NATIONAL CYBER SECURITY POLICY DEVELOPMENT TO DETER THREATS AND MINIMIZE THE RISK OF DATA BREACH FROM AN AIR-GAPPED NETWORK

By

Zaheer Shaukat Khan

00000325139

A thesis submitted to the faculty of Information Security Department, Military College of Signals, National University of Sciences and Technology,Islamabad, Pakistan, in partial fulfillment of the requirements for the degree of MS in Information Security

SEPTEMBER 2021

DECLARATION

I certify that this research work titled “National Cyber Security Policy Development to Deter Threats and Minimize the Risk of Data Breach from an Air-Gapped Networks” is my own work. No portion of this work presented in this dissertation has been submitted in support of another award or qualification either at this institution or elsewhere. The material that has been used from other sources has been properly acknowledged / referred.

_____

Signature of Student

Zaheer Shaukat Khan

0000325139

ABSTRACT

Worldwide connectivity and digitalization of services have escalated the usage of information and communication technology which in turn has resulted in greater exposure of information assets to a hub of sprouting cybersecurity vulnerabilities and threats. Cybersecurity policies are a cornerstone for governing cybersecurity in an air-gapped network. These policies define the need to safeguard an organization's assets for confidentiality, integrity, and availability. Therefore, the present research aims to develop governing and technical policies to ensure resilience against cyberthreats in an air-gapped network. After the development of a main governing policy, five subsidiary/ technical policies were developed namely Personnel Policy, Social Engineering Policy, Physical Security Policy, Infrastructure Hardening Policy, and Access Control Policy. Personnel Policy was developed for the compliance of recruitment, training, and departure of personnel with the security safeguards to the access and use of info technology resources and data. A subsidiary policy on Social Engineering being indispensable to inform employees that fraudulent social engineering assaults do occur, and processes exist for detecting such attacks was included in the current study. Likewise, a Physical Security Policy to protect the physical security of all humans and info assets effectively stops unauthorized physical access, destruction, and interference with info and info processing facilities was developed. An Infrastructure Hardening Policy was added as a subsidiary policy as it is direly needed to harden the system or structure by reducing its surface of vulnerability and mitigating the possibility of a successful attack by further decreasing the obfuscation. The Access Control Policy specifying the rules related to authorizing, monitoring, and controlling access to an organization's accounts, information, and information systems was added as part of the sub-policies. After an extensive elaboration of the aforementioned governing and technical policies, guidelines on system hardening as an illustration of describing the procedural details have been described delivering step-by-step instructions on the 'how' of taking out the policy statements. System hardening guidelines enable end-users to secure their PCs and laptops from various threats, vulnerabilities, and viruses. In conclusion, robust enforcement, consistent audit, and regular up-gradation of policies and guidelines is the only viable mechanism to safeguard the confidentiality, integrity, and availability of assets in an air-gapped network.

COPYRIGHT STATEMENT

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 beloved **Parents, Wife, Siblings, Children**, and respected teacher **Brig. Dr. Imran Rashid** whose unflinching trust, help, support and prayers paved the way for me in the timely completion of this work.

ACKNOWLEDGEMENTS

I humbly thank Allah Almighty, who is most Beneficent and the most Merciful, Whose blessings are abundant and favours are unlimited. I offer humble durood-o-salam to the praiseworthy Holy Prophet Muhammad ﷺ.

I would like to express my deep and sincere gratitude to my research supervisor, Brig Dr. Imran Rashid Ph.D., for giving me the opportunity to do research and providing invaluable guidance throughout this research. His dynamism, vision, sincerity, and motivation have deeply inspired me. It was support, privilege and honor to work and study under his guidance. I am extremely grateful for what he has offered me. I would also like to thank him for his friendship, empathy, and great sense of humor.

I am extremely grateful to my parents for their love, prayers, care and sacrifices for educating and preparing me for my future. I am highly indebted to my wife, no matter how badly I failed, she always treated me like a winner, thanks for being so supportive. I am very much thankful to my children Mustafa and Ibrahim for their love, understanding, prayers and continuing support to complete this research work.

I would also like to extend my feelings of gratitude towards Lt Col Khawar Mehmood and Maj Maj Umar Malik for their continuous guidance, help, and endless support.

Finally, I would like to express my appreciation to all the people who have provided valuable support to my study and whose names I could not bring to memory.

Table of Contents

List of Figures

List of Tables

Acronyms

AG	Air-Gap/ Air-Gapped
AGN	Air-Gapped Networks
CPT	Cybersecurity Program Team
DDOS	Distributed denial of Service
DOS	Denial of Service
EB	Executive Board
HR	Human Resource
Info	Information
ICT	Information Communication Technology
IO	Information Owner
IT	Information Technology
PC	Personal Computer
SO	Security Officer
SQL	Structured Query Language

Chapter 1

Introduction and Thesis Organization

1.1 Overview

Data has superseded money in the recent times as one of the most invaluable property whether it comes to an individual or an organization. It is almost impossible that a precious data, if compromised could be regained in a state, where its confidentiality, integrity and availability is guaranteed. On the contrary, financial resources once lost could be recuperated, redeemed, and restored with time. The situation becomes graver when it comes to the organizations where a data breach could have serious consequences in terms of national security. In this respect, robust measures are sought by the national organizations to guarantee the safety and security of the data, including the incorporation of AGN that physically isolates the internal organizational networks from the rest of the world. The protection of ICT networks from advanced cyber-threats is a challenging task, comprising host level and network level security layers. This incorporates updates of protection software in host computers, management of access controls, routers and firewalls configuration, Digital telephonic systems etc. However, even though a high level of protection is attained, given that the local area network relates to the outside world (e.g., the Internet), a ground-breaking and innovative attacker will sooner or later probe a way to breach the network, snoop, and spread sensitive data as is evident from past experiences. From this history, governments and enterprises have taken robust measures to guarantee the security and safety of the classified info, including the employment of AGNs that genuinely segregates the inside authoritative organizations from the remainder of the world. The AGNs are isolated (both physically and logically) from rest of the public networks (such as, the Internet).

Such networks are mostly used in defence forces, critical infrastructure and control systems, stock exchanges, insurance companies, biomedical manufacturers, and wide range of industries. The AG isolation is aimed at deterring the disclosure of classified info that include confidential personal info, intellectual property, financial data, and trade secrets etc [1].

Cybersecurity may be defined as a multi-disciplinary approach that encompasses both the software and hardware with a goal of preventing the incidence of cybercrime at the first instance or waning its impact if it has already occurred. Cybersecurity is a crucial challenge for several corporations such as government databanks, financial companies as well as banks and military. Security policies are an official set of rules that are made by an institute to safeguard that the user approved to gain access to company info and technology endowments abide by the rules and procedures related to the info security. It is a written paper in the company which is accountable for how to safeguard the corporations from risks and how to manage them when they occur. The security document is a high-level text that describes the organization's vision regarding security, needs, goals, responsibilities, and scope. A security policy is regarded as a "living document" which implies that the document is never done, but it is constantly updated as conditions of the technology and employee varies. A security policy should achieve many goals. It should: guard people and data; set the guidelines for anticipated behaviour by users, system administrators, management, and security personnel; sanction security personnel to monitor, inquire, and examine; define and sanction the consequences of violation; outline the corporation consensus baseline stance on security; help curtail risk; and assist track compliance with regulations and legislation. Cybersecurity policies are also perilous to the public image and integrity of a cooperation. Customers, partners, shareholders, and prospective employees need

evidence that the corporation can keep its sensitive info. Without a cybersecurity policy, an organization may not be able to furnish such proof [2].

Continuing from the prehistoric times till to date, the art of war is an ever-evolving phenomenon, cyber warfare being one of them. It is mutating exponentially causing a lot of untoward events, ranging from data theft to the acquisition of state secrets and classified data of national interest. The modern world has become a digital realm; therefore, the cyber security threats are also increasing proportionately. Pakistan being a territory of utmost geopolitical location and a nuclear power is at an increased risk of cyber security threats. Lack of a national cyber security policy may be a great threat to the sensitive organizations having classified data [3].

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 network is considered as sole guarantee of protection of data from spillage of classified info. However, news of recent successful attacks and consequent data loss from the AGNs (nuclear sites of a country) reveal that technical controls alone do not provide due assurance against data breach. Cybersecurity policies are crucial because cyberattacks and info breaches are potentially expensive. Also, employees are frequently the weak connections in a company's security. Moreover, the human being working in the organization is considered as the weakest link in the chain of security. Since he also retains his footprints on social media network in one form or another; an intentional or accidental slippage of even a slight confidential info can lead to a big security risk, making the very isolation of AGN questionable. Upgraded cybersecurity policies can assist employees and consultants better comprehend how to sustain the security of info

and applications. Thus, design of a comprehensive national cyber security policy, its implementation, auditing, and continuous upgradation remains a customary pre-requisite to ensure any security breach.

1.3 Research Objectives

The main objectives of the present study are:

- Study and analyze the various threats that could lead to potential security breach in an AGN.
- Propose a comprehensive national cybersecurity policy to deter threats and minimize the risk of data breach from an AGN.
- To develop procedures and guidelines in accordance with the developed cybersecurity policy for military and civil organizations.

1.4 Scope

The research has following implications:

- **Public/Private Sector:** Reputation is one of the most valuable assets of an enterprise. Any loss to the reputation can have far-reaching adverse effects on the firm's standing, stakeholder's trust and loyalty, the general acceptability of the operations, and very survival of the business. Besides that, a data breach has potential to put millions of customers at risk and poses considerable costs to the businesses. National firms of Pakistan, directly responsible as custodians of public data (including NADRA, telephone/ mobile phone companies) have a lot at stake if any data breach happens. Besides, they implement technical controls for protection of sensitive info; the research will assist all such organizations to further enhance their security parameters by reviewing and updating their policies in lines to the identified common mistakes by the legitimate user.

- **Military:** Military organizations, as a matter of common security practice across the globe, keep their classified info isolated from the outside networks (internet). Owing to the value and sensitivity of the info, it is imperative to further strengthen its defense by suitably updating already deployed security mechanisms. The proposed policy would help to further increase air in the AGNs, while also deterring the slippages that could eventually bridge the gap caused by the leakage of confidential info.

1.5 Contribution

The modern world has become a digital realm; therefore, the cyber security threats are also increasing proportionately. Pakistan being a territory of utmost geopolitical location and a nuclear power is at an increased risk of cyber security threats. Lack of a national cyber security policy may be a great threat to the sensitive organizations having classified data. Therefore, the research would enable the policymakers to adopt the proposed policy or refine their policies and include the missing perspectives addressed in the present study. The research would also assist in improving the overall data security of the air-gapped networks. It will be 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. It would assist civil and military sensitive organizations having AGNs 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 entails an introduction to cybersecurity and AGN. Cybersecurity elements along with cyber resiliency techniques and implementation approaches have been discussed. The chapter also describes the various structural features of an AGN with a brief description of its components and applications.
- Chapter 3 highlights intimidations and attack routes against an organization. The contents encompass a general threat landscape and proceed on to a more specific description of cyber-attacks.
- Chapter 4 ponders some light on cyber-attacks on an AGN including social engineering as an important vulnerability to AGN security.
- Chapter 5 is exclusively dedicated to the importance of policies and procedures and their implications in ensuring cybersecurity in an organization. Some of the challenges in the development of security policies are also discussed.
- Chapter 6 proposes a governing cybersecurity policy for an AGN followed by subsidiary policies and as a sample, guidelines for system hardening have also been included.
- Chapter 7 overviews the recently approved National Cybersecurity Policy of Pakistan 2021 trailed by an opinion on its strengths and weakness and way forward.

1.7 Research Methodology

In the current study, the literature review was done by studying diverse research articles of reputed journals from Google Scholar. For the purpose of national cyber security policy development for an AGN, a review based upon a number of scientific papers retrieved from various academic databases, such as IEEE, ACM, Springer and ScienceDirect, and reports of several information security, such as SANS. The security policies of contemporary countries such as Australia, Japan, the United Kingdom, and the United States were also studied for policy development. Furthermore, security policy templates from SysAdmin, Audit, Network, and Security (SANS), and the National Institute of Standards and Technology (NIST) were also reviewed for the policy write-up.

Chapter 2

Cybersecurity and Air-gapped Network

2.1 Introduction

Progressively systems are being digitized in a run towards smaller costs, increased efficiency, and lessened time to market. However, this push to digitization also makes these systems vulnerable to a progressively erudite and incapacitating array of cyber-attacks. Cybersecurity may be described as a multi-disciplinary method that incorporates both the software and hardware with a goalmouth of avoiding the frequency of cybercrime at the first case or waning its effect if it has already happened. Cybersecurity implies to machineries, procedures, and systems intended to protect networks, tools, databases, and the data from the incident, loss, and unapproved access. It is a crucial problem for many establishments such as government catalogues, economic corporations including banks and military establishments. Cybersecurity is a worldwide phenomenon demonstrating an intricate socio-technical question for governments but needing the participation of individuals. Although it is one of the most crucial challenges encountered by governments today, the outlook and public understanding remains restricted. The Internet is all too frequently believed as a safe atmosphere for sharing material, transactions and regulating the physical world. Yet, cyberwars are already unending, and there is a vital need to be better equipped. The incapability to border cybersecurity has rose in a failure to progress appropriate policies [4].

The necessity for cybersecurity is becoming more and more important due to our dependency on Info and Communication Technology (ICT) across all facets of our cyber physical civilization. Cybersecurity is important for individuals, community and

non-public organizations, but promising security to everyone often proves to be challenging. The internet sites of many governments have restricted security and could be easily hacked. The question of security is not partial to the administrative power, but it is also applicable to political parties, energy substructure providers, water-boarding, road administration, ministries, secretarial organizations, NGOs and sporting establishments (such as the International Olympics Committee), all of which have previously been the mark of clefts and the robbery of info. The hack on World Antidoping Agency (WAPA) published the medical record of Olympic athletes to concede them, whereas the Stuxnet virus was intended at damaging a nuclear substructure. Cybersecurity infringements can thus be said to affect all shareholders in our society [5].

2.2 Cybersecurity

2.2.1 Cybersecurity Elements

For effective cyber security, an organization must coordinate its efforts throughout its whole info system. Components of cybersecurity include:

2.2.1.1 Network security

The course of shielding the network from undesirable users, spells, and invasions. Network-security refers to the network manager's all-encompassing security strategies and provisions for discouraging and monitoring illegal access, deliberate mistreatment, amendment, rejection of a facility for a host or client computer, and other available network and communication related capitals in an adaptive and upbeat manner. It entails examining workers' freedom rights in order to verify users' legitimacy and grant them access to network records or permission to exchange data. To establish their authorization and subsequent use of permitted spheres, workers are assigned ID and

passcodes or extra forms of verification checks. Network security broadens reporting across a variety of computer networks, both public and private, that are applied for executing and collaborating amid corporations [6]. The security process starts with worker authentication, which can be accomplished using one, two, or three elements. The first element entails password authentication, whereas the second element implies password authentication in conjunction with a safety dongle, coupon, mobile phone, or card; and the third element implies retinal examination or thumbprint authentication in conjunction with the first two elements. A web firewall enforces entry policies, such as which facilities can be opened by network users, once the validation is complete. Antivirus software and interference avoidance systems assist in detecting and preventing the possibly malevolent content that spread across the web as Trojans and worms. For checking the network stream of traffic for dubious or unusual content or behaviour, an anomaly-based intrusion recognition method may be used. This will assist in preventing situations like DOS attack or a dissatisfied employee tampering with files, thus safeguarding the reserves. Individual occurrences that happen inside the network can be recorded for later review or top-level inspection. The transmission between network hosts can be encrypted to prevent spying. The placement of false network reachable resources will assist with supervision and in advance notice actions. Following the advancement of new manipulation tools, the techniques used by invaders for conceding the trap resources might be analyzed post-strike to understand their logic. The frequent types of outbreaks met by networks include passive outbreaks such as port scanner, idle scan, wiretapping; or active outbreaks such as spoofing, DDOS attack, buffer or heap overflow, smurf attack, ARP poisoning, format string attack, and SQL injection [7].

2.2.1.2 Application security

Application security refers to the procedures taken throughout the life of an info product to prevent any shots from violating the permission limitations imposed by the core system's security requirements. The safety protocols outline the exceptions for systems that are fundamentally flawed in terms of design, development, and implementation, as well as application up-gradation and maintenance. Applications are merely involved with regulating the use of resources provided to them. The precise usage of resources is established through the application consumers through application defense. The approach to deal with menaces to application security entails knowing about the prospective hazards, adequately augmenting the safety measures of the application, host, or network, and implanting protection within the software improvement method [8]. An asset in the perspective of application security refers to a valuable resource, such as info in a database or the file structure, or a system reserve. The goal is to find vulnerabilities inside a parental system that, when subjected to a cyber intruder, could be used to provide useful insight into the functionality of an application. By bending security within the application, the threat can be reduced [9].

General application risks and assault types are numbered below.

- Input authentication-related such as buffer overflow, cross site coding, SQL injection, and canonicalization.
- Verification related such as network eavesdropping, brute force assault, dictionary assaults, stealing credentials and replaying cookies, etc.
- Approval related such as privilege elevation, tampering with critical data, inviting attacks, intentional revelation of sensitive info etc.
- Alignment managing related such as illegitimate entry into configuration stores, illegitimate access to administrative controls and absence of user’s

accountability, retrieving clear text configuration info, procedural accounts, and higher-privilege service.

- Classified info related like trying to penetrate storage space for obtaining important data, tapering with data, and eavesdropping network lines.
- Session managing related such as replaying session, man in the middle, hijacking session etc.
- Cryptography related like weak encryption, poor public, or private key production or key management,
- Parameter exploitation linked like query manipulating query string, cookie, HTTP header, or form field.
- Exception managing correlated like DOS or info disclosure.
- Inspecting and logging are associated like misuse of an application by the intruder and comprising up the trail, denial by a user to perform an operation [10, 11].

2.2.1.3 Information security

- Info security includes safeguarding confidential info from illegal entry, disclosure, reading, disruption, usage, modification, assessment, recording or loss. This is a guarantee that crucial data or info is not missing when any other matter like natural disasters, stealing, system breakdown, or possibly other destructive situation occurs [12].
- The qualities shaping security are availability, confidentiality, and integrity. The info systems are a corporation of software, hardware, and networks. The purpose is to recognize and utilize info security concerning safety and deterrence mechanisms at the three stages. The measures generated, act as

strategies for officials, employees, and workers to stick to secure usage habits for intensified security [13].

- Data confidentiality communicates to preventing willful or unintentional info release to illegal systems or people. Confidentiality is implemented through encoding of crucial info during communication over delicate communication networks susceptible to spying. The sites where info will be detectable are restricted such as backups, databases, printed receipts, log files, etc., and by putting limitations on the data storage space. It inhibits security violations which can be in lead to the revelation of confidential info from a secure system [14].
- Data integrity mentions the upkeep and guarantees the liability, stability, and precision of the secret data during its life. This means blocking unauthorized or unnoticed amendment of data both in storing or while in transfer [15].
- Data availability implies that the info is obtainable for usage when needed by approved services and clients. This demands for proper operation of systems utilized for collecting and controlling info, security systems used for protecting info, and the web networks used for retrieving it. The system should always be accessible by not permitting service disturbances owed to hardware glitches, power failures, and system improvements. This also relates to discouraging the rejection of service spells [3].
- Authenticity involves the authenticity of the operations, info, communications, or records. It includes examining the qualifications of the clients getting to enact with system. Non-repudiation says that the parties engaged in an agreement cannot refute their role with data communication or reception.
- Risks that could possibly harm the info system are evaluated and necessary alleviation steps are undertaken [16].

2.2.1.4 Endpoint security

Remote entry is an important component of business, but it can also be a data vulnerability. Endpoint security is a means of preventing unauthorized remote access to a company's network.

- **Data security:** Data is inside the applications and networks. A distinct layer of protection protects company and client info.
- **Identity management:** In essence, this is a means of determining the level of access that each individual has within an organization [17].

2.2.1.5 Database and infrastructure security

Databases and physical equipment are used in every aspect of a network. It's also critical to safeguard these devices.

2.2.1.6 Cloud security

Several documents are in digital settings or “the cloud”. Protecting data in a 100% online situation poses many risks.

2.2.1.7 Mobile security

In and of itself, cell phones and tablets entail a plethora of security concerns [18].

2.2.1.8 Disaster Recovery/Business Continuity Planning

Data must be kept safe in the event of a break, natural adversity, or other incidents, and company must continue. A strategy is required for this. The trickiest task in cybersecurity is the evolving nature of security dangers themselves. Conventionally, officialdoms and the government have fixated most of their cybersecurity capitals on border security to safeguard only their most critical system elements and protection against notorious risks. Once a cyber-attack has brought the firm to a halt by disabling the info systems, disaster recovery planning is critical in keeping the grave parts ticking in order for the business to survive. The planning aids in the reduction of recovery costs

and operating expenses. The critical criteria described below should be carefully considered when developing effective business continuity strategies that will allow companies to successfully navigate through difficult times. What are the primary areas where care should be given in the event of a disaster affecting the info system? Should be approved users be contacted to confirm their safety, or should the bank or e-payment gateways be contacted to ensure that the company's funds are safe? The emergency response convoy should be well-prepared to stop the calamity, and the Crisis Management team should get to work. Which areas of the business should be prioritized for recovery first? Should this be the cash cow part, or should it be the one to which the majority of the capital has been allocated? Which aspect of the info system is critical for long-term success? The most serious business unit should be the most well-known division. What should be the suitable time range for recovering critical info units? The answer to this question will entail calculating the amount of money required to recover from a disruption. What resources and structures would be necessary to restore IT operations? The proportional importance of each contributing factor should be carefully considered. This will make it easier to understand the costs involved. The responsibility for ensuring business continuity falls on the shoulders of CEOs. What is the most calculated way to handle business retrieval? Will the business center have enough space, or will it be overrun with other disaster stricken people?

Once the adversity recovery strategy has been activated and production has begun at a reduced capacity, an evaluation must be carried out to determine the life of such ventures in the absence of primary operational locations. To understand the strength of a firm, it is necessary to do a thorough analysis. Should a company recovery be required, the recovery plan should be reviewed at least once a year to ensure that it produces the

desired results. The technique can be assessed for suitability, and necessary rewrites/updates can be implemented.

A business stability plan takes a comprehensive approach to dealing with the effects of a crisis on the entire organization. A disaster recovery plan is essentially a subset of business stability, and it focuses on taking the necessary steps to get normal business operations back up and running as soon as possible. The disaster recovery strategy is implemented immediately following a calamity. It is a detailed list of activities to be taken in order to recover classified info technology infrastructure as quickly as possible. Disaster recovery planning entails the formation of a planning group to conduct risk assessments, focus on jobs, establish recovery methods, compile records, and finalize the plan. The plan's implementation is being led by the development of certification benchmarks and auditing techniques [17].

2.2.1.9 End User Education

The human factor in cybersecurity is that the weakest link must be properly taught in order to be formlessly vulnerable. Users who regularly interact with the highly protected system and access classified info must have a thorough understanding of the security policies, tactics, and procedures. End-user education and surveys are required on a regular basis to bring the user's attention to organizational flaws, system vulnerabilities, and security flaws. Users' safe behavior should take precedence above all other considerations.

It has been discovered that training delivered at random or at a high level is less effective than frequent, granular training and exercises tailored to users' individual behavioral patterns and practices. Senior executives should be required to attend training programs in order to demonstrate the necessity of responsible security conduct in order to combat the threat of cyber-attacks.

Strong cybersecurity programs employ a combination of technological and human resources. Aside from technology infrastructure, organizations should show a genuine interest in donating to areas of human-based security. Providing increased openness and demonstrating a readiness to adopt emerging ways by users can yield significant benefits.

The training should be based on an investigation of user behavior and courage at various levels of info security. Better human element protocols within the security chain are frequently built by learning about users' perspectives on technology and how they respond to security issues. The training sessions will lead to more research in the area of human-machine interactions.

Cybercrime is progressively morphing into social engineering, in which criminals devote resources in gaining knowledge about organizational stakeholders. Senior management will benefit from training because they will get more familiar with system users, which will help to raise knowledge of user-specific access privileges and internal sources that can provide access to secret info. User training will assist in removing resistance to change and increasing user scrutiny [19].

