

Cybersecurity



Contents

**Introduction to
Cybersecurity**

**Cybersecurity
Axes**

**Cyberspace and
Cyber Warfare
Threats**

Viruses

Cybercrime

Introduction to Cybersecurity

Cybersecurity is defined as the activity that ensures the protection of human and financial resources associated with information and communication technology. It guarantees the capability to minimize losses and damages resulting from risks and threats, facilitating a swift return to normalcy. This prevents production disruptions and the transformation of damages into permanent losses. In addition, it encompasses the tasks outlined in the report issued by the International Telecommunication Union on "Reform Trends in Telecommunications for the Year 2010-2011." This involves the assembly of means, security policies, procedures, guiding principles, risk management approaches, training, best practices, and techniques that can be utilized to safeguard the cyber environment, assets of institutions, and users.

National Cybersecurity Authority:



The National Cyber Security Authority is defined as: "Protecting networks, information technology systems, operating technology systems, and their components, including hardware, software, services provided, and data contained, from any unauthorized access, disruption, modification, entry, use, or exploitation. This concept also includes information security, electronic security, digital security, and the like."

The authority's [responsibilities](#) can be accessed through its official website.

Risks and Threats:

systems and devices connected to the global information network in our daily lives, such as mobile phones and personal computing devices, the number of individuals connected to cyberspace is growing. This expansion raises the likelihood of attacks and crimes, with incidents ranging from system breaches to data theft and leaks, exemplified by the Sony information systems breach that led to the leakage of millions of user data. The information flowing through and stored in cyberspace is a critical asset sought after by all stakeholders in this space. Companies, governments, and internet users pursue information according to their respective objectives. Cyber threats arise from purposeful actions such as hacking and attacks, as well as aimless actions such as neglect, lack of awareness, and understanding.

التعريف بالأمن السيبراني

Comparison between Information Security and Cybersecurity

Information Security:	Cybersecurity:
Protects information, whether in the form of physical documents or electronic data, safeguarding it from unauthorized access	Focuses on securing information that is transmitted, stored, or processed in communication systems and information technology
Encompasses vast areas such as encryption, storage, physical security, security standards, information and risk management, among other domains	Emphasizes protective and defensive measures for all computer systems and smart networks, placing less emphasis on foundational methods like encryption, and more on utilizing these methods in digital defense
Prioritizes the protection of information with importance equal to the availability of electronic services	Ensures service availability and safety by delivering them through Cyberspace, akin to the delivery of electricity
Data backup	Concerned with data backup and encryption.
Regular system updates to enhance security	Involves regular system updates, protection, awareness initiatives, and combating malicious software.

Information Security is more comprehensive and broader than Cybersecurity.

Cybersecurity Axes



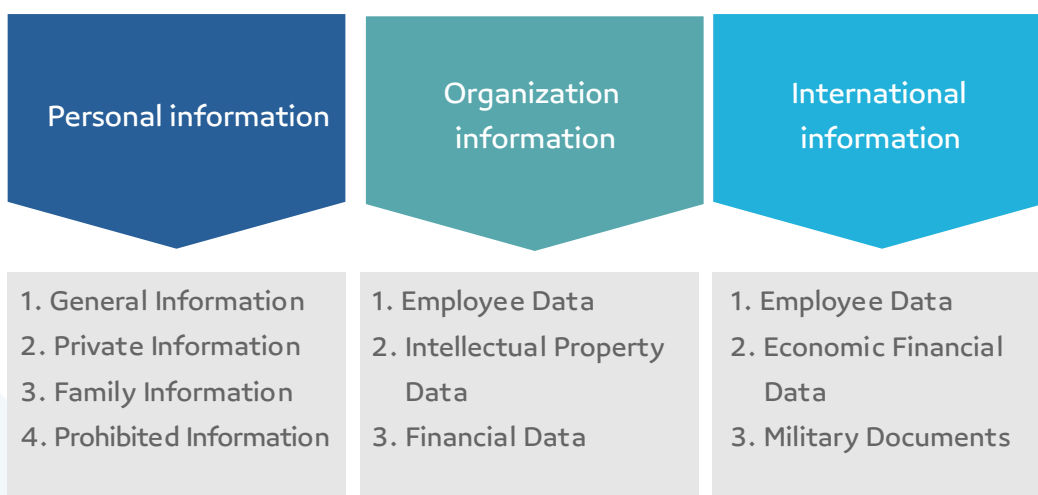
First Axis: Fundamentals of Security

First: Confidentiality

This involves maintaining the privacy of data and preventing disclosure to unauthorized individuals, achieved through:

