أمن تكنولوجيا المعلومات وإدارة المخاطر

IT Security and Risk Management

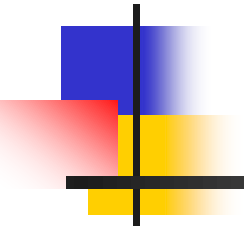
Cybersecurity

ا.د. حنان الطاهر الداقيز

h.dagez@uot.edu.ly

خريف 2023

https://t.me/+1iMQn29WU0o0Zjc8



Chapter 4

Cybersecurity Framework

Cybersecurity

Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users via ransomware; or interrupting normal business processes.

It's also known as information technology security or electronic information security.

NIST vs. ISO Cybersecurity Framework

NIST :National Institute of Standards and Technology

ISO: International Organization for Standardization

The NIST CSF is designed as a guide, whereas ISO 27001 is designed as a standard. The difference here is that NIST CSF serves as an instruction manual and ISO 27001 is more of a test that requires certain measures to pass. In the NIST CSF, there is no certification or audit process.

Which one to choose, NIST or ISO?

- Company looking to earn ISO 27001 certification, then ISO 27001 is the one.
- The NIST Framework a good starting point for company has never considered its cyber security in the past and is trying to build a risk management program for the first time.

ISO 27001 Framework

- ISO 27001 is a standard that focuses on keeping customer and stakeholder information confidential, maintaining integrity by preventing unauthorized modification and being available to authorized people and systems.
- ISO 27001 outlines the requirements for Information Security Management Systems (ISMS) and gives organizations guidance on how to establish, implement, maintain and continually improve an ISMS.
- Everyone in the organization gets involved in Cybersecurity to create a more secure environment, with risks that are clearly established and planned for.

ISO 27001 Framework …

- ISO 27001 standard has **10 clauses**, the first three of which go over the references, terms and other basic information that is covered in the regulation. The other seven clauses guide companies in establishing and maintaining their Information Security Management System.
- **4. Organisation's Context:** The company looks at the environment that it's working in, the systems involved and the goals that it has. Some of the areas covered include the overall scope that the ISMS covers, relevant parties and the assets that should fall under the system.

ISO 27001...

- **5. Leadership and Commitment:** Information security comes from the top down. When upper management is actively involved with following these requirements and offering guidance throughout the process, it's more likely that the project will succeed. The business strategy should inform the information security measures that are part of the ISMS and leadership should provide the resources needed to support these initiatives.
- **6. Planning:** Businesses should have a way to identify cybersecurity risks, treat the most concerning threats and discover opportunities. A risk management process is the most important part of this clause. Organisations must prepare for ongoing cybersecurity assessment as new threats come up.

ISO 27001....

- **7. Support:** Successful cybersecurity measures require enough resources to support these efforts. Organisations need the right combination of infrastructure, budget, people and communications to achieve success in this area.
- **8. Operation:** This clause covers what organisations need to do to act on the plans that they have to protect and secure data.
- **9. Performance Evaluation:** After the plan deploys, companies should track whether it's effective at managing the risk to determine if they need to make changes.

ISO 27001….

- **10. Improvement:** Effective information security management is an ongoing process. Organisations should plan to re-evaluate their ISMS on a regular basis to keep up with the latest risks.

NIST Cybersecurity framework

- The National Institute of Standards and Technology (NIST) has a vøluntary Cybersecurity framework available for organizations overseeing critical infrastructure.
- Its goals are the same as ISO 27001, with an emphasis on identifying, evaluating and managing the acceptable risks to information systems.

NIST 800-53 Cybersecurity framework ..

The NIST framework uses **Five Functions** to allow companies to customize their cybersecurity measures to best meet their goals and unique challenges that they face in their environments.

1. Identify
2. Protect
3. Detect
4. Respond
5. Recover

NIST Cybersecurity framework ..

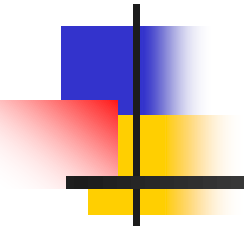
- **Identify:** What cybersecurity risks exist in the organisation? The context of the company is important, similar to clause 4 in ISO 27001, as well as the infrastructure and capabilities that are present. Assessments of existing cybersecurity measures and risks fall under this category.
- **Protect:** A company needs to design the safeguards that protect against the most concerning risks and minimizes the overall consequences that could happen if a threat becomes a reality. The protective measures that organisations put in place can include data security systems, cybersecurity training among all employees, routine maintenance procedures, access control and user account control.