2.2.2 Framework of cyber resilience

Cyber resilience is the capability to plan for, act in response to and recoup from cyber attacks. It facilitates organisations to safeguard themselves from cyber hazards, shield against and reduce the gravity of attacks, and make sure that company processes continue to function.

Although the concept is new, it is based on long-standing solutions to common issues and is fast becoming an important response to the contemporary threat landscape. Cybercrime is growing, and assaults are indiscriminate, so all organisations must be prepared for a disruption..

The Cyber Resilience Framework was designed to assist increase awareness about cyber resilience as shown in Figure 2.1.

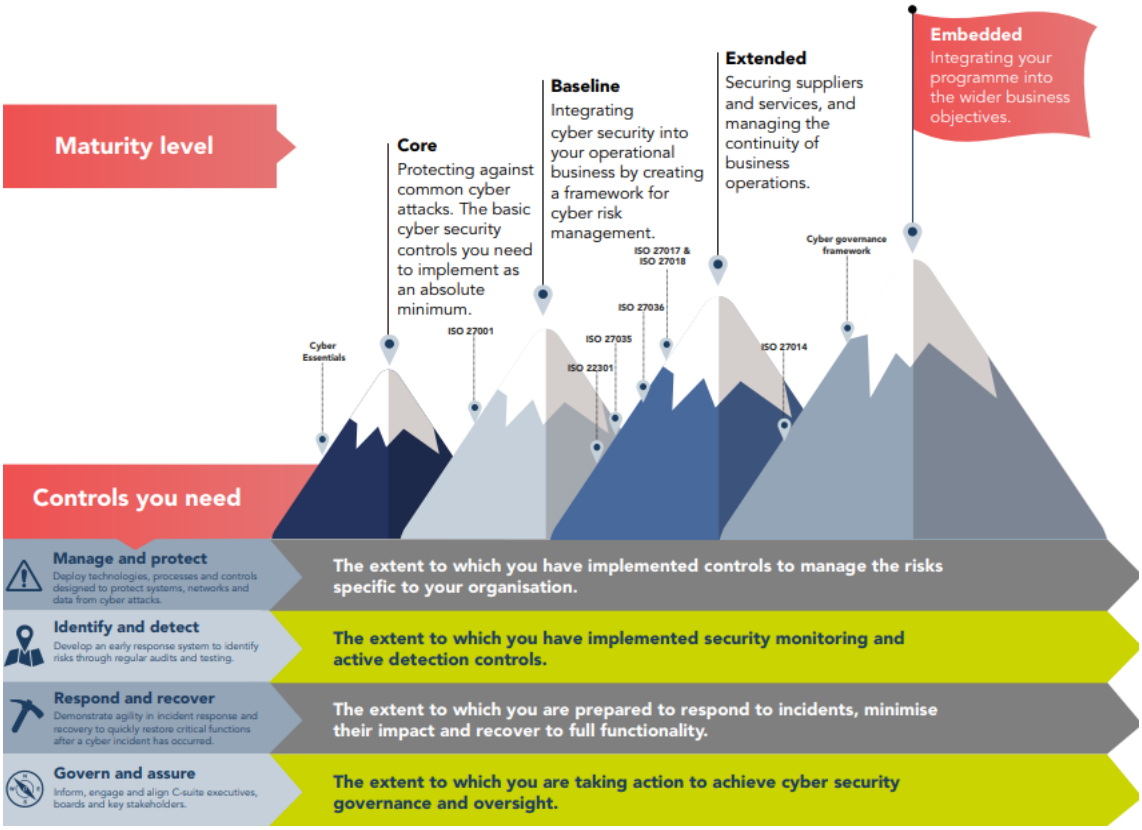


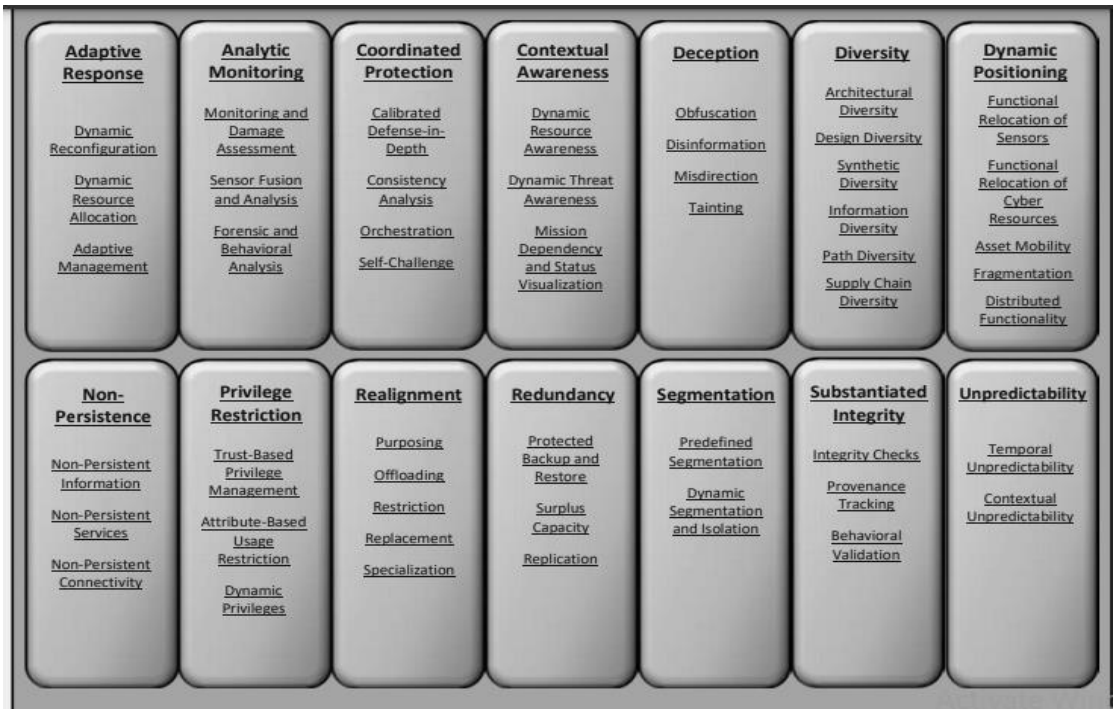
Figure 2.1 Framework of cyber resilience

2.2.3 Resilience to Cyber Threats

National Institute of Standards and Technology (NIST) lists fourteen techniques that more broadly promote resilience to cyber threats. Some of the methods include segmentation, realignment, sameness, unpredictability, dynamic positioning, multiplicity, and betrayal which are discussed below [20].

- **Segmentation** entails isolating components based on mission functions, employing system partitioning, and employing process isolation, an air-gapped network being one of its examples.

- **Realignment** means aligning "system resources with core factors of organizational goals or business functions". This incorporates restricting privileged accounts from non-privileged functions or requests like peer-to-peer music. It also involves coating the network for mission-essential functions.
- **Unpredictability** could involve executing random channel-hopping on network channels or requiring re-authentication at random intervals.
- **Dynamic positioning** encompasses altering the physical locations of components like routers, storage sites, or detectors. Diversity incorporates many concrete examples like using alternate communication protocols, multiple protocols standards, or diverse operating systems when applicable.
- **Deception** naturally would be used against the opponent and involves encrypting conveyed data, authenticators, and processing. It also entails disinformation, creating false credentials, using beacon traps, honeypots, and decoys [21].



. Figure 2.2 Cyber resiliency techniques and implementation approaches

2.3 Air-gapped network

An air gap may be a network security estimate want to make sure that a network is physically isolated to stop it from establishing an outer connection, specifically to the web. The concept is that a physical gap can avoid unauthorized entry, staving off hackers, and malware. An air-gapped network could even be specified as a “security measure enforced for computers, computer systems or networks requiring airtight security without the danger of settlement or emergency. It enables total isolation of an allotted system from other networks, especially people that aren't secure". An air-gapped computer is one that is physically separated from the internet or from other networks. As a result, data can only transfer through removable media such as USB [22].

2.3.1 Functions of an Air-Gapped Network

Security and handling efficiency are the two fundamental functions of an AG system. This explains why they will be found among several of the world's most secure organizations. They're employed to protect a variety of critical systems, including those that support the military, the government, and the stock exchange. Because of its capacity to act as a security attorney, the term "air-gapped network" has become fairly popular. Many compliance-conscious organizations, such as healthcare, utilities, and finance, are now using ‘air gapping' protection for their sensitive applications and networks as a result of the rise in cybercrime [23].

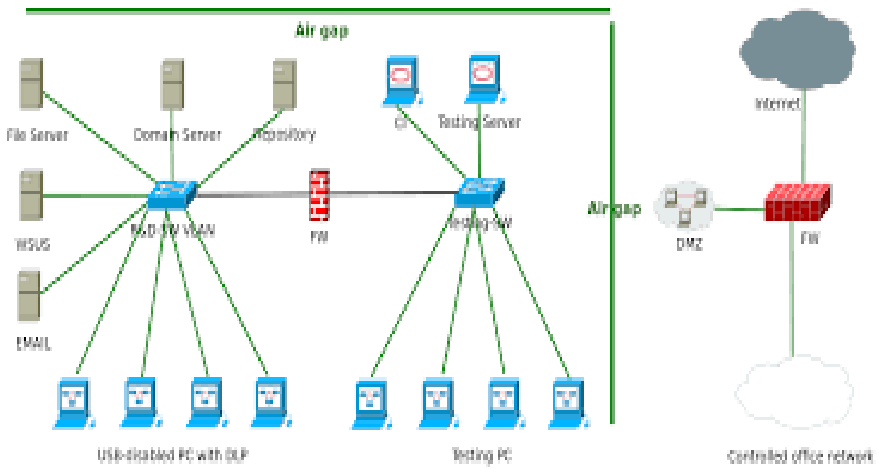


Figure 2.3 Pictorial representation of an air-gapped network

2.3.2 Applications of Air-Gapped Networks

High-security networks, such as confidential military networks and expenditure networks, use air gapped computers. Here are a few additional examples of systems that could benefit from being AG:

- Military computer systems and networks
- Government computer systems and networks
- Financial computer systems and networks
- Industrial control systems:
    - Supervisory control and data acquisition (SCADA)
- Life-critical systems:
    - Nuclear power plants
    - Aviation Computers:
        - Full authority digital engine control (FADEC)
        - Avionics
- Medical Equipment

Various products that were previously air gapped, such as thermostats, electrical sprinklers, and vehicle components, are now linking to the public internet as more and more electronics come online and become "smart" [24].

2.3.3 Architecture of an Air-Gapped Network

What establishes an AG system may be contingent on its purpose, but it will typically require:

- **No Wired Network Access** – To ensure that network access is controlled, wired network access may be blocked by software, or networking gear may be removed entirely for maximum security.
- **No Wireless Network Access** – To avoid malware reversing the software block, Wi-Fi, Bluetooth, Near Field Communication, Infrared Communication, and any other wireless data transfer mechanism will need to be deactivated at least through software, and the hardware may need to be physically disconnected or disabled.
- **No Removable Storage Device Access** – USB drives can be immobilized to prevent malware from being installed on the system by someone who has physical access to the device. Because the device is not connected to the internet, re-enabling such access (if necessary) must be done physically with direct contact to the device.
- **Restricted Physical Access** – Physical access to the device/network should be restricted. As a security policy to be closely followed, who can access, when they can access, who should approve such access, and who should administer such access should all be decided and reinforced.
- **Restricted Use of Other Devices** – If a consumer can take a photograph of the data on the device screen with their phone, air gapping may fail to protect the system. Near air gapped systems, devices that may secure and transfer data may need to be restricted.

- **Clean Installation** – To eliminate malware that may have already infected the device, a clean installation of the operating system and relevant software may be required.
- **Physical Security** – All of these protections will be rendered useless if the gadget is robbed. If the gadget is transportable and the data it holds is critical, physical safeguarding may be required [25].

2.3.4 Challenges to Breach an Air-Gapped Network

It is extremely stimulating to break an AGN because all the security spells require you to be physically close to each other. Most of the defined attack methodologies discussed in depth in the following chapters are proof-of-concept assaults, which means they are all:

- Difficult to implement
- Dependent upon various conditions being met
- Established by security scientists for research purposes

That last point is particularly important. These activities were carried out only to increase comprehension; they are not situations that are seen in everyday life. In contrast, most cybercriminals do not provide proof of concept, therefore there may be other ways to remain anonymous [26].

2.4 Conclusion

Cybersecurity is a multi-disciplinary method that incorporates both the software and hardware with a goal of avoiding the frequency of cybercrime at the first case or waning its effect if it has already happened. In this chapter, some of the foremost elements of cybersecurity which includes application security, network security, information security, data security and end user security have been discussed. Some of the techniques used to make the systems resilient to cyberattacks include segmentation, realignment, unpredictability, dynamic positioning, and deception are discussed in this chapter.

Chapter 3

Cyber Attacks

3.1 Introduction

Due to rapid technological advancements, social networks, internet transactions, cloud computing, and automated processes have taken over the world. But it also leads to the advancement in field of cybercrime, which are coming with new attack types, tools, and techniques that make the more vulnerable environment to attack and damage the technology-based subjects. The present chapter is an overview of the cyberattacks to determine patterns and trends in cybercrime which will ultimately pave a pathway for policy development have been discussed [27].

3.2 Cyberattacks

"A computer-to-computer bout that dents the integrity, confidentiality, or availability of a computer or info resident on it". A cyberattack is any attempt to gain illegal access to a computer, computing system, or computer network that could cause harm to the system. Their main objective is to get access and control of computer system in order to use it for personal illegal, and criminal purposes and get advantage of using or selling the data. In current days the challenging problem is to make a secure and protected system that can handle the cyberattacks. By using technology specific types of malwares have been designed to attack the specific target that make the normal security system of computer network quite weak. As a result, there have been reports of increasing vulnerabilities in the protection of business, government and citizen data by Symantec, FireEye, and Verizon [28].

3.3 Characteristics of Cyber-Attacks

A computer network attack, often known as a cyber attack, is an attempt to compromise the integrity or validity of data or info. A malware changes the logic coding of the program resulting in error output. The hacking process involves search of the systems that have weak security control and are inspecting for incorrectly configured systems. Whenever the hacker gets access to the system by infecting it, it can be completely controlled by the attacker remotely. There are more chances to making the system perform as a mole for other attackers and infect the security of other systems that are connected to the attacked system in any manner. Flawed systems like bugs in software, deficiency in anti-virus, are more likely to be attacked by hackers to get the access. The basic purpose of the cyberattack is to take over the system and steal the info in any organization. The hackers follow certain pattern to achieve the goal of getting access and steal the data [29].

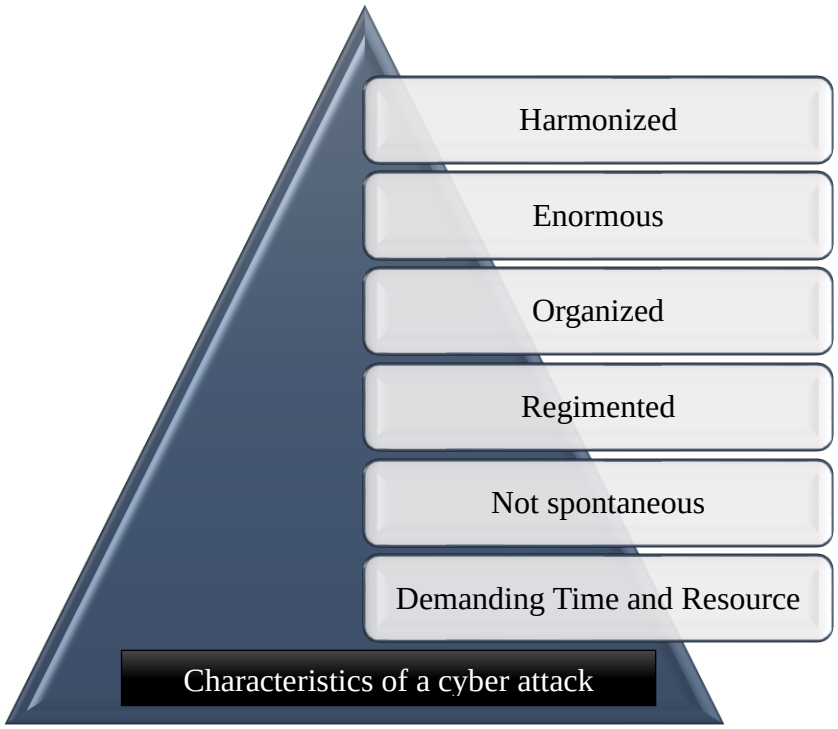


Figure 3.1 Characteristics of a cyber attack

3.3.1 Harmonized

The aggressor would anticipate the course to be altered in order to have an impact on the system. They get what they want since the stages required in stealing info are well-coordinated. Hackers will receive their results on schedule, step by step, and in accordance with their instructions.

3.3.2 Organized

The hackers follow the organized patterns and methods to infect the system without any obstruction. Obviously more the organized pattern, more the efficiency to get the desired results.

3.3.3 Enormous

The attacks are made in bulk on vast number of virtually infected computer systems that have weak security system that lead to large scale loss of data and finances.

3.3.4 Regimented

The attacks are organized with perfect consistency to make the damage more severe and well enough compromising the organization's work.

3.3.5 Not Spontaneous

Attacks that are intentionally complicated with a careful plan to cause maximum destruction.

3.3.4 Demanding Time and Resource

All the cyber-attacks are well planned to get the desired results and it requires lots of time taking research and money [29].

3.4 Rationale and Goals of Cyber-Attacks

The major purpose of cyber-attacks is to steal data or info from government, banking, news and media, online discussion forums, and military / defense network websites [30]. There are purposes and motives of cyber-attacks that include certain actions, that are:

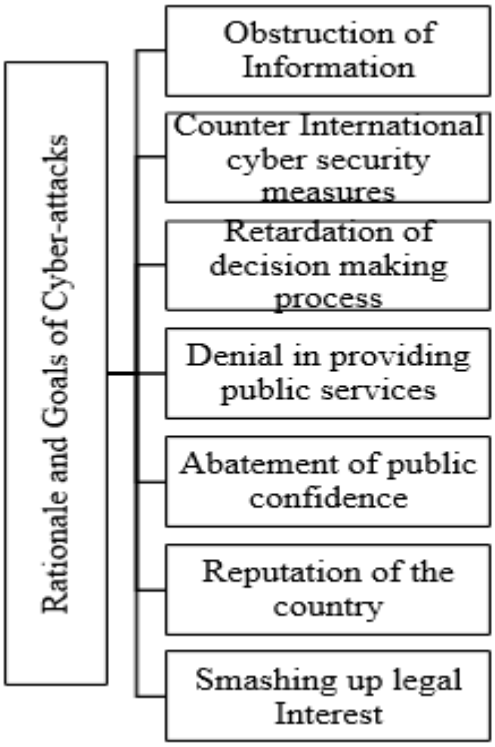


Figure 3.2 Rationale and goals of cyber-attacks

3.4.1 Obstruction of Info

The basic plan of hacker is to resist the assessment of important data of any company or government secretariat when they require the specific type of info. Due to this attack, the authorized person becomes unable to do the required task. They limit the organization's or government's ability to organize and process future occurrences in this way [31].

3.4.2 Counter International Cyber Security Measures

Cyber-attacks are designed to test the international cybersecurity community's security procedures for preventing cyber-attacks. Attackers usually achieve their aims by stuffing their complex bugs in some normal looking programs that can evade the security [32].

3.4.3 Retardation of Decision-Making Process

Cyber-attacks have wreaked havoc on essential sectors like emergency services and the military, delaying critical decision-making processes like tactical deployments and life support activation, and resulting in death or military defeat.

3.4.4 Denial in Providing Public Services

Attackers can disrupt fields such as railway, banking, and airline services, and the stock market by prohibiting authorized users from accessing government info connected to an organization or public service.

3.4.5 Abatement of Public Confidence

Stealing info or hacking causes a great deal of distrust in public of an organization and they lose the confidence on the organization due to security issues.

3.4.6 Reputation of the Country will be Denigrated

The main purpose of cyberattacks is to tarnish the image of a country. Due to technological advances, each country has capabilities that are enhancing its status in various developing countries and could be severely damaged if it could penetrate the network of large-scale cybersecurity countries.

3.4.7 Smashing up Legal Interest

One of the goals of cyber-attacks is breaking formally authorized work. Security targets must be clearly defined to deal with cyber-attacks [33].

3.5 Types of cyber-attacks

The various types of cyber-attacks are shown in figure 3.3:

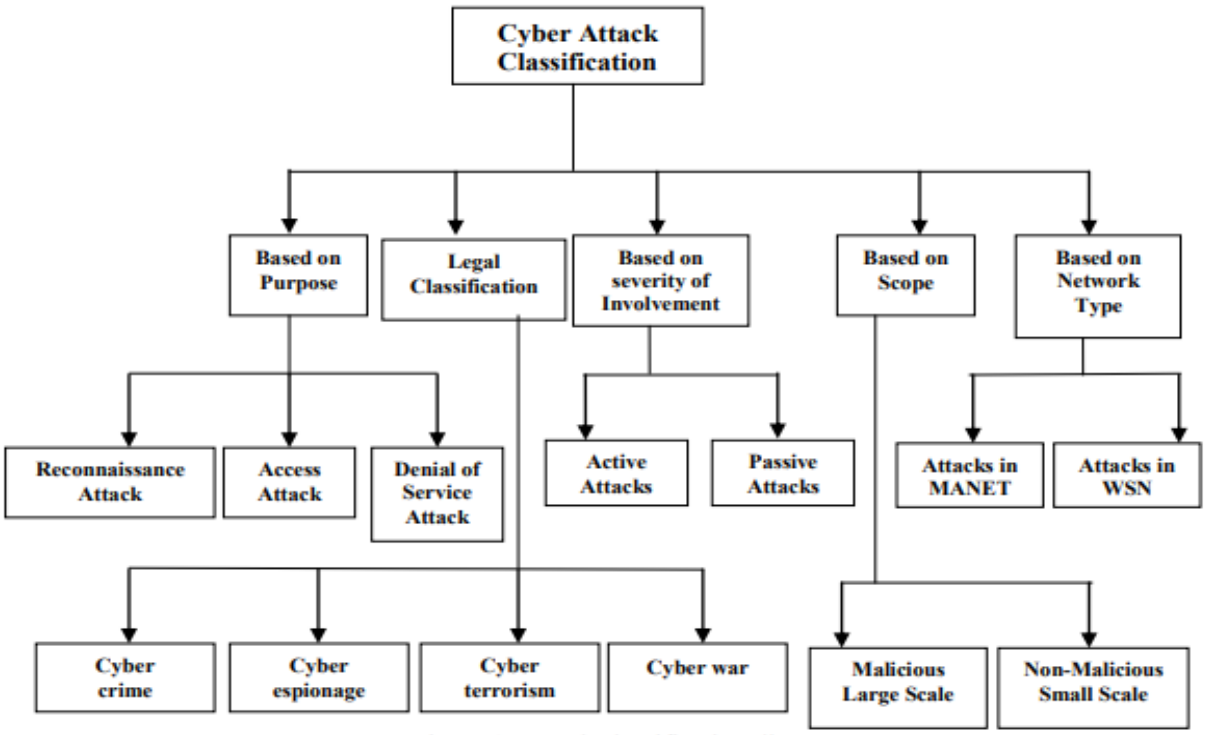


Figure 3.3 Types of cyber-attacks [34]

3.5.1 Based on Purpose

The attacks based on the purpose are:

- Reconnaissance Attack
- Access Attack
- Denial of service Attack

3.5.1.1 Reconnaissance Attack

Reconnaissance attacks are defined as unauthorized detection, system mapping, and services. It is like a burglary in a neighborhood in danger of breaking into homes that are deserted, doors that aren't strong, and windows that aren't open. Reconnaissance attacks could include of the following [35]:

- **Packet Sniffers**

  When there is a lot of traffic between the computers on the network, a particular device is employed to capture the data from other machines and save it for later analysis.

- **Scanning the Port**

  An attacker attempting to get into a computer sends a sequence of packets to determine which computer services are associated with each known port number.

