they can be gradually brought to immerse into the details of more specific security-related incidents, followed by remedial actions.

6.5 Social Networking, Online Identity, and Data Protection – Guidelines

Online social media has conventionally merged into our lifestyles and the executive staff/ officer cadre of all organizations are no exception to it. At its fundamental level, social media is a powerful new tool of communication. What distinguishes it from other communication tools is the immediacy, freedom, and the extent to which the messages can travel. Accordingly, we have embraced it as a very useful tool for our personal and professional communication including sharing news and engaging with our audiences [98]. In this regard elaborate guidelines are proffered in the following sections:

6.5.1 Guidelines for the account and data protection

- Must use strong pass-phrase instead of common passwords.
- Employees to enable all the requisite security settings on the social media platform.
- Be extra careful of the social media account, and apply requisite security measures including the configuration of two-factor authentication. It will enable us to effectively combating impersonators.
- Must have a separate password for every online account, and avoid using the same password for more than one social media platform.
- Avoid playing third-party games or surveys on social media, since the developers/ owners gain access to user's personal information, required by the particular games/ survey application.
- Innocuous web links on social media platforms are a big risk, and clicking any of those, can cause a device to get infected with malware, that may exploit social media accounts or take control of the user device.
- Minimize online presence and footprints to reduce the vulnerability of compromising any personal information.
- Block the *auto-download* feature from all social media apps, it will deter the arrival of malicious files into the mobile device.

6.5.2 Things to consider before posting information on social media

- All employees and their families are personally responsible for all the contents that they publish on social networking sites, blogs, and other websites [99].

- All the posts are public since the social media platforms/ websites can always revise their user privacy policy; hence sooner or later the posted information is susceptible to be accessed by anyone.
- 3x channels to pass through while engaging in electronic communication:
  - **Reasoning**. Thinking about the message being electronically communicated vis-à-vis the potential audience.
  - **Sorting**. Sorting the contents and the language of the message, to ensure its consistency with organizational values and policy.
  - **Posting**. Posting only those messages that don't expose personal as well as organizational security.
- Avoid misusing the trademarks or violating the copyright.
- Limit the amount and type of information you post online.
- **Self-expression**. All employees may generally express their personal views on matters of public interest matters via social media platforms, in their personal capacity, not linking it with the organization or its policies. However, it's better to avoid unnecessary arguments on public social groups.
- Avoid making any endorsements in the discussions.
- Beware of the interpretability of the post and bear in mind the consequences.
- Make sure, the intended post doesn't contain any classified information.
- Keep in mind the difference between an opinion and official information, and use the best judgement against provocations.
- "Employees must be careful not to comment, post, or link to material that violates the service regulations of the organization. e.g. releasing sensitive information, showing contempt for public officials, or posting unprofessional material that is prejudicial to good order and discipline" [99].

- **Double-checking the information before posting**. There's a need to deliberately have a close review of all the photos or videos before posting online. It would ensure that sensitive or personal information is not released inadvertently (e.g., organizational mission, locations, equipment, job cards, security procedures, and the number of personnel or their personal/ administrative problems, etc.).
- Even a family member or friend's account can be hacked, beware of sharing the information that is not desired to be exposed to the bad actors.

6.5.3 Guidelines for social media connections

- Must verify all the existing social media friends and pending connection-requests face-to-face or at least through verbal communication before going ahead to accept them.
- Have a clear differentiation among friends, family, and others while giving away the access rights to personal information, and therefore, adjust the settings accordingly.
- Put a stronger privacy policy by keeping the profiles private and limiting the information accessible to friends only.

6.5.4 Reporting and disposal of misconduct

- Any employee experiencing or witnessing any online misconduct should immediately report the matter to the chain of command/ supervision.
- The organization must create hierarchical avenues for timely reporting and information.
- Should an employee be proven guilty of online misconduct, he should be promptly trialed with the requisite litigation process.

6.5.5 Guidelines for safe use of Social Media for families & friends

- Be it known that despite all the measures of protecting personal data, the friends and family form the weakest link in the already weaker chain of security, since they may not be very security conscious.
- **Educating family is the employee's responsibility**. Employees should be instructed to suitably educate their families on the material that can and cannot be posted online.

- Never post online the job portfolio and exact whereabouts of the spouses. Developed countries like China and the USA have already been taking measures to educate better halves of the employees, working with sensitive organizations. It focuses on inducing requisite cognizance with the existing threat while ensuring responsible social media behaviour [100].
- It's better to be general about the dates and locations of personal trips.
- Avoid making vacation dates and activities as public.
- Avoid posting the dates, time periods, routines, and portfolio of the spouse's deployment.
- Beware of posting children's photographs, names, and other identities including schools.
- Educate children to timely report any anonymous advancement towards them in cyberspace.
- Educate your children and colleagues to be skeptical and not so trusting.

6.5.6 Responsibility of Executive staff/ officer cadre

- Leaders have a lot of responsibility to mentor their subordinates on organizational values and standards.
- Leaders need to reinforce a climate among all ranks where online-related incidents are not only discouraged but also timely reported, and where necessary adequately addressed at the lowest possible level.
- Leaders provide their subordinates the requisite guidance on how to interact with the public while creating an atmosphere of trust and confidence.
- Part of this mentorship is reinforcing the fact that serving in such a sensitive organization is not less privilege, and as a professional, an employee's private life carries weight into their professional life. This calls upon all employees to uphold the organizational values in and out of its premises.
- All the employees having a role as leaders or supervisors are responsible for fostering an environment where current and future employees understand that online misconduct is inconsistent with organizational values [101].

