Cybersecurity Guidelines for cloud computing

Presentation Slides

Trainer's kit

CyberEco

معًا لدعم السلامة الرقمية
Together to support digital safety

الوكالة الوطنية للامن السيبراني
National Cyber Security Agency

Intellectual Property rights

December, 2023

Doha, Qatar

This content is produced by the team of
National Cybersecurity Excellence Management, National Cyber Security Agency.

For inquiries about the initiative or program, you can contact us through the following websites or phone numbers:

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

🌐 https://www.ncsa.gov.qa/
✉ cyberexcellence@ncsa.gov.qa
📱 00974 404 663 78
📱 00974 404 663 62

Time Table for the Lecture

Content	Allocated Time
General introduction	10 minutes
The theoretical aspect	30 minutes
Educational Videos	30 minutes
Short break	20 minutes
Dialogue and discussion with students	30 minutes
Total training time	2 hours

Scientific Content Index

Chapter One:

Chapter Two:

Chapter Three

Chapter One
The Concept of Cloud Computing

Cloud computing

Cloud computing refers to accessing a range of services, including tools and applications such as data storage, servers, databases, networks, and software, over the internet. Instead of storing files on your local hard drive or private drive, you can store documents in a database on the network using the cloud. So long as your electronic devices have an internet connection, you can access the data and software needed to run them.

What is the reason behind the naming of cloud computing?

As for the reason behind naming it 'cloud computing,' it is because the information accessed is remotely stored in the cloud or virtual space. Companies that offer cloud services enable users to store files and applications on remote servers, allowing access to all data over the internet. It is a general term used by professionals in the technology industry to describe these servers and network infrastructure. Users do not need to be in a specific location to access them.

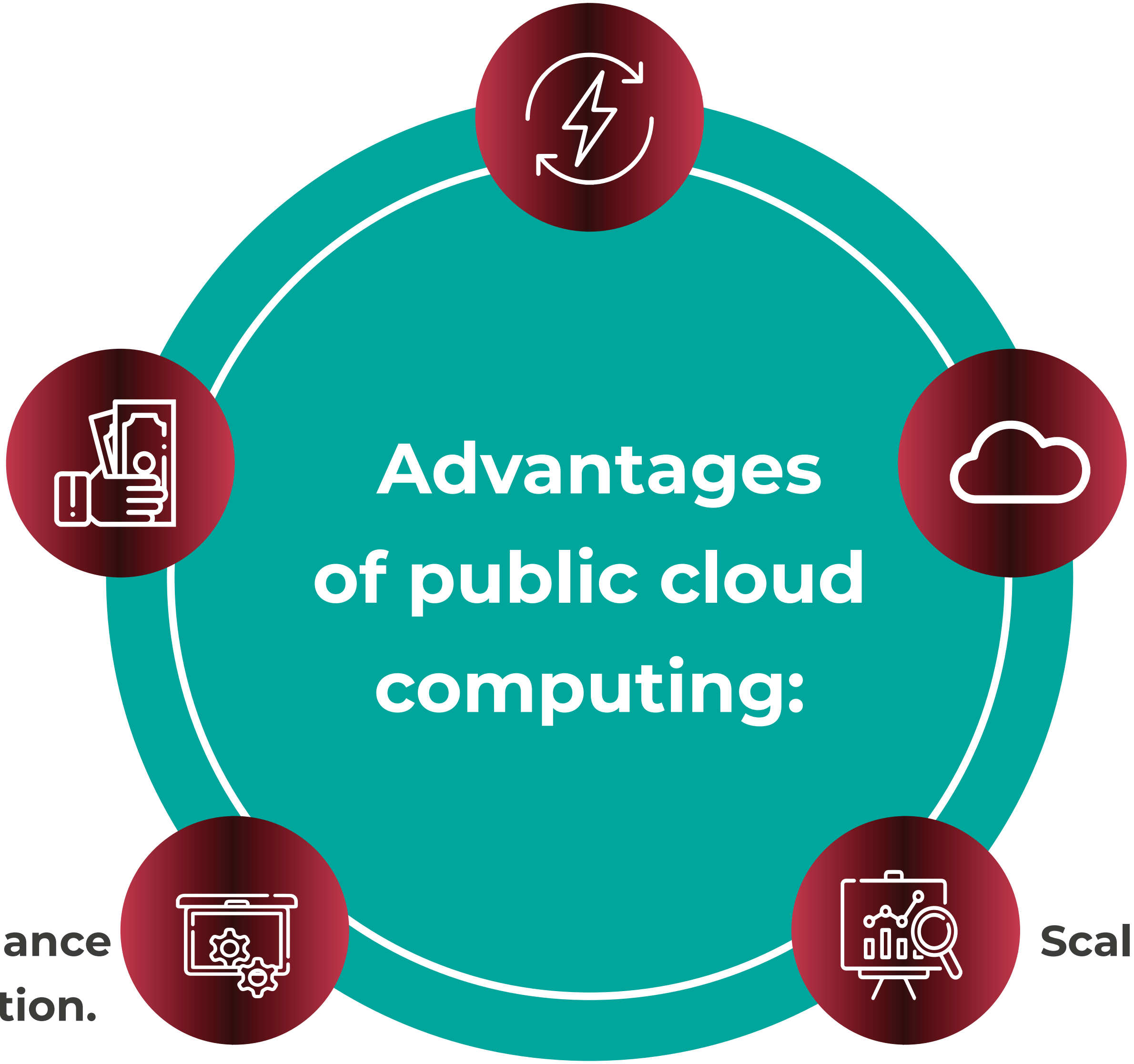
The importance of cloud computing is evident in the following aspects:

1. Cost savings
2. Increase productivity.
3. Speed, efficiency, and security.
4. Cooperation: Cloud computing companies have teams of experts and technicians dedicated to ensuring the security of data on their servers.
5. Developability: Cloud computing is characterised by its flexibility and complete developability according to business needs. Users can expand or reduce their cloud capacity based on their personal and operational requirements.

Types of cloud computing

1- Public cloud

It is open and available to everyone to store and access information online using the pay-as-you-go model.



Advantages of public cloud computing:

Ease of access.

Common infrastructure.

Scalability.

Ease of maintenance and administration.

pay-as-you-go.

Disadvantages of public cloud computing

1. It is less secure because the resources stored are publicly accessible.
2. The effectiveness of cloud computing is directly linked to high-speed internet connection to the cloud provider.
3. The data is not under the user's control.
4. Relying on the cloud service provider.
5. Concerns regarding data privacy and confidentiality.
6. The potential for unforeseen additional expenses to the user with usage-based pricing models.
7. The absence of customisation alternatives and flexibility.

2- Private cloud computing

It is also known as an internal cloud or corporate cloud, and is employed by enterprises to create and manage their private data centres, either in-house or through external service providers.

