INFORMATION SECURITY AND CONTROLS

Group 1

Soha Mohamed Ahmed Mahmoud
Rola AlaaEldeen Mohamed AbdEl-kareem
Aya Khaled Abdellah Abdallah
Ziad Walid Abdelmoneim Elhoseny

Information can be:

-physical or electronic one.

-Anything like Your details or we can say your profile on social media, your data in mobile phone, your biometrics ,etc.

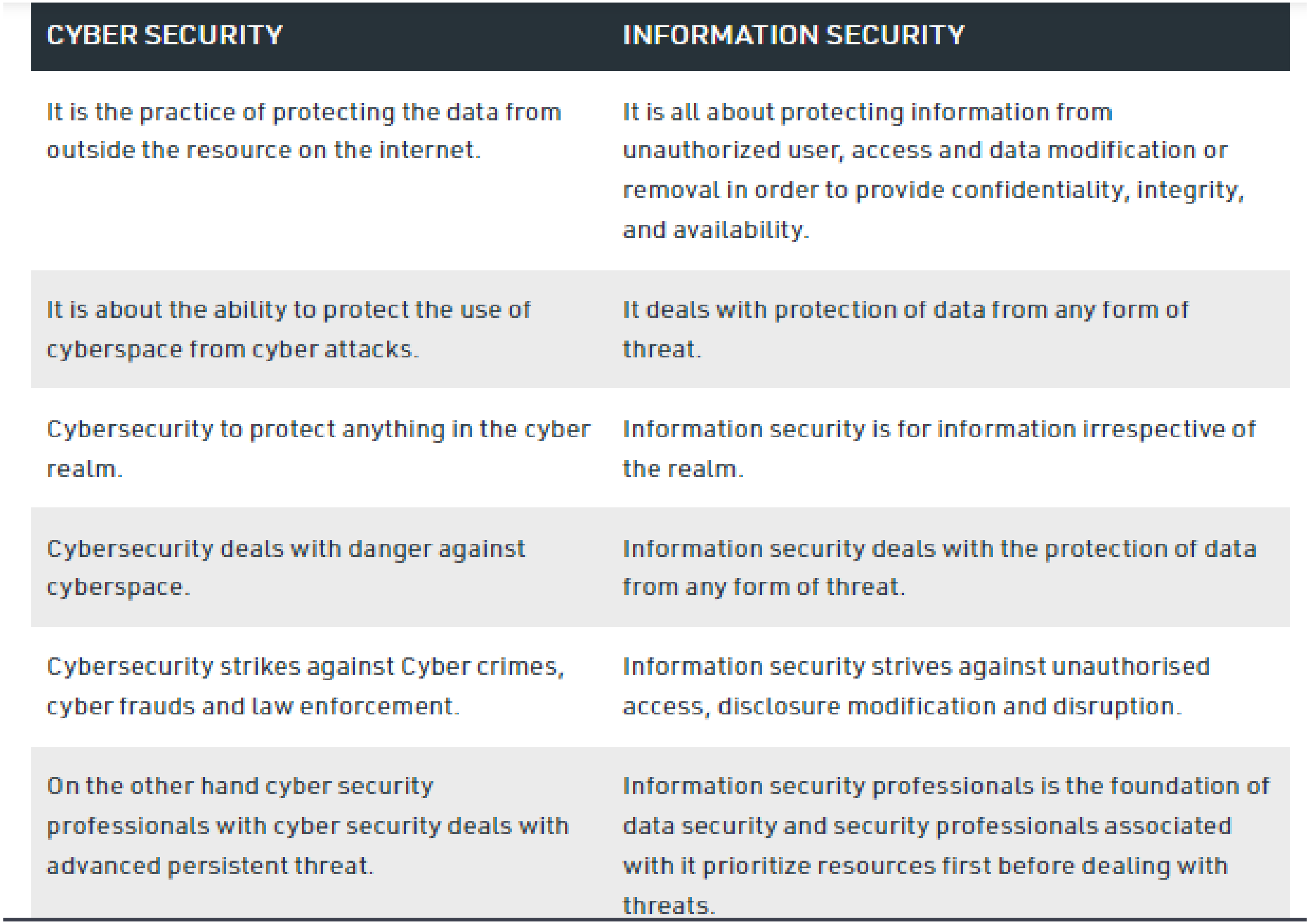
Information Security:

It is not only about securing information from unauthorized access, it is basically the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information.