6.5.7 Guidelines for Organization

- **Training of newly enrolled employees**. Many newly hired employees in a sensitive organization are not fully aware of the repercussions of their online misconduct, since they have been unconcernedly using social media. They and their families are the ones, who need to be specially educated to understand the underlying security threats and ensuing regulations of the organization, before their actual posting.
- Arrangement of regular cybersecurity and social media training at all levels.
- Making cybersecurity courses a criterion for promotion and personal & professional growth.
- A dedicated cell at the organizational level may be established that study and understand how the employees conduct themselves on social media and thus put forward the recommendations on how to educate them to behave against certain expected standards.
- Have a thorough periodical review of the latest trends in cyber threats, and learn from the outside world, while taking precautionary measures accordingly.

6.6 Breaking the kill-chain

While chapter 2, focuses upon the general threats and attack vectors, it specifically defines the potential attack methodology as generally resorted upon by the attacker. It usually begins with reconnaissance – that essentially includes the collection of information of the target organization, including its employees. Subsequently, the attack plan is devised based upon the collected information, and thus initial compromise is made by installing a backdoor or a malware. This further leads to the establishment of a foothold in the organization and its network. Having securely done it, the attacker goes for actual exploitation, followed by carrying out anti-forensic measures.

In all the above discussion, each of the following steps is exquisitely dependent upon the success of the preceding one. That makes it a perfect chain, in which mitigation at one step can break the entire chain. As part of the way forward to the thesis, all the subsequent sections are going to focus upon deterring the adversary to attain that required information which could help him to achieve his objective of compromising an air-gapped network.

Thus, a timely strike against an adversary on the very first step would help an organization to contain the attack, or at least delay it to the extent where it is exposed, and ultimately foiled.

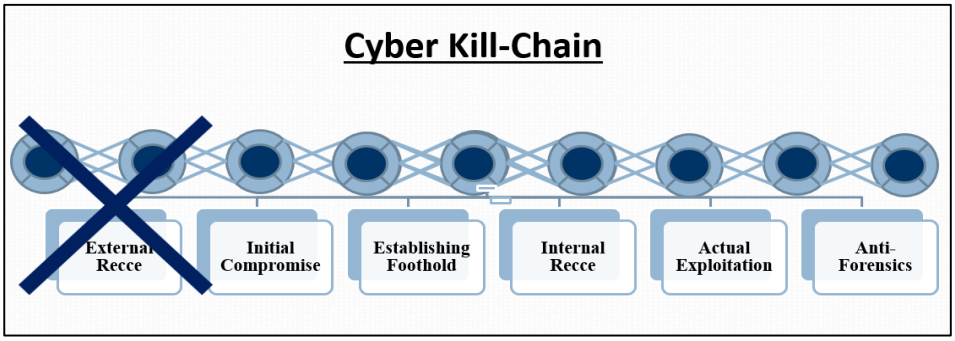

Figure 21: Cyber Kill-Chain

6.7 Conclusion

This chapter has been designed to address the common errors as highlighted in chapter 5 ante. In this regard, the safety measures against each point raised in the previous chapter have been mentioned. Besides that, special emphasis has been laid upon social media guidelines to avert those threats. The chapter has ended by mentioning the need for curbing the potential enemy from seeking information, to kill the chain of a cyber-attack.

Chapter 7

Framework for Human Error, Weaknesses, Threats & Mitigation Measures

7.1 Introduction

Human conduct depends upon their psycho-social behaviours which they develop over the due course of their lifetime. Their behaviours are actually transpired by several personality traits that incite them to go for some (mis)adventure either willfully (violations) or inadvertently (errors & mistakes). The intrinsic weaknesses of human personality fuel the committing of errors, and cause the existing threat to materialize. This chapter seeks to establish a relationship among four variables through a conceptual framework:

- Common human error
- Their underlying personality weaknesses
- Consequent threats
- Mitigation measures

Further, the framework subdivides the errors into four sections, having inferred from previous chapters, keeping in view the state/ place of the person committing errors; i.e. air-gapped site, during transit, after working hours, error by family members. The framework enlightens about the relationships among these entities. The effort in succeeding paragraphs is intended to enlighten policymakers and recruiters at an air-gapped facility. It would help in the incorporation of human weaknesses perspective besides human errors in overall security policy, training, and recruitment of the employees.

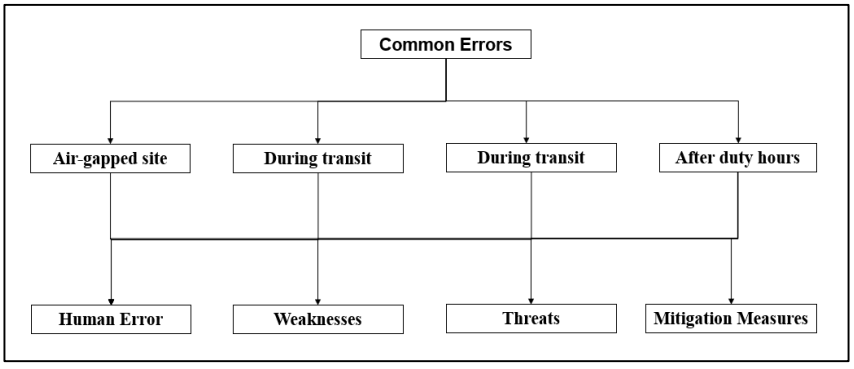

Figure 22: Bird-eye view of Framework

7.2 Common Errors at Workplace / Air-gapped Site

The air-gapped site is the work-place that has been specifically taken into consideration for human errors. Since it is generally believed that a site with air-gapped security measures would be otherwise secured with regards to technical controls. Only the shortcoming at the human end would act as a catalyst in a successful breach of the data. This section seeks to list down the human errors vis-à-vis likely weaknesses, consequent threats, and their mitigations.