Types of private cloud computing:

01

Private cloud computing within the enterprise: This entails a private cloud integrated within the infrastructure of the enterprise.

02

Private cloud computing that involves leveraging external resources: This pertains to leveraging external resources, such as collaborating with an external service provider to host and manage the cloud infrastructure on behalf of the enterprise.

Advantages of private cloud computing:

1. It provides enterprises with increased control over their data, applications, and security.
2. It is particularly well-suited for enterprises with stringent compliance requirements or sensitive data.
3. The exclusive leveraging of private cloud computing is allocated for a sole enterprise.
4. It offers greater control and security compared to public cloud alternatives.
5. Empowers enterprises to customise the infrastructure in accordance with their specified requirements.
6. Private cloud computing permits enterprises to increase their resources in accordance with demand and customise them accordingly.
7. Private clouds provide enterprises with greater command over their infrastructure, thus augmenting both performance and reliability.
8. Private clouds may be integrated with public cloud, which enables enterprises to leverage the advantages of both private and public clouds.

Disadvantages of private cloud computing

1. Effective management and operation of cloud services necessitates a proficient workforce.
2. Private clouds can be accessed within the enterprise, thereby constraining the operational area.
3. Private clouds may not be suited for enterprises that lack pre-existing infrastructure and requisite workforce to ensure optimal maintenance and management of the cloud.
4. The elevated primary costs along with incessant maintenance expenditures.
5. Increasing resources can pose a challenge when compared to public or hybrid cloud alternatives.
6. Internal IT personnel are dependent upon to manage, detect, and rectify issues.
7. Restricted accessibility to the latest advancements and innovations rendered by public cloud service providers.
8. The necessity for periodic infrastructure updates.

3- Hybrid cloud:

It is a combination of public and private cloud computing. In this type of clouds, enterprises can leverage the advantages of both public and private clouds to create a flexible and scalable computing environment.

Advantages of Hybrid cloud:

1 Operates by integrating both the public and private clouds, facilitating the utilization of the features of both cloud types.

2 Offers flexibility in resource allocation and scalability.

3 It provides a secure and dedicated environment, while leveraging public cloud resources for non-sensitive tasks.

4 Cost optimisation through the use of cloud for non-critical workloads, while retaining important applications and data on the private cloud.

5 The capability to transfer data and applications between public and private clouds as required.

6 Enables the facilitation of disaster recovery and business continuity by duplicating essential data and applications between the private and public cloud, ensuring redundancy and mitigating the risks of data loss or service interruption.

Disadvantages of hybrid cloud:

1. The security feature is deficient.
2. Managing a hybrid cloud is complicated due to the challenge of running multiple usage models.
3. The reliability of services is dependent on cloud providers.
4. The growing challenges in data integration and the assurance of connectivity between diverse cloud platforms.
5. Increased expenditures result from the necessity to manage and integrate various cloud environments.
6. Increased intricacy in managing data across multiple cloud providers.
7. Dependence on stable, high-band width internet connections for effective hybrid cloud operations.
8. Demands proficient and experienced IT personnel.

4- Community Cloud

It permits access to systems and services provided by consortium of multiple enterprises for the purpose of sharing information within the enterprise and a particular community. It is owned and managed by one or more enterprises within the community, a third party, or a consortium of them. Such as: The healthcare community cloud.

Community Cloud advantages

1. Provides a shared infrastructure that can be accessed by a specific community of enterprises.

2. Provides resources, applications, and services that are customised to meet the needs of the participating enterprises, promoting effective communication and information exchange.

3. It allows for the implementation of robust security controls, access management, and compliance frameworks that meet the organizational requirements of the community and industry standards.

4. Participating enterprises benefit from the sharing of costs.

5. Facilitate communication and information exchange between participants.

6. Enable enterprises to increase or decrease their resources as needed in response to demand.

Disadvantages of Community Cloud

01 Security features are not as good as in a private cloud.

02 Unsuitable if there is no collaboration between participants.

03 The scalability options are limited as shared resources define the capacity of the community cloud.

04 The potential conflict of interests among community members regarding resource allocation and utilization.

05 Transparent governance frameworks and agreements are essential to address potential conflicts and ensure fair resource allocation.

Challenges of Cloud Computing

01 **Security:** Storing data in the cloud makes it more susceptible to hacking and cybercrimes.

02 **Performance challenge,** it is essential to ensure that the cloud is not prone to outages.

03 The necessity of a contingency plan in the event of a power outage.

04 The necessity of being cautious about the unintended buildup of your cloud platform. For instance, if your cloud resources are not well-organized and optimized, storage space for files could accumulate quickly.