It spans so many research areas like Cryptography, Mobile Computing, Cyber Forensics, Online Social Media ,etc.

Information Security programs are build around 3 objectives, commonly known as CIA – Confidentiality, Integrity, Availability.

Difference between Cyber Security and Information Security:



CYBER SECURITY	INFORMATION SECURITY
It is the practice of protecting the data from outside the resource on the internet.	It is all about protecting information from unauthorized user, access and data modification or removal in order to provide confidentiality, integrity, and availability.
It is about the ability to protect the use of cyberspace from cyber attacks.	It deals with protection of data from any form of threat.
Cybersecurity to protect anything in the cyber realm.	Information security is for information irrespective of the realm.
Cybersecurity deals with danger against cyberspace.	Information security deals with the protection of data from any form of threat.
Cybersecurity strikes against Cyber crimes, cyber frauds and law enforcement.	Information security strives against unauthorised access, disclosure modification and disruption.
On the other hand cyber security professionals with cyber security deals with advanced persistent threat.	Information security professionals is the foundation of data security and security professionals associated with it prioritize resources first before dealing with threats.

Threats to Information Security:

Information Security threats can be many like Software attacks, theft of intellectual property, identity theft, theft of equipment or information, sabotage, and information extortion.

Threat can be anything that can take advantage of a vulnerability to breach security and negatively alter, erase, harm object or objects of interest.

Software attacks means attack by Viruses, Worms, Trojan Horses etc. Many users believe that malware, virus, worms, bots are all same things. But they are not same, only similarity is that they all are malicious software that behaves differently

Malware is a combination of 2 terms- Malicious and Software. So Malware basically means malicious software that can be an intrusive program code or anything that is designed to perform malicious operations on system

Malware can be divided in 2 categories:

- Infection Methods
- Malware Actions

New generation threats:

-Technology with weak security.

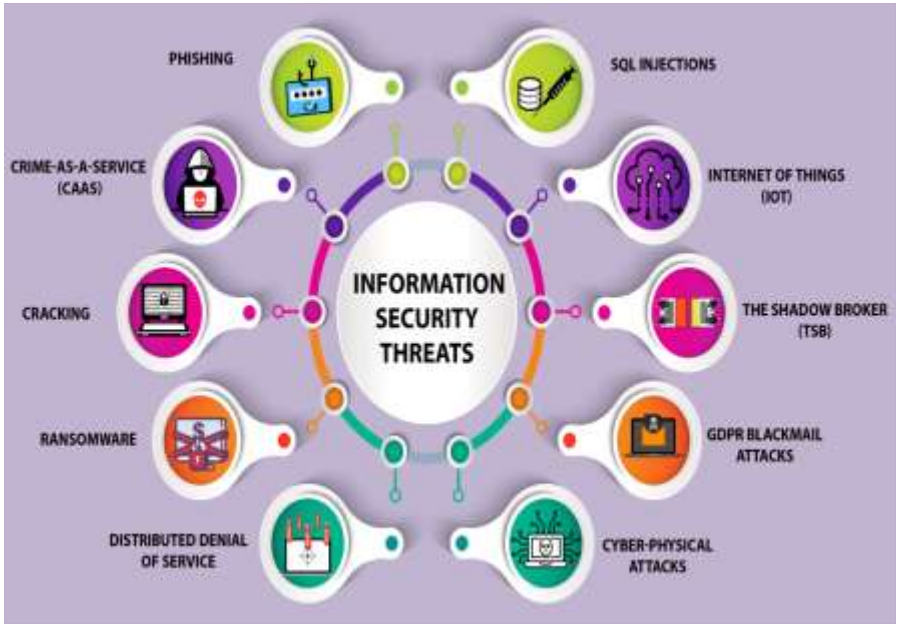
-Social media attacks.