Ser	Error	Human Weakness	Threat	Mitigation
1.	Casual disclosure of confidential information	Candidness, Trustfulness	Disclosure of confidential information	Implementation of the need-to-know principle and Non-Disclosure Agreement, Awareness training
2.	Negligently disposing off documents / CDs in Wastebin	Carelessness	Dumpster diving, Loss of data	Implementation of official-waste policy
3.	Inability to report an error	Fearfulness Embarrassment	Recurrence of error	Establishment of the error reporting platform
4.	Disinclination towards cybersecurity	Complacence	Susceptibility to leakage of classified data	Security & awareness training
5.	Physical security lapse	Negligence, Complacence	Unauthorized access, Loss of data Theft of equipment, Physical destruction	An effective access control mechanism DLP measures
6.	Data transfer with unsecured USB drives	Operational comfort	Introduction of malware, Unauthorized data copying	Software restrictions by an access control mechanism Awareness campaigns, Use of secured USB

Ser	Error	Human Weakness	Threat	Mitigation
7.	Bringing of compromised personal devices to the workplace	Lack of security knowledge	Susceptibility to leakage of classified data	Strict implementation of security policy
8.	Use of smart wearable devices	Lack of security knowledge	Potential compromise of air-gapped system	Strict implementation of security policy
9.	Imprudent security culture	Lack of security knowledge	Error repetition and propagation	Security & awareness training
10.	Delays in software patching	Sluggishness, Fatigue	Exploitation of vulnerabilities	Implementation of on-time patch-management
11.	Poor password practices	Forgetfulness, Taking shortcuts	Exposure of classified information	Strong password practice, Repeated practices, spot-checking

Table 1: Framework - Common Human Errors at Air-gapped Site

7.3 Common Human Errors During Transit

The employees often have to find themselves in transit, and therefore, any error committed during transit has definite repercussions for the security of their data. In this regard, the following section seeks to draw relation among the potential errors of the employee during travel vis-à-vis their likely human weaknesses, consequent threats followed by mitigations.

Ser	Error	Human Weakness	Threat	Mitigation
1.	Disclosure of classified information to travel mates	Naiveté, Ingenuousness, Candidness, Trustfulness	Failure to keep classified information	Implementation of the need-to-know principle, NDA Social engineering awareness
2.	Negligence towards luggage items (during travel and at hotels)	Complacence, Carelessness, Trustfulness	Loss of data or storage devices	Awareness training Data Encryption
3.	Considering hotels, a safe place	Naiveté	Leakage of classified data	Not to keep any classified data in a hotel room
4.	Falling into social engineering techniques (physical world): e.g. honey trapping, kidnapping, device-sharing, unacquainted friend-requests	Covetousness, Passion, Curiosity, Helpfulness	Loss of classified data, Life imperilment Physical seizure of person or property	Requisite security clearance Social engineering awareness Avoid sharing of undue information
5.	Lapses on social media (location sharing, status updates, photographs sharing in specific uniforms, etc.)	Curiosity, Excitement, Enthusiasm, Boastfulness	Physical seizure of person or property Getting tracked by a potentially bad actor Potential identity theft	Social media awareness, and its restricted use More private security settings

Ser	Error	Human Weakness	Threat	Mitigation
6.	Inappropriate device charging measures during travel	Lapse	Juice-jacking at public charging points	Carrying of portable power bank
7.	Misplacing personal laptop/ electronic device inadvertently	Carelessness	Loss of property, loss of data	Carrying along throw-away devices with no official data, Suitable encryption measures, Configure auto-wipe for mobile phones
8.	Use of public Wi-Fi	Appeal to costless availability of service	Man-in-the-middle attack	Discouraged use of public Wi-Fi
9.	Apathy towards shoulder surfing	Carelessness	Disclosure of confidential information	Use of data privacy covers Social engineering awareness
10.	Carrying along electronic devices with excessive data during travel abroad	Human curiosity, Anticipation Undue precaution	Loss/ theft of electronic devices containing classified data	Rational selection of items Enciphering crucial data Carrying along throw-away devices with no official data
11.	Deluded to use an infected USB drive	Curiosity, Covetousness	Infected laptop Data compromise	Disposal of gifted/ found items Device sanitizations in a sandboxed environment before use
12.	Oblivion to policies and procedures of the foreign country	Lapse, Conceitedness	The potential target of surveillance	Awareness of local laws and policies before departure Persistent contact with home-embassy

Table 2: Framework - Common Human Errors During Transit

7.4 Common Human Errors After Working Hours

The employee has some of the time, including the period on various holidays/ official leave, and the period after one working-day to another; that he spends as per his own discretion. Certain potential errors are committed in their leisure time, not realizing their underlying threats. The following section mentions the relation of those errors, in relation to potential weaknesses, the arising threats, followed by the mitigation measures.