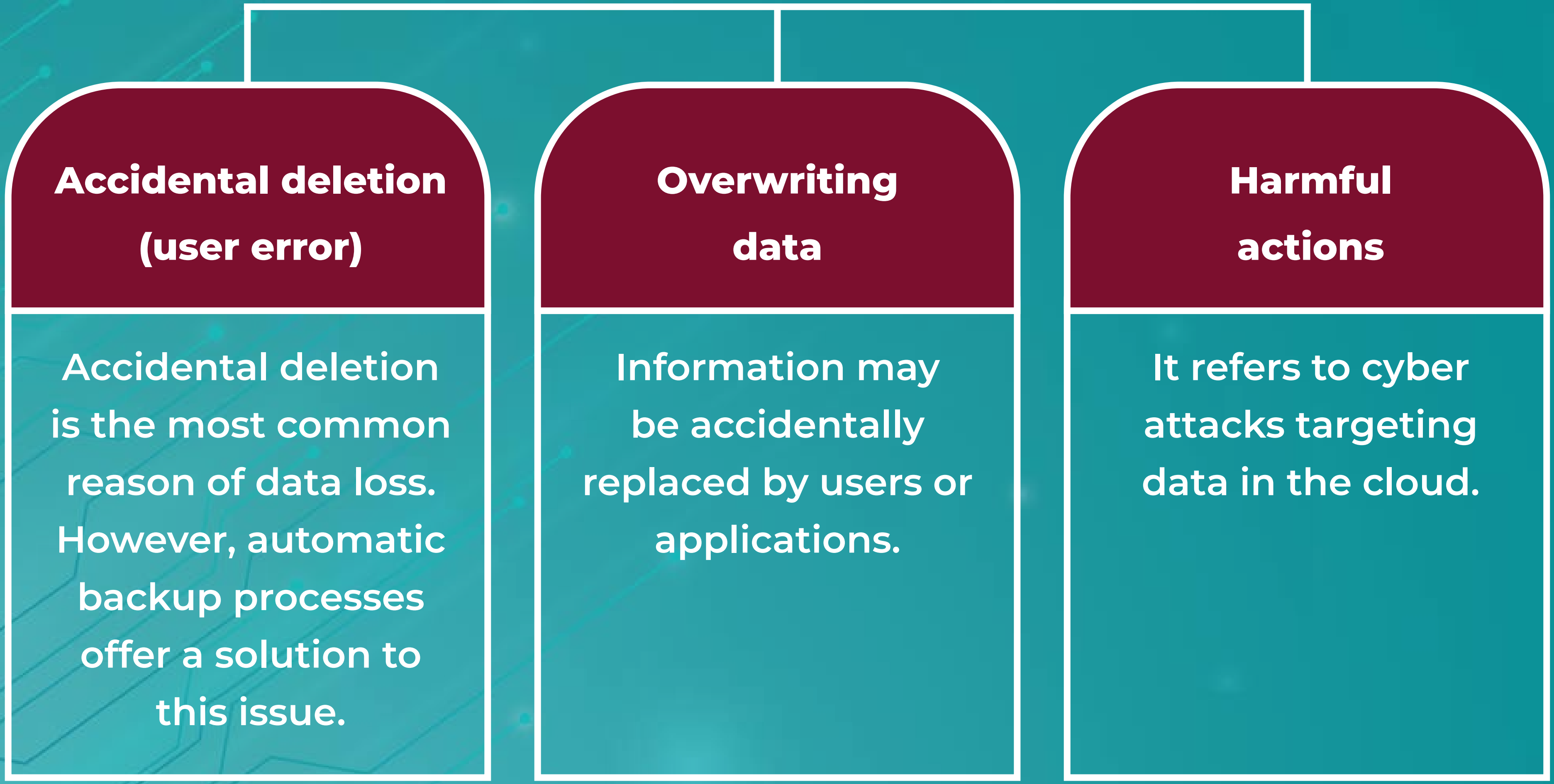
Chapter Two

Digital Threats in Cloud Computing

Data loss

Data loss is regarded as one of the most prevalent security risks in cloud computing, also known as ‘data leakage.’ Data loss is the process in which information is deleted, destroyed, and rendered unreadable by a user, program, or application.

The most common reasons for data loss in the cloud:



Accidental deletion (user error)

Accidental deletion is the most common reason of data loss. However, automatic backup processes offer a solution to this issue.

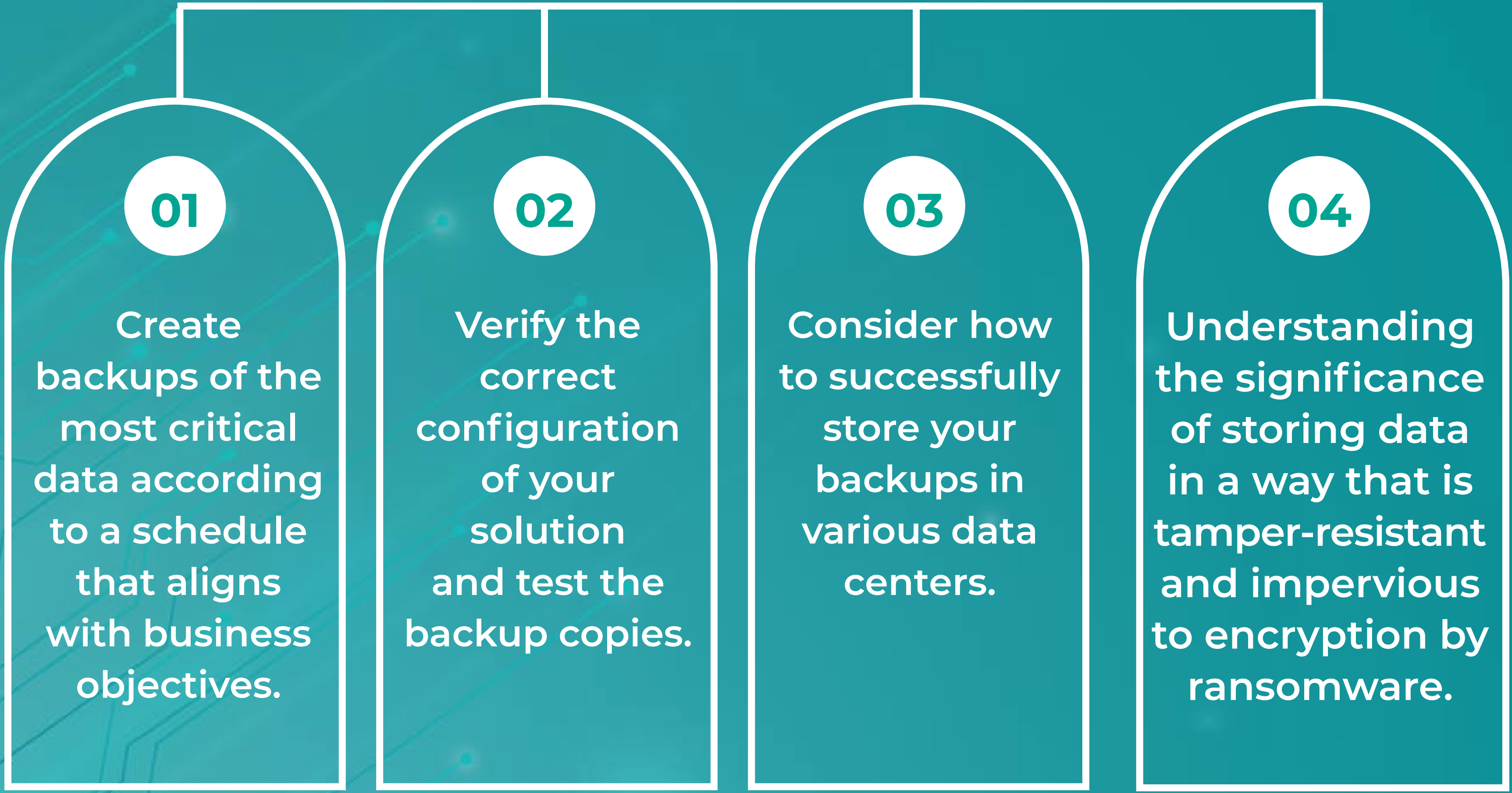
Overwriting data

Information may be accidentally replaced by users or applications.

Harmful actions

It refers to cyber attacks targeting data in the cloud.

How to protect data stored in the cloud from loss



01

Create backups of the most critical data according to a schedule that aligns with business objectives.

02

Verify the correct configuration of your solution and test the backup copies.

03

Consider how to successfully store your backups in various data centers.