- **Sweeping the Ping**

  The attacker uses the method of scanning to determine the range of IP addresses created or mapped directly for the hosts.

- **Queries**

  DNS queries can be used by an Internet attacker to discover who owns a field or domain and what addresses are allocated to it.

3.5.1.2 Access Attack

Unauthorized intruder can gain access to a machine or IT device even if the burglar does not have access to the password or account. Anyone who does not have access to the data will hack it or design a program to exploit the vulnerability of the hacked or attacked application. Known vulnerabilities of verified services, web services, and FTP (file transfer protocol) services will be exploited to get unauthorized access to web accounts, secret databases, and other sensitive info. The following are examples of access attacks.

- **Attacks on Secret Code**

  Unauthorized users attempt to break into a small domain account using all conceivable password combinations, often known as a dictionary attack. Password guessing and password resetting are the two forms of assaults.

- **Utilization of Trust Port**

  An intruder compromises a trusted host and further using it to perform stage attacks on a trusted host.

- **Port Redirection**

  To access other hosts or users which are protected by a network firewall, an intruder uses a trusted host.

- **Man-in-the-middle Attacks**

  Also called as Janus attack or bucket brigade attack and it is an dynamic form of snooping in which the intruder makes separate connection with victims and relays communications between them to make them believe they're in private contact.

- **Social Engineering**

  Through SQL injection, social engineering websites are infected with malicious code, allowing any user who visits them to become infected or change the content.

- **Phishing**

  An act of sending an incorrect email while pretending to be a reputable organization in order to dupe the recipient into providing personal info that will be used for identity theft [36].

3.5.1.3 Denial of Service Attack

Denial of service attacks are defined as attacks that cause the system to crash or become unusable by slowing it down. It also entails the deletion or corruption of info. With the purpose of denying services to thoughtful users, the attacker will turn off the network or corrupt the network system [37].

3.5.2 Legal Classification

The following is a list of legal classifications for cyber-attacks:

- Cyber crime
- Cyber espionage
- Cyber terrorism
- Cyberwar

3.5.2.1 Cyber Crime

Canadian law enforcement organizations have gradually recognized the following working definition: “a criminal offence involving a computer as the object of the crime, or the tool used to commit a material component of the offence.” The goal of cybercrime is to turn the computer into a tool of crime and the system into an incidental of the crime. Computer crimes arise because to their secrecy, computer storage capacity, operating system flaws, and a lack of user attention [38].

3.5.2.2 Cyber Espionage

It is the act or practice of acquiring secret info of individuals, groups, and governments for personal gain utilizing banned abuse tactics in order to collect content without the permission of the holder employing outrageous techniques and spiteful software such as Trojan horses and spy ware. It's also known as "cyber spying." It might be carried out entirely online from the PCs of specialists stationed in far-flung locations. It might be computer-trained traditional spies and moles infiltrating your home, or it could be

the criminal activity of amateur mischievous hackers and software programmers in other circumstances [39].

3.5.2.2 Cyber Terrorism

Attacks or terrorist activity done by the use of internet, which includes acts of large-scale computer network disruption using kits or tools such as computer viruses [40].

3.5.2.3 Cyberwar

The action of a nation's state infiltrating the computers or networks of another nation in order to cause harm or disruption is known as cyber war

3.5.3 Based on Severity of Involvement

The severity of the cyber-attacks and their involvement could use to classify them as follows:

- Active Attacks
- Passive Attacks

3.5.3.1 Active Attacks

An attack authorizes the attacker to send data to all parties or to block data transfer in unidirectional or multidirectional directions. Because the attacker is placed between the conversing parties, he or she may try to terminate the data transmitted by them. When the authentication procedure is complete, the attacker attempts to impersonate the client because the source of the data cannot be validated by the server without justification of the info received. A computer is deployed as a link between two subnets without much difficulty, allowing an individual to adapt an entity like this on a computer [41, 42].

3.5.3.2 Passive Attacks

An attack in which an unsanctioned attacker listens in on two parties' conversations in order to snoop on info stored in a system through monitoring or other means. It is also

separate from active attack in that it does not seek to interfere with the database, yet it may still be illegal [43].

3.5.4 Based on Scope

Cyber-attacks are often divided into categories based on their scope, such as

- Malicious Large Scale
- Non-Malicious Small Scale

3.5.4.1 Malicious Large Scale

The Malicious term here means "with deliberate intent to cause damage". An individual or a group commits a malicious large-scale attack for personal benefit or to inflict disruption and disorder. Such attacks are big scale, affecting thousands of systems worldwide, resulting in the loss of a large amount of data and the company's reliability.

3.5.4.2 Non-Malicious Small Scale

Small scale non-malicious attacks are generally unintentional attacks or damage caused by a poorly qualified individual's mismanagement or operational missteps, which can result in modest data loss or system breakdowns. Only a few systems in the network collaborate in such instances, and data is usually recoverable. It has a small price tag attached to it [44].

3.5.5 Based on Network Type

Here the attacks are classified according to the network types such as [45]

- Mobile Adhoc Networks (MANET)
- Wireless Sensor Networks (WSN)

3.5.5.1 Attacks in MANET

The attacks in MANETs are elaborated as under:

- **Byzantine Attack**

  It is basically a attack on mobile adhoc network in which a verification device or set of devices that ordinarily provides security is compromised owing to info leakage, making it impossible to distinguish between a real device and an unresponsive user

- **The Black Hole Attack**

  Black Hole Attacks are defined as routing all network traffic to a given node as if that node does not exist, resulting in the disappearance of all data transmitted. The node is referred to as a black hole in this case. This attack will be built using the RREQ (Route Request) and RREP (Route Reply) protocols

- **Flood Rushing Attack**

  There will be a race between those who support the flood (legitimate flood) and those who oppose it. When there is propagation, it happens. The verification methods employed will fail to establish an adversarial free route

- **Byzantine Wormhole Attacks**

  Byzantine Wormhole Attacks have the capability of compromising several nodes, and there will be a contribution of an attack in the collaboration for the nodes. This assault will be launched when there are oppositions to tunneling packets between them so that a network shortcut may be formed. This assault is quite powerful, but it requires the cooperation of at least two nodes

- **Byzantine Overlay Network Wormhole Attacks**

  The super-wormhole attack is another name for this technique. This attack is the most robust of all the attacks, and it is also the most effective. Using this

technique, one can generate a massive amount of traffic in routing protocols, causing network interruption.

3.5.5.2 Attacks on Wireless Sensor Networks (WSN)

The attacks discovered in the WSN will be classified according to the layers, processes employed, and attack domain. The attacks are:

- **Cryptography and non-cryptography related attacks**

  Pseudorandom number attack, digital signature assault, and hash collision attack are some of the attacks that fall into this category

- **Attacks based on the Network Layers**

  Repudiation and data corruption are assaults on the application layer. Session theft and SYN flooding are attacks on the Transport layer. The network layer attacks include wormhole, blackhole, Byzantine, flooding, resource consumption, and location finding. Traffic analysis, monitoring, and MAC interruption are all part of the data link layer. Jamming, interceptions, and snooping are examples of physical layer attacks. The following are examples of multi-layer attacks. Denial-of-service attacks, impersonation attacks, and man-in-the-middle assaults are all examples of cyber-attacks [46].

Table 3.1 Different types of cyberattacks

Cyberwar	The act of a nation with the intention of disruption of another nations network to gain tactical and military advantages	a) Russia's war on Estonia (2007) b) Russia's war on Georgia (2008)
Active Attacks	An attack with data transmission to all parties thereby acting as a liaison enabling severe compromise	a) Masquerade b) Reply c) Modification of message
Passive Attacks	An attack which is primarily eaves dropping without meddling with the database	a) Traffic analysis b) Release of message contents
Malicious Attacks	An attack with a deliberate intent to cause harm resulting in large scale disruption	a) Sasser Attack
Non Malicious Attacks	Accidental attack due to mis-handling or operational mistakes with minor loss of data	a) Registry corruption b) Accidental erasing of hard disk
Attacks in MANET	Attacks which aims to slow or stop the flow of information between the nodes	a) Byzantine Attacks b) Black Hole Attack c) Flood Rushing Attack d) Byzantine Wormhole Attack
Attacks on WSN	An attack which prevents the sensors from detecting and transmitting information through the network	a) Application Layer Attacks b) Transport Layer Attacks c) Network Layer Attacks d) Multi Layer Attacks

3.6 Attack Artifacts

3.6.1 Virus

Primarily, a virus is a computer code that is intended to get rooted with another computer file, such that, when performed it can replicate itself and get transmitted on the host computer. There can be various objectives of designing a virus that include but not limited to infecting the host computer by debasing files, stealing hard disk space, pocketing CPU time, keylogging to steal valuable info, and various other activities performed without the approval of a legitimate computer-user

3.6.2 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.

3.6.3 Trojan Horse

It is a malicious program that pretences 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

3.6.4 Botnets

A botnet is a network of compromised computers that are remotely controlled and coordinated by bad actors to achieve the desired mischievous purpose. 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 conceded 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 commands of the Bot Master and implements the malevolent tasks as and when communication between the two is established, and instructions are given.

3.6.6 Spyware

It is a malicious program that has a one-point agenda that is to seek and exfiltrate user info without the user's knowledge or consent [47].

3.7 Conclusion

Computers and the Internet are used in practically every area of our daily lives. In recent years, cyber security has become increasingly important. Greater usage of internet also opens the door to increased cyber threats such as hacking or stealing data from a government website, causing the country to fall behind in its future actions. Due to rapid

technological advancements, social networks, internet transactions, cloud computing, and automated processes have taken over the world. But it also leads to the advancement in field of cybercrime, which are coming with new attack types, tools, and techniques that make the more vulnerable environment to attack and damage the technology-based subjects. The present chapter is an overview of the cyberattacks to determine patterns and trends in cybercrime which will ultimately pave a pathway for policy development.

Chapter 4

Cybersecurity Attacks in an Air-Gapped Network

4.1 Introduction

An organization often resorts to AG isolation when handling classified/sensitive data. Isolation via an AGN is achieved by means of both logical and physical separation, thus securing the data from malicious outsiders. The isolation in AG is ensured by implementing stringent protocols, for instance barring connectivity to unapproved equipment or system and hardening the workstations in the network. Currently, AGNs are employed in military installations, critical infrastructure, and other important organizations in a country. The organizations have been following various security standards, while deploying subsequent technical controls, to mitigate the identified risks. When it comes to an AGN, the existence of the air between the internal and outside network is considered as the sole guarantee of protection of data from spillage of classified information. However, news of recent successful attacks and consequent data loss from the AGNs reveals that technical controls alone do not provide due assurance against data breaches. Therefore, in this chapter ways of a data breach in an air-gapped network have been discussed with special emphasis on social engineering as an important factor [48].

4.2 Attack 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 AGN?[49].

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

4.2.1 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 designed to control and observe specific industrial processes. Being discovered in June 2010, it successfully targeted and adversely affected Iran's nuclear facility at Natanz. The worm did not 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 AG 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 devised to target only Siemens SCADA systems, that are responsible to monitor and control 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 [50].

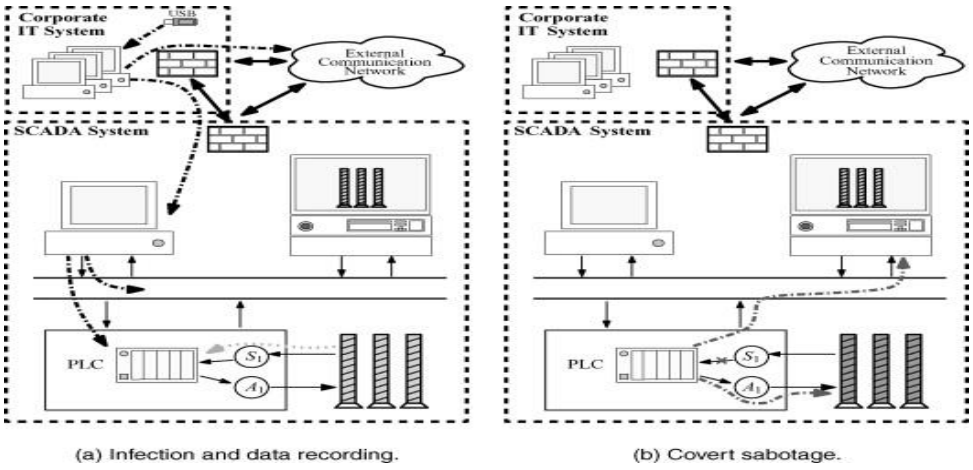


Figure 4.1: Pictorial representation of Stuxnet

4.2.2 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 [51] The leak elaborates working of the Brutal Kangaroo and mentions that it creates a custom clandestine network within the target inaccessible network that provides functionality for executing surveys, arbitrary executables, and directory listings. 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 AGN 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.

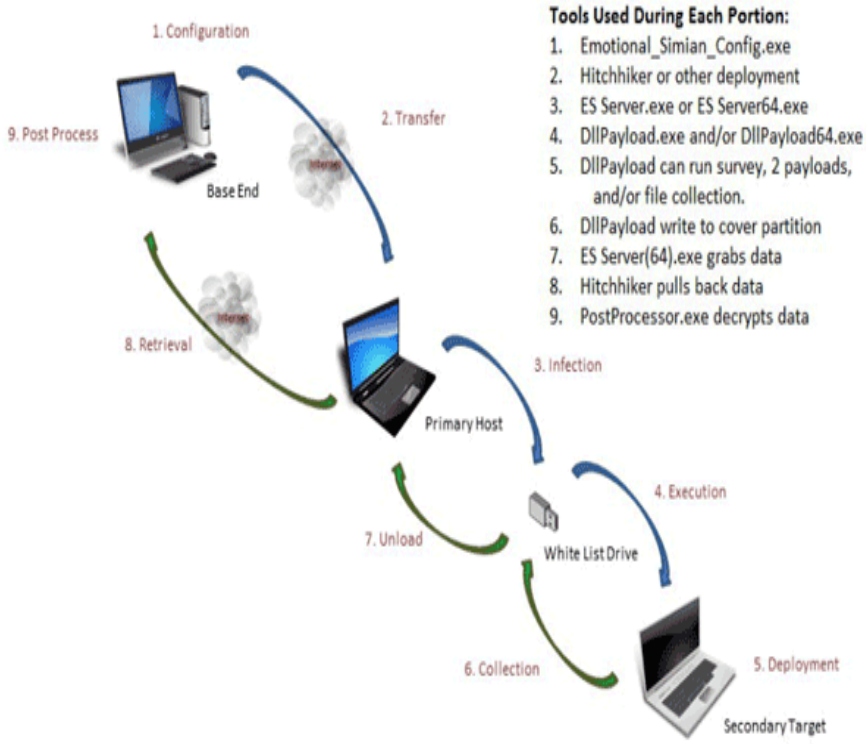


Figure 4.2: Pictorial representation of Brutal Kangaroo attack.

4.2.3 Agent.btz

This attack finds its traces to the year 2008 when the United States sensitive AG 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 [52].

4.2.4 Cycldek

Cycldek (also known as Goblin Panda and Conimes) is 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, 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. 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 [53].

4.2.5 Indian Navy Air-Gapped Computers

According to the reports, a sophisticated attack that allegedly used a USB vector penetrated the workstations of the Indian Navy's Eastern Naval Command. Being attributed to Chinese hackers, the attack bridged their AGN, leading to leakage of confidential info abroad.

4.2.6 DTrack

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 created by a North Korean hacker group called Lazarus. Primarily designed to extricate data such as keylogging, IP hosts, browser history, running processes, and all files on a computer; the malware sought domain controller-level on a server computer. Resultantly, the AG systems at the facility were breached, as also confirmed by the Nuclear Power Corporation of India Limited (NPCIL) – the regulating body for nuclear power plants in India [54].

4.3 Air-Gap Covert Channels

The researchers have been working on covert channels to discover ways and means to jump the AG and get access to the internal networks of the organization or at least extract some info 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 AG systems, forcing the specialists to take suitable measures to maintain the requisite gap. Some of the concepts have been made part of this study:

4.3.1 MAGNATO

An earlier study shows that an attacker can leak data from secluded AG computers to nearby smartphones through hidden magnetic signals. According to the research, malware would be installed in an AG computer to control the magnetic fields originating from the computer by adjusting workloads on the CPU cores. Moreover, the malware would encode sensitive data including passwords, keylogging data, or encryption keys 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 [55].

4.3.2 HOTSPOT

This study shows that the signals generated from an AG computer can be sent covertly to a nearby smartphone and then on to the Internet, which is done in the form of thermal pings. 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 examiners further suggest the countermeasures to mitigate the threat by using the "Zoning" tactic; i.e. to mark defined areas or zones around AG computers where smartphones and other smart devices are prohibited. Moreover, insulation of the compartment walls may be helpful to mitigate signal reception distance growth [56].

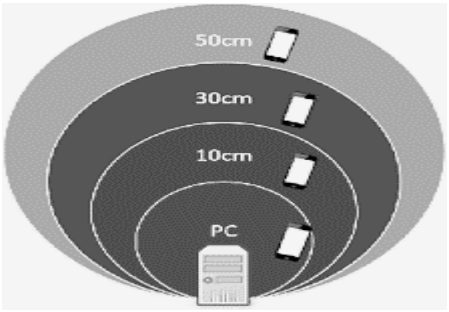


Figure 4.3: The Threat Radius of the Thermal Covert Channel

4.3.3 aIR-Jumper

This research is based on the use of IR light which is invisible to humans, but detectable by any cameras due to their optical sensitivity. Researchers reveal the feasibility of establishing bi-directional covert contact between an organization's internal networks and outside 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 gain access to the surveillance

or watch cameras across the local network and control the IR illumination. Consequently, complex data such as encryption keys and passwords would then be encoded, modulated, 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 or watch 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 [57].

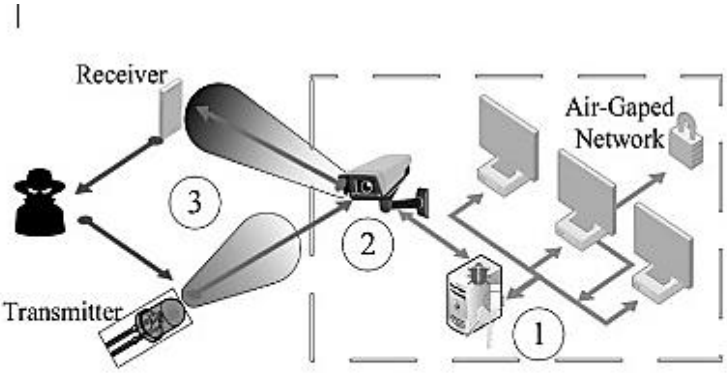


Figure 4.4: aIR-Jumper: Covert air-gap exfiltration/ infiltration via security cameras & IR

4.3.4 AirHopper

It is a technique that is used to bridge the AG between isolated networks and mobile phones using radio frequencies. In this attack, the compromised computer is made to produce compatible radio signals by making use of the electromagnetic (EM) radiations related 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 AGN, harmful code can be triggered and contaminate the systems within the targeted network. In case the appropriate connectivity with the attacker is sporadic, the covert program running on the smart

phone may be configured to store the acquired info and transmit it to the attacker once the desired connection is available. At the fundamental level the method consists of two key elements:

- **Electromagnetic (EM)** pulses emitted from a computer's display connection, as well as data modulated on those signals.
- **Frequency Modulating (FM)** receiver on a mobile or smart phone that can receive, extract and save the modulated data from transmitted signals. For experimentation purposes, measures like the effective transmitting distance, the presence of receiver antenna, type of cable, etc.; have been assumed [58].

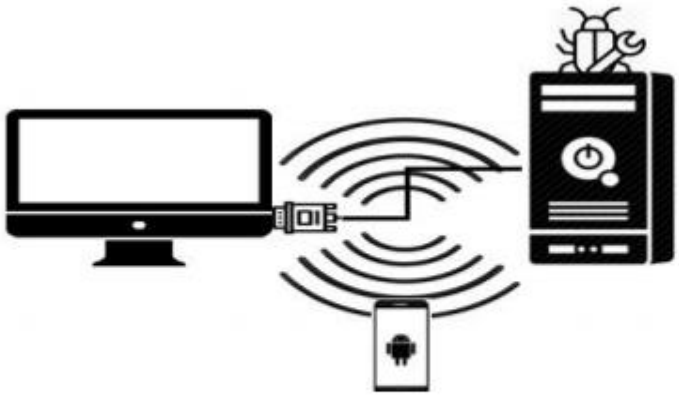


Figure 4.5: AirHopper: Bridging the air-gap between isolated networks and mobile phones using radio frequencies

4.3.5 PowerHammer

PowerHammer is malware that uses Alternating Current (AC) power lines to extract data from AG computers. It requires malware to run on a computer that regulates the power utilization of the system by managing and channelizing the CPU workload. Binary data is modulated on the variations of the current flow, and then transmitted duly encoded, on top of the current flow fluxes. It is further conducted and transmitted 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, passwords, credential tokens, or encryption keys, etc. Fundamentally, this attack model requires running malicious code in the targeted AG computer which is achievable by infiltrating the AGNs using social engineering, malicious insiders, or supply chain attacks [59].

4.3.6 USBee

Researchers have been working on the use of USB connectors implanted with RF transmitters to exfiltrate data from AG 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 deliberately generate controlled electromagnetic emissions from the data bus of a USB connector. Furthermore, the emanated RF signals can be monitored, 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) [60].

Type	Method
Electromagnetic	AirHopper GSMem USBee Funthenna
Magnetic	MAGNETO ODINI Myhayun
Acoustic	Fansmitter (computer fan noise) DiskFiltration (hard disk noise)
Thermal	BitWhisper
Optical	LED-it-GO (hard drive LED) VisiSploit (invisible pixels) Keyboard LEDs Router LEDs
Infrared (IR)	aIR-Jumper (security cameras & infrared) Implanted infrared LEDs

Table 4.1: Summary of existing air-gap covert channels

4.4 Social Engineering

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 normal and grim consequences. Considering the case of cybersecurity and AG systems, there are many incidents that suggest that human failings are one of the key factors that lead to the 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. There are 4x well-established stages of social engineering attack: research and info gathering, rapport and relation-building, relation exploitation, and attack culmination. 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 [61].

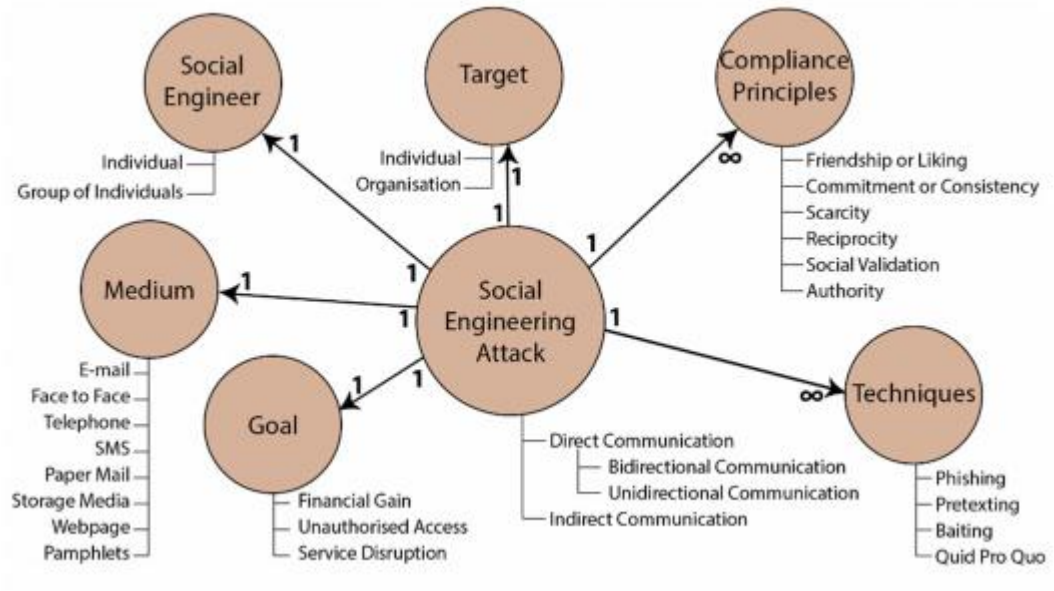


Figure 4.6 Model of a social engineering attack [62].