Ser	Error	Human Weakness	Threat	Mitigation
1.	Sharing of confidential information with family and friends	Trustfulness, Social stimulation, Enticement	Potential leakage of classified information by family and friends	Security & awareness training, Dissuasion of sharing confidential information
2.	Falling to social engineering attacks (in the online world): e.g. Phishing, Baiting, Pretexting,	Naiveté, Reciprocity, Liking, Audaciousness, Trustfulness	Loss of classified data, Life imperilment Physical seizure of person or property Social engineering	Social engineering awareness, Multi-factor authentication, Exercising restraint, Inculcation of skepticism while visiting online resources
3.	Falling to romance-scam/ sextortion/ sex-espionage	Frustration, Carnality, Arousal, Lustfulness, Impulsion	Susceptibility to blackmailing, financial loss, and data loss, Fully compromising of the employee's loyalties	Security & awareness training, Establishment of the error reporting platform Requisite security clearance of the suspect Restrict personal information from public access
4.	Doing official work at home on internet-connected devices	Commitment, Dedication	Inadvertent leakage of data	Restrict office work to office premise only Dissuasion of storing or processing official data on personal devices

Ser	Error	Human Weakness	Threat	Mitigation
5.	Storing confidential data on internet-connected devices	Lack of security knowledge, Frugality	Leakage of confidential information	Segregated devices for internet Use of data encryption
6.	Falling for gifts (electronic gadgets) from less known sources; e.g. USB drives, mobile devices, etc.	Affection, Trustfulness, Acquisitiveness, Intimacy	Loss of personal/ confidential information	Security & awareness training, Learn to smartly turn down offers
7.	Inadvertently revealing of classified information in paid lectures	Opportunism, Financial advantage	Leakage of classified information	Security & awareness training, Learn to smartly turn down offers Report the offers to the concerned platform for clearance & validation
8.	Inappropriately disposing-off data containing/ processing devices (repairs/ selling)	Lack of security knowledge, Insensitivity to the value of held data,	Leakage of confidential information	Removal of data containing devices before overall disposal Physical destruction of data storage device
9.	Negligence towards mobile connections (Wi-Fi, Bluetooth, mobile data)	Lapse, Lack of security knowledge	Susceptible to device hacks by covert connections	Revoke all connections immediately after use
10.	Relinquished password protection on a mobile device	Reposefulness	Loss of personal/ confidential information, if the device got stolen	Implementation of password policies
11.	Relying on default settings of MCD	Contentment, Negligence	Susceptible to device hacks	Security enhancements through device settings
12.	Installing riskware apps on mobile devices with broad permissions	Lack of security knowledge	User data susceptible to mining and leakage	Use of thoroughly sifted apps with rational permissions Closing down background apps

Ser	Error	Human Weakness	Threat	Mitigation
13.	Naiveté attitude towards unusual happenings on a mobile device (performance lag, battery draining)	Lack of security knowledge	Persistence of potential attack source on the device	Security & awareness training, Inculcation of skepticism, Factory-reset device
14.	Keeping camera's lenses uncovered	Lack of security knowledge	Susceptibility to privacy infringement by bad actors	Security & awareness training, Applying physical lens covers
15.	Visiting unsafe websites (e.g. HTTP-based, having shortened links, having pirated or profane contents)	Lack of security knowledge, Frustration, Carnality, Arousal,	Downloading of malicious contents, Device compromise, Leakage of data	Security & awareness training, Exercising restraint
16.	Abstinence from the security-related conversation at home	Time constraints, Inattentiveness	Unpreparedness for security threats	Regular sessions of security-related conversation
17.	Furnishing detailed personal information on social media platforms (e.g. Facebook, LinkedIn, etc.)	Self-conceitedness, Longing for wider social connectivity	Personal information readily accessible to a potential attacker Susceptibility to social engineering attacks	Removal of overstated information with customized security settings having more privacy
18.	Auto-download option enabled for apps	Reposefulness, Amusement	Auto-downloading of unwanted/ malicious files	Revoke the auto-download features from settings
19.	Visiting unsafe websites (e.g. HTTP-based, having shortened links, having pirated or profane contents)	Lack of security knowledge, Frustration, Carnality, Arousal,	Downloading of malicious contents, Device compromise, Leakage of data	Security & awareness training, Exercising restraint
20.	Default administrative password for internet-device at home	Lapse, Insouciance	Internet traffic monitoring and redirection	Suitable password implementation

Table 3: Framework - Common Human Errors After Working Hours

7.5 Common Human Errors by Employee's Family

Often, the employee substantially realizes the threats, and take requisite measures for the safety and security of their own and organizational privacy. However, the family hardly stays in line with the required safety measures, and fall for errors inadvertently. The following section tries to mention a few of those errors with a broader perspective; concerning likely human weaknesses, and consequent threats. Broader mitigation measures have also been mentioned against each.

