Security Controls

Lect 3

Potential Losses due to Security Attacks

- The potential loses in this cyberspace are many even if you are using a single computer in your room e.g:
  - **Losing your data** – If your computer has been hacked or infected, there is a big chance that all your stored data might be taken by the attacker.
  - **Bad usage of your computer resources** – This means that your network or computer can go in overload so you cannot access your genuine services or in a worst case scenario, it can be used by the hacker to attack another machine or network.
  - **Reputation loss** – Just think if your Facebook account or business email has been owned by a social engineering attack and it sends fake information to your friends, business partners. You will need time to gain back your reputation.
  - **Identity theft** – This is a case where your identity is stolen (photo, name surname, address, and credit card) and can be used for a crime like making false identity documents.

When Are We Secure?

- Defining the exact point at which we can be considered secure presents a bit of a challenge. **Are we secure if our systems are properly patched? Are we secure if we use strong passwords? Are we secure if we are disconnected from the Internet entirely**? From a certain point of view, all of these questions can be answered with a "no."
- Even if our systems are properly patched, there will always be new attacks to which we are vulnerable. When strong passwords are in use, there will be other avenues that an attacker can exploit. When we are disconnected from the Internet, our systems can be physically accessed or stolen. In short, it is very difficult to define when we are truly secure. We can, however, turn the question around.
- Defining when we are insecure is a much easier task and we can quickly list a number of items that would put us in this state:
  - Not patching our systems
  - Using weak passwords such as "password" or "1234"
  - Downloading programs from the Internet
  - Opening e-mail attachments from unknown senders
  - Using wireless networks without encryption

- We could go on for some time creating such a list. The good thing is that once we are able to point out the areas in an environment that can cause it to be insecure, we can take steps to mitigate these issues.
- This problem is akin to cutting something in half over and over; there will always be some small portion left to cut again. Although we may never get to a state that we can definitively call “secure,” we can take steps in the right direction.

Controls

- Security controls are parameters implemented to protect various forms of data and infrastructure important to an organization.
- Any type of safeguard or countermeasure used to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets is considered a **security control.**
- **Controls are divided into three categories:**
  - **physical,**
  - **logical,**
  - **and administrative.**

TYPES OF SECURITY CONTROLS	CONTROL FUNCTIONS		
	PREVENTATIVE	DETECTIVE	CORRECTIVE
PHYSICAL CONTROLS	• Fences • Gates • Locks	• CCTV • Surveillance Cameras	• Repair physical damage • Re-issue access cards
TECHNICAL CONTROLS	• Firewall • IPS • MFA • Antivirus	• IDS • Honeypots	• Vulnerability patching • Reboot a system • Quarantine a virus
ADMINISTRATIVE CONTROLS	• Hiring & termination policies • Separation of duties • Data classification	• Review access rights • Audit logs and unauthorized changes	• Implement a business continuity plan • Have an incident response plan

PHYSICAL

- Physical controls are those controls that protect the physical environment in which our systems sit, or where our data is stored. Such controls also control access in and out of such environments. Physical controls include items such as fences, gates, locks, bollards, guards and cameras, but also include systems that maintain the physical environment such as heating and air conditioning systems, fire suppression systems and backup power generators.
- Although at first glance, physical controls may not seem like they would be integral to information security, they are actually one of the more critical controls with which we need to be concerned. If we are not able to physically protect our systems and data, any other controls that we can put in place become irrelevant.
- If an attacker is able to physically access our systems he can, at the very least, steal or destroy the system, rendering it unavailable for our use in the best case.
- In the worst case, he will have access directly to our applications and data and will be able to steal our information and resources or subvert them for his own use.

Premises and company surroundings	Fences, gates, walls, guards, alarms, CCTV cameras, intruder systems, panic buttons, burglar alarms, windows and door bars, deadlocks, etc.
Reception area	Lock the important files and documents Lock equipment when not in use
Server and workstation area	Lock the systems when not in use, disable or avoid having removable media and DVD-ROM drives, CCTV cameras, workstation layout design
Other equipment such as fax, modem, and removable media	Lock fax machines when not in use, file the faxes obtained properly, disable auto answer mode for modems, do not place removal media at public places, and physically destroy the corrupted removal media
Access control	Separate work areas, implement biometric access controls (fingerprinting, retinal scanning, iris scanning, vein structure recognition, face recognition, voice recognition), entry cards, man traps, faculty sign-in procedures, identification badges, etc.
Computer equipment maintenance	Appoint a person to look after the computer equipment maintenance
Wiretapping	Inspect all the wires carrying data routinely, protect the wires using shielded cables, never leave any wire exposed
Environmental control	Humidity and air conditioning, HVAC, fire suppression, EMI shielding, and hot and cold aisles

LOGICAL

- Logical controls, sometimes called **technical controls**, are those that protect the systems, networks and processes used to transmit and store our data.
- Logical controls can include items such as **passwords, encryption, logical access controls, firewalls and intrusion detection systems.**
- Logical controls enable us, in a logical sense, to prevent unauthorized activities from taking place. If our logical controls are implemented properly and are successfully an attacker or unauthorized user cannot access our applications and data without subverting the controls that we have in place.

ADMINISTRATIVE

- Administrative controls are based on rules, laws, policies, procedures, guidelines and other items that are “paper” in nature. In essence, administrative controls set out the rules for how we expect the users of our environment to behave.
- Depending on the environment and control in question, administrative controls can represent differing levels of authority. We may have a simple rule such as “turn the coffee pot off at the end of the day,” aimed at ensuring that we do not cause a physical security problem by burning our building down at night. We may also have a more stringent administrative control, such as one that requires us to change our password every 90 days.

- One important concept when we discuss administrative controls is the ability to enforce compliance with them. If we do not have the authority or the ability to ensure that our controls are being complied with, they are worse than useless, because they create a false sense of security.
- For example, if we create a policy that says our business resources cannot, in any fashion, be used for personal use, we need to be able to enforce this. Outside of a highly secure environment, this can be a difficult task. We will need to monitor telephone and mobile phone usage, Web access, e-mail use, instant message conversations, installed software, and other potential areas for abuse. Unless we were willing to devote a great deal of resources for monitoring these and other areas, and dealing with violations of our policy, we would quickly have a policy that we would not be able to enforce. Once it is understood that we do not enforce our policies, we can quickly set ourselves up for a bad situation.

Read on the concept of defense in depth

Assignment 1 – Individual

- Discuss the various cybersecurity controls in respect to the threats/attacks discussed in lesson 2.
- Mode of submission: Moodle
- Date of submission:

- Thank you