4.4.1 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. 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:

4.4.1.1 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.

4.4.1.2 Technical Methods

These methods do not necessarily require the physical presence of the attacker. However, he must rely on technical equipment ranging from as low as a simple telephone and going up to higher ones including 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 [61].

4.4.2 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 [63].

4.4.3 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 info 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”. The exploitation can take place through the revealing of seemingly unimportant info 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 info 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 [64].

4.4.4 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 info 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 [65].

4.5 Conclusion

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

Cybersecurity Policy

5.1 Introduction

Cybersecurity may be defined as a multi-disciplinary approach that encompasses both the software and hardware to prevent the incidence of cybercrime at the first instance or wane its impact if it has already occurred. Cybersecurity is a crucial challenge for several corporations such as government databanks, financial companies as well as banks, and the military. Security policies are an official set of rules that are made by an institute to safeguard that the user approved to gain access to company information and technology endowments abide by the rules and procedures related to data protection. This is a written paper in company that is accountable for how to safeguard the corporations from risks and how to manage them when they occur. The security document is of high standard text that describes the company's vision regarding safety, needs, objectives, responsibilities, and scope. A security policy is regarded as "living document" which implies that it is never done, but it is constantly revised as conditions of the technology and worker vary.

Many objectives should be met by a security policy. It should: safeguard people and data; provide guidelines for anticipated behaviour by users, system supervisors, administration, and safety personnel; allow security employees to observe, investigate, and inspect. Describe and punish the ramifications of the breach; describe the organization's security standard position, assist in risk reduction, and track compliance with the regulation. Cybersecurity measures are also harmful to the public's perception of collaboration and its integrity. Consumers, associates, stockholders, and future employees all seek confirmation that the organisation is capable of safeguarding their

personal data. If a business does not have a cybersecurity policy, it may not be able to produce such paperwork [3].

However, as the importance of cybersecurity for businesses becomes more widely recognized, cybersecurity policies vary from company to company, depending on the complexity of the challenges. These policies differ based on the scale of the business, the sensitivity of the company's assets, transactions with other firms, the type of data, and the technological equipment they employ. A large corporation cannot create a distinct policy statement that define all sorts of employers and tackles all of the required cybersecurity problems. A more practical option is to create a collection of policy papers that incorporate all security-related information; these can then be directed to certain viewers and make it a more effective way for everybody. There is no technique for the purpose of creating a security policy or policies. Other consideration is present development of the policy formulation procedure. Companies without any policy framework or which has only a basic framework follow already established policies or use a different strategy and use policy for more complicated objectives, such as tracking regulatory compliance. Starting with a fundamental policy structure is a good approach towards making major policies and other large numbers of policies that are required and then revising already established ones and making changes to add guidelines and documents for job aid which will help support policy [16].

5.2 Significance of Cybersecurity Policy

Organizations and companies whether they are small or large face security threats, and these threats are increasing day by day. It is becoming complex to meet the security requirements. Organizations and companies whether they are small or large must make a complete security program to meet the challenges. And without cybersecurity policy, administration of security database is not possible to direct

security programs in an organization. It is also not possible to communicate with third parties and external auditors about security measures. Sensitive information can be secured by updating security policy and by giving access to only authorized persons. Security gaps can be prevented by making effective security policies and by ensuring compliance [2].

Cybersecurity policy structure provides best practices to be followed by all staff. It helps minimize the security threats and effectively manage them. Cybersecurity policies will also help turn workers into members in securing information assets of the company, and the method of emerging these policies will assist in defining organization's information resources. A cybersecurity policy helps in protecting information from unauthorized access and modification, destruction, or disclosure of information and declares it to be an asset of the company [66].

5.3 Characteristics of an Effective Cybersecurity Policy

A good cybersecurity framework is based on the policies it contains. They aim to contain all features of security management and to provide direction and focus. Cybersecurity policy has many characteristic features, and these features can be defined as a principles of the organization. Few organizations have a solid culture of 'command and control'. Guidelines resulting from these cultures contain strong, commanding statements such as, 'log off at the end of each working day. Few organizations may practice indirect expressions, to influence those who are on focus to the policy. Whatever principles or administration chic the company uses, the main aim of the data safety policy is to help in managing the threat and diminishes the leakage of information to a minimum [67]. Following are some of the features of an effective security policy:

- A security policy, maintain and implement security information by giving clear policy directions and support.

- An effective policy is appropriate, reachable, and reasonable to all future users throughout the organization.
- The development of a security policy network requires commitment, management, and a suitable official framework, within which it can be executed. It also needs an appropriate degree of specialty, ways through which agreement can be tested, and a legitimately established reaction in the event of it being desecrated.

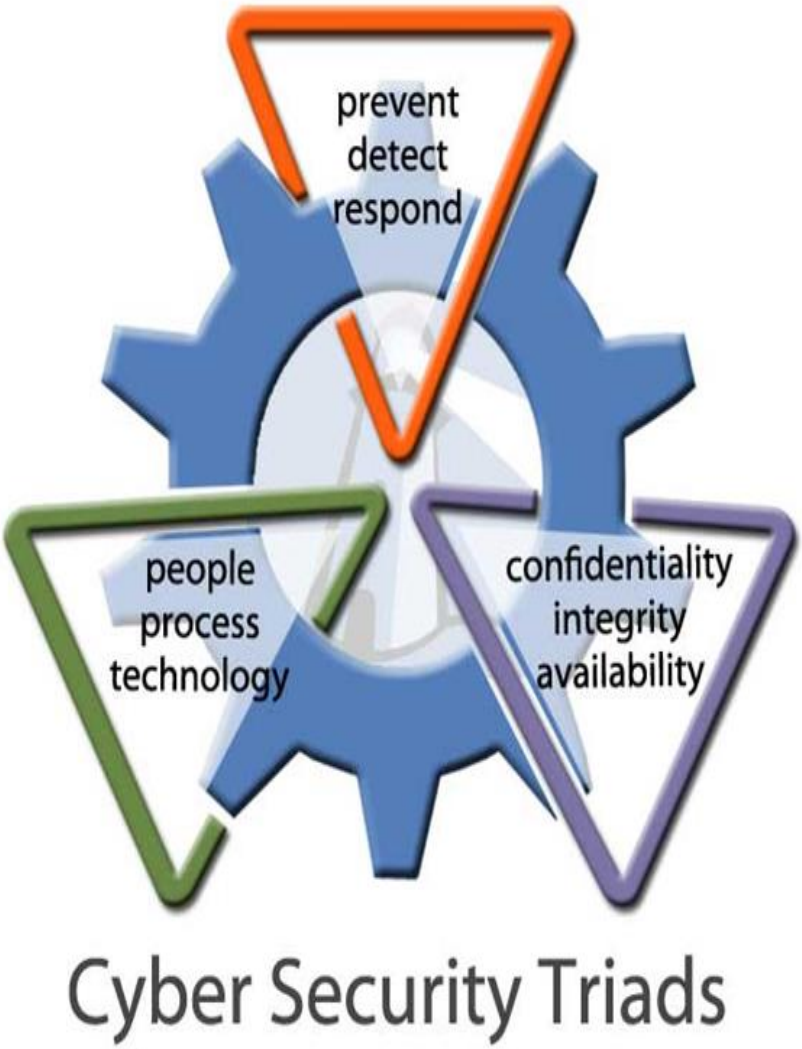
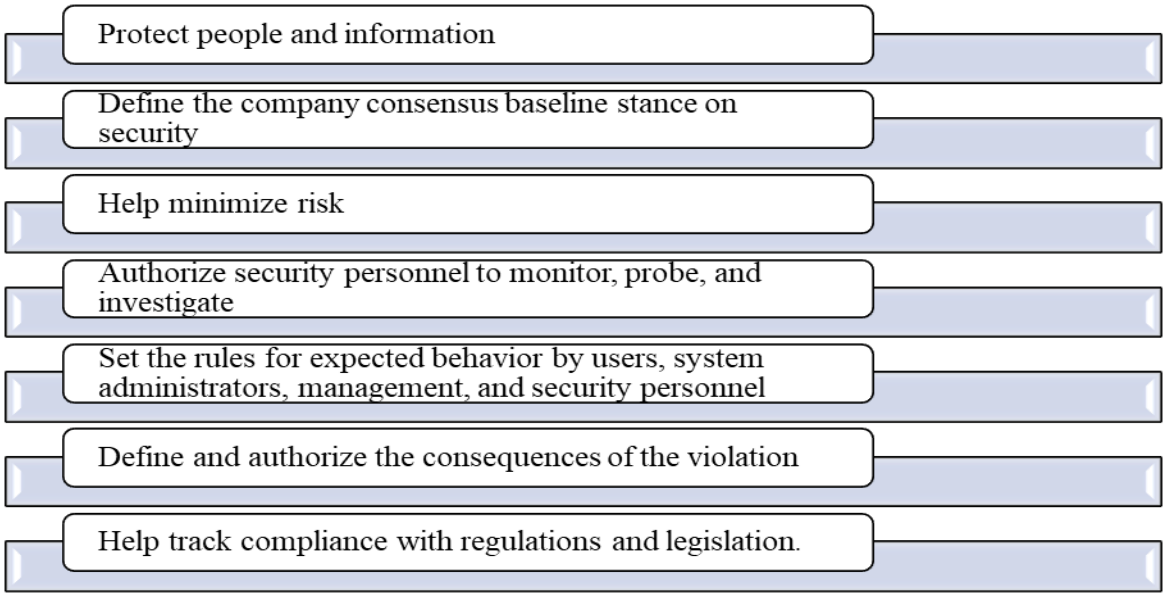


Figure 5.1: Cybersecurity triad.

5.4 Need for a Cybersecurity Policy

A cybersecurity policy is needed for the following reasons:



5.5 Elements of a Cybersecurity Policy

Cybersecurity policy is as extensive as IT security, as well as the security of connected physical assets, are both enforceable in their entirety. while developing an information security policy following considerations should be taken into mind.

5.5.1 Purpose

The purpose of the Cybersecurity policy can be to:

- Generate complete method of data safety.
- Identify and prevent data safety gaps like misapplication of web links, information, presentations, and computer systems.
- Keep up the repute of the company and maintain proper and authorized duties.
- Respect client privileges, as well as how to react to investigate and object to non-compliance.

5.5.2 Audience

Define the target audience for the cybersecurity policy. It may also be indicated by certain audiences who are not covered by the policy, such as personnel in another business unit who are responsible for their own security.

5.5.3 Cybersecurity Objectives

The management team should be guided in deciding on unique methods and security goals. The three main objectives of cybersecurity are as follows:

- **Confidentiality**: Access to data and information assets should be restricted to authorized employees only
- **Integrity:** Data must be complete, accurate, and undamaged, and IT systems must continue to function.
- **Availability:** When users require information or access to systems, they should be able to acquire it quickly.

5.5.4 Policy on Control of Authority & Access

- Ordered structure—a senior director may have the ability to choose which data is shared and with whom. The security policy of a senior management may differ from that of a junior employee. The amount of accountability for data and IT systems for each organisational position should be defined in the policy.
- According to the network security policy, users can only access corporate networks and servers via unique logins that need confirmation, such as PINs, biometrics, ID cards, or proofs. All systems should be monitored, and all login attempts should be recorded.

5.5.5 Data Classification

The policy should define data classifications, such as "top secret," "secret," "confidential," and "public." The following are the goals of data classification:

- To ensure that people with lower levels of clearance do not have access to sensitive information.
- To protect sensitive information while avoiding needless security measures for less sensitive information.

5.5.6 Support & Operations for Data

- Data protection rules—organizational standards, paramount practices, business compliance requirements, and related guidelines must all be monitored while storing private information or other delicate documents. Most security needs demand encryption, a firewall, and anti-malware safety.
- Encrypt backups of data in accordance with industry best practices. Backup media should be kept safe, or the backup should be transferred to a safe cloud storing site.
- Information drive—use only secure methods to transport data. Encrypt any data copied to portable devices or sent over a community web link.

5.5.7 Security Sensitivity & Conduct

Your company's cybersecurity rules should be communicated to all employees. Employees should be informed about security processes and mechanisms, such as information security, access regulator, and profound information categorization, through training sessions.

- Social engineering—focuses on the hazards of social engineering assaults (such as phishing emails). Identifying, avoiding, and reporting such attacks should be the responsibility of employees.

- Clean desk policy—protect PCs with a cable lock. Shredding documents that are no longer needed is a good idea. Keep the printer area clean to avoid papers getting into the in the wrong hands.
- Adequate Internet usage strategy— Specify how internet access should be limited. Is it okay to use YouTube, Facebook, and other social media sites? Using a alternative, you can block websites that you don't want to visit.

5.5.8 Personnel Responsibilities, Duties, and Rights

Allocate people to perform user access evaluations, training, modification of administration, incident management, security policy implementation, and episodic apprises. Responsibilities should be clearly defined as part of the security policy clearly defined as part of the security policy [68].

5.6 Corporate Cybersecurity Policy

A business policy outlines an organization's cybersecurity goals and values. It should be ageless, with little variation from year to year. Corporate policies must be followed:

- Make your point very flawless and unmistakable.

Reports on the scope, legitimate and supervisory obligations, roles and responsibilities, strategic approach and values, risk management plan, and what to do if a policy is broken are all included. The policy should be supported at the uppermost level possible, such as by the CEO or MD [69].

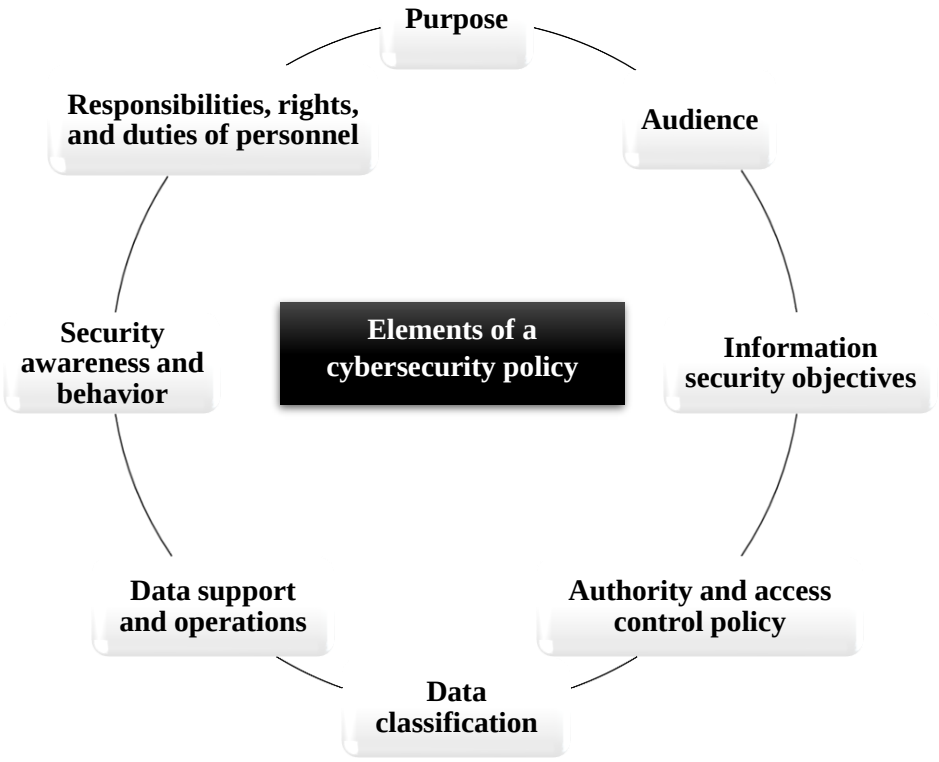


Figure 5.2 Basic elements of a cybersecurity policy.

5.7 Specific Policies

These evolve at a faster rate than business policies. They require more frequent examination since they are more comprehensive. Specialized policies include information categorization, access control, operations, incident management, physical security, human resources, third-party access, and business continuity management.

5.8 Standards

Security standards give direction for implementing certain security rules, which are typically tied to specific technology or products. These are generated from business top practices, knowledge, occupational drivers, and interior challenges and are utilized as a baseline for audit reasons. They must be reviewed on a regular basis to ensure that new releases and vulnerabilities are dealt with properly. UNIX server builds, firewall settings, and connection protocols are all examples of standards.

5.9 Procedures

Processes must be flawless, explicit, current, tested, and recorded. Procedures include incident reporting, incident management, user identification addition/exclusion, and server backup.

5.10 Policies as Incentives for Change

Policies may also be used to propel new corporate efforts ahead, with policies serving as a catalyst for future projects aimed at improving security and general procedures. A regulation requiring a certain sort of encryption for sensitive material communicated over email, for example, might assist to promote the need for such a capability in the future. Because of this legislative need, the desire to build an email encryption project has not waned. In conclusion, a safety policy should be a useful tool for maintaining the Enterprise's safety, which all employees may use as a direct and data basis in their everyday work. Security policies, on the other hand, are all too frequently treated as "shelfware," with users seldom reading, using, or even being aware of them, and separated from the other organization's policy and safety practices [70].

5.11 Workability of Policies

The key to making a firm's security policy-relevant and usable is to create a set of policy documents that are tailored to the target audience and tie in with current corporate rules. Useable, practical, and realistic policies are required. To do this, significant players in policy formulation and maintenance (such as senior administration, inventory, and legitimate) must be involved, and buy-in is essential (such as business stuff specialists, organization supervisors, and end-users). One key component in doing this is communicating the necessity and utility of guidelines to people who must live with them. Frequently, consumers appear to believe that policy will obstruct their day-to-day operations. The communications that guidelines are beneficial to employers:

providing an outline in which they can operate, an orientation for top performance, and ensuring users obey with legitimate responsibilities is a key aspect of policy formulation and ensuring policies are put into effect and not rejected by users is a key aspect of policy formulation and ensuring policies are put into effect and not forbidden by users is a key aspect of policy formulation and ensuring policies are put into effect and not rejected by users. Users are far more likely to be open to both helping you establish policy and living according to it to guarantee acquiescence once they understand it would benefit them in their work. Likewise, when senior administration understands that policy is a weapon they can employ to ensure compliance with authorized requirements and advance much-needed novel initiatives, they are considerably policy champions in terms of economic and resource backing [71].

5.12 Policy Audience Groups

The target audience is corporate workers, but this assembly may be subdivided into viewer sub-classes, with individuals of each sub-class mostly to seek out various information security policies. The primary target audiences are:

- Administration
- Official workforce
- End-operators

Every user will be classified into at least one of the three categories (end-user), and few will be divided into all three.

5.13 Audience and Policy Content

What will be included in each policy paper will be determined by the policy's target audience. For example, if the person who reads is a official guardian of system configuration, an explanation of why something is required for a policy may not always be essential because they are likely to previously understand why that definite act is

required. A director, on the other hand, is not worried about the technical details of why anything is carried out, but they could be looking for a high-level summary of the action's underlying notion. If the reader is an final user, however, it may be beneficial to describe why a specific security measure is essential since this will not only assist them to comprehend the policy but will also make them more likely to follow it.

Permission for the possibility that person who reads will wish to utilize the policies in a variety of means, potentially even at the same time. When reading a policy document for the first time, an end-user may want to read the entire page to understand everything they need to know about helping to protect the company's safety. However, the user may return to the document at a later date to double-check the exact language of a particular policy report on a certain issue. Organizations should make sure that their security data policy documents meet the needs of their target audiences, which often involves the use of many document formats within a policy agenda. The audience for the document will determine which sort of document to utilize in a significant part. For example, A job aid or guidelines document will be used to outline how to design the instant messaging system to ensure that it conforms with the Acceptable Use Policy, on the other hand a document that specifies how to design the prompt messaging system to guarantee compliance with the Acceptable Use Policy, will be in the form of a task help or guidelines manuscript. Directors and end-users are more inclined to employ the first, whereas organisational staff choose the second [72].

5.14 Governing Policy

Governing Policy should provide a high-level overview of cybersecurity ideas, define these terms, explain why they are essential, and state your corporation's position on them. Managers and end-users will read the Governing Policy. Technical custodians (especially security technical custodians) will be able to read it by default because they

also end users. The policy will be used by all of these groups to get an intellect of the corporation's overarching safety policy perspective. This may be used to update their interactions with business units across the organization regarding information security. HR (Human Resources) and other business policies, both current and future, should be closely connected to the Governing Policy, particularly any that include security-related issues. These company-wide policies will be on the same level as the Leading Policy paper. Technical Policies complement the Governing Policy by delving further into subjects and expanding on them by trading with them for every applicable expertise. Few issues might be addressed at the Leading Policy level, obviating the necessity for a comprehensive procedural policy on these matters. Declaring the company's overarching password policy, for example, ensures that specifics of particular password restrictions may be handled in the applicable technical policy for each working organisation or presentation, rather than requiring a technical policy for all systems' password management. In a smaller firm, when there are fewer systems/applications and a single technical password policy may suffice, this may not be the case. However, in a larger organization, the former technique provides a more well-organized procedure for operators since they will have to refer to fewer papers — streamlining this process increases the likelihood that employees will follow strategy, thus refining safety. On a more detailed level, governing policy should address the "what" in terms of security policy [73].

5.15 Technical Policies

Technical custodians will utilize Technical Policies to fulfill their safety obligations for the organization they work in collaboration. These custodians will be more tailored to a system or issue than the Governing Policy. Many of the same issues as Governing Policy will be covered in Technical Policies, and some extra subjects related to the

broader technical topic. They are security standards for OS systems and network devices. They specify what should be done but not how; technical papers, that are the subsequent level of detail lower than the Leading and Technical Policy, are utilised for that. Technical Policy should cover the "what," "who," "when," and "where" of security policy on a more detailed level [73].

5.16 Job Aids/Guidelines

Procedural documents detail how to carry out policy declarations in a step-by-step manner. For example, one or more secondary papers for a Technical Windows Policy may be a direction to harden a Windows server. At the next level of granularity, measures and rules should be created, describing how something should be done. They give methodical, real-world evidence on how to put policy texts' necessities into practice. Depending on the needs, they may be written by many organizations within the firm and possibly it may or may not be cited in the appropriate policy. Technical papers can be written in backing of other sorts of policy documents to assist readers understand what the policy means by giving more thorough explanations. Not all rules will necessitate the submission of supporting documentation. These supporting papers do not have to be created by the same policy making team that creates the Leading and Procedural policies. Individual business units may find it more effective to make their own supportive papers as needed, due to a lack of funds on the policy making team as well as the fact that official workforce in professional have the most comprehensive and informed practical information in the company, allowing them to transcribe such papers more effectively. The policy lays out the structure for them to follow (the "what," "who," "when," and "where" of security policy), and all they have to do now is implement the controls and sketch out the "how." If a staff member quits, job aids and

guidelines will serve as a backup, ensuring that their expertise is not lost and that policy requirements are met.

5.17 Policy Development Process

5.17.1 Development Process Maturity

The level of process maturity will be a significant element in every company's policy creation process. Businesses (particularly bigger ones) must not set their sights too high and attempt to establish a complete and sophisticated policy database right soon. For a variety of explanations, comprising a lack of administration buy-in, inadequate business values and assets, and other criteria that aren't in place, this is unlikely to succeed. In this case, it's best to start simple, maybe with checklist-style policies and simply a skeletal policy structure with the most important rules written first. Organizations will be able to establish the complete spectrum of guidelines, with greater information and are associated with technical certification as needed, as the process matures. Education, awareness, and communication systems will mature to cope with the promotion of an ever-increasing number of policies. This should be in line with the policies' increasing corporate power. The corporate culture will begin to recognize the importance of policies and may even begin to utilize them to advocate for required reforms throughout the organization.

5.17.2 Top-Down Versus Bottom-Up

There are several places to start when drafting policy. New or upcoming legislation, as well as recent security events or passionate administrators fresh off the last training session, can serve as significant impetuses for policy development. All of these are valuable policy inputs, but the issue is to strike a balance. If you create your policy entirely from the top-down, utilizing just laws, rules, and best practices, you will end up with an impractical, fake policy which will not operate in reality. Likewise,

depending solely on a "bottom-up" approach based solely on system manager information might lead to policies that are too specialised to a certain environment (perhaps just one division of a big business), based too much on local current practise or the most recent training ideas, and therefore impractical. Top-down and bottom-up methods will combine to produce the optimal policy. It is something that must be considered from the start to achieve this, and it must be represented in the range of areas engaged in policy formulation as well as the sorts of policy reviews that occur. This balanced approach will very certainly lead to a more mature policy formulation process. It may be used in both small and large organizations (where there is minimal distance between the top and bottom) when a broad range of expertise is required to create a realistic and functional strategy [74].