Ser	Error	Human Weakness	Threat	Mitigation
1.	Sharing of confidential information with others in the physical world (e.g. traveling pass-time with co-passengers, kids revealing information with their friends, etc.)	Trustfulness, Social stimulation, Enticement	Leakage of classified information	Security & awareness training, Dissuasion of sharing confidential information
2.	Diligent & zestful presence on social media platform (e.g. publicly sharing status updates, check-ins & photographs, making spouse-groups, actively participating on social forums, responding to less-acquainted friend-requests, etc.)	Lack of security knowledge, Socialization, Kindness, Trustfulness	User profiling through social media habits, Leakage of classified information including job-nature, postings, Potential identity theft, Social engineering	Security & awareness training, Social engineering awareness, Dissuasion of sharing confidential information, More private security settings

Table 4: Framework - Common Human Errors by Employee's Family

7.6 Conclusion & Future Work

The security of air-gapped networks is indeed a complex phenomenon that needs extensive tailoring of people, processes, and technology. In this contest, adequate measures in the domain of processes and technology are generally taken. However, in the case of the human – the weakest link in the chain of security, the efforts often remain short of the required standards, owing to their inconsistent and unpredictable nature, which can potentially compromise all the measures taken in the prior two domains. The human errors, studied here, applies equally in the almost entire spectrum of cybersecurity-related situations, let alone be the security of air-gapped networks. Thus, an effort has been made to limelight the common errors of the human being vis-à-vis their inherent psycho-social weaknesses and instinctive behaviours. In this regard, the corresponding threats have been identified which finally lead to the requisite remediation measures.

Owing to the enormous magnitude of the topic of human error, the scope of research has been curtailed to the common errors only, which is based upon various online studies and surveys. Taking the lead from this study, the context of research can further be magnified by digging deeper into other circumstances and behavioral aspects of the human being, that incite them to fall for errors. Consequently, more errors, acquired threats, and requisite mitigation measures would help out in preserving the overall security of air-gapped networks.

References

[1] Eric Cole, Ronal Krutz and James W. Conley, Network Security Bible, Foster City: John Wiley & Sons Inc, 2005, p. 694.

[2] Thomas A. Johnson, CyberSecurity - Protecting Critical Infrastructure, Florida: CRC Press, 2015, p. 347.

[3] V. P. A. T. N. F. Pedram Hayati, "Definition of Spam 2.0: New Spamming Boom," in *International Conference on Digital Ecosystems and Technologies*, Dubai, UAE, 2010.

[4] Christopher C. Elison, Malware, Rootkits and Botnets: A Beginner's Guide, New York: McGraw-Hill Education, 2012, p. 432.

[5] J. P.Welch, "Behind Closed Doors: Sex, Love and Espionage: The Honeypot Phenomenon," 2012.

[6] S. Mijalkovic, "'Sex-espionage' as a method of intelligence and security agencies," *Bezbednost Beograd*, pp. 5-22, 2014.

[7] A. O'driscoll, "What is Sextortion (with examples) and how can you avoid it?," 05 February 2019. [Online]. Available: https://www.comparitech.com/blog/information-security/what-is-sextortion-examples/.

[8] Thorn, "Sextortion is an emerging form of online abuse," 2020. [Online]. Available: https://www.thorn.org/sextortion/.

[9] Katie Lange, Defense.gov, "These social media scams target the military," 08 October 2019. [Online]. Available: https://www.army.mil/article/225228/these_social_media_scams_target_the_military.

[10] T. B. Monica T. Whitty, "The online dating romance scam: The psychological impact on victims - both financial and non-financial," *Criminology and Criminal Justice*, 2015.

[11] Steve Piper, Definitive Guide to Next Generation Threat protection: Winning the War Against the New Breed of Cyber-Attacks, Annapolis: CyberEdge Press, 2013.

[12] Donna Leinwand Leger, "Hackers Holding Computers Hostage," 15 May 2014. [Online]. Available: https://www.pressreader.com/usa/usa-today-us-edition/20150515/281496454311814. [Accessed 23 08 2020].

[13] S. Al-Rabiaah, "The “Stuxnet” Virus of 2010 As an Example of an “APT” and its “Recent” Variances," in *21st Saudi Computer Society National Computer Conference (NCC)*, Riyadh, 2018.

[14] Hewlet Packard, "HP 2012 Cyber Risk Report," HP Enterprise Security Products, 2013.

[15] Eric Cole, Advanced Persistent Threat: Understanding the Danger and How to Protect Your Organization, Oxford: Newnes, 2012.

[16] Trend Micro, "A Look at the Threats to Air-Gapped Systems," *Cybercrime & Digital Threats*, 28 September 2017.

[17] FireEye and Mandiant, "Cybersecurity's Maginot Line: A Real-world Assessment of the Defence-in-Depth Model," FireEye Inc, Milpitas, 2014.

[18] George Loukas, Cyber-Physical Attacks, Oxford, UK: Waltham, MA, USA, 2015.

[19] GReAT, "The "Red October" Campaign - An Advanced Cyber Espionage Network Targeting Diplomatic and Governme nt Agencies," 14 January 2013. [Online]. Available: https://securelist.com/the-red-october-campaign/57647.

[20] Snorre Fagerland, Morten Krakvik, and Jonathan Camp, "Operation Hangover - Unveling an Indian Cyberattack Infrastructure," Norman Shark, San Diego, USA, 2013.

[21] GReAT, "The Epic turla Operation," 7 August 2014. [Online]. Available: https://securelist.com/the-epic-turla-operation/65545.

[22] G Data Red Paper, "Uroburos - Highly complex espionage software with Russian roots," G Data. Security Made in Germany, Berlin, Germany, 2014.