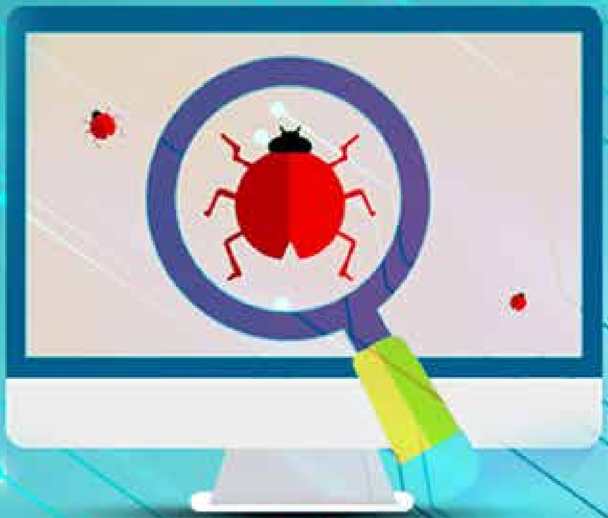
04

Understanding the significance of storing data in a way that is tamper-resistant and impervious to encryption by ransomware.

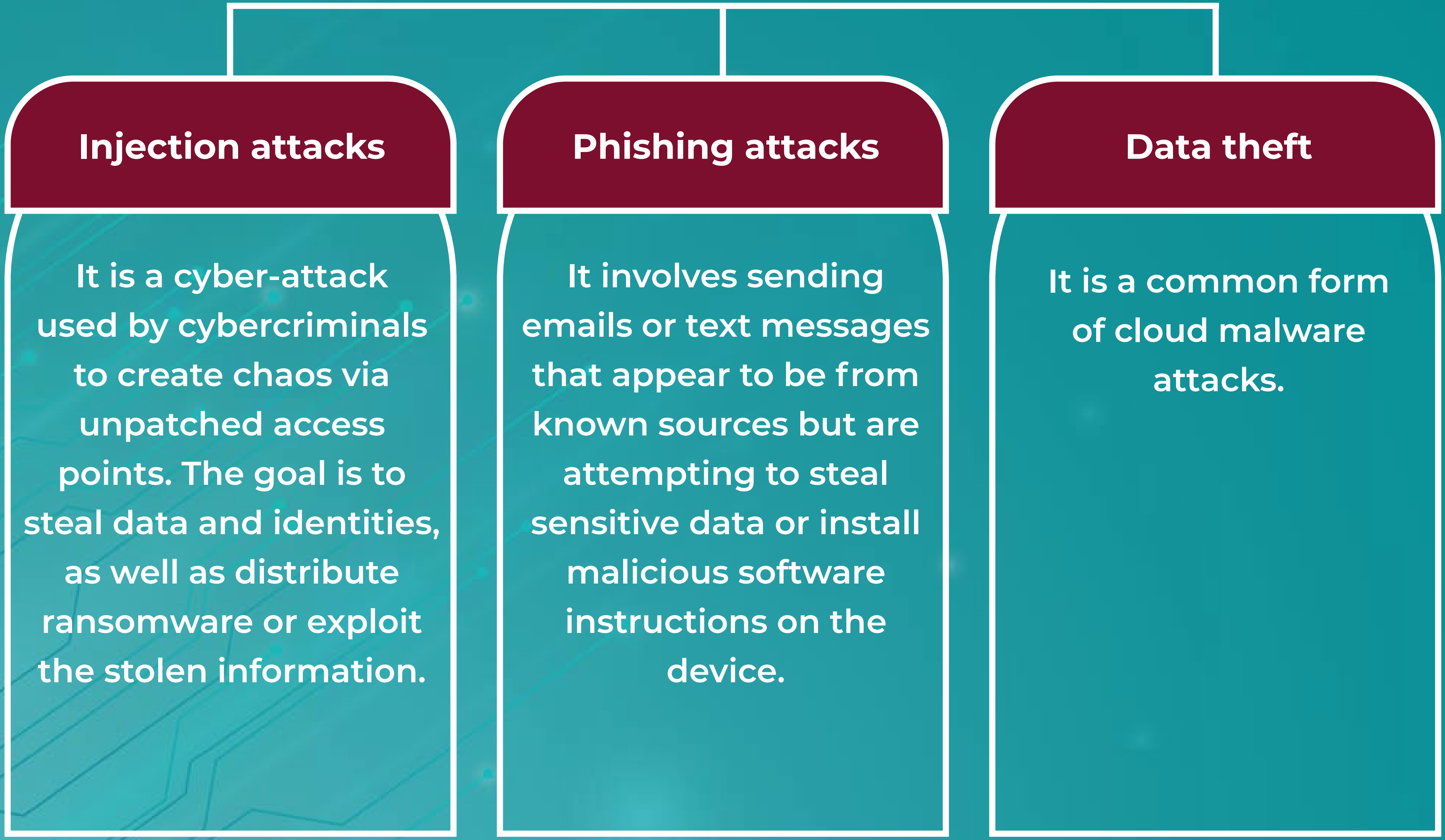
Malware

Cloud malware

It is cloud malware denotes harmful software created and distributed within cloud computing environments, aiming to pilfer data from users and enterprises, disrupt their operations, and induce diverse issues.



Types of cloud malware attacks



Injection attacks

It is a cyber-attack used by cybercriminals to create chaos via unpatched access points. The goal is to steal data and identities, as well as distribute ransomware or exploit the stolen information.