5.17.3 Current Practice Versus Preferred Future

Policymakers should also ponder on how much of the policy should represent current behavior vs a desirable future. A policy that simply shows what is done today and that it may be not important the time it is published. But one that has limitations that cannot yet be applied may be impossible to comply with for practical causes, and so be disregarded as impractical and unfeasible. This must be deliberated at the early step, because if not, and if the policy evolves too far in the direction of the impractical, desirable upcoming model, it may not become evident until the policy breach documentation stage, when a significant amount of time and effort has been squandered producing something of little value. The ideal policy finds a stability between present training and the expected future, and this should be the goal of the policy making team [75].

5.17.4 Consider All Threat Types

The ideal policy finds a equilibrium between present training and the desired prospect, and this should be the goal of the policy development team. While spiteful exterior invaders in the form of viruses and young insect receive a lot of media attention and should be considered when writing policy, there are other factors to consider as well, such as usual tragedies, discontented present, and previous workers, and unawareness leading to unintentional safety experiences. Controls should be included in policies to address all of these threat categories [76].

5.18 Policy Development Lifecycle

You may begin the policy creation process once you've established who will be engaged in creating the policy.

5.18.1 Senior Administration Buy-in

Creating a set of policy document will need a high degree of dedication from not just the principal originator and manufacturer team, but also many additional business information security employees. Administration acquisition must be obtained from the start of the policy project to ensure that these capitals are accessible for you when required and you get the data you want. Administration must be made aware of the task's importance and scope so that resource allocation in the latter phases does not become a stumbling block. Senior administration also contributes to the policy formulation and upkeep procedure by promoting the resultant policies all over the organization and placing their mass after them, ensuring that the policy is regarded as having "teeth they should also be ready to help initiatives that arise as a result of the policy to assure acquiescence. These two forms of support are critical to the policy program's long-term survival [77].

5.18.2 Determine a Compliance Grace Period

You should refer with the Interior Inspection assembly early in the policy development process to determine as early as possible, after the policy is published they will inspect centred on the policy. Through giving an elegance phase for agreement, you assist in the enforcement of the regulations. This refinement period will provide employers who must adhere to the policies ample time to examine them and execute any required projects, procedures, or internal messages to guarantee compliance. The refinement period might last from few months to a year, depending on the size of the firm.

5.18.3 Regulate Resource Engrossment

At this point, you need to find out whom you should speak with to regulate and decide on the policy's substance. People that were involved should be enlisted in the policy development group section. You must estimate how much time each team member will devote to the mission. Policy developments that are delayed because subject-matter experts (SMEs) are overworked risk becoming obsolete before they are completed. Obtain direct buy-in from line administrators if required. Individuals will, in most circumstances, see the importance of policy and will be delighted to assist you in developing something that will benefit them in their employment, but you must first ensure that they are on panel before head proceeding.

5.18.4 Review Existing Policy

Examine any current security policies in your organization to see if they may be incorporated into the new set of policies. Gather any relevant processes, guidelines, and high-level policy papers. These may all be used to gain a sense of the firm's current position on a certain topic or knowledge, or simply to illustrate how a particular expertise is protected in a different way across the company. This is something that the

new policy paper will need to reflect. Existing instructions or job aids can also serve as the foundation for a policy paper on the same subject [77].

5.19 Policy Document Outline

Each policy should have the following parts in count to the policy statements that will constitute the primary body of the policy paper.

- **Introduction**

  This segment names the policy and place it in the context of other current data security and corporate policy papers.

- **Purpose**

  Declare the policy's key objectives; this will assist readers to understand why the policy exists and how it should be implemented. Authorized and acquiescence concerns should also be addressed. Comprise any particular rule that the policy is intended to follow.

- **Scope**

  The scope of the policy is a list of the substructure and data systems that it covers, as well as the individuals who are affected by it. Anyone who uses the material or organizations covered by the policy would be considered a stakeholder.

- **Roles and Duties**

  This is a description of the organizational structures that assign policy implementation duties throughout the firm. Database Administrators (DBAs), Technical Custodians, Field Office workers, and other job roles may be mentioned in this area.

- **Sanctions and Violations**

  This section explains what constitutes a policy breach (e.g., is it HR-related and thus connected to worker's agreement, or is it an issue for the data safety branch?) This section should also include information on how to report infractions, whom to report them to, and what measures should be taken if they occur. It should also state what penalties will be imposed if a violation occurs (like oral or transcribed notices, etc).

- **Revisions and Updating Schedule**

  This section outlines who is accountable for policy changes and modifications, as well as how frequently they will occur. It can be beneficial to refer to the manuscript as a "living document" that can be rationalised as needed by people in charge of changes and updates. This will guarantee that both ad hoc and planned changes are taken into consideration. It's also a good idea to add information on where the policy will be issued and how personnel will be able to view it.

- **Contact information**

  Indicate who should be notified about the policy. It's better to use a collection or letterbox rather than an individual because they're less likely to alter.

- **Definitions/Glossary**

  Define terminologies that the reader might not be familiar with. The need for this will vary depending on the audiences; for example, the distribution of a Practical Policy for Linux is possibly to be acquainted with Linux practical jargon, thus it will not be required to define them. However, the cryptography part of the user policy may contain words that users are unfamiliar with, and

these terms should be explained in footnotes or a glossary to help comprehension.

- **Acronyms**

  Where there are a high number of acronyms or the text is long or complex, a distinct segment explaining out acronyms may be necessary. Acronyms can be spelled out in the body of a text for shorter papers.

- **Troubleshooting**

  It discusses few of the issues that arise in policy formation, as well as potential solutions to these issues [78].

5.20 Conclusion

Any company's cybersecurity policy serves as both a beginning point and a reference point. The policy demonstrates the organization's commitment to safety and serves as a live device for each worker to assist create and uphold that degree of protection. As a result, having an accurate, comprehensive, and usable cybersecurity policy is critical. Producing a policy that meets this criterion can be a difficult undertaking. Using the techniques described in this chapter to assess policy audiences, themes, and methodologies will assist to guarantee that policy papers are as efficient and usable as feasible.

Chapter 6

National Cyber Security Policy for an Air-Gapped Network

6.1 Introduction

Cybersecurity may be defined as a multi-disciplinary approach that encompasses both the software and hardware to prevent the incidence of cybercrime at the first instance or wane its impact if it has already occurred. Cybersecurity is a crucial challenge for several corporations such as government databanks, financial companies as well as banks, and the military. Security policies are an official set of rules that are made by an institute to safeguard that the user approved to gain access to company information and technology endowments abide by the rules and procedures related to data protection. A security policy is regarded as "living document" which implies that it is never done, but it is constantly revised as conditions of the technology and worker vary.

Cybersecurity policies are crucial because cyberattacks and information breaches are potentially expensive. Also, employees are frequently the weak connections in a company's security. Moreover, the human being working in the organization is considered as the weakest link in the chain of security. Since he also retains his footprints on social media networks in one form or another; an intentional or accidental slippage of even slight confidential information can lead to a big security risk, making the very isolation of AGNs questionable. Upgraded cybersecurity policies can assist employees and consultants in better comprehend how to sustain the security of information and applications. Thus, design of a comprehensive national cyber security policy, its implementation, auditing, and continuous up-gradation remains a customary pre-requisite to ensure any security breach.

6.2 National Cyber Security Policy for an Air-Gapped Network

Policy ID no_____

NATIONAL CYBERSECURITY POLICY FOR AN AIR-GAPPED NETWORK

This policy applies to: organizations having air-gapped networks

DOCUMENT CONTROL

Managed by:	Responsible position:	Version:
Contact person:	Approved by:	File number:
Contact position:	Date approved:	Status:
Contact number:	Next review date:	Security classification:

REVISION RECORD

Date	Version	Revision description

6.2.1 Title

National Cyber Security Policy for an Air-Gapped Network (AGN)

6.2.2 Policy Statement

It is the policy of an Air-Gapped Network (AGN) that all data and info handled by it be completely protected from any threat (inside/outside) in order to shield against the impacts of violations of confidentiality, failures of integrity, or disruptions in availability of that data and info.

6.2.3 Purpose

- The AGN cybersecurity policy is a cornerstone for air-gapped cybersecurity. This policy aims to define what needs to be done to safeguard an organization's assets for confidentiality, integrity, and availability.
- The cybersecurity policy designates accountability and ownership for meeting these cybersecurity needs by defining key roles and responsibilities in meeting the organization's cybersecurity goals.

6.2.4 Scope

Implies to:

- To all info assets and ICT means operated by the organization.
- Pertains to all authenticated workers (employees) of the organization's information assets and IT resources involving but not restricted to staff, senior officers, governors, consultants, security personnel, and administration.
- Encompasses all info/ data stored, handled, shared, or processed by the organization regardless of whether that info originates with or is held by the organization.
- Applies to non-computer-based info system owned by the organization.

6.2.4 Objectives

Following are the objectives of the policy:

- To establish and preserve the confidentiality and protection of info, info systems, networks, and applications owned or held by the organization.
- Ensuring that all employees/ staff are cognizant of their tasks, responsibilities, and accountability and obey the relevant legislation.
- Illustrating the rules of security and describing how they shall be implemented in the routine.
- Establishing a consistent attitude to security, ensuring that aa employees/ staff fully know their duties and responsibilities.
- Creating and sustaining an understanding of the importance of cybersecurity as a day-to-day routine inside the practice.
- Adheres to PECA law of Pakistan, and National cybersecurity policy 2021 of Pakistan.

6.2.5 Policy Documentation Set's Structure

- The policy document set is made up of a hierarchy of subordinate security policies, all of which have equal weight.
- The status of the policy documents is given on the title page of this document.

6.2.6 Approval Process for the Policy

- The governing policy must be approved by the organization's head via the Executive Board (EB) to be included in the organization's policies on expected standards of conduct and behavior. Applies to and will be conveyed to administrative staff, employees, security personals, and others concerned.
- The cybersecurity program team will be in charge of reviewing and approving any subsidiary security policies (CPT).

6.2.7 Responsibility for the Cybersecurity Policy Documentation

- The CPT is responsible for maintaining the cybersecurity policy documentation set, and individual policies may be delegated to department heads.

6.2.8 Maintaining the Policy Document Set

- The EB and CPT will review and revise this policy, as well as any subsidiary policies, on a regular basis to make sure that everything is still appropriate in light of any significant changes to the legislation, organizational rules, or prescribed requirements.

6.2.9 Cybersecurity Policy Details

- The organization will make sure that everyone who uses information systems or handles sensitive data is aware of and understands the policies that apply, as well as the repercussions of non-compliance.
- The organization will employ suitable physical and logical controls to limit access to information systems, any ICT equipment, and information to only authorized users when necessary.
- Planning, creating, implementing, and using IT-based information systems will take full consideration of the cybersecurity policy's requirements.
- The organization will employ legal ways of monitoring the use of info systems and networks to prevent and detect violations of the cybersecurity policy.
- To ascertain the suitable levels of security actions applied to info systems, each system must go through a risk assessment procedure to determine the likelihood and consequences of security failures.
- Expert security advice must be made available throughout the organization to ensure that it retains and implements a current understanding of risks and mitigations in its information management procedures.

- All workers will be bound to abide by the organizations' policies before being authorized to access the installation's data and info systems.
- The organization will maintain and establish relevant contacts with other regulatory bodies, law enforcement authorities in respect of its cybersecurity policy.

6.2.10 Responsibilities for Implementing the Cybersecurity Policies

- A cybersecurity working group comprised of important system administrators, managers, IT experts, and representatives from all key sectors of the organization shall formulate plus implement the security/ safety controls through mutual coordination.
- CPT will be responsible for ensuring the security of IT-based info systems and ensuring that appropriate security processes are followed.
- The effectiveness and implementation of the cybersecurity policy shall be reassessed periodically by the organization's internal audit team as part of its regular audit program.

6.2.11 Monitoring, Evaluation, and Review

- A nominated representative from each department who is also part of the CPT will supervise and monitor policy implementation in true letter and spirit within his/her department.
- The departmental head will inspect all security arrangements weekly/fortnightly.
- This policy will be reviewed after every 4 months or when instructed by the organizational head.
- Any change will be allowed by the head after the consultation with EB.

6.2.12 Definitions and Abbreviations

Term	Meaning
Cybersecurity Program Team (CPT)	A team constituted by the head of the organization as per nominations of representatives received from each departmental head.
AGN	Air-gapped network
EB	Executive Board
Info	Information
IT	Information Technology

6.3 Subsidiary Cybersecurity Policies for AGNs

In the light of governing policy, various subsidiary/ sub-policies encompassing various facets of cybersecurity pertinent to an AGN have been developed and are described as follows.

6.3.1 Personnel Policy

Policy ID no_____

PERSONNEL POLICY FOR AN AIR-GAPPED NETWORK

This sub-policy applies to: organizations having air-gapped networks

DOCUMENT CONTROL

Managed by:	**Responsible position:**	**Version:**
Contact person:	**Approved by:**	**File number:**
Contact position:	**Date approved:**	**Status:**
Contact number:	**Next review date:**	**Security classification:**

REVISION RECORD

Date	Version	Revision description

6.3.1.1 Title

Personnel Policy for an AGN

6.3.1.2 Policy statement

It is the policy for an AGN that the recruitment, training, and departure of personnel shall comply with the security safeguards to the access and use of information technology resources and data.

6.3.1.2 Purpose

The following are the goals of the personal security policy:

- Establish rules on the employment, training, and termination of all personnel (e.g. employees, staff, contractors) to enforce compliance with the cybersecurity policy.
- Define the Organization's requirement for personnel security controls and how and where they should be applied, and in so doing mitigate the risk of unauthorized access to the data, electronic systems, and physical premises.

This policy reflect

- Employment/ Enrolment of staff
- Training of all staff
- Departure of staff

6.3.1.3 Scope

This policy pertains to all the organization's personnel which includes temporary and permanent staff, governors, security personnel, head of departments, senior staff, and internal auditors, and partner organizations (if any) with access to the info and info systems of the organization.

6.3.1.4 Objectives

- The personnel policy is aimed to protect the workforce member as well as info systems and the organization's holdings. This contains safeguarding assets from unsanctioned access, modification, disclosure, destruction, or intrusion.
- All employees are required to implement appropriate security activities or processes to protect info systems and assets.
- Individuals should be given responsibility for any actions taken or activities that occur under their scope of duties.

6.3.1.5 Policy details

<u>On staff employment</u>

- The organization's terms and conditions of employment must contain the employer's and employee's obligations to follow cybersecurity policies/ procedures.
- All personnel/ employees must sign a formal agreement acknowledging the need of maintaining info confidentially and to follow the cybersecurity policies both during and after their employment, as part of their terms and conditions of employment.
- Any visitor or temporary staff must be given an appropriate description of the cybersecurity policies and must agree to it before the use of IT services and physical access inside the premises.
- When the confidentiality, sensitivity, or worth of the material/ info being disclosed is critical, non-disclosure agreements must be used.
- To raise awareness and educate employees about the spectrum of threats, suitable safeguards, and the need of reporting suspected problems or threats, all employees will be given information security awareness tools.

- Before employing the staff, thorough on-ground verification such as police verification must be ensured.
- Any data security occurrences stemming from non-compliance should be met with severe repercussions.
- If a user is determined to have violated the organization's security policies or protocols after an investigation, they will be punished in accordance with the disciplinary sanctions.

Training of staff

- Training to all users of the new system must be ensured so that their use is both efficient and secure.
- Periodic training for nominated Security Officers (SO) should be prioritized in order to educate and teach them on the most recent threats and security measures.
- As part of their induction, all new employees must take a security awareness course.
- When IT or other employees change positions or tasks, their information security requirements must be reevaluated, and any further training required should be offered as soon as possible.
- IT employees must get training in info security, threats, and safeguards, with the level of training reflecting the job holder's responsibilities for configuring and maintaining information security standards.

Departure/ termination of staff

- Access credentials to the organization's info assets and systems shall be terminated for departing employees upon termination of employment.

- Concerned IT members of the cybersecurity program team should remove the access of departing staff from the applications or systems that process sensitive info.
- Revocation of all digital certificates is required at priority.
- Tokens, smart cards, and passes issued to them must be deposited back to issuing authority of the organization.
- Any identification cards or keys they were given during their employment should be returned.
- Physical access to the organization's facilities should be revoked immediately.
- Before leaving the organization, the departing personnel must be physically checked by the concerned security staff.
- They should not be given access to their desk or office, and if they are, it should be limited and closely monitored.
- Departing staff ought to return any equipment and info assets belonging to the organization.

6.3.1.6 Roles and responsibilities

The organization's personnel security policy is intended to be implemented and followed by all employees. Any security incidents, potential events, or other security threats should be reported to the departmental head or cybersecurity program team.

6.3.1.7 Policy compliance

- The cybersecurity program team representative will ensure that all staff and contractors receive education and training as per this policy.
- The CPT is responsible for enforcing compliance with the policy under the direction of the Executive Board.

6.3.2 Social Engineering Awareness Policy

Policy ID no_____

SOCIAL ENGINEERING AWARENESS POLICY FOR AN AIR-GAPPED NETWORK

This sub-policy applies to: organizations having air-gapped networks

DOCUMENT CONTROL

Managed by:	Responsible position:	Version:
Contact person:	Approved by:	File number:
Contact position:	Date approved:	Status:
Contact number:	Next review date:	Security classification:

REVISION RECORD

Date	Version	Revision description

6.3.2.1 Title

Social Engineering Awareness Policy

6.3.2.2 Policy Statement

To raise awareness of social engineering threats in cybersecurity to safeguard the organization's assets. All employees ought to protect the confidentiality and integrity of assets against social engineering vulnerabilities and threats.

6.3.2.3 Purpose

To inform employees that (a) fraudulent social engineering assaults do occur, and (b) processes exist for detecting such attacks.

- Educate employees on the strategies employed in such assaults and are given regular protocols to follow in the event of an attack.
- Employees are aware of who to contact in these situations.
- Employees understand that they play a vital role in an organization's security. To safeguard the organization’s assets and sensitive info, maintaining the integrity of employees represents the best line of defense.

To provide precise guidelines/ procedures for staff to adhere in order to assist them in making the best decision when:

- Somebody is making contact with the employee - by phone, fax, in person, email, or online - and attempting or seeking to gather sensitive info about the organization.
- The employee is being "socially coerced," "socially urged," or "tricked" into disclosing sensitive info.

6.3.2.4 Scope

All employees of the organization are included in the scope, also temporary contractors if any.

6.3.2.5 Policy details

- Employees will make every single effort to prevent falling into the trap of social engineering. They will preserve all information owned by or delivered to the organization, including sensitive personal info about the organization and its constituents, as well as information regulated by law.
- Employees will diligently listen and attend to any social engineering training that the administration/relevant authorities direct them to attend.
- Employees will note warning signs for social engineering attacks and report them to CPT. Unauthorized individuals, for example, may exhibit the following warning indications:
    - Any reference to a higher authority figure that is not accompanied by documentation and confirmation from that authority figure is invalid.
    - Any claims of immediacy or exigency that aren't backed up by evidence.
    - Any requests for unlawful, undocumented info releases, including passwords, sensitive personal information, and financial info.
    - Unknown individuals communicating with you via phone, email, text, fax, social media applications, or in person. Unknown individuals could include those who have not been authenticated or verified.
    - Any requests for information that are not accompanied by adequate paperwork or approval.
    - Any suspicious person or unknown person contacting you on your way to home trying to discuss your job or organization.
    - When at home using some social application on your laptop, PC, or mobile device and you receive a request from an unknown account or person, or somebody sends you a link to click.

- Any person asking for an official USB or Laptop for usage.

- 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.
- A strict ban must be imposed on carrying personal Mobile computing devices, USBs or external hard disks etc.
- 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.
- Always be mindful that fool-proof security can only be accomplished if everyone assumes his responsibility and stays vigilant.

6.3.2.6 Roles and responsibilities

All employees are responsible for adhering to the policy.

6.3.2.7 Policy Compliance

Compliance will be assessed by the organization's administration and security team using a variety of ways, including training attendance, internal reports, violation monitoring, compliance exercises, and responses. Non-compliance with this policy will be dealt with at the administration's discretion, up to and including termination depending on the severity of the infraction.

6.3.3 Physical Security Policy

Policy ID no_____

PHYSICAL SECURITY POLICY FOR AN AIR-GAPPED NETWORK

This sub-policy applies to: organizations having air-gapped networks

DOCUMENT CONTROL

Managed by:	**Responsible position:**	**Version:**
Contact person:	**Approved by:**	**File number:**
Contact position:	**Date approved:**	**Status:**
Contact number:	**Next review date:**	**Security classification:**

REVISION RECORD

Date	Version	Revision description

6.3.3.1 Title

Physical Security Policy

6.3.3.2 Policy statement

To protect the physical security of all human and info assets in order to stop unauthorized physical access to, destruction/ damage to, and interference with info and info processing facilities.

6.3.3.3 Purpose

Following are the goals of the policy:

- Establish the procedures for controlling, scrutinizing, and removing physical access to the organization's premises.
- Physical protections required to safeguard people, info, and assets (including ICT equipment) to reduce or remove security threats.

6.3.3.4 Scope

This policy applies to the physical areas where information assets are kept. These areas include server rooms, telecom closets and office areas that may contain organization's sensitive information. These areas must be physically secured to prevent theft, tampering, or tapping, or damage. It also pertains to all permanent employees, temporary employees, trainees, internal auditors, consultants, and all other visitors.

6.3.3.5 Objectives

Following are the goals of physical security policy:

- To prevent, delay, deter, and/or detect unauthorized access.
- To prevent an attack on, a site and mitigate the brunt should they occur.
- To protect or safeguard all assets.

6.3.3.4 Policy details

The policy details for preserving Physical Security are as follows:

- Physical access to server areas/ rooms must be strictly regulated, and servers must be stored in server racks under key and lock.
- Only designated systems and operations staff will have access to the servers. Besides them, if any other individual likes to work on the servers in the facility area, he or she must connect to the servers exclusively via a remote desktop connection using a controlled user account.
- Vital backup media must be stored off-site in a vault that is fire-resistant.
- Security boundaries shall be created to safeguard areas or zones that contain info systems to thwart unlawful physical access, interference, and damage.
- With suitable authorization credentials, a list of individuals with permitted access to the facilities where info systems are housed must be maintained. Authorized staff must examine and approve the authorization credentials and access list on a regular basis.
- All physical access points to the facilities where info structures are housed (including specified entry/exit points) must be managed, and access to individuals must be provided only after authentication of access authorization.
- Physical access to info systems must be supervised in order to identify, detect, notice, and respond to physical security incidents.
- Fire, earthquake, flood, explosion, and other natural or man-made calamities require physical protection, which must be developed and implemented.
- Physical safety and standards for working in locations where information systems are located must be developed and implemented.
- Info systems, IT eqpt, and their components must be located within the facility to reduce risks from environmental and physical hazards, as well as potential for unauthorized access.

- Info systems should be shielded from power shutdown as well as other interruptions affected by a malfunction in supporting services.
- Telecommunications and power cabling delivering info or supporting info utilities must be safeguarded against damage or interception.
- The surveillance equipment and physical intrusion alarm must be scrutinized in real-time.
- The physical access to info systems must be distinct from the physical access to the site. This restriction may be applied to server areas or info systems that have a greater effect than the rest of the facility.
- Automated technologies for detecting possible intrusions should be utilized to initiate appropriate response measures.
- Physical access to the info systems should be granted only after visitors have been verified before granting entrance to the facility where the information systems are housed, except in places designated as "publicly accessible".
- Visitors' access logs must be kept.
- Visitors must be accompanied by authorized personnel, and their activities must be monitored if necessary.
- Systems personnel must evaluate visitors' laptops and other devices (if permitted to bring them inside) for the most recent updates, patches, anti virus definition, and every type of vulnerability or weakness that could be dangerous to the system or network.
- Every user or employee who needs to connect to an outside network for official purposes must first receive approval from the cybersecurity program team. Before issuing any sanction, this staff must assess security threats.
- All physical accesses by guests and authorized personnel must be recorded.