[23] Matthieu Faou, "Tracking Turla: new backdoor delivered via Armenian watering holes," 12 Mar 2020. [Online]. Available: https://welivesecurity.com/2020/03/12/tracking-turla-new-backdoor-armenian-watering-holes/.

[24] S. Al-Rabiaah, "The "Stuxnet" Virus of 2010 As an Example of an "APT" and its "Recent" Variances," in *21st Saudi Computer Society National Computer Conference (NCC)*, Riyadh, KSA, 2018.

[25] Julain Assange, "WiKiLeaks - Vault 7," 22 June 2017. [Online]. Available: https://wikileaks.org/vault7/#BrutalKangaroo.

[26] Jasper Mauel and Artem Semenchenko, "Rehashed RAT Used in APT Campaign Against Vietnamese Organizations," 05 September 2017. [Online]. Available: https://www.fortinet.com/blog/threat-research/rehashed-rat-used-in-apt-campaign-against-vietnamese-organizations.

[27] GReAT, Mark Lechtik, Giampaolo Dedola, "Cycldek: Bridging the (air) gap," 03 June 2020. [Online]. Available: https://securelist.com/cycldek-bridging-the-air-gap/97157.

[28] Kenneth Geers, Darien Kindlund, Ned Moran, Rob Rachwald, "World War C: Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks," FireEye, Inc., Milpitas, California, 2014.

[29] H. V. P. a. K. Bommakanti, "Decoding motives behind the Kudankulam intrusion," 22 Novermber 2019. [Online]. Available: https://www.hindustantimes.com/analysis/decoding-motives-behind-the-kudankulam-intrusion/story-c3odQAUqOT1nDgjOMFQRPK.html.

[30] M. Rao, "Kudankulam at cyber risk: Why the govt needs to be more transparent, prepared," 02 November 2019. [Online]. Available: https://www.thenewsminute.com/article/kudankulam-cyber-risk-why-govt-needs-be-more-transparent-prepared-111615.

[31] A. D. Y. E. Mordechai Guri, "MAGNETO: Covert Channel between Air-Gapped Systems and Nearby Smartphones via CPU-Generated Magnetic Fields," *Elsevier - Future Generation Computer Systems*, pp. 115-125, In progress (February 2021).

[32] M. Guri, "HOTSPOT: Crossing the Air-Gap Between Isolated PCs and Nearby Smartphones Using Temperature," in *2019 European Intelligence and Security Informatics Conference (EISIC)*, Oulu, Finland, 2019.

[33] D. B. Y. E. Mordechai Guri, "aIR-Jumper: Covert Air-Gap Exfiltration/Infiltration via Security Cameras & Infrared (IR)," *Elsevier - Computers & Security*, pp. 15-29, 2019.

[34] M. Guri, G. Kedma, A. Kachlon and Y. Elovic, "AirHopper: Bridging the air-gap between isolated networks and mobile phones using radio frequencies," in *9th International Conference on Malicious and Unwanted Software: The Americas (MALWARE)*, Fajardo, Puerto Rico, 2014.

[35] B. Z. D. B. Y. E. Mordechai Guri, "PowerHammer: Exfiltrating Data from Air-Gapped Computers through Power Lines," *IEEE Transactions on Information Forensics and Security*, 2018.

[36] M. M. Y. E. Mordechai Guri, "USBee: Air-gap covert-channel via electromagnetic emission from USB," *14th Annual Conference on Privacy, Security and Trust (PST)*, pp. 264-268, 2016.

[37] A. S. K. A. E. N. A. &. A. A. A. H. Ahmad K. AL Hwaitat, "Computer Hardware Components Ontology," *Modern Applied Science*, pp. 35-40, 2018.

[38] E. F. B. Milosevic, "Wireless MEMS for wearable sensor networks," in *Wireless MEMS Networks and Applications*, Kidlington, UK, Woodhead Publishing, 2017, pp. 101-127.

[39] E. Chang, "What Does a SIM Card Do and Why Do You Need One?," 03 December 2018. [Online]. Available: https://www.thestreet.com/technology/what-does-sim-card-do-14796633.

[40] V. Beal, "WiFi Definition & Meaning," 2020. [Online]. Available: https://www.webopedia.com/TERM/W/Wi_Fi.html.

[41] S. John, "'What is Bluetooth?': A beginner's guide to the wireless technology," 20 May 2020. [Online]. Available: https://www.businessinsider.com/what-is-bluetooth.

[42] J. H. J. J. K. S. J. T. J. D. Bethel Afework, "Battery," 20 April 2020. [Online]. Available: https://energyeducation.ca/encyclopedia/Battery.

[43] T. Stiger, "I/O Control Methods: Types & Explanation," 14 July 2020. [Online]. Available: https://study.com/academy/lesson/i-o-control-methods-types-explanation.html.

[44] M. Fong, "Limiting the potential abuse of smartphone sensors," 11 January 2019. [Online]. Available: https://gcn.com/articles/2019/01/11/smartphone-sensor-risk.aspx.

[45] S. F. P. R. N.L. Clarke, "Biometric Authentication for Mobile Devices," in *Protecting the infrastructure: 3rd Australian information warfare & security conference 2002 security conference 2002*, Churchlands, Western Australia, 2002.

[46] A.-K. K. B. K. Dr. Horst Stipp, "Number of smartphone users worldwide from 2016 to 2021 (in billions)," Statista S. O'Dea, Hamburg, Germany, 2020.