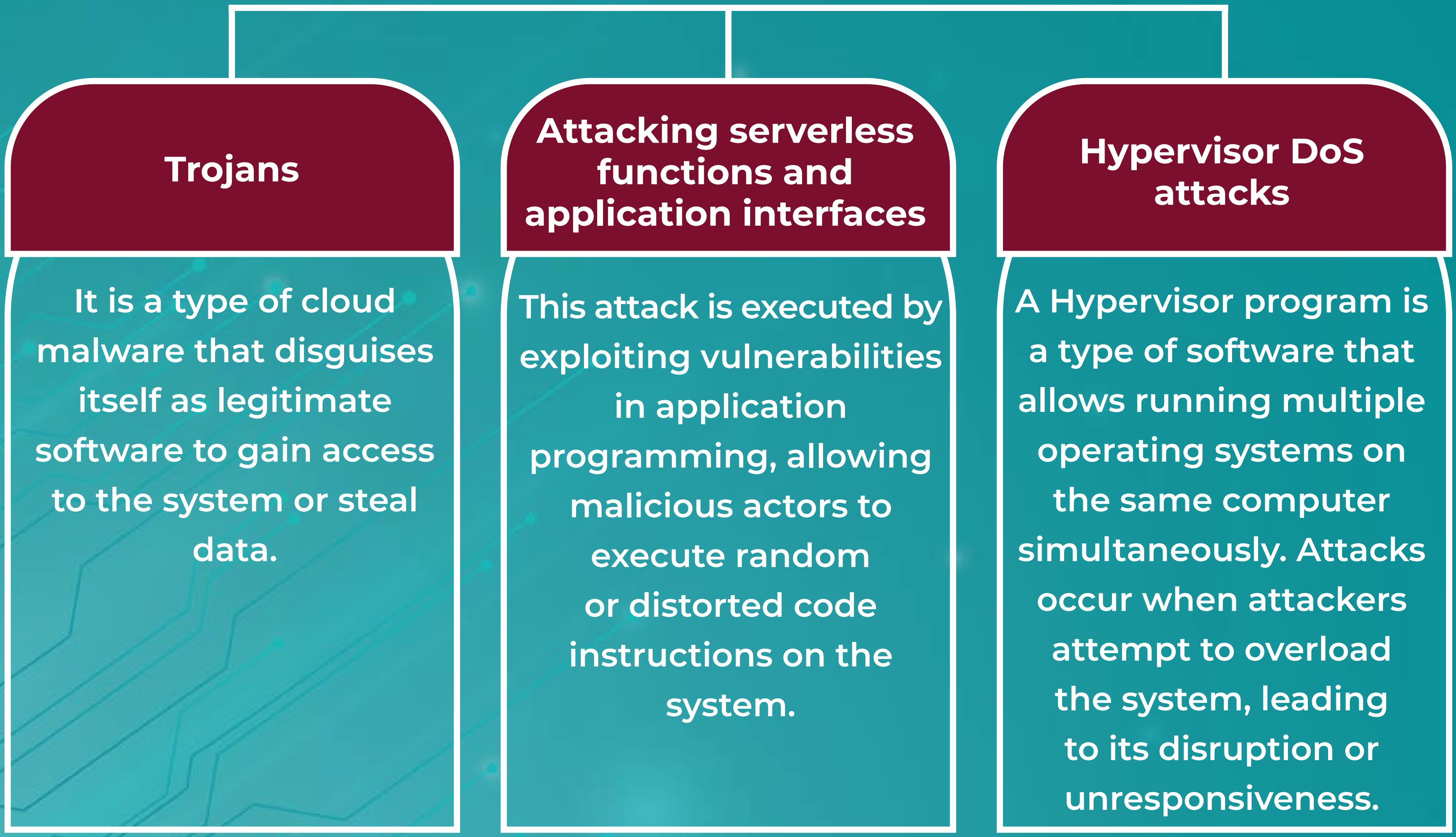
Phishing attacks

It involves sending emails or text messages that appear to be from known sources but are attempting to steal sensitive data or install malicious software instructions on the device.

Data theft

It is a common form of cloud malware attacks.

Types of cloud malware attacks



Trojans

It is a type of cloud malware that disguises itself as legitimate software to gain access to the system or steal data.

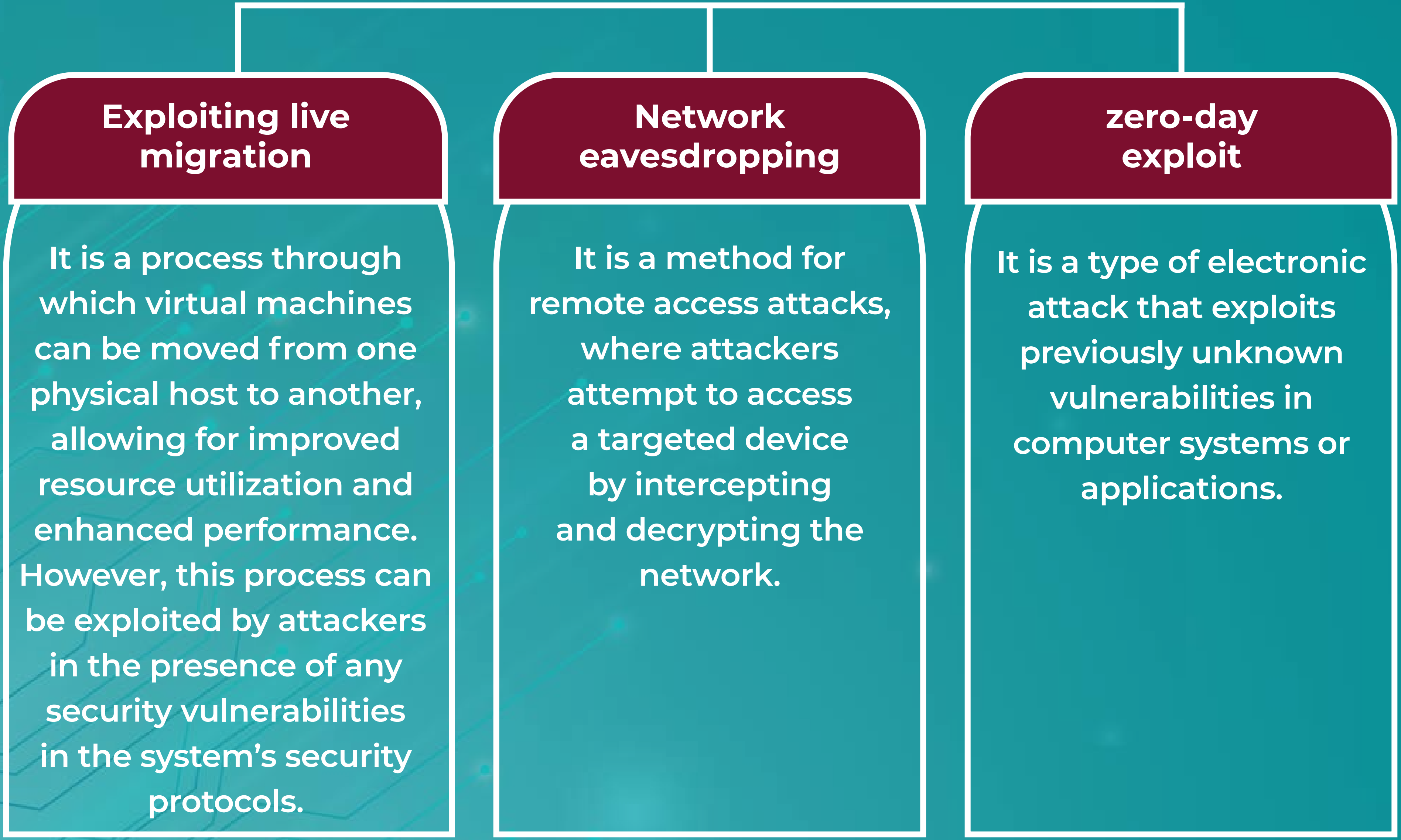
Attacking serverless functions and application interfaces

This attack is executed by exploiting vulnerabilities in application programming, allowing malicious actors to execute random or distorted code instructions on the system.

Hypervisor DoS attacks

A Hypervisor program is a type of software that allows running multiple operating systems on the same computer simultaneously. Attacks occur when attackers attempt to overload the system, leading to its disruption or unresponsiveness.

Types of cloud malware attacks



Exploiting live migration

It is a process through which virtual machines can be moved from one physical host to another, allowing for improved resource utilization and enhanced performance. However, this process can be exploited by attackers in the presence of any security vulnerabilities in the system's security protocols.

Network eavesdropping

It is a method for remote access attacks, where attackers attempt to access a targeted device by intercepting and decrypting the network.

zero-day exploit

It is a type of electronic attack that exploits previously unknown vulnerabilities in computer systems or applications.