- All of the policy described above must be checked, monitored, and scrutinized on a regular basis for any modifications.

6.3.3.5 Roles and responsibilities

The chief security officer/designated personnel is in charge of ensuring that the physical security policy is followed.

6.3.3.6 Monitoring, evaluation, and review

A senior security officer will supervise and monitor policy implementation in true letter and spirit with assistance of cyber security program team.

- All nominated departmental officers will inspect respective systems of the organization fortnightly.
- This policy will be reviewed after every 6 months or when instructed by executive board.
- Any change will be allowed by the senior security officer after the consultation from head of organization.

6.3.4 Infrastructure Hardening Policy

Policy ID no_____

INFRASTRUCTURE HARDENING POLICY FOR AN AIR-GAPPED NETWORK

This sub-policy applies to: organizations having air-gapped networks

DOCUMENT CONTROL

Managed by:	Responsible position:	Version:
Contact person:	Approved by:	File number:
Contact position:	Date approved:	Status:
Contact number:	Next review date:	Security classification:

REVISION RECORD

Date	Version	Revision description

6.3.4.1 Title

Infrastructure Hardening Policy

6.3.4.2 Policy statement

To harden the system or structure by reducing its surface of vulnerability and mitigating the possibility of a successful attack by further decreasing the obfuscation. This policy makes it difficult for a potential attacker to identify the system being targeted, and the attack is unable to simply exploit known vulnerabilities.

6.3.4.3 Purpose

This policy establishes the practises that will be used for infrastructure hardening.

6.3.4.4 Scope

This policy covers all aspects of the IT infrastructure, including:

- Application hardening
- Operating system hardening
- Server hardening
- Database hardening
- Network hardening
- Telephone Systems

6.3.4.5 Objectives

Infrastructure hardening aims to diminish security risk by purging potential attack vectors and minimizing the attack surface of the system. This will ensure:

- Enhanced system functionality: Because there are fewer applications and functions, there is a lower danger of operational problems, incompatibilities, misconfigurations, and compromise.
- Significantly improved security: Data breaches, illegal access, system hacking, and malware are all minimized when the attack surface is lowered.

- Simplified auditability and compliance: Auditing the environment is usually easier and more straightforward because there are fewer applications and accounts, as well as a less complex environment.

6.3.4.6 Policy details

Following are the policy details for ensuring system hardening:

- Software that has been permitted or approved for usage by IT department must be installed or setup on the organization's computing equipment.
- Software and services that aren't absolutely necessary will be deleted or disabled as needed.
- Servers, laptops, and PCs will be set up to prevent unauthorized or unwanted software from running.
- Unapproved apps will be deleted automatically by inventory and vulnerability scanning tools.
- BIOS passwords should be enforced on all PCs and laptops to guard against unauthorized and illegal alterations.
- PCs and laptops will have their boot order adjusted to prevent illegal booting from alternate media.
- Access to the local administrator account will be restricted to IT Department personnel to avoid the installation of undesirable software and the alteration of security software and controls.
- Where applicable, default keys or passwords will be altered upon installation and before usage.
- On all official laptops, PCs, and servers, anti-virus and anti-spyware software shall be installed. Antivirus software will be updated on a regular basis.

- Intrusion detection and intrusion prevention system to be placed on every network of the organization.
- On all PCs and laptops, a local firewall will be deployed. Only traffic from allowed ports and sources will be allowed via this firewall.
- Removeable or detachable media usage will be severely monitored. Detachable media will be managed by endpoint security and protection software.
- Before use, all servers must pass a vulnerability assessment. The servers will be examined for vulnerabilities using the organization's vulnerability scanning tools. Before use, all vulnerabilities in the network and operating system will be fixed.
- Every device will be scanned for vulnerabilities on the organization’s network every three months. Any problems that are discovered will be investigated and addressed as needed.
- All devices and IT eqpt on the organization's network will be patched regularly to address the most recent risks.
- A thorough audit of the existing equipment and technology will be performed. To detect faults in the system and prioritize remedies, penetration testing, configuration management, vulnerability scanning, and other security auditing technologies will be used. System hardening measurements must be performed against resources using industry standards such as NIST, Microsoft, and ISO, among others.
- Robust and automated vulnerability detection and patching system should be maintained.
- Firewall hardening necessitates that all systems be correctly configured and audited on a regular basis; secure remote access points and users; close

unwanted network ports (if any); disable and remove unnecessary protocols and services; use access lists and encrypt network communication.

- All servers must be housed in a locked or secure data center. Servers should be hardened enough so that they become resilient to getting connected to external networks if attempted by an insider or outsider. Unnecessary software should not be installed on an organization's server and should be strictly prohibited.
- Admin limitations on what users may do in a database must be implemented, such as by regulating privileged access; node checking must be enabled to validate applications and users; Encrypt database data while it is in transit and at rest; enforce the use of strong passwords; introduce privileges for role-based access control (RBAC); Idle and unused accounts should be removed.
- Hardening of the operating system must be ensured by automatically installing OS updates, patches, and service packs. File sharing, Unnecessary drivers, software, libraries, services, and functionality should be removed. tighten registry and other system permissions; encrypt local storage; Keep track of every activity, faults, errors, and warnings. enact privileged user controls.
- Apply the principle of least privilege to your IT infrastructure by eliminating unnecessary accounts (such as orphaned and unused accounts) and rights.

6.3.4.7 Roles and responsibilities

This policy must be understood and followed by all employees in the IT Department. IT personnel are responsible for ensuring that the IT infrastructure is hardened and that any subsequent changes to systems do not compromise system hardening.

6.3.4.8 Monitoring, evaluation, and review

- Senior IT officer will supervise and monitor policy implementation in true letter and spirit with assistance of cyber security program team.
- All nominated departmental IT officers will inspect respective systems of the organization fortnightly.
- This policy will be reviewed after every 6 months or when instructed by executive board.
- Any change will be allowed by the senior IT officer after the consultation from head of organization.

6.3.5 Access Control Policy

Policy ID no_____

ACCESS CONTROL POLICY FOR AN AIR-GAPPED NETWORK

This sub-policy applies to: organizations having air-gapped networks

DOCUMENT CONTROL

Managed by:	Responsible position:	Version:
Contact person:	Approved by:	File number:
Contact position:	Date approved:	Status:
Contact number:	Next review date:	Security classification:

REVISION RECORD

Date	Version	Revision description

6.3.5.1 Title

Access Control Policy

6.3.5.2 Policy statement

This policy specifies the rules relating to authorizing, controlling, and monitoring access to an organization’s accounts, info & info systems.

6.3.5.3 Purpose

To guarantee that all access to info assets is correctly permitted to legitimate users and permissions to access are monitored, maintained, and reviewed.

6.3.5.4 Scope

This policy applies to all employees and systems who have access to accounts, info, or info systems owned or maintained by the organization.

6.3.5.5 Objectives

- By implementing suitable access controls, the appropriate info is made available to the appropriate people at the appropriate time, and access to information in all systems is appropriately monitored and audited on a regular basis.
- To ensure that unauthorized access is prevented and denied.

6.3.5.6 Policy details

- All info assets must be "owned" by a certain person within the organization.
- On a quarterly basis, a procedure for employee access requests that outlines the steps to be followed when generating or changing employee access must be created, documented, analyzed, and revised. This process's scope must cover network, application, and database access.

- Access to assets containing data or info must be limited to authorized employees and shielded by appropriate logical and physical authentication/ authorization mechanisms.
- Accounts and passwords must be used to verify/authenticate users accessing info systems.
- Employers who have met all of the conditions may be provided access to info assets only if they have particular need to know about, or have access to, said info assets.
- Classification or categorization of an info asset does not specify which employee has access to that info. Access is further restricted by any other privacy limitations imposed by other security rules.
- Access rights must be allowed by the relevant info keeper and assigned to employees based on the fewest privileges needed to carry out their job duties.
- Administrator accounts should only be accorded to those employees who need them to complete their work duties. Administrator accounts must be stringently managed, with their usage tracked, monitored, and evaluated on a regular basis.
- An employee with administrator access will only access sensitive info if it is essential to complete a specific activity.
- Owners of info assets, line managers, and authorized users must ensure that the privileges and rights granted to users of info assets are appraised at least every one twenty days to ensure that they remain applicable and to compare user functions with documented responsibility. This includes access to user accounts, which will be terminated if they have been inactive for longer than 3 months or 90 days.

- Access shall be allowed only to those IT systems that are required for the user's job function. The management of privilege creep will be addressed through regular maintenance.
- Detailed methods for changing, or cancelling an employee's access must be defined and followed as part of the movers and leavers process.
- Special access may be needed in some circumstances for emergency occasions, such as performing emergency system maintenance. Requests for emergency access must be forwarded to the Head of IT or senior member of a Cybersecurity Program Team and approved by the owner of the info asset or an authorized user. Requests and approvals should be documented, if possible before the alteration is necessary, and a termination term for the access privileges that will be enforced should be specified. Where it is not practicable to do so in advance, a change request must be documented retrospectively.
- Access to secure locations on the organization's facilities should be restricted to authorized employees only.
- All-access to places containing systems that process, store, or transfer classified data (for example, server rooms) must be monitored, regulated, and logged. Logs must be audited on a regular basis, linked with other logs, and securely maintained for at least ninety days unless otherwise banned by law.
- Every visitor must obtain authorization before visiting any of the organization's facilities, in accordance with the physical security policy.
- All visits must be documented, and the documentation must be preserved for at least three months.

- Employees must question, challenge, and report any visitors who are found acting suspiciously or unsupervised at any place where sensitive data is stored or processed.
- Audit logging capabilities must be used to record user account identities and actions performed.

6.3.5.7 Roles and responsibilities

- To guarantee that Access Control Policy is followed, the IT team must create, provide, and publish standards and guidelines.
- IT asset owners (individuals and teams in charge of IT networks, storage, and servers) and authorized personnel must be assigned to each recognized IT asset to approve or deny requests for system access.
- Before implementation, IT asset owners and authorized users must validate each user's access requests to info assets owned by them.
- IT asset owners and authorized users shall approve employees needing access to info assets owned by them.
- The Human Resources (HR) department must notify the IT department when new workers join, move within, or leave the firm.

6.3.5.8 Monitoring, evaluation, and auditing

The IT team is responsible for ensuring that Users receive adequate and clear info to abide by the Access Control Policy. To guarantee compliance with Access Control Policy, the IT Team must keep track of timetables for all info security access audits conducted across the organization.

6.4 Guidelines/ Procedures for an Air-Gapped Network

Procedural details provide step-by-step instructions on the 'how' of taking out the policy statements. For instance, a guide to hardening a PC/ laptop or IT eqpt may be one or several supporting documents to a Technical Infrastructure hardening Policy. Guidelines and procedures are a policy aide, and they should be transcribed at the next level of granularity, explaining how something should be performed. They give systematic practical info about how to fulfil the requirements or conditions set out in policy papers. These may be transcribed by a variety of units or groups all through the organization and depending on requirements, they may or may not be referenced in the appropriate policy. Guidelines may be penned where needed in support of and in addition to the other sorts of policy papers, to assist readers in knowing what is required in policy through extended descriptions. It is not necessary that all policies will need aiding documents. However, if one receives requests for job aids for every policy document one prepares, then original materials may be too difficult to comprehend. So it is recommended that everything one writes should be clear, brief, and comprehensible in the first place, to save readers time.

Governing policy or technical policies might be the same for all the AGN or critical infrastructure organizations but the guidelines or procedures will be different for each organization depending upon their working environment or requirements. Now as a sample, I am assuming an AG military organization "ABC" and will make system hardening guidelines for it.

6.4.1 Introduction

ABC being an AG organization has swiftly transmuted into a paperless IT environment. Therefore, cybersecurity threats have also increased exponentially. To thwart the existential peril, various actions are being taken that involve both physical and IT security.

A key part of our IT infrastructure is PCs and laptops used by organizational employees at all levels and a need was felt to contain vulnerabilities and security gaps in them.

6.4.2 Purpose

To enable end-users to secure their PCs and laptops from various threats, vulnerabilities, and viruses.

6.4.3 Scope

The system hardening details in this document are for the systems, laptops, or PCs having Windows operating system. This document provides a guideline and can serve as a reference document for system hardening. It is kept generic to accommodate Windows 7 and above. All the legitimate users who are authorized to use organization's PCs or Laptops have to implement or follow the system hardening guidelines.

6.4.4 Objectives

Following are the objectives

- Protect PCs/ laptops from viruses through authorized and updated antivirus
- Software.
- Prevent unwanted Windows functions through group policy.
- Use physical protection stickers and tape on the camera/ mic.
- Stop vulnerable and unwanted devices like Wifi.
- Deactivate vulnerable options like F8/ Safe mode etc.

- Encrypt hard disk and USB (organization issued) through Bitlocker.
- Shield BIOS with a password and allowing only boot from internal hard disk of the system.

6.4.5 Guidelines

Following are the guidelines for the hardening of PCs/ Laptops.

- BIOS/ UEFI of every PC/ laptop has a different GUI and depending on its version, various features/ settings are available. However, as a generic guideline following options to be enabled on BIOS.
    - **Password protection**
        - Strong 8-16 characters administrator password be enabled so that any unauthorized attempts to change BIOS/ UEFI settings are prevented. A strong password is a combination of alphanumeric and special characters i.e AbCd@$%1a23d
        - Do not use familiar/ easily guessable password
        - Do not share a password with anyone and keep it safe in a sealed envelope.
        - Change the password after every change in BIOS.
    - **Boot from HDD only**
        - Only enable booting from internal hard disk. Booting from other media i.e floppy disk drive, USB, external hard disk drive, network devices and CD/ DVDs is disabled.
    - **Onboard/ Peripheral devices disabling**
        - All onboard/ peripheral devices like Wifi, Bluetooth, LAN, PCI slots should be disabled.

- Since USB requirement persists, they will be selectively enabled through operating system.

- **Stickers for physical security**

  A highly recommended option is to ensure placing stickers on the opening. This is because BIOS setting can be reset to factory mode by changing jumpers installed on the mainboard. In case stickers are not held with establishment, stickers can be made by applying transparent tape on paper cuts and affixing on sides of laptop/ PC.

- **Taping of camera/ mic**

  Camera and mic should be covered with adhesive tape.

- **Disable F8/ safe mode**

  In administrator mode run following command in cmd.exe

  Bcdedit /set{bootmgr} displaybootmenu no

  Significance: It will disable the safe mode menu and user cannot access the recovery mode.

- **Disable startup repair option**

  In administrator mode run following command in cmd.exe

  bcdedit /set {default} recoveryenabled no

  bcdedit /set {default} bootstatuspolicy ignoreall failures

  Significance: It will disable the recovery mode and if PC/ laptop is accidently powered off then recovery menu will not appear on startup.

- **Disable default administrator account**

  Default administrator account must be disabled. However, another user account may be created with administrator privileges before disabling default administrator account.

- **Windows firewall**

  Windows built-in firewall must be kept on all profiles (i.e, public, private, and domain). In case a service or application needs to interact with a network, a specific rule may be created.

- **Windows group policy**

  By enabling or disabling different features of Group Policy increases the security of user's computer and further harden the system to defend against both insider and outsider attacks. Enable the required features as per the working environment of the ABC organization or as approved by the IT team.

- **Windows Applocker**

  Applocker must be configured in enforced mode, in order to check unauthorized and unwanted applications from running on hardened machines.

- **Bitlocker drive encryption**

  Data drives (i.e.,D,E,F drives) to be protected with windows bitlocker, as it has a built-in feature to encrpt the data on drives. No data should be placed on desktop or windows drive (i.e C drive).

- **Turn off remote assistance and remote desktop**

  To prevent anyone from accessing your PC/ laptop remotely, turning off remote desktop service is necessary. Right Click on this PC or My computer and select properties. Navigate to remote tab and select "Don't allow remote connections to this computer" and uncheck "Allow remote assistance connections to this computer".

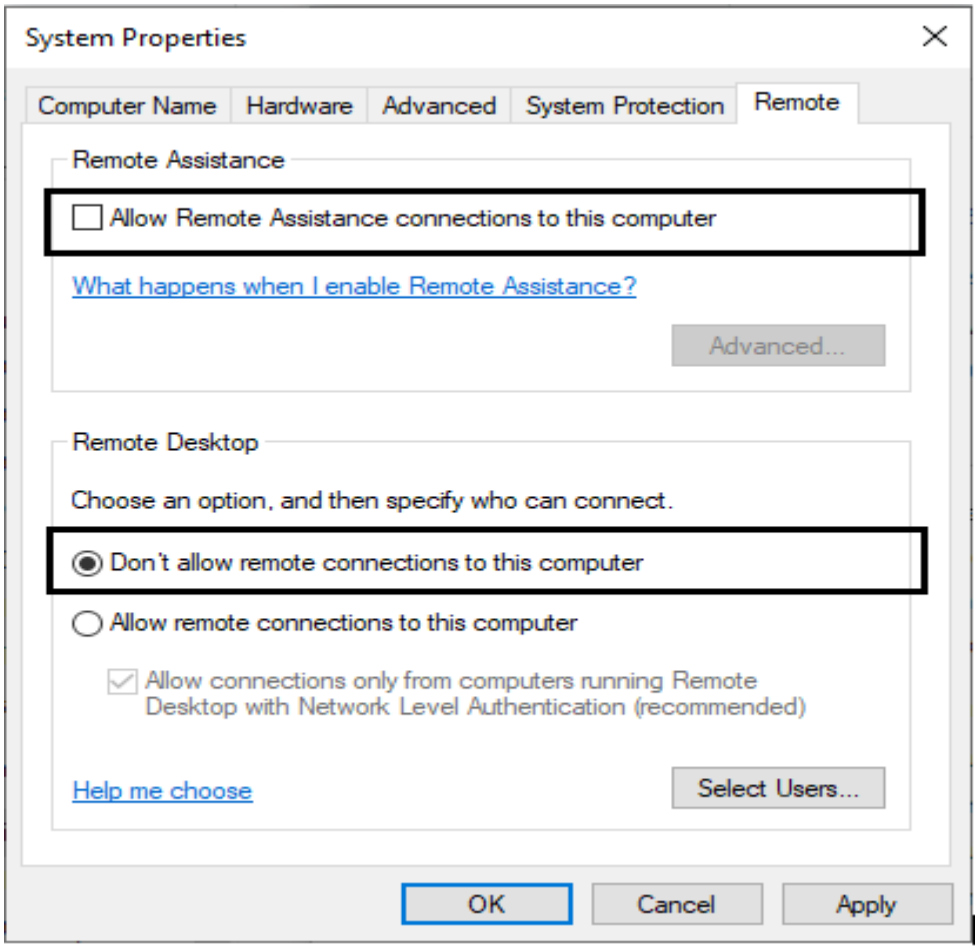


Figure 6.1: Showing turning off remote assistance connection to this computer

- **Disable unnecessary services**

  Following un-necessary services must be stopped and disabled

  - DNS client
  - DHCP client
  - Win HTTP web proxy auto discovery
  - FTP
  - Telnet

- **DO's**

  - Keep AV running and updated at all times.
  - Keep windows updated ny installing authorized update patches.

- Keep strong passwords.
- Keep windows firewall ON.
- Inform IT security team regarding security related incident.

- **DONT's**
  - Donot plug-in unknown USB/ external hardisks.
  - Donot leave PC unattended.
  - Donot connect official PCs/ laptops to internet.
  - Donot keep confidential info in USBs.
  - Donot share your PCs/ laptops password with anyone.
  - Donot temper with security configurations unless instructed officially.

- **Security checklist**

  A checklist should be created for the user self-assessment or counter checking by another security or IT officer of the department. The checklist will ensure all security controls described earlier are applied on the machine.

6.4.6 Roles and responsibilities

It is the responsibility of every senior member of each department to implement the guidelines. Every user or employee to strictly adhere the system hardening guidelines for PCs/ laptops. IT security team of the organization to randomly check the PCs/ laptops of every department at any time. IT security team to ensure that guidelines are followed in true letter and spirit.

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

Following are the guidelines for the safe use of social media for employees families and 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.
- 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.

6.6 Conclusion

The AGN cybersecurity policy is a cornerstone for governing air-gapped cybersecurity thus defining the needs to safeguard an organization's assets for confidentiality, integrity, and availability. Enforcement of Personnel Policy is mandatory for the compliance of recruitment, training, and departure of personnel with the security safeguards to the access and use of info technology resources and data. A subsidiary policy on Social Engineering is indispensable to inform employees that fraudulent social engineering assaults do occur, and processes exist for detecting such attacks. Likewise, a Physical Security Policy to protect the physical security of all humans and info assets effectively stops unauthorized physical access, destruction, and interference with info and info processing facilities. An Infrastructure Hardening Policy was added as a subsidiary policy as it is direly needed to harden the system or structure by reducing its surface of vulnerability and mitigating the possibility of a successful attack by further decreasing the obfuscation. The Access Control Policy specifies the rules relating to authorizing, monitoring, and controlling access to an organization's accounts, info and info systems. After an extensive elaboration of the aforementioned governing and technical policies, the chapter concludes with guidelines on system hardening as an example describing the procedural details and delivers a step-by-step instruction on the 'how' of taking out the policy statements. System hardening guidelines enable end-users to secure their PCs and laptops from various threats, vulnerabilities, and viruses. Guidelines for safe use of social media by employee's families and friends will enable them to remain vigilant and also give them awareness about the hazards of usage of internet social applications. Principally, robust enforcement, consistent audit, and regular upgradation of policies and guidelines is the only viable mechanism to safeguard the confidentiality, integrity and availability of an organization's assets.

Chapter 7

An Overview of National Cybersecurity Policy of Pakistan 2021 and Future Prospects

7.1 Introduction

Worldwide connectivity and digitalization of services have escalated the usage of info and communication technology which in turn has resulted in a greater exposure of info assets to a hub of sprouting cybersecurity vulnerabilities and threats. These assets have become particularly expensive after The Fourth Industrial Revolution. Owing to the rapid proliferation and consistent growth of the Internet, the cyberspace has emerged with a lot of troublesome trends. An increase in the number of episodes of malicious practices of ICTs in cyberspace is distressing the civil rights and integrity of institutions. A diverse class of users including Businesses, Individuals, and State are exposed to financial and security risks which could possibly inflict serious impediments to accomplishing national development objectives in several economic segments. Keeping in view the above scenario, it was an ultimate need to develop a comprehensive national cybersecurity policy. Hence, a Consultation Draft v1.0 of national cybersecurity policy of Pakistan was published on January 25th, 2021, by the ministry of Information Technology & Telecommunication (MoITT) which later on 21st July 2021 has been published as Pakistan's first National Cybersecurity Policy (attached as Appendex). Considering the significance of the issue, a Cyber Governance Policy Committee (CGPC) has been constituted by the Prime Minister of Pakistan consisting of all related ministries and bodies. A comprehensive review of the policy is as under:

7.2 Aim, Scope, and Objectives

The National Cybersecurity Policy aims at developing resilient and secure cyberspace for both private and public sector info and communication systems. It encompasses the

establishment of a framework to govern institutions with a secure cyber-ecosystem. Hence, the scope of Cybersecurity Policy encompasses to shelter the cyberspace of Pakistan entirely involving all the info and communication systems employed in both private and public and sectors.

In line with the aim following objectives have been included:

- Instituting an authority and organizational framework.
- Establishment of security and data sharing process.
- To safeguard the national critical info infrastructure.
- Boosting protection of infrastructure and info systems of the government.
- Design of a data assurance structure of compliance and audits.
- To ensure the integrity of info and communication technology systems, products, and services by developing a system of screening, testing, accreditation, and forensics.
- To develop a public-private partnership.
- To create a state-wide culture awareness regarding cybersecurity.
- To ensure the readiness of competent cybersecurity professionals.
- Encouragement and support of indigenization via Research and Development.
- Various collaborations at national and global level would be established to develop a framework.
- Legislative and regulatory actions would be taken promptly.