1. Data and Privacy Protection

Types of Information and Data:



2. Controlling Access to Information:

Verification of user identity before granting access to the system through three factors:

1. Something unique to you, such as fingerprint or eye scan.
2. Something you possess, like an ID card.
3. Something you know, such as a password.

Cybersecurity Axes

Secondly: Integrity

It refers to the accuracy and consistency of data at every stage, including storage, retrieval, and transfer. It ensures that data modification is performed only by authorized individuals.

Data integrity is ensured through several methods:

Verification of integrity by comparing sent and received data to prevent information loss



Third: Data Availability

This implies the necessity of accurate information availability, along with detecting system weaknesses and slowness, working to alleviate system pressure.

Fourth: Personal Identity

It refers to everything indicating a specific person. There are two types of personal identity:


- **Real Identity:** Actual personal information known to people in real life
- **Electronic Identity:** Everything chosen to be shared and published about a person in the Cyberspace

Fifth: Digital Footprint

These are data directly or indirectly indicating a person:


Direct

Information the person publishes about themselves for specific services or on social media.



Indirect:

Data related to a person's online activity, such as purchases, visited websites, and searched topics.



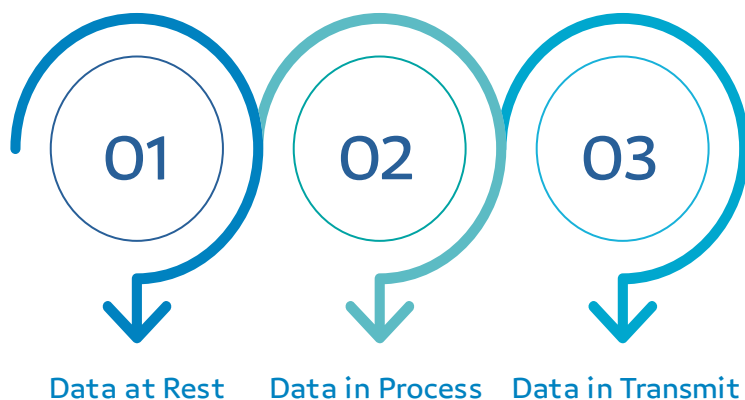
Cybersecurity Axes

Sixth: Cookies

These are tiny text script files stored on a user's device when visiting a website. They facilitate browsing and are non-executable, but are often targeted by hackers to obtain account and password information.

Second Axis: Information States

Data States



Third Axis: Precautionary Measures

- 01 Awareness and knowledge of hacking techniques and cyber warfare
- 02 Regular backup and secure storage
- 03 Continuous software and operating system updates
- 04 Examination of devices and software before use

Viruses

Exposure to viral attacks is considered a form of cyber assault that can lead to the disruption of organizations. Therefore, protection against viruses is crucial.

Definition of Viruses:

A virus is a malicious program programmed by professionals. It disrupts the properties of targeted files, placing them under the control of the programmer. This can involve deleting, sabotaging, or modifying files. The goal of these programs is to sabotage computer systems, and they may also aim to obtain crucial files and data from a user's device.

