Module code: athe 5.1 cyber security

**NAME: FATIMA EJAZ BARRI**

**EMAIL: mishalfatimaeb@gmail.com**

**Mobile No: 0557436985**

TOPICS GIVEN BY TUTOR: SHAHID MUSTAFA

# What is a cyber-security framework and why is it important?

Cyber security is a combination of processes, technologies as well as controls purposely planed for data, networks as systems protection from cyber-attacks. It involves collecting policies, tools, equipping personal, approaches to risk management, assurance, and actions as well the organization. These assets comprise of installed devices for computing, workers infrastructure, applications and the entire sent or data stored in the cyberspace.

Raising the awareness of cyber security is a key element of promoting the success of the strategy. The goal is to build a more secure information society that is perfectly aware of cyber security risks. One of the key objectives of this strategy is to address any risks, threats or attacks, as well as allowing user access to various aspects of information technology so as to promote the success of the strategy in the future.

# Explain feathers of 5 strategy domains of Dubai cyber security vision

The Dubai cyber security strategy requires the introduction of the following 5 primary domains:

1. **Cyber smart nation:**

The goal of this area is to raise public awareness of the importance of cyber security and to maintain a community that is fully aware of the dangers of cybercrime. It aims at developing the skills and capabilities needed by government and private institutions and individuals in Dubai to handle cyber security risks.

1. **Innovation:**

Innovation and scientific research in the field of electronic security and the development of open, equal and safe cyberspace are at stake in this domain.

1. **Cyber security:**

By implementing controls to protect the confidentiality, integrity, availability and privacy of data, this domain aims to create a safe cyberspace.

1. **Cyber resilience:**

In the event of any cyber threats, this domain will concentrate on preserving the flexibility of cyberspace and ensuring the continuity and efficiency of IT systems.

1. **National and international collaboration in cyber security:**

This field is intended to develop local and global collaborations to develop collaboration mechanism at global and local levels with different sectors to address cyberspace threats and risks.

# Any 5 types of attacks which could harm an organization and what measurers should be taken to prevent them?

1. **Ransomware:**

This is a form of malware (malicious software) that attempts to encrypt (scramble) your data and then extort a ransom to release an unlock code. Most ransomware is delivered via malicious emails. Follow these key steps.

• Staff awareness: staff should be wary of unsolicited emails, particularly those that ask for a prompt response.

• Malware protection: install and maintain good anti-virus and malware protection software.

• Software updates: keep your applications up to date.

• Data backups: a series of well managed data backups will allow you to recover from an unencrypted version of a file. Make sure you regularly test your backups.

1. **Phishing:**

Phishing is an attempt to gain sensitive information while posing as a trustworthy contact, for example a bank or online service. Spear phishing is a highly targeted attempt to gain information from an individual. Phishing emails may look completely convincing, often with faultless wording and genuine logos. There is a form of spear phishing, where a fake email from a CEO applies pressure on a CFO into making an urgent payment, this has become known as Whaling. It is worth considering ways to add additional safeguards to protect the identity of CEOs and CFOs to prevent impersonation. Here are a few steps you can use to protect yourself.

• Keep in mind that companies simply do not ask for sensitive information.

• Be suspicious of unexpected emails.

• Make use of anti-malware software.

 • Make sure you have spam filters turned on. Check them regularly in case they have accidentally trapped an innocent email.

1. **Data leakage:**

While cyber security in the office may seem challenging, it is essential to understand that security extends well beyond the office these days. The use of smart phones and tablets has become widespread. The ubiquitous and cheap nature of portable storage devices makes them a useful tool for the backup and transportation of data. Those features mean they are also a target for data thieves. The following pointers provide useful first steps to prevent data leaking from your organization.

• Ensure mobile devices have passcode locks.

• Turn on the tracking by GPS and the option to remotely wipe the device if it is lost.

• The use of encryption software is highly recommended when using portable storage devices.

• Keep an eye on your mobile devices and paperwork at all times. A large proportion of crime is opportunistic, taking your eye off your briefcase or smart device could result in a serious loss of data.

1. **Hacking:**

Gaining access to IT systems from outside an organization still offers rich pickings for criminals. Traditionally they have attempted to gain access to bank account information or credit card databases. However, intellectual property is another source of value. The use of social engineering, tricking staff into revealing user names and passwords, remains a threat.

• The primary methods to protect yourself from hacking are network firewalls, data access security, procedures for providing and removing access, and user awareness and training.

1. **Insider threat:**

If your organization employs staff (full time or as contractors), there is a possibility they could leak data by mistake or maliciously. The potential damage from a leak of documents cannot be underestimated. Use these tips to mitigate the size of any data leak.

• Educate your team to be alert to issues and minimize careless mistakes.

• Limit how much data staff has access to. The principle of ‘least privilege accesses should apply to all IT systems. Only provide staff with the minimum access they need to do their roles.

• Control the use of portable storage devices, such as USB memory keys, portable hard drives and media players.

• Consider using applications in certain situations to monitor staff behavior − who copies what.

In all these areas it is key to remember that alongside technology, well-developed processes, procedures and staff training go a long way to protecting your valuable data. For example, if someone leaves your employment, make sure you remove their access. The reality today is that you should protect your digital assets with the same vigilance as you do when locking your office door at the end of the day.