7.3 Policy Framework

The Cybersecurity Policy asserts that to attain the objectives, an execution framework shall be constituted by a selected organisation of the Federal Government. The stated organisation will also behave as the Central Entity (CE) at the Federal level for synchronizing and executing all cybersecurity associated issues. According to the

Cybersecurity Policy, the CE has a three-tier extent including: (i) National level (ii) Sectoral Level, and (iii) Organisational Level. It is yet to be decided that the Federal Government will nominate an already existing organisation as the CE, or a new organisation will be formed to pursue the proposed Cybersecurity Act. Following specific areas have been included in the Cybersecurity Policy's framework:

7.3.1 Active Defense

Under the umbrella of active defense comes blocking the attacks of malware, averting email spoofing, and phishing activity, encouraging superlative security practice, working, and collaborating with global law enforcement agencies, controlling and securing the routing of internet traffic for government sectors, and capitalising in skills augmentation of law enforcement bodies and relevant ministries.

7.3.2 Protection of Internet Based Services

The policy framework has included the development of an Internet Protocol Reputation Service to safeguard the government's digital services, installation of products on government networks so that swift software running would be ensured. Lastly it also includes expanding further beyond the domain of gov.pk domain.

7.3.3 Protection and Resilience of the National Critical Info Infrastructure

The policy framework incorporates the protection of national critical info infrastructure by operating necessary technological platforms. For the cloud based and other mobile systems, a secure ICT environment shall be ensured through implementation of national security guidelines and standards. The policy framework further incorporates development of a robust mechanism to safeguard the critical info infrastructure. The formation and enforcement of risk management practices, hiring of skilled info security personnel, and appointment of a Chief Security Officer along with the enforcement of

certification of national security standards are the main points to develop resilient national critical info infrastructure.

7.3.4 Protection of Government's Information and Infrastructure

For the protection of government's info systems and critical infrastructure a robust mechanism to authenticate and protect the data will be constituted. Other framework modalities in this subsection includes creation of a vulnerability evaluation and patch management procedure, guaranteeing obligatory apportionment of a particular percentage of budget for ICT projects, articulating a procedure for the formation and implementation of staff selection and authorisation system, and refining security in government procurement and outsourcing.

7.3.5 Framework for Information Security Assurance

For the assurance of info security, it is pertinent to implement its concept by design and develop contemporary national cybersecurity screening and forensic setups. Creation of an info assurance framework to ensure compliance and regular cybersecurity audit, development of new infrastructure and leverage of current facilities for conformism assessment, accreditation of cybersecurity compliance best practices, forensics, screening, and certification facilities.

7.3.6 Public-Private Partnership

The national cybersecurity policy framework proposes to bridge the gap between research institutions, academia, government, and industry by fostering a progressive entrepreneurial environment. The government has also included start up grants to support such activities.

7.3.7 Research and Development in Cybersecurity

The policy framework has included as its customary part, short-term, medium-term, and long-term R&D programs that would result in solving the indigenous security

issues cost effectively. The policy framework has also incorporated research outcome measurement in the form of innovation and commercialization as well as establishment of various centres of excellence at the national level.

7.3.8 Capacity Building

Capacity building being an integral part for the success of any program has also been included in the National Cybersecurity Policy Framework. The government shall found state of the art centres of excellence for the training and education of personnel and Human Resource Development (HRD) in cybersecurity. The formulation and implementation of a personalized HRD program complying with the cybersecurity demands, increase in the cybersecurity R&D budget, inclusion of updated curriculum related to cybercrime to the graduate and post graduate students at the law and related institutions has been considered as integral part of the newly accepted policy framework.

7.3.8 Awareness for National Culture of Cybersecurity

This part of the policy framework includes planning and implementation of education programs relating to cybersecurity ethical concerns adapted for specific segments of society, promoting the corporate sector to shield the cyberspace, formulating, and effecting a national responsiveness plan for the end user education, employing cybersecurity preparedness program for government systems, and incorporating the cybersecurity responsiveness to the national curricula at secondary and higher secondary school level.

7.3.9 Global Cooperation and Collaborations

Under the umbrella of global cooperation, collaborations with international cohorts, provision of expert participation from Pakistan to all the chief regional and global organizations and qualified bodies, development of a trusted mechanism of info

exchange regarding cyberthreats, attacks, and vulnerabilities across government and public sector organization shall be ensured both regionally and globally.

7.3.10 Cybercrime Response Mechanism

Cybercrime response mechanism would include supporting and augmenting the government's capability by expanding law administration agencies procedural competence, creating coordination and liaison with various international and national cybercrime related agencies for sharing of info and cooperation, reinforcement of the cybersecurity related procedures and processes in the private and public and sector networks susceptible to cyberthreats.

7.3.11 Regulations

As an integral part of the cybersecurity framework, Regulatory bodies will formulate the Cybersecurity Act and Cybersecurity Policy. They shall also make rules and regulations for an effective national cybersecurity framework. The regulatory bodies shall also furnish digital accreditations for the legitimacy of businesses and individuals. Furthermore, protection of privacy of citizens, data protection, standardization of network and digital forensics procedures and infrastructures would be established.

7.4 Strength and Limitations

7.4.1 Strengths

Presently, Pakistan's cabinet endorsed "National Cyber Security Policy 2021" as a much-needed step to ensure the cybersecurity of the exponentially growing cyberspace of Pakistan. The policy document after coming on the surface was approved on urgent basis as the current news on "Pegasus spyware" broke out internationally, wherein the said software was meant to spy on the Prime Minister of Pakistan. The recently approved National Cyber Security Policy 2021 seeks to constitute a policy document that would assist Pakistan with innovative organizational governance and framework to

safeguard Pakistan's "Cyber Ecosystem". Policy framework to be instituted will comprise of Computer Emergency Response Teams (CERTs) and Security Operation Centres (SOCs). The policy envisages safeguarding the whole cyberspace of Pakistan, including both public sector and private sector info and communication systems across the whole country. Additionally, the policy clearly shows that it not only encompasses a secure cyberspace but a "resilient cyber system and network". Resilience is a crucial element because it empowers the systems to operate even in case of assault while absorbing the attack. The steering principle of contemporary cybersecurity policy is to "protect the people" with simultaneous enhancement of the progress and success of the nation. Likewise, the assault on Pakistan's cyberspace will be classified as Category-I and Category-II level threat and would be countered accordingly.

The policy also includes constitution of direly needed National Pakistan Computer Emergency Response Teams (PK-CERTs) which may be a collaborative response structure of military, government, public and private sector. The inclusion of CERTs is a practical step towards responding and reacting to the critical events. Connection of PK-CERT with CERT setups at provincial level is a robust measure in the Policy document however practical implementation needs to be done to pave the path towards a secure cyberspace. The PK-CERT would also act as a bridge between international CERTs for sharing best practices.

7.4.2 Limitations

On every Independence Day, the attack on Pakistani websites by Indian hackers is a wake-up call to the agencies concerned. The National Cybersecurity Policy 2021 is the need of the hour and a much-demanded policy document in Pakistan. It demonstrated what Pakistan intends to attain in its cybersecurity, how it will accomplish its goals, but there are several essential things which the Policy document have missed. The

document describes a “Central Entity” as the organization accountable for executing the policy document, but the details of what the entity will be, who will constitute it and other relevant obligatory details are missing. The same was observed in case of previous National Cybersecurity Policy 2018-2023 in which a Command Force comprising of military and civil representation was proposed but was not implemented as the details for its constitution were not present in the policy draft. Likewise, the policy document included the terms “Privacy by Design” and “no-legacy” without adequately describing the concept.

With a lack of indigenous national ICT and cybersecurity industry, Pakistan depends mainly on imported hardware and software. This dependence along with deficiency of national security standards and weak accreditation have made Pakistan vulnerable to foreign exploitation through imbedded malwares, backdoors, and chipsets. The policy should also include development and employment of indigenously developed software in critical infrastructures where data of national interest is dealt with.

The National Cybersecurity Policy document’s governing policy appears to be a general policy lacking depth and totality. Various subsidiary policies along with the procedures and guidelines must also be worked on to ensure implementation of the policy draft.

7.5 Way Forward

With an increase in the utility of internet and an incredible refinement of cyber attacks by the national and foreign actors, it has turned out to be a grave concern to either restrict the internet usage or thwart these cyber threats. Hence cybersecurity has emerged as a crucial concern for Pakistan’s government, policy makers, and military which are facing continued cyber threats to the country’s Critical Infrastructures (CIs). The CIs such as e-government, hospitals, nuclear arsenals, military institutions, Civil Aviation System, NADRA, emergency services, election commission of Pakistan etc

are the key assets containing classified and critical info. Pakistan’s government has been involved in creating policies for thwarting cyber attacks since 2003, unfortunately no concrete implementation has been achieved. Dynamic developments are influencing the landscape of cybersecurity policy making. No matter what the driving force is behind these transformations-new skills, new threat types, and innovative methods in society, government or industry must be foreseen to formulate novel policies against the challenges, opportunities, and interdependencies posed. The development of a cybersecurity policy requires commitment, management, and a suitable official framework, within which it can be executed. It also needs an appropriate degree of specialty, ways through which agreement can be tested, and a legitimately established reaction in the event of it being desecrated. Any company's cybersecurity policy serves as both a beginning points and a reference point. The policy demonstrates the organization's commitment to safety and serves as a live device for each worker to assist create and uphold that degree of protection. As a result, having an accurate, comprehensive, and usable cybersecurity policy is critical. Producing a policy that meets this criterion can be a difficult undertaking. Upgraded cybersecurity policies can assist employees and consultants better comprehend how to sustain the security of info and applications. Thus, design of a comprehensive national cyber security policy, its implementation, auditing, and continuous upgradation remains a customary pre-requisite to ensure any security breach.

REFERENCES

1. Guri, M., *Exfiltrating data from air-gapped computers via ViBrAtIoNs.* Future Generation Computer Systems, 2021. **122**: p. 69-81.
2. Sohrabi Safa, N., R. Von Solms, and S. Furnell, *Information security policy compliance model in organizations.* Computers & Security, 2016. **56**: p. 70-82.
3. Höne, K. and J.H.P. Eloff, *Information security policy — what do international information security standards say?* Computers & Security, 2002. **21**(5): p. 402-409.
4. Srinivas, J., A.K. Das, and N. Kumar, *Government regulations in cyber security: Framework, standards and recommendations.* Future Generation Computer Systems, 2019. **92**: p. 178-188.
5. Cavelty, M.D., *Cybersecurity*, in *The routledge handbook of new security studies*. 2010, Routledge. p. 166-174.
6. Jain, J. and P.R. Pal, *A recent study over cyber security and its elements.* International Journal of Advanced Research in Computer Science, 2017. **8**(3): p. 791-793.
7. Marin, G.A., *Network security basics.* IEEE security & privacy, 2005. **3**(6): p. 68-72.
8. Yip, A., et al. *Improving application security with data flow assertions*. in *Proceedings of the ACM SIGOPS 22nd symposium on Operating systems principles*. 2009.
9. Huang, Y.-W., et al. *Web application security assessment by fault injection and behavior monitoring*. in *Proceedings of the 12th international conference on World Wide Web*. 2003.

10. Curphey, M. and R. Arawo, *Web application security assessment tools.* IEEE Security & Privacy, 2006. **4**(4): p. 32-41.
11. Enck, W., et al. *A study of android application security*. in *USENIX security symposium*. 2011.
12. Whitman, M.E. and H.J. Mattord, *Principles of information security*. 2011: Cengage learning.
13. Von Solms, R. and J. Van Niekerk, *From information security to cyber security.* computers & security, 2013. **38**: p. 97-102.
14. Stamp, M., *Information security: principles and practice*. 2011: John Wiley & Sons.
15. Peltier, T.R., *Information security fundamentals*. 2013: CRC press.
16. Bulgurcu, B., H. Cavusoglu, and I. Benbasat, *Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness.* MIS quarterly, 2010: p. 523-548.
17. Kadrich, M., *Endpoint security*. 2007: Addison-Wesley Professional.
18. Li, Z., *The Analysis of US Policy on Protecting Critical Infrastructure Security [J]*. Information Security and Technology, 2013. **7**.
19. Robila, S.A. and J.W. Ragucci, *Don't be a phish: steps in user education.* Acm Sigcse Bulletin, 2006. **38**(3): p. 237-241.
20. Linkov, I., et al., *Resilience metrics for cyber systems*. Environment Systems and Decisions, 2013. **33**(4): p. 471-476.
21. Gisladottir, V., et al., *Resilience of cyber systems with over-and underregulation.* Risk Analysis, 2017. **37**(9): p. 1644-1651.

22. Guri, M., et al. *Acoustic Data Exfiltration from Speakerless Air-Gapped Computers via Covert Hard-Drive Noise ('DiskFiltration')*. 2017. Cham: Springer International Publishing.

23. Guri, M., et al. *xLED: Covert Data Exfiltration from Air-Gapped Networks via Switch and Router LEDs*. in *2018 16th Annual Conference on Privacy, Security and Trust (PST)*. 2018.

24. Dhanush, V., et al. *Application of deep learning technique for automatic data exchange with Air-Gapped Systems and its Security Concerns*. in *2017 International Conference on Computing Methodologies and Communication (ICCMC)*. 2017. IEEE.

25. Guri, M., et al. *CTRL-ALT-LED: Leaking Data from Air-Gapped Computers Via Keyboard LEDs*. in *2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)*. 2019.

26. Lee, E., H. Kim, and J.W. Yoon. *Various threat models to circumvent air-gapped systems for preventing network attack*. in *International workshop on information security applications*. 2015. Springer.

27. Kim, S.H., Q.-H. Wang, and J.B. Ullrich, *A comparative study of cyberattacks.* Communications of the ACM, 2012. **55**(3): p. 66-73.

28. Uma, M. and G. Padmavathi, *A Survey on Various Cyber Attacks and their Classification.* Int. J. Netw. Secur., 2013. **15**(5): p. 390-396.

29. Ye, N., B. Harish, and T. Farley, *Attack profiles to derive data observations, features, and characteristics of cyber attacks.* Information Knowledge Systems Management, 2005. **5**(1): p. 23-47.

30. Kugler, R.L., *Deterrence of cyber attacks.* Cyberpower and national security, 2009. **320**: p. 309-340.

31. Rid, T. and B. Buchanan, *Attributing cyber attacks.* Journal of Strategic Studies, 2015. **38**(1-2): p. 4-37.

32. Llansó, T., A. Dwivedi, and M. Smeltzer. *An approach for estimating cyber attack level of effort*. in *2015 Annual IEEE Systems Conference (SysCon) Proceedings*. 2015. IEEE.

33. Onwubiko, C. and K. Ouazzane, *Challenges towards building an effective cyber security operations centre.* International Journal on Computational Science & Applications, 2019. **4**(1): p. 11-39.

34. Lu, M. and J. Reeves, *Types of cyber attacks.* Trustworthy Cyber Infrastructure For The Power Grid, 2014. **18**: p. 2017.

35. Akbari Roumani, M., et al., *Value analysis of cyber security based on attack types.* ITMSOC: Transactions on Innovation and Business Engineering, 2016. **1**: p. 34-39.

36. Bendovschi, A., *Cyber-attacks–trends, patterns and security countermeasures.* Procedia Economics and Finance, 2015. **28**: p. 24-31.

37. Mahjabin, T., et al., *A survey of distributed denial-of-service attack, prevention, and mitigation techniques.* International Journal of Distributed Sensor Networks, 2017. **13**(12): p. 1550147717741463.

38. Wall, D., *Cybercrime: The transformation of crime in the information age*. Vol. 4. 2007: Polity.

39. Weissbrodt, D., *Cyber-conflict, Cyber-crime, and Cyber-espionage.* Minn. J. Int'l L., 2013. **22**: p. 347.

40. Lewis, J.A., *Assessing the risks of cyber terrorism, cyber war and other cyber threats*. 2002: Center for Strategic & International Studies Washington, DC.

41. Lu, W., S. Xu, and X. Yi. *Optimizing active cyber defense*. in *International Conference on Decision and Game Theory for Security*. 2013. Springer.

42. Eom, J.-h., et al. *Active cyber attack model for network system's vulnerability assessment*. in *2008 International Conference on Information Science and Security (ICISS 2008)*. 2008. IEEE.

43. Thulasiraman, P., T. Haakensen, and A. Callanan, *Countering passive cyber attacks against sink nodes in tactical sensor networks using reactive route obfuscation.* Journal of Network and Computer Applications, 2019. **132**: p. 10-21.

44. Cohen, F., *Simulating cyber attacks, defences, and consequences.* Computers & Security, 1999. **18**(6): p. 479-518.

45. Ping, Y., et al., *Multi-agent cooperative intrusion response in mobile adhoc networks.* Journal of Systems Engineering and Electronics, 2007. **18**(4): p. 785-794.

46. Hou, L. and H. Qu, *Automatic recognition system of pointer meters based on lightweight CNN and WSNs with on-sensor image processing.* Measurement, 2021: p. 109819.

47. Brewster, B., et al., *Chapter 8 - Cybercrime: Attack Motivations and Implications for Big Data and National Security*, in *Application of Big Data for National Security*, B. Akhgar, et al., Editors. 2015, Butterworth-Heinemann. p. 108-127.

48. Safa, N.S., R. Von Solms, and L. Futcher, *Human aspects of information security in organisations.* Computer Fraud & Security, 2016. **2016**(2): p. 15-18.

49. Evans, M., et al., *HEART-IS: A novel technique for evaluating human error-related information security incidents.* Computers & Security, 2019. **80**: p. 74-89.

50. Langner, R., *Stuxnet: Dissecting a cyberwarfare weapon.* IEEE Security & Privacy, 2011. **9**(3): p. 49-51.

51. Ramírez, F., et al., *Automatically detect hidden networks from USB devices.*

52. Anderson, B. and B. Anderson, *CHAPTER 3 - USB-Based Virus/Malicious Code Launch*, in *Seven Deadliest USB Attacks*, B. Anderson and B. Anderson, Editors. 2010, Syngress: Boston. p. 65-96.

53. Strupczewski, G., *Defining cyber risk.* Safety Science, 2021. **135**: p. 105143.

54. H. V. P. a. K. Bommakanti, " *Decoding motives behind the Kudankulam intrusion.* 22 Novermber 2019. [Online]. Available:.

55. Guri, M., *MAGNETO: Covert channel between air-gapped systems and nearby smartphones via CPU-generated magnetic fields.* Future Generation Computer Systems, 2021. **115**: p. 115-125.

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

57. Guri, M. and D. Bykhovsky, *aIR-Jumper: Covert air-gap exfiltration/infiltration via security cameras & infrared (IR).* Computers & Security, 2019. **82**: p. 15-29.

58. M. Guri, et al., *AirHopper: Bridging the air-gap between isolated networks and mobile phones using radio frequencies.* 9th International Conference on Malicious and Unwanted Software: The Americas (MALWARE), , 2014.

59. Guri, M., et al., *PowerHammer: Exfiltrating Data From Air-Gapped Computers Through Power Lines.* IEEE Transactions on Information Forensics and Security, 2020. **15**: p. 1879-1890.

60. Nissim, N., R. Yahalom, and Y. Elovici, *USB-based attacks.* Computers & Security, 2017. **70**: p. 675-688.

61. Steinmetz, K.F., A. Pimentel, and W.R. Goe, *Performing social engineering: A qualitative study of information security deceptions.* Computers in Human Behavior, 2021. **124**: p. 106930.

62. Merwe, J.V.D. and F. Mouton. *Mapping the Anatomy of Social Engineering Attacks to the Systems Engineering Life Cycle*. in *HAISA*. 2017.

63. Grassegger, T. and D. Nedbal, *The Role of Employees' Information Security Awareness on the Intention to Resist Social Engineering.* Procedia Computer Science, 2021. **181**: p. 59-66.

64. Verweijen, J. and A. Dunlap, *The evolving techniques of the social engineering of extraction: Introducing political (re)actions 'from above' in large-scale mining and energy projects.* Political Geography, 2021. **88**: p. 102342.

65. Hatfield, J.M., *Virtuous human hacking: The ethics of social engineering in penetration-testing.* Computers & Security, 2019. **83**: p. 354-366.

66. Albrechtsen, E. and J. Hovden, *Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study.* Computers & Security, 2010. **29**(4): p. 432-445.

67. Bernard, R., *Information Lifecycle Security Risk Assessment: A tool for closing security gaps.* Computers & Security, 2007. **26**(1): p. 26-30.

68. Cheng, L., et al., *Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory.* Computers & Security, 2013. **39**: p. 447-459.

69. Lippert, R.K., K. Walby, and R. Steckle, *Multiplicities of corporate security: Identifying emerging types, trends and issues.* Security Journal, 2013. **26**(3): p. 206-221.

70. Ifinedo, P., *Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory.* Computers & Security, 2012. **31**(1): p. 83-95.

71. Wolff and Josephine, *Models for Cybersecurity Incident Information Sharing and Reporting Policies.* TPRC 43: The 43rd Research Conference on Communication, Information and Internet Policy Paper, , August 13, 2014.

72. Morrow, A.B., *Chapter 10 - Information security and cyber threats and vulnerabilities,* in *Intermodal Maritime Security*, G.A. Gordon and R.R. Young, Editors. 2021, Elsevier. p. 169-193.

73. Schoenefeld J and J.A. Jul;. *Governing policy evaluation? Towards a new typology.* Evaluation., 2017. **23**(3): p. 274-93.

74. Sutton, R., *THE POLICY PROCESS: AN OVERVIEW*. August 1999, Overseas Development Institute Portland House Stag Place London SW1E 5DP: Chameleon Press Ltd, London SW18 4SG.

75. Weible, C.M., et al., *Understanding and influencing the policy process.* Policy Sciences, 2012. **45**(1): p. 1-21.

76. Deleon, P., *Reinventing the policy sciences: Three steps back to the future.* Policy Sciences, 1994. **27**(1): p. 77-95.

77. Chapin, R.K., *Social Policy Development: The Strengths Perspective*. Social Work, 1995. **40**(4): p. 506-514.

78. Althaus, C., Davis, G., & Bridgman, P, *The Australian Policy Handbook: A practical guide to the policy making process* (6th ed.). ed, ed. Routledge. (1998).

APPENDIX

Ministry of Information Technology
& Telecommunication

DIGITAL PAKISTAN

NATIONAL CYBER SECURITY POLICY 2021

JULY 1, 2021

MINISTRY OF INFORMATION TECHNOLOGY & TELECOMMUNICATION

Government of Pakistan

Table of Contents

1 Background

1.1 INTRODUCTION

Information and Communication Technologies (ICTs) have played a key role in revolutionizing the world, making it truly a Global Village within the last decade. The innovation in Information and Communication Technology is redefining the dimension of socio-economic development in the world, resulting in commercial, economic, cultural, and social opportunities for users of Cyberspace.

This unprecedented growth has ushered in a new era, marked with easy and low-cost access to highly interconnected networks around the globe. With the developments in the ICTs, and reliance on Broadband infrastructure, in particular, the Internet has taken center in today's modern world. The world is now increasingly interconnected and people have unprecedented access to information and knowledge.

To harness the benefits of ICT technologies and the Fourth Industrial Revolution (4IR), Pakistan has also adopted the path of Digital Transformation.

The increased use of information and communication technologies enhanced global connectivity, mobility, and versatility of digital services exposes information assets to a host of new and evolving Cyber Security threats. The Fourth Industrial Revolution has made these assets highly valuable. However, with the organic growth and proliferation of the Internet, some worrisome trends in the use of cyberspace have also emerged. The concerns over safety and security potentially impede the objective of accelerated development and affect the confidence of people in using applications and services offered to traverse cyberspace.

The rise in incidents related to malicious use of ICTs in cyberspace is affecting the integrity and the civil rights protections guaranteed by the state, level-playing field, transparency, and the socio-economic equilibrium by posing security and financial risks to the whole spectrum of users including Individuals, Businesses, Sectors, and States and could potentially impose serious barriers to achieving development goals in various economic sectors.