Chapter Three

How to Secure Cloud Computing from Digital Attacks

Cloud security

It involves procedures and technologies designed to secure cloud computing environments against both external and internal cybersecurity threats. Security in cloud computing centrally oversees all your applications, devices, and data to guarantee comprehensive security. It streamlines task execution, facilitating the implementation of disaster recovery plans, optimizing network event monitoring, refining web filtering.

DDoS attacks

DDoS attacks pose significant threats to cloud computing, targeting servers with large traffic simultaneously to inflict damage. Cloud security protects servers from these attacks through vigilant monitoring and distribution.

Is the cloud sufficiently secure?

Users are increasingly dependent on cloud storage and processing, but they often feel concerned. However, experience has demonstrated that this concern is baseless.

Cloud service providers implement procedures and technologies to prevent their employees from accessing customer data. In practical terms, cloud service providers are accountable for maintaining the operational environment for users, while users are accountable for events occurring within that environment.

In brief, the cloud can be secure for your content if you have a good understanding of cloud security tools.

Essential elements of cloud security

- **Restricting access,** as it is crucial to ensuring that only the right people are granted access to the right tools at the right time.

- **Securing Data,** because users of cloud computing services need to know the location of their data and establish appropriate controls to secure the data and infrastructure hosting that data.

- **Data recovery,** there must be good backups of the data and a data recovery plan to avoid any damage in the event of a security breach.

- **Response plan,** when exposed to attacks, there must be a plan to mitigate the impact of these attacks.

- Checking for security vulnerabilities at an early stage.

- **Directing the focus of security teams towards eliminating emerging threats** by enhancing cloud resource configurations through software to reduce security issues faced by production environments.

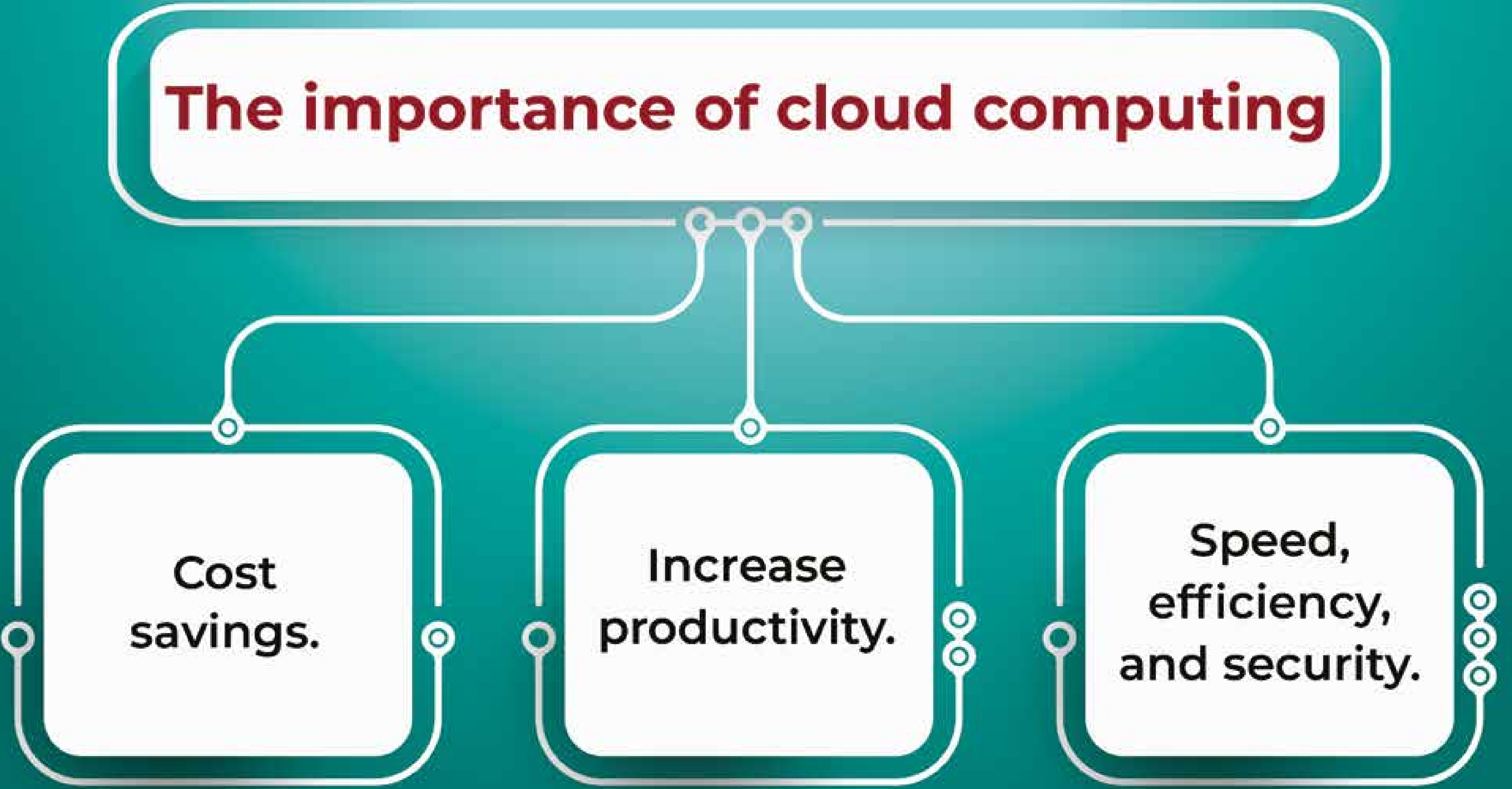
Securing Data in cloud against hacking

- Utilize strong passwords that include letters, numbers, and special characters.
- Secure all the devices you use to access your cloud data, including smartphones and tablets, especially if your data is synchronized across multiple devices.
- Create backup by storing a copy on your home computer.
- Use permissions to prevent any individual or device from accessing all your data.
- Use antivirus and anti-malware software.
- Do not access your data on a public Wi-Fi network.
- Use a Virtual Private Network (VPN) to secure your gateway to the cloud.
- Multi-Factor Authentication (MFA) is an intelligent way to secure your access, whether through fingerprints, a password, or a separate code sent to your mobile device.
- If you no longer use a service or program, close it properly, and make sure not to leave an old account open, as hackers exploit such accounts to find a loophole into your system and devices.

Training cards

Cloud computing

Refers to accessing a range of services, including tools and applications, such as data storage, servers, databases, networks, and software, over the internet. Instead of storing files on your local hard drive or private drive, you can store documents in a database on the network using the cloud.



The importance of cloud computing

Cost savings.

Increase productivity.

Speed, efficiency, and security.

Public cloud computing

It is available to everyone to store and access information online using the pay-as-you-go model. The compute resources are managed and operated by a cloud service provider who takes care of the supporting infrastructure and ensures that resources are available and scalable for users.