-Mobile Malware.

-Corporate data on personal devices.

-Outdated Security Software.

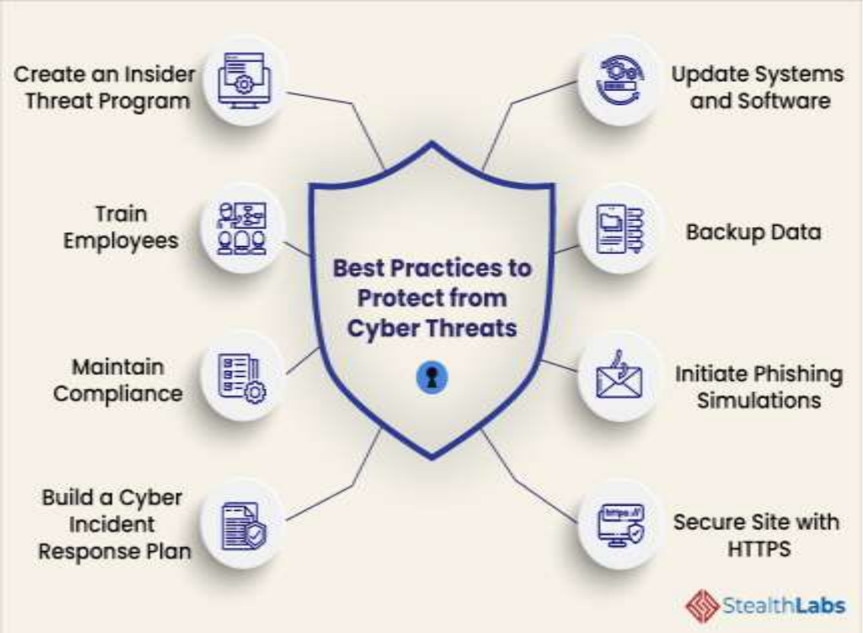
-Social Engineering.



Security Threats

How to deal with risk:

- Ensure you have anti-malware software installed and updated on your device.
- Back up your data, especially your important files, and make sure you can store them in an offline location.
- Only open files and software that you know is from a trusted source.
- Inspect content and correspondence to identify any features that seem amiss (as you would with phishing scams).
- Have a plan in place to deal with a potential malware attack.


Create an Insider Threat Program
Update Systems and Software
Train Employees
Best Practices to Protect from Cyber Threats
Backup Data
Maintain Compliance
Initiate Phishing Simulations
Build a Cyber Incident Response Plan
Secure Site with HTTPS
StealthLabs

How to deal with Risks

- Ensure you have antivirus software installed and up to date. The same applies to your IT devices.
- Set up your devices so that only authorized software and applications can run on them. Avoid opening applications and files from unknown sources.
- Make sure your IT equipment is updated and installed with the necessary security software.