1.2 REVIEW OF PAKISTAN'S CYBER SECURITY LANDSCAPE

In order to ensure the online safety of the citizens of Pakistan and to ensure the security of the digital systems, various initiatives are already in place by different federal & provincial bodies and sectoral regulators under the enactments such as the Electronic Transaction Ordinance, 2002 (covering only electronic financial transactions and records), Investigation for Fair Trial Act (IFTA) – 2013, Pakistan Telecommunication (Re-Organization) Act - 1996 and Prevention of Electronic Crime Act (PECA) 2016 which cover some but not all aspects of information and Cyber Security. In addition, the State Bank of Pakistan (SBP) issues guidelines on Cyber Security for the financial sector, and the PTA has notified the Telecom Computer Emergency Response Team (CERT). However, the inter-departmental coordination and holistic approach to address the Cyber Security challenges and their emerging trends requires a special focus on a national level.

With regards to setups responsible for Cyber Security in the country, only the selective Cyber Security Incident Response Teams (CSIRTs) are operational at the organizational level in the public, private, and defense sectors. However, there is a need to enhance existing legislative and institutional frameworks, and strengthen the principal, organization, mandated for national Cyber Security. The legal framework, structures, and processes related to Cyber Security need to be constantly monitored, assessed, and improved.

To undertake academic research, National Center for Cyber Security was established in 2018. The HEC has also formulated new academic degrees that include BS, MS, and Ph.D. Cyber Security and MS Systems Security programs. However, the demand and supply gap for digital skills in general and Cyber Security, in particular, is ever-increasing, which underscores the importance of upskilling the existing resources.

In the absence of an indigenous national ICT and Cyber Security industry, Pakistan relies heavily on imported hardware, software, and services. This reliance, inadequate national security standards, and weak accreditation

has made computer systems in Pakistan vulnerable to outsider cyberattacks and data breaches through embedded malwares, backdoors, and chipsets.

1.3 CHALLENGES AND RISKS

Since data treated as an economic asset, it faces threats and risks like any other asset. To mitigate IT security vulnerabilities, a comprehensive Cyber Security policy is a baseline mechanism to address the following risks and challenges globally. The most important of these are as follows.

1.3.1 Ownership at the Top

Information is one of the fundamental pillars of knowledge-based economies. Hence, information being a National asset, its management, governance, and regulation must be synchronized at the National level using all available resources, to secure this time-sensitive valuable asset. Cyber Security requires administrative support due to its sensitive nature, challenging domain, and cross-sectoral application.

1.3.2 Governance and Implementation challenges of Cyber Security Policy and Strategy

In the absence of a centralized policy and strategy for Cyber Security, attempts at securing the digital assets of the country are liable to be random and uncoordinated.

i. WEAK ENFORCEMENT OF STATUTES

The existing legislation related to Cyber Security does not provide effective legal protection of Pakistan's digital assets. The existing legislation related to Cyber Security is not sufficient to provide an adequate mechanism and there is a dire need to transform it in such a manner that it should keep the interest of the nation in letter and spirit without fail. For that matter, an appropriate ***legislative*** structure could help to ***comply against a centralized and robust compliance framework***.

ii. ASSESSMENT AND CONTINUAL IMPROVEMENT

The legal framework, structures, and processes related to Cyber Security require monitoring, assessment, and improvement on a continuous basis or they will lose their viability and become a threat themselves. The implementation with regards to the compliance framework of Cyber Security policy needs to be constantly monitored, assessed, and improved.

For that matter, a holistic approach and appropriate legal and technical structures could help to identify the potential threats and consequences attached thereto, and properly it could investigate and no weak area be left to be exploited by the wrongdoers.

1.3.3 Enforcement of Required Structures and Processes

The assurance of Cyber Security requires proper structures and processes for governance, regulation, implementation, and enforcement. Any absence or weakness of the regulation structures poses a threat to Cyber Security.

i. Inadequate and Poor Quality of Resources

Cyber Security is a rapidly growing field that requires a continually updated set of relevant skills and resources as the inadequacy of the required skills shall lead to weaknesses in Cyber Security. Moreover, bridging the demand and supply gap in the digital workforce is an emerging challenge. The absence of a mechanism for ensuring the quantity and quality of these skills and resources is a threat to the Cyber Security of the country.

ii. Lack of Data Governance

Countries face the threat of data colonization whereby data is managed, controlled, and processed out of the legal jurisdiction of the country and there is limited or no bilateral agreement among the stakeholders in this regard. Threat actors are liable to pollute the information domain and citizen data may be sold to third parties without due consent or validation. Such proliferation and abuse of data lead to the exploitation of selected segments of society.

Weak governance of data, poor data quality, and absence of data stewardship generate unreliable information resources and poses a threat to Cyber Security.

ii. Reliance on External Resources

With the increasing use of information technology in all domains including operations technology, critical information assets are likely to be exposed to cyber-attacks. In absence of adequate local resources, reliance on external resources including skills, hardware, and software, is a direct threat to Cyber Security.

iv. Challenges of Coordinated Response to Threats and Attacks

An effective response to risks, threats, and attacks requires a coordinated effort through a series of response teams (CERTs). The absence of such teams and lack of coordination between them is a major threat. This is majorly due to the weak Cyber Security posture and functions within the affiliate organizations. Empowering support organizations is vital to a successful Cyber Security ecosystem.

1.4 COURSE OF ACTION

This Policy will serve as the foundation for the construction of a holistic digital ecosystem with supporting frameworks and components for the delivery of secure, reliable, and standardized digital services, applications, and digital infrastructure. This Policy will drive the fundamental demand in the local IT industry to ensure quality delivery of its products and services. This will provide an opportunity for local & international entrepreneurs and firms to offer core competencies, services, and solutions and offer an opportunity to local industry to become better positioned to compete and prosper on the international stage. The focus will also be on promoting online businesses enabling the smooth running of digital payments within and outside Pakistan.

Moreover, to mitigate cyber threats, the country faces today and to improve the national Cyber Security outlook, it is imperative to undertake the strengthening of national Cyber Security capabilities through the development of essential and well-coordinated mechanisms, implementation of security standards and regulations under a policy and legislative framework.

In this regard, the Government of Pakistan constituted Cyber Governance Policy Committee (CGPC). Noting the strategic importance of

Cyber Security, the present Government has prioritized the formulation of the first National Cyber Security Policy – 2021. This initiative is in conformity with the national cyber vision.

2 Vision, Scope & Objectives

2.1 VISION

The vision is for Pakistan to have a secure, robust, and continually improving nationwide secure digital ecosystem ensuring accountable confidentiality, integrity, and availability of digital assets leading to socio-economic development and national security.

2.2 SCOPE

This policy framework is envisaged to secure the entire cyberspace of Pakistan including all digital assets of Pakistan, data processed, managed, stored, transmitted or any other activity carried out in public and private sectors, and the information and communication systems used by the citizens of Pakistan.

2.3 OBJECTIVES

- To establish **governance and institutional framework** for a secure cyber ecosystem.
- To enhance the security of **national information systems** and infrastructure.
- To create a **protection and information sharing mechanism** at all tiers capable to monitor, detect, protect and respond against threats to national ICT/ CII infrastructures.
- To protect National Critical Information Infrastructure by mandating **national security standards and processes** related to the design, acquisition, development, use, and operation of information systems.
- To create an **information assurance framework** of **audits and compliance** for all entities in both public and private sectors.

- To ensure the **integrity of ICT products**, systems, and services by establishing a mechanism of **testing, screening, forensics, and accreditation**.
- To protect the **online privacy of the citizens** by provisioning the required support and system to all the concerned institutions and organizations that are dealing with citizens' data-related matters be more equipped and able to render their services, accordingly.
- To develop **public-private partnerships** and collaborative mechanisms through technical and operational cooperation.
- To create a country-wide culture of **Cyber Security awareness** through mass communication and education programs.
- To train **skilled Cyber Security professionals** through capacity building, skill development, and training programs.
- To encourage and support **indigenization and development** of Cyber Security solutions through **R&D Programs** involving both public and private sectors.
- To provide a framework on **national-global cooperation and collaborations** on Cyber Security.
- To identify and process **legislative and regulatory actions** under the mandates of relevant stakeholders assigned in the policy.
- Risks related to Cyber Security need to be managed continuously. Encourage adoption of a **risk-based approach** to Cyber Security through frameworks including those for regulation, assurance, threat management, and incident management.

2.4 PRINCIPLES

Guiding principles to achieve policy objectives are: -

- All actions will be driven to protect online data privacy and security of citizens and enhance national and public prosperity in the digital domain.

- Respective public and private organizations responsible to ensure the Cyber Security of their data, services, ICT products, and systems will be supported to deliver the same.
- In case of any incident, the government will lead the national response with support from both the public and private sectors.
- Will regard a cyber-attack on Pakistan CI/ CII as an act of aggression against national sovereignty and will defend itself with appropriate response measures.
- Will act per national and international Cyber Security frameworks, standards and best practices and expect reciprocal respect of our national digital sovereignty.

3 Policy Deliverables

3.1 CYBER SECURITY GOVERNANCE

3.1.1 POLICY FORMULATION AND OVERSIGHT: CYBER GOVERNANCE POLICY COMMITTEE (CGPC)

A Cyber Governance Policy Committee (CGPC) has been constituted to assert national level ownership to policy initiatives related to cyber-governance and security. Cyber Governance Policy Committee is responsible for strategic oversight over national Cyber Security issues.

- **Core Functions:**
  - Formulate, guide, and recommend for the approval of the **National Cyber Security Policy** and **Cyber Security Act**.
  - Assist in addressing requirements of organizational structures, technical, procedural, and legal measures to support the policy mandate and implementation mechanisms.
  - Harmonize the working and operational reporting mechanism of all departments dealing with the subject.
  - Carry out consultations on aspects related to cyber governance on a regular and permanent basis.

- Assign roles to national institutions for international representation and collaboration with global and regional bodies and organizations.
- Guide to align policy with emerging cyberspace requirements through updates and periodic reviews.

- The policy recommendations of CGPC will be approved/endorsed by the Federal Cabinet.

3.1.2 INSTITUTIONAL STRUCTURE FOR IMPLEMENTATION

To achieve the objectives, an implementation framework shall be developed by a designated organization of the Federal Government, dealing with the subject of Cyber Security. This organization shall also act as the Central Entity at the federal level for coordination and implementing all Cyber Security related matters **on the below levels:**

i. **National Level**: The Central Entity along with its National Computer Emergency Response Team (nCERT) and National Security Operation Center (nSOC).
ii. **Sectoral Level**: Sectoral Regulator(s)/ CERTs (including but not limited to Defense, Telecom, Banking and finance, Power, Federal, and Provincial public sector).
iii. **Organizational Level**: Enterprises, entities, and individual users.

3.2 ACTIVE DEFENCE

The relevant stakeholders will also undertake specific actions which including but not limited to the following:

- Working with **Internet Service Providers (ISPs) and Telecom operators to block malware attacks**, by restricting access to specific domains or websites that are known sources of malware (known as Domain Name System (DNS) blocking / filtering, etc.). Active defense strategies will be formulated with the engagement of respective stakeholders.
- Preventing **email phishing and spoofing activity** on public networks.
- Promoting **security best practice** through Internet governance organizations; such as **Internet Corporation for Assigned Names and**

Numbers (ICANN), Asia Pacific Network Information Center (APNIC), the Internet Engineering Task Force (IETF), European Regional Internet Registry (RIPE), and UN Internet Governance Forum (IGF), etc.

- Work with **international law enforcement channels** to protect Pakistan citizens from cyber-attacks from unprotected infrastructure overseas.
- Work towards **implementation of controls** to secure the **routing of Internet traffic for government departments** to avoid illegitimately re-routed by malicious actors.
- Investing in capabilities enhancement programs of Law Enforcement Agencies (LEAs) and concerned Ministries/Divisions to enable them to respond against state-sponsored and criminal cyber activities targeting Pakistan networks and systems.

3.3 PROTECTING INTERNET-BASED SERVICES

The relevant stakeholders will initiate actions, including but not limited to:

- Develop an **Internet Protocol (IP) reputation service** to protect government digital services (this would allow online services to get information about an IP address connecting to them, helping the service get more informed on risk management decisions in real-time).
- Seek to install **products on government networks** to ensure that software is running correctly and not being maliciously interfered with.
- Look to **expand beyond the gov. pk domain** into other digital services measures that notify users who are running outdated technologies.
- Sharing of confidential information between public and private organizations, **safeguarding online data privacy of citizens, and ensuring complete data protection.**
- Strive for **protecting digital systems and services** attached thereto.

3.4 PROTECTION AND RESILIENCE OF NATIONAL CRITICAL INFORMATION INFRASTRUCTURE

To achieve this critical objective, the stakeholders will;

- **Operate requisite technical platforms** to protect National Critical Information Infrastructure, information and communication technologies (ICT), Next Generation(s) Mobile Service and Networks, and IoT security and work as a modal organization in the country. Encourage a culture of "accountability" and "self-governance" such that respective public and private organizations will be responsible to safeguard their digital assets, data, products, and services to improve their confidentiality, integrity, and availability.
- **Institute processes** for identification, prioritization, assessment, and protection of Critical Information Infrastructure.
- Ensure a secure **ICT environment including mobile systems and cloud-based solutions** through state-of-the-art security measures.
- Mandate implementation of **national security standards** by all critical sector entities, to reduce the risk of disruption.
- **Develop a mechanism for the protection of Critical Information Infrastructure** and its integration at the entity level through relevant sectoral CERTs.
- Establish and **enforce Cyber Security risk management methodologies** according to any of the prevalent international standards inter alia ISO/IEC 27005:2008 and ISACA RISK IT etc.
- Mandate all **operators of national, provincial, and organizational** Critical Information Infrastructure to **hire qualified Cyber Security individuals** and add an appointment of **Chief Information Security Officer (CISO)**.
- **Enforce the use of digital certifications and its accreditation including accreditation of national security standards** in developed, developing, and deployed information and communications networks or systems in public and private sectors.

3.5 PROTECTION OF GOVERNMENT'S INFORMATION SYSTEMS AND INFRASTRUCTURE

To cater to a specific need of public sector information infrastructure, the stakeholders will:

- access to all government systems with the mandated and desired access control technology
- Encourage the establishment of national Data Centers to co-locate servers and telecom Quality infrastructure for all government entities - federal & provincial.
- Define and enforce a **robust Government Authentication** and **Data Protection Framework** including data classification and to ensure that appropriate controls exist to protect data.
- Create **vulnerability management and patch management program** for all government technical systems.
- Work with relevant government entities to ensure **mandatory allocation of a certain percentage of the ICT project budget** for Cyber Security Assurance.
- Formulate a mechanism for the creation and enforcement of **staff vetting and clearance schemes** across the government.
- Improve **security in government and critical infrastructure outsourcing and procurement** through vetting and assurance of suppliers and enforcement of security clauses in contracts. Enforce **periodic security & risk assessments** of critical suppliers.

3.6 INFORMATION SECURITY ASSURANCE FRAMEWORK

For the attainment of this objective the stakeholders will:

- Implement the concept of "**Cyber Security by Design**" in ICT products and services through screening and accreditation of national security standards.
- Upgrade and establish next-generation **national Cyber Security forensic and screening setups** to safeguard against advanced cyber threats in Artificial Intelligence (AI) driven environment.
- To create an information assurance framework for **Cyber Security audit and compliance** requirements for all entities in both public and private sectors.

- Create infrastructure and/or leverage existing facilities/ platforms/ resources for conformity assessment and certification of compliance to Cyber Security best practices, standards, and guidelines (e.g., ISO 27001 ISMS certification, PCI/PA DSS for FIs, or other industry standards and benchmarks, internal security system audits, Penetration testing / vulnerability assessment, application security testing, web security testing, business continuity planning test, etc.).
- Develop and mandate organizations for the **establishment of testing, screening, forensics, and accreditation facilities** in line with laid national and international best standards in order to gain from evolving best practices and standards.

3.7 PUBLIC-PRIVATE PARTNERSHIP

The stakeholders will develop a framework to: -

- Nurture an environment for entrepreneurship based on cooperation among government, industry, academia, and research institutions in different areas e.g. supply chain risk management, etc.
- Provide governmental support to start-ups and facilitate them to grow into competitive companies.
- Enable privately-owned Cyber Security groups/ organizations to collaborate with government bodies and regulate their actions.
- Facilitate the exchange of information on the development of new legislation and regulation between stakeholders.
- Any other framework as deemed appropriate by the Federal Government.

3.8 CYBER SECURITY RESEARCH AND DEVELOPMENT

Considering the importance of indigenous security product design, development, and manufacture; the stakeholders will develop and implement a framework involving all segments in public and private sectors to:

- Undertake Research & Development programs aimed at short-term, medium-term, and long-term goals.

- Research & Development programs shall address all aspects including the development of Cyber Security systems, testing, deployment, and maintenance throughout the life cycle.
- Encourage Research & Development to produce cost-effective, tailor-made indigenous security solutions meeting a wider range of Cyber Security challenges.
- Facilitate commercialization of the outputs of Research & Development into commercial products and services for use in public and private sectors.
- Set up Centers of Excellence in areas of strategic importance for the security of cyberspace.
- Mandate all local entities at the appropriate time (depending on the growth of indigenous capabilities) to gradually shift on indigenous products.

3.9 CAPACITY BUILDING

With the ever-growing need for enhanced Cyber Security measures, there is an equal demand for producing well-trained human resources. Therefore, the stakeholders will:

- Establish **Centers of Excellence** to educate and train human resources in Cyber Security domains to strengthen and uplift the human support base.
- Formulate and implement customized **human resource development programs** to fulfil the Cyber Security needs of both public and private sectors.
- Increase Cyber Security **research and development (R&D) budget** for the development of indigenous Cyber Security solutions to minimize dependency on foreign technologies.
- Establish a **special court** to adjudicate the matters related to Cyber Security and related proceedings.

- Include **cybercrime-related curriculum in the graduate and post-graduate Engineering and Law related degrees**, training of prosecutors, lawyers and judges, etc.

3.10 AWARENESS FOR NATIONAL CULTURE OF CYBER SECURITY

Mass awareness effort is of paramount importance to create knowledge on relevant risks, preventive measures, and effective responses to cyber threats in all public and private entities. Both top-down and bottom-up approach is essential to create a cyber-aware culture. The stakeholders will:

- Plan and implement **education programs on cyber-ethics and security** programs customized for specific sectors of society, such as students, government officials, law enforcement agencies, and private organizations employees.
- Encourage the **corporate sector to protect cyberspace** by maintaining the desired level of Cyber Security in their products and services.
- Preparation and execution of **national awareness program** to educate end-users at home or workplace.
- Implementation of a **Cyber Security awareness program for government** systems.
- Add Cyber Security awareness to the **national education curriculum** at the middle and secondary levels.

3.11 GLOBAL COOPERATION AND COLLABORATIONS

The Ministry of IT & Telecom and the Central Entity will play a key role in recommending the country's viewpoint for the international forum and will make recommendations for joining international collaborations. Representation at the national and international events on information and Cyber Security shall include the Ministry of IT & Telecom, Ministry of Foreign Affairs, Ministry of Law & Justice, Ministry of Interior, and other stakeholders including the Central Entity as per requirement. The Ministry of IT & Telecom, in consultation with the Central Entity, will:

- Work with all international partners such as ITU-IMPACT etc.

- Maintain continuous presence and provide professional input from Pakistan to all major global and regional organizations and professional bodies related to the subject including ICANN, GAC, ITU, APT, and other such UN and non-UN agencies.
- Affiliation of all national, regional, and international bodies to establish desired coordination and cooperation to establish cyber situational awareness.
- Develop a mechanism for trusted information exchange about cyber-attacks, threats, and vulnerabilities with the public, inter-governmental and non-governmental bodies locally and globally.

3.12 CYBERCRIME RESPONSE MECHANISM

The stakeholders will:

- Assist and enhance government capacity by augmenting law enforcement agencies' technical capability to respond to cybercrimes.
- Establish liaison and coordination with other national and international cybercrime agencies for sharing of information and cooperation.
- Strengthen the processes and procedures and embed Cyber Security in the public and private service networks vulnerable to cybercrimes.

3.13 REGULATIONS

In order to achieve defined objectives and effectively implement National Cyber Security Policy, it is imperative to introduce appropriate objective-based legal frameworks for cyber governance. These will be formulated after consultation with stakeholders and will include, but not limited to the following:

- Formulation of National Cyber Security Plan and Cyber Security related Law(s).
- Rules and regulations for national Cyber Security framework.
- National Cyber Security /Governance Operations and information sharing mechanism, for incident handling, management capability, and cyber situational awareness.

- Compliance, screening, accreditation, and risk management regulations: for Critical Information Infrastructure, public-private partnerships, capacity building, Cyber Security awareness, R&D programs, and global cooperation.
- Standardization of Digital and Network Forensics processes and Infrastructure for Cyber Governance in harmonization with this policy and PECA 2016/ any other relevant law.
- Compliance for auditing and ensuring the national Cyber Security standards across Pakistan.
- Prioritizing initiatives to address growing dimensions of the cybercrimes by empowering the legal entities and rectifying the shortcomings under PECA 2016.

3.14 ESTABLISHING TRUST IN DIGITAL TRANSACTIONS

In order to build and maintain the trust of users in the security and integrity of digital services. This will cover the below-mentioned areas:

- Enforce Digital Certifications for the authenticity of individuals and businesses including enhancing technology for enabling digital signature / electronic transactions.
- Encourage work on scalable Public Key Infrastructure (PKI) as per future business requirements (e-passport, e-voting, e-filing, e-procurement, e-governance, etc.).
- Encourage multiple Certification Service Providers and enabling the security and trust of digital services such as E-commerce, Fin-tech, and other government to citizen services.

3.15 IMPROVE PAKISTAN'S ICT RANKING

The objective of improving Pakistan's ICT ranking based on international indices and benchmarks will be achieved by focusing on the below areas:

- Map the existing position of Pakistan in the international market with regards to ICT keeping in view the business and innovation environment, infrastructure, affordability, skills readiness, and socioeconomic impact.

- Support the measures to improve the provision of data to the international rating agencies.

3.16 RISK MANAGEMENT AND RISK-BASED APPROACH

The management of incidents and problems will require risk management because of resource limitations. The objective of risk management and adoption of a risk-based approach will be achieved by requiring and encouraging organizations to define the risk criteria, risk appetites, and risk tolerances for themselves as part of their enterprise risk management activity. In addition to that, risk mitigation plans will be required to be maintained by all bodies and organizations themselves.

The notable Cyber Security risks/challenges could be the Internet of Things, Ransomware, AI (Artificial Intelligence), Serverless Apps, Critical National Infrastructure, Sophisticated Phishing Campaigns, Strategic Use of Information Operations, Cloud Computing, Cyber Security awareness, Hacker-for-hire services, and Skills shortages, etc.

3.17 APPENDIX – GLOSSARY OF TERMS

- **Critical Sector** - Government systems, utility infrastructure (electricity, gas, and water), education, health, transport system (air, road, rail, and sea), emergency services, manufacturing facilities, banking and financial sector, telecommunication/ ICT sector, dams, etc.
- **Critical Information Infrastructure (CII)** - This generally includes the energy, telecom, finance, water & healthcare sectors.
- **Accountability** - State of being answerable for decisions and activities.
- **Cyber Security** - Preservation of confidentiality, integrity, and availability of information in Cyberspace.
- **Digital Asset** – Systems, applications, services in cyberspace or any other sandbox environment.

4 Interim Measures

The implementation mechanism provided for this policy may require considerable time to be completely functional. Therefore, during this interim

period, the capacities and capabilities which state organizations and institutions currently have and are supportive of the implementation of this policy will be utilized and their continued use will be integrated with an all-encompassing implementation mechanism.

Pakistan Telecommunication Authority as per Telecom Act 1996, Telecommunications Policy 2015, and PECA 2016 will implement Telecom Sector technical platform (sectoral CERT as provided herein) in collaboration with the telecom industry.

To achieve the short term, medium, and long-term objectives sectoral bodies such as banking, telecom, education, and provincial institutions will be empowered to strengthen the national Cyber Security posture. In short term, capacity building of relevant stakeholders around stated policies, standards, and procedures will be prioritized and planned to achieve within the first year of the policy.

5 Policy Review and Implementation

The National Cyber Security Policy 2021 is subject to inclusive review after every three years and as when required, depending on the emerging global cyber trends and technological advancements by the relevant organization in consultation with all stakeholders.