[47] D. Juliao, "Loss of Mobile Devices: Risks & Remediation," [Online]. Available: https://study.com/academy/lesson/loss-of-mobile-devices-risks-remediation.html.

[48] Martin Gontovnikas, "10 Mobile Security Threats (and What You Can do to Fight Back)," 4 December 2017. [Online]. Available: https://auth0.com/blog/ten-mobile-security-threats-and-what-you-can-do-to-fight-back/.

[49] Y. Kumar, "Juice Jacking - The USB Charger Scam," *Elsevier*, 2020.

[50] M. Drolet, "7 potential security concerns for wearables," 11 April 2018. [Online]. Available: https://www.csoonline.com/article/3054584/7-potential-security-concerns-for-wearables.html.

[51] A. Mayor, "Smartphones becoming prime target for criminal hackers," 2014. [Online]. Available: https://www.cbc.ca/news/technology/smartphones-becoming-prime-target-for-criminal-hackers-1.2561126.

[52] Larry G. Wlosinski, "Mobile COmputing Devices Threats, Vulnerabilities and Risk are Ubiquitous," *ISACA*, vol. 4, 2016.

[53] M. B. F. G. F. Ana-Maria Suduc, "Ethical Aspects on Software Piracy and Information and Communication Technologies Misuse," *Elsevier IFAC Proceedings Volumes*, pp. 30-35, 2009.

[54] Kaspersky, "Top 7 Mobile Security Threats in 2020," 2020. [Online]. Available: https://www.kaspersky.com/resource-center/threats/top-seven-mobile-security-threats-smart-phones-tablets-and-mobile-internet-devices-what-the-future-has-in-store.

[55] E. T. S. F. S. F. H. Maryam Mehrnezhad, "Stealing PINs via mobile sensors: actual risk versus user perception," *International Journal of Information Security*, pp. 291-313, 2018.

[56] R. Linke, "Your phone's sensors can spy on you -- here's how," 12 April 2017. [Online]. Available: https://www.computerworld.com/article/3189265/you-phones-sensors-can-spy-on-you-heres-how.html.

[57] The Neilsen Company, "So Many Apps, So Much More Time for Entertainment," 06 November 2015. [Online]. Available: https://www.nielsen.com/us/en/insights/article/2015/so-many-apps-so-much-more-time-for-entertainment/.

[58] Jens Rasmussen, "Skills, Rules, and Knowledge; Signals, Signs, and Symbols, and Other Distinctions in Human Performance Models," *IEEE Transactions on Systems, Man, and Cybernetics,* pp. 257-266, 1983.

[59] James Reason, Human Error, Cambridge: Cambridge University Press, 1990.

[60] D. A. Norman, "Categorization of action slips," *Psychological Review*, pp. 1-15, 1981.

[61] Paul Slovic, Percieved Risk, Trust, and Democracy, New Jersey: John Wiley & Sons, 1993.

[62] Ernst Fehr, Bettina Rocknbach, "Detrimental Effect of Sanctions on Human Altruism," *Nature,* pp. 137-140, 2003.

[63] Karen S. Cook, Trust in Society, New York, USA: Russdel Sage Foundation, 2001.

[64] Arthur Stukas, E Gil Clary, "Altruism and Helping Behaviour," in *Encyclopedia of Human Behaviour*, Kiddlington, UK, Academic Press, 2012, pp. 100-107.

[65] Willium G. Graziano and David A. Schroeder, The Oxford handbook of Prosocial Behaviour, New Yord: Oxford University Press, 2015.

[66] I. A. M. Abass, "Social Engineering Threat and Defense: A Literature Survey," *Journal of Information Security*, pp. 257-264, 2018.

[67] S. Lohani, "Social Engineering: Hacking into Humans," *International Journal of Advanced Studies of Scientific Research,*, p. 10, 2019.

[68] Z. &. S. L. &. Z. H. Wang, "Defining Social Engineering in Cybersecurity," *IEEE Access*, 2020.

[69] A. Nyirak, "The Social Engineering Framework," [Online]. Available: https://www.social-engineer.org/framework/attack-vectors/attack-cycle/.

[70] M. Ahola, "The Role of Human Error in Succesful Cyber Security Breaches," 18 October 2019. [Online]. Available: https://blog.usecure.io/the-role-of-human-error-in-successful-cyber-security-breaches.

[71] IBM Security, "Cost of a Data Breach Report 2020," 2020. [Online]. Available: https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/.

[72] James Reason, Human Error, Cambridge, UK: Cambridge University Press, 1990.

[73] Lee Kiss, "Cyber Security: Identifying and mitigating threats," 22 July 2019. [Online]. Available: https://www.army.mil/article/224804/cyber_security_identifying_and_mitigating_threats.

[74] A. Singhal, "Spoken Words Quotes," [Online]. Available: https://www.goodreads.com/quotes/tag/spoken-words.

[75] Ekran System, "How to Prevent Human Error: Top 4 Employee Cyber Security Mistakes," 24 Spetember 2019. [Online]. Available: https://www.ekransystem.com/en/blog/how-prevent-human-error-top-5-employee-cyber-security-mistakes.

[76] D. B. G. N. Yan Michalevsky, "Gyrophone: Recognizing Speech from Gyroscope Signals," in *23rd Usenix Security Symposium*, San Diego, 2014.