Computer viruses exhibit several characteristics, including:

- ❖ Automatic replication and spread capability
- ❖ Self-binding to a Host program
- ❖ Inability to spontaneously generate
- ❖ Classification as a computer disease

Components of a computer virus program are classified into four main parts:

Replication	Provides the virus with the ability to clone and spread
Protection	Imparts the ability to remain secretive and not easily detectable
Trigger	Gives the ability to spread before detection, usually within a specific timeframe
Payload	The task assigned to the virus for execution upon activation and spread

Viruses

Viruses move through computers in two main ways:

- **Direct Infection:** The virus invades computer files, and when any of these files are run or used, the virus becomes active, spreading between files on the computer.
- **Infection:** The infected program with the virus is transferred to the computer's memory upon starting the infected file. The computer then executes the original file's commands. After that, the virus infection spreads to any file loaded into memory. This type of spread stops if the power is disconnected or the computer is restarted, like an infected Word file.

Users are usually advised to protect their devices from viruses and prevent them by following these steps:



- 01 Do not download any programs without conducting a thorough scan
- 02 Download antivirus programs, and avoid running files from unknown sources
- 03 Keep backup copies of files and programs
- 04 Rely on Firewall programs
- 05 Install more secure operating systems, such as GNU/Linux

Protecting Your Social Media Accounts:

- [Protecting your Snapchat account.](#)
- [Protecting your WhatsApp account.](#)

المركز الوطني للإرشادي
للأمن السيبراني
S A U D I C E R T



For further information, you can refer to educational materials published on the [Saudi CERT's website.](#)

Cybercrime

There are various definitions for the term cybercrime, reflecting the diverse perspectives of researchers. Some prominent definitions include:

- Unauthorized access to an independent computer or one connected to another through a local network with the intention of committing an act prohibited by law and ethics.
- The use of modern technology, such as computers, for executing suspicious and unethical purposes contrary to societal morals.
- Any unlawful act subject to legal punishment, committed through a computer system, referring to any crime occurring in the information environment.

Types of Cybercrimes

Cybercrimes are classified into four main categories based on:

01

Perpetrator, motives, and execution methods

(e.g., hackers, malicious infiltrators, and professionals).

02

Impact on individuals and property

(e.g., identity theft, defamation, forgery, and theft).

03

Tampering with computer systems, systems, and data

(e.g., data and information tampering, hacking).

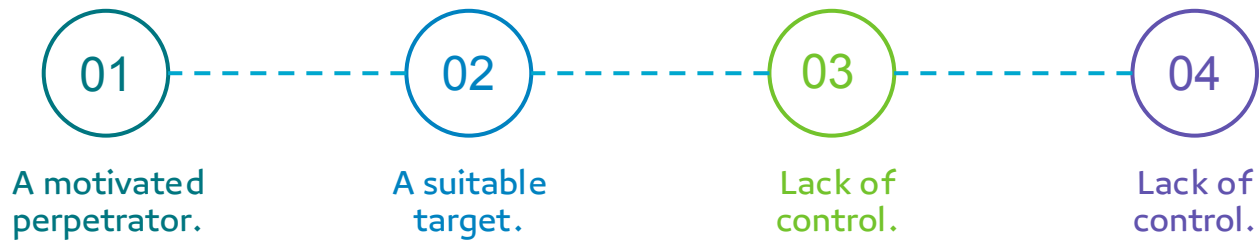
04

Impact on public order and morals

(e.g., cybercrimes related to drug trade, spreading pornography, or privacy piracy).

Cybercrime

Cybercrime occurs when its four elements are verified:



The "Kollona Amn" application allows reporting any crime, such as threats, extortion, or harassment on social media. Users can capture the incident, attach an image to the report, and send it to the Cybercrime Department in the security patrols. The department then handles the crime, applying the law to the perpetrator.



Cybercrime law and regulation in the Kingdom of Saudi Arabia

Recognizing the importance of keeping up with modern technological advancements to achieve individual and societal information security and to mitigate the misuse of information systems, the Kingdom of Saudi Arabia issued Royal Decree No. (M/17) on 8/3/1428 AH, approving the [Cybercrime Prevention Law](#). This law defines cybercrimes, prescribes penalties, and designates jurisdictions.

The law, consisting of 16 articles, includes definitions, the purpose of the law, penalties for cybercrime offenders, and the responsibility of the Communications and Information Technology Commission.

منشآت
monsha'at

الهيئة العامة للمنشآت الصغيرة والمتوسطة
Small & Medium Enterprises General Authority