Private cloud computing

It is also known as an internal cloud or corporate cloud, and is employed by enterprises to create and manage their private data centres, either in-house or through external service providers.

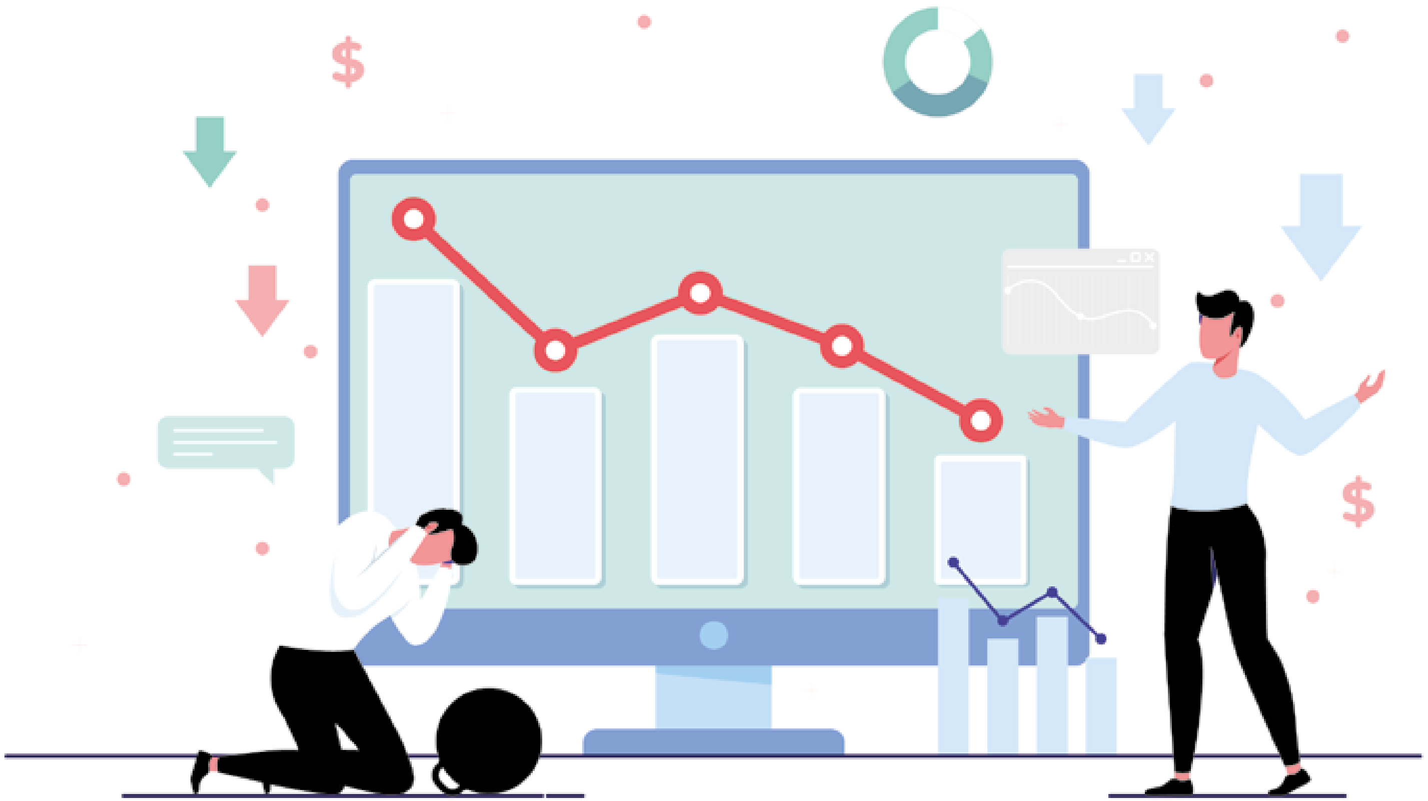
Hybrid cloud:

It is a combination of public and private cloud computing. In this type of clouds, enterprises can leverage the advantages of both public and private clouds to create a flexible and scalable computing environment.

Community Cloud:

It permits access to systems and services provided by consortium of multiple enterprises for the purpose of sharing information within the enterprise and a particular community.

It is owned and managed by one or more enterprises within the community, a third party, or a consortium of them. Such as: The healthcare community cloud.



Data loss

It is regarded as one of the most prevalent security risks in cloud computing, also known as 'data leakage.' Data loss is the process in which information is deleted, destroyed, and rendered unreadable by a user, program, or application.

Cloud malware

Cloud malware denotes harmful software created and distributed within cloud computing environments, aiming to pilfer data from users and enterprises, disrupt their operations, and induce diverse issues.

Hypervisor DoS attacks

A Hypervisor program is a type of software that allows running multiple operating systems on the same computer simultaneously.

Attacks occur when attackers attempt to overload the system by sending an excessive number of data or resource requests, leading to its disruption or unresponsiveness.

Trojans

It is a type of cloud malware that disguises itself as legitimate software to gain access to the system or steal data.

Phishing attacks

It involves sending emails or text messages that appear to be from known sources but are attempting to steal sensitive data or install malicious software instructions on the device.

Injection attacks

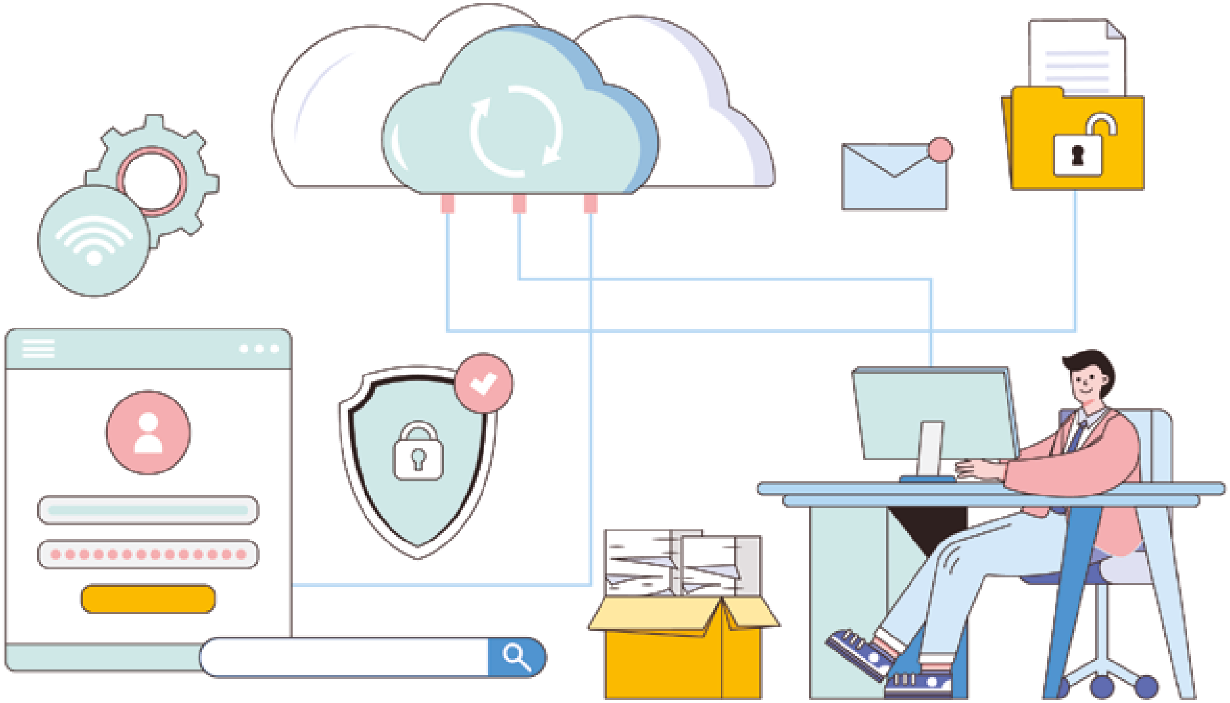
It is a cyber attackused by cybercriminals to create chaos in unprotected terminal servers through infiltration via unpatched access points. The goal is to steal data and identities, as well as distribute ransomware or exploit the stolen information.