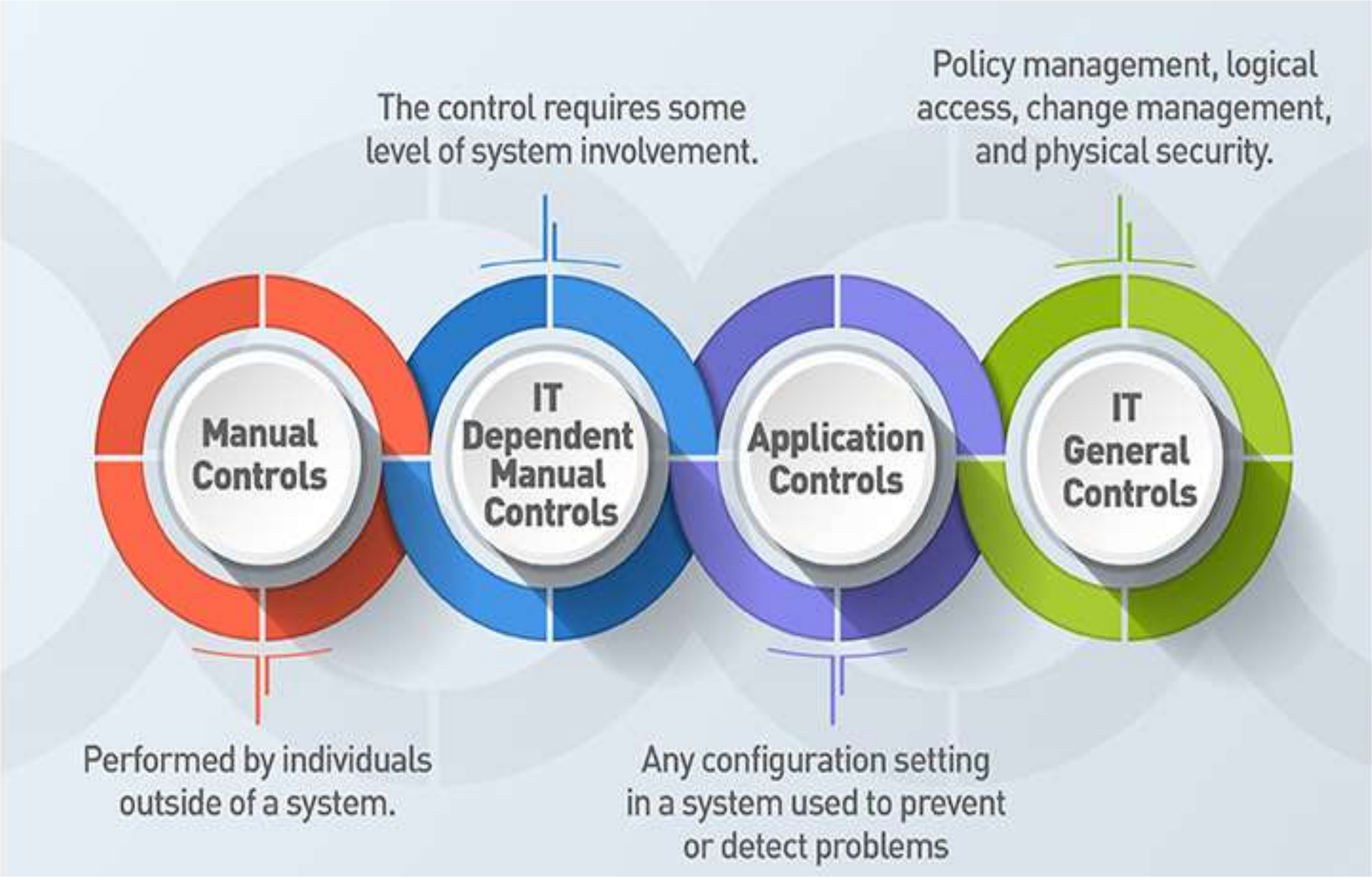
information security controls:

are measures taken to reduce information security risks such as information systems breaches, data theft, and unauthorized changes to digital information or systems. These security controls are intended to help protect the availability, confidentiality, and integrity of data and networks, and are typically implemented after an information security risk assessment.

There are three categories of information security controls:

- Preventive security controls, designed to prevent cyber security incidents
- Detective security controls, aimed at detecting a cyber security breach attempt (“event”) or successful breach (“incident”) while it is in progress, and alerting cyber security personnel
- Corrective security controls, used after a cyber security incident to help minimize data loss and damage to the system or network, and restore critical business systems and processes as quickly as possible (“resilience”).

Types of internal controls:



Manual Controls

Performed by individuals outside of a system.

IT Dependent Manual Controls

The control requires some level of system involvement.

Application Controls

Any configuration setting in a system used to prevent or detect problems

IT General Controls

Policy management, logical access, change management, and physical security.