Cybersecurity

AL Mansour University College

Digital Media Department

4th Class

Lecturer Mustafa Muhanad

-4-

1. 9. Need for a Comprehensive Cyber Security Policy

Security policies are a formal set of rules issued by an organization to ensure that the users authorized to access company technology and information assets comply with rules and guidelines related to information security. It is a written document in the organization responsible for how to protect the organization from threats and how to handle them when they occur.

A security policy is also considered a "living document," which means that the document is never finished but is continuously updated as the requirements of technology and employees change.

The following issues describe the requirements of security policies:

1) It increases efficiency.

The best thing about having a policy is being able to increase the level of consistency, which saves time, money, and resources. The policy should inform the employees about their duties, telling them what they can do and what they cannot do with the organization's sensitive information.

2) It upholds discipline and accountability.

When any human mistake occurs and system security is compromised, the security policy of the organization will back up any disciplinary action and also support a case in a court of law. The organization's policies act as a contract, which proves that the organization has taken steps to protect its intellectual property as well as that of its customers and clients.

3) It can break a business deal.

Companies don't need to provide a copy of their information security policy to other vendors during a business deal that involves the transference of their sensitive information. It is true in the case of bigger businesses, which ensure their security interests are protected when dealing with smaller businesses, which have less high-end security systems in place.

4) It helps educate employees on security literacy.

A well-written security policy can also be seen as an educational document that informs the reader about the importance of responsibility in protecting the organization's sensitive data. It involves choosing the right passwords and providing guidelines for file transfers and data storage, which increase employees' overall awareness of security and how it can be strengthened.

The following is a description of some important cybersecurity policy recommendations:

1. Virus and spyware protection policy

This policy provides the following protection:

• It helps to detect, remove, and repair the side effects of viruses and security risks by using signatures.

• It helps to detect threats in the files that the users try to download by using reputation data from Download Insight.

• It helps detect applications that exhibit suspicious behavior.

2. Firewall Policy

This policy provides the following protection:

• It blocks unauthorized users from accessing the systems and networks that connect to the Internet.

• It detects attacks by cybercriminals.

• It removes unwanted sources of network traffic.

3. Application and Device Control

This policy protects a system's resources from applications and manages the peripheral devices that can attach to a system. The device control policy applies to both Windows and Mac computers.

4. Exceptions policy

This policy provides the ability to exclude applications and processes from detection by virus and spyware scans.

5. Host Integrity Policy

This policy provides the ability to define, enforce, and restore the security of client computers to keep enterprise networks and data secure.