Live migration

It is a process through which virtual machines can be moved from one physical host to another, allowing for improved resource utilization and enhanced performance. However, this process can be exploited by attackers in the presence of any security vulnerabilities in the system's security protocols.

Zero-day exploit

It is called "Zero-Day Attack" a type of online attack that exploits previously unknown vulnerabilities in computer systems or applications.



Cloud security

It involves procedures and technologies designed to secure cloud computing environments against both external and internal cybersecurity threats.

Security in cloud computing centrally oversees all your applications, devices, and data to guarantee comprehensive security. It streamlines task execution, facilitating the implementation of disaster recovery plans, optimizing network event monitoring, refining web filtering.

DDoS attacks

DDoS attacks pose significant threats to cloud computing, targeting servers with large traffic simultaneously to inflict damage. Cloud security protects servers from these attacks by monitoring and addressing them immediately upon occurrence.

Sketches

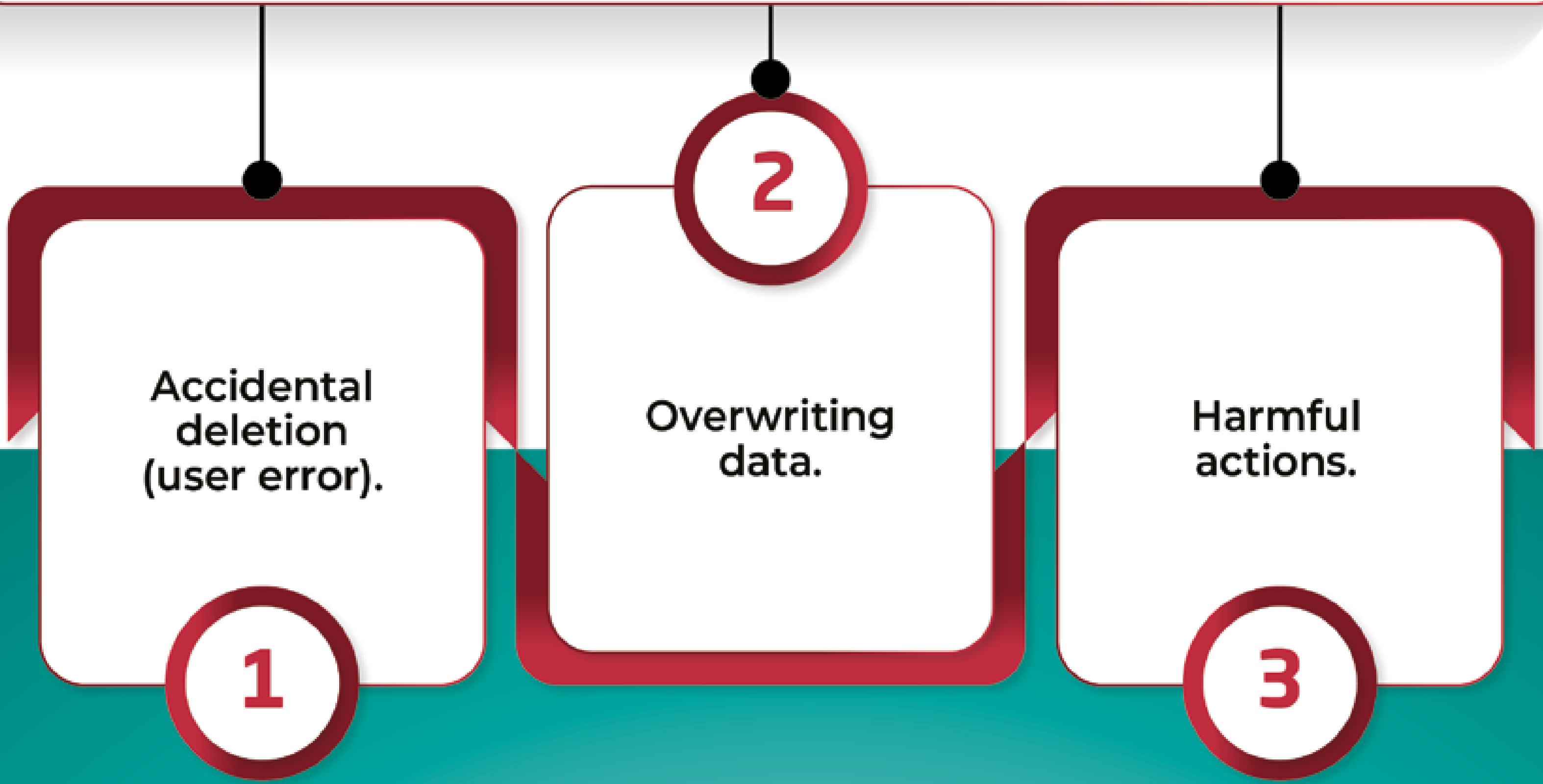
How to prevent data loss in the cloud?

1 Create backups of the most critical data.

2 Store your backups in various data centres.

3 Understanding the significance of storing data in a way that is tamper-resistant and impervious to encryption by ransomware.

What are the reasons for data loss in the cloud?



1. Accidental deletion (user error).

2. Overwriting data.

3. Harmful actions.

What is the reason behind the naming of cloud computing?

The reason for this name is that the accessed information is stored remotely in the cloud or virtual space. Companies that offer cloud services enable users to store files and applications on remote servers, allowing access to all data over the internet.

CyberEco

معًا لدعم السلامة الرقمية
Together to support digital safety

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency