Information Security and Controls

Group 1

رولا علاء الدين محمد عبدالكريم

سها محمد أحمد محمود

آية خالد عبداللاه عبدالله

زياد وليد عبدالمنعم الحسيني

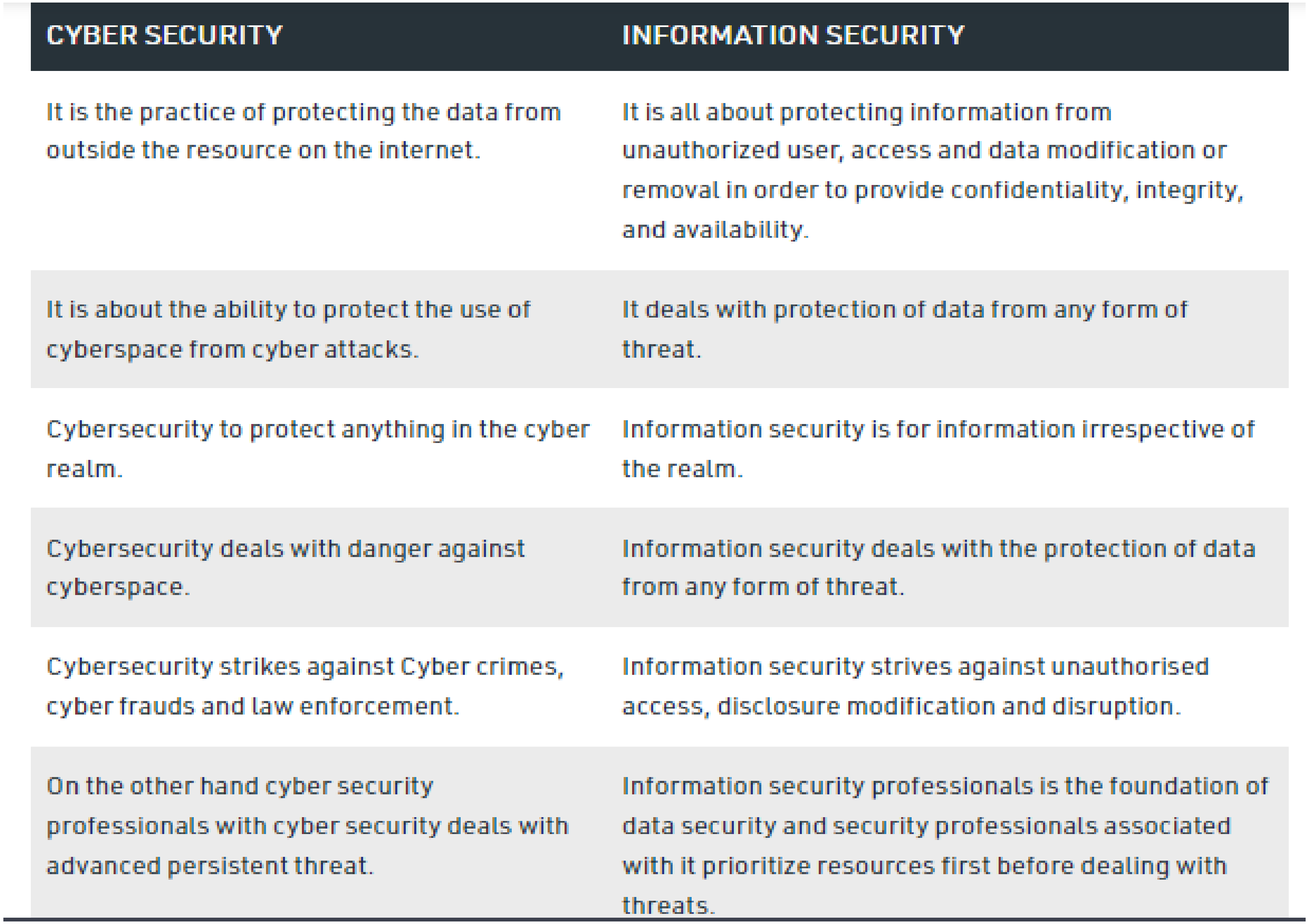
Information can be:

-Either a physical or an electronic one-Anything like your personal information, or as we call it, your social media profile, your mobile phone data, your biometrics, and so on.

Information Security:

It is the process of preventing illegal access, use, disclosure, interruption, alteration, inspection, recording, or destruction of information, and it is not just about securing information against unwanted access. It covers a wide range of topics, including cryptography, mobile computing, cyber forensics, online social media, and so on. Confidentiality, Integrity, and Availability (CIA) are the three main goals of information security programmers.

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:

Software assaults, loss of intellectual property, identity theft, theft of equipment or information, sabotage, and information extortion are all examples of information security concerns.

Threat can be anything that uses a security flaw to compromise security and negatively change, erase, or injure an object or objects of interest.

Software attacks Viruses, Worms, Trojan Horses, and other threats Malware, virus, worms, and bots are all conflated in the minds of many people. But they are not identical; the only thing they have in common is that they are all malicious software that behaves differently.

Malware Malicious Software is a mixture of two terms. Malware is a general term for malicious software, which can range from intrusive programmer code to anything designed to perform malicious operations on a computer system.

Malware can be divided in 2 categories:

- Infection Methods
- Malware Actions

New generation threats:

-Technology with weak security.

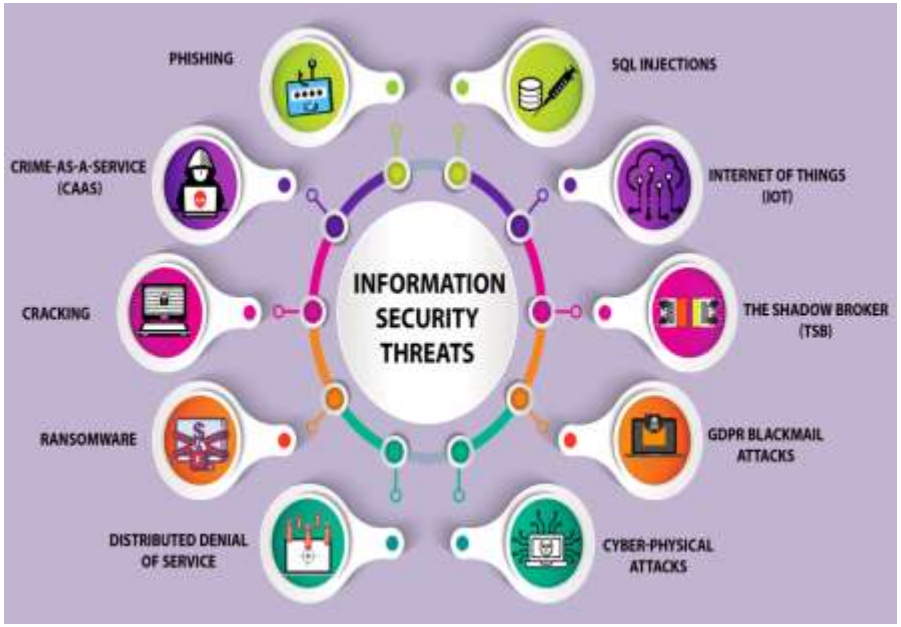
-Social media attacks.

-Mobile Malware.

-Corporate data on personal devices.

-Outdated Security Software.

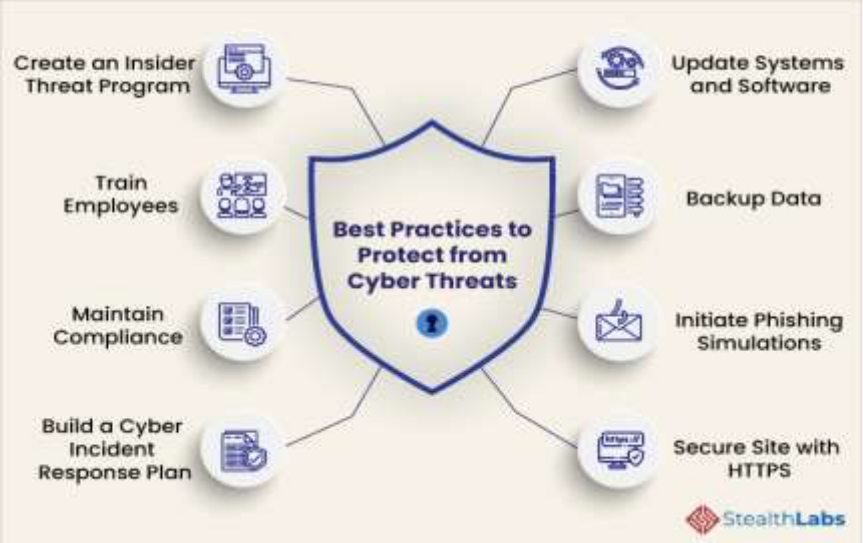
-Social Engineering.



Security Threats

How to deal with risk:

- Make sure your anti-malware software is up to date and installed on your computer.
- Make a backup of your data, especially crucial information, and make sure you can save it somewhere other than your computer. Only open files and software that you know is from a trusted source.
- Examine the content and correspondence for any unusual characteristics (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
Backup Data
Best Practices to Protect from Cyber Threats
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.

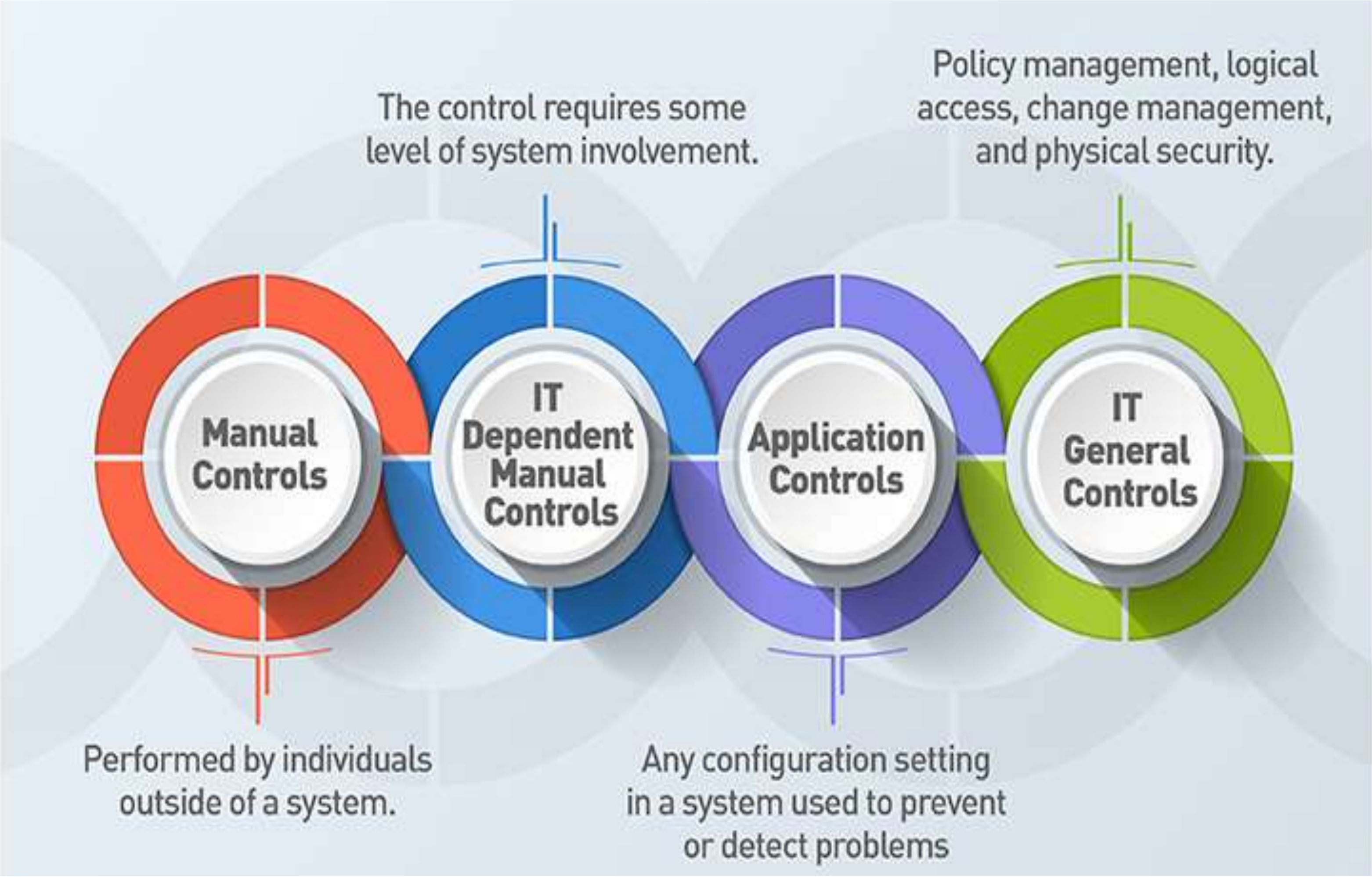
information security controls:

are steps made to reduce information security threats such as data breaches, identity theft, and unauthorized alterations to digital data or systems. These security controls are often installed following an information security risk assessment to assist safeguard the availability, confidentiality, and integrity of data and networks.

There are three categories of information security controls:

- Preventive security procedures are intended to keep cyber security events from happening. Detective security controls designed for detecting and alerting cyber security workers during a cyber security breach attempt ("event") or successful breach ("incident") in progress. After a cyber security incident, corrective security procedures are employed to help limit data loss and damage to the system or network, as well as restore important business systems and processes as rapidly 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.