[77] P. O. Lawrence Trautman, "Wannacry, Ransomware, and the Emerging Threat to Corporations," *SSRN Electronic Journal*, pp. 503-556, 2018.

[78] G. M. McKay Smith, "Equi-Failure: The National Security Implications of the Equifax Hack and a Critical Proposal for Reform," *Journal of National Security Law & Policy, Vol. 9, No. 3*, p. 40, 2018.

[79] U. National Cyber Security Centre, "Most hacked passwords revealed as UK cyber survey exposes gaps in online security," 21 April 2019. [Online]. Available: https://www.ncsc.gov.uk/news/most-hacked-passwords-revealed-as-uk-cyber-survey-exposes-gaps-in-online-security.

[80] B. S. Syed, "Mystery as retired army officer goes ‘missing’ in Nepal," 09 April 2017. [Online]. Available: https://www.dawn.com/news/1325799.

[81] R. Beckhusen, "Mexican Cartels Enslave Engineers to Build Radio Network," 01 November 2012. [Online]. Available: https://www.wired.com/2012/11/zeta-radio/.

[82] P. G. K. L. F. C. N. S. Janice Y. Tsai, "Location-Sharing Technologies: Privacy Risks and Controls," *Elsevier- Social Sciences Research Network (SSRN),* 2012.

[83] J. Thomas, "Individual Cyber Security: Empowering Employees to Resist Spear Phishing to Prevent Identity Theft and Ransomware Attacks," *International Journal of Business and Management* , 2018.

[84] S. Mijalkovic, "'Sex-espionage' as a method of intelligence and security agencies," *Bezbednost Beograd*, pp. 5-22, 2014.

[85] F. J. F. Francesca Gino, "Give them what they want: The benefits of explicitness in gift exchange," *Elsevier - Journal of Experimental Social Psychology*, pp. 915-922, 2011.

[86] J. I. S. Yujin Jeong, "Threat of Falling High Status and Corporate Bribery: Evidence from the Revealed Accounting Records of Two South Korean Presidents," *Strategic Management Journal,* pp. 1083-1111, 2018.

[87] D. o. Justice, "Justice News - Former CIA Officer Sentenced to Prison for Espionage," 17 May 2019. [Online]. Available: https://www.justice.gov/opa/pr/former-cia-officer-sentenced-prison-espionage.

[88] A. Greenberg, "A Tesla Employee Thwarted an Alleged Ransomware Plot," 27 August 2020. [Online]. Available: https://www.wired.com/story/tesla-ransomware-insider-hack-attempt/.

[89] M. Woburn, "Kaspersky Lab Finds Over Half of Consumers Don't Password-Protect their Mobile Devices," 28 June 2018. [Online]. Available: https://usa.kaspersky.com/about/press-releases/2018_kaspersky-lab-finds-over-half-of-consumers-don-t-password-protect-their-mobile-devices.

[90] Kaspersky, "Top 7 Mobile Security Threats in 2020," 2020. [Online]. Available: https://www.kaspersky.com/resource-center/threats/top-seven-mobile-security-threats-smart-phones-tablets-and-mobile-internet-devices-what-the-future-has-in-store.

[91] Abigail Kelly, "Army Families: Are you doing your part on social media to keep Soldiers safe?," 10 August 2018. [Online]. Available: https://www.army.mil/article/209671?st.

[92] B. Osborne, "10 Benefits of Security Awareness Training," 17 August 2018. [Online]. Available: https://resources.infosecinstitute.com/10-benefits-of-security-awareness-training/.

[93] L. V. A. A. B. M. H. Adéle Da Veiga, "Defining organisational information security culture – Perspectives from academia and industry," *Elsevier - Computers & Security,* 2020.

[94] Kensington Computer Products Group, "Privacy Begins on Screen," 2020. [Online]. Available: https://www.kensington.com/product-finder/privacy-screens/.

[95] Mr. Colby T Hauser (USACIDC), "U.S. Army CID Pleads with Public, Warns Against Romance Scams, Female victims being cyber-robbed dai," 26 Novemebr 2012. [Online]. Available: https://www.army.mil/article/91787/us_army_cid_pleads_with_public_warns_against_romance_scams_female_victims_being_cyber_robbed_dai.

[96] CISA, "Security Tip (ST18-005) - Proper Disposal of Electronic Devices," 14 Novermber 2019. [Online]. Available: https://us-cert.cisa.gov/ncas/tips/ST18-005.

[97] B. E. Justin Creech, "INSCOM shares tips to keep online information secure," 14 March 2013. [Online]. Available: https://www.army.mil/article/98599/inscom_shares_tips_to_keep_online_information_secure.

[98] D. o. Defence, "Army Social Media - Army Leaders," 2017. [Online]. Available: https://www.army.mil/socialmedia/leaders/.

[99] D. o. Defence, "Army Social Media - Soldiers And Families," 2017. [Online]. Available: https://www.army.mil/socialmedia/soldiers/.

[100] Lei, Zhao, "Military wives warned about risk of secret leakage on WeChat," 07 April 2015. [Online]. Available: http://www.chinadaily.com.cn/china/2015-04/07/content_20011532.htm.

[101] C. B. Michael W. Johnson, "Professionalization of online conduct," 25 July 2018. [Online]. Available: https://www.army.mil/e2/downloads/rv7/socialmedia/ALARACT_058_2018_PROFESSIONALIZATION_OF_ONLINE_CONDUCT.pdf.