NIST Cybersecurity framework ..

- **Detect:** Early threat detection can make a significant difference in the amount of damage that it could do. This function allows companies to discover incidents earlier, determine whether the system has been breached, proactively monitor all of the infrastructure and surface anomalies that could be the result of a cybersecurity problem.
- **Respond:** How does the company respond to a cybersecurity attack after it happens, and do they have procedures in place that cover these eventualities? Everything should be planned out ahead of time so there's no question about who needs to be contacted during an emergency or an incident. The chain of command and lines of communication also get established under this function. Post-incident analysis can provide excellent information on what happened and how to prevent it from reoccurring.

NIST Cybersecurity framework ..

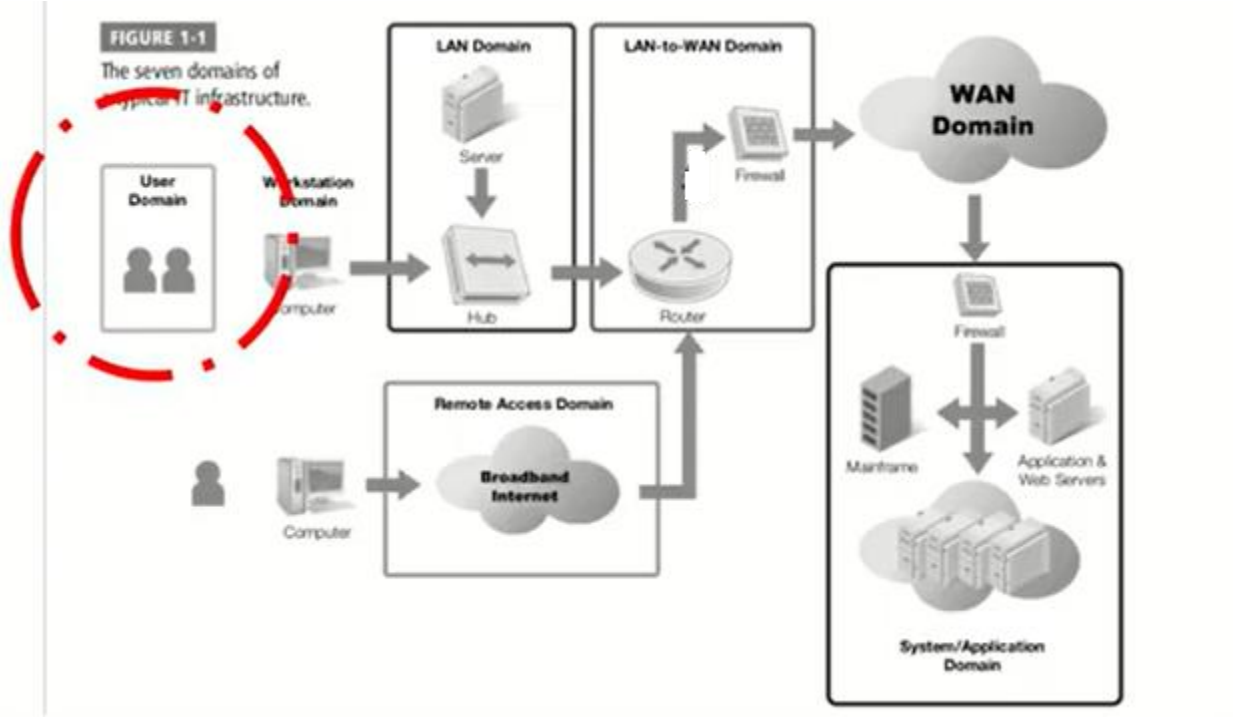
- **Recover:** What needs to happen to get the organisation back to normal following a Cybersecurity incident? Business continuity planning should cover how to restore the systems and data impacted by an attack. It also dictates how long it takes to recover and what needs to happen moving forward.



Chapter 5

Social Engineering

Social Engineering in 7 Domains



Social Engineering ..

Assets in every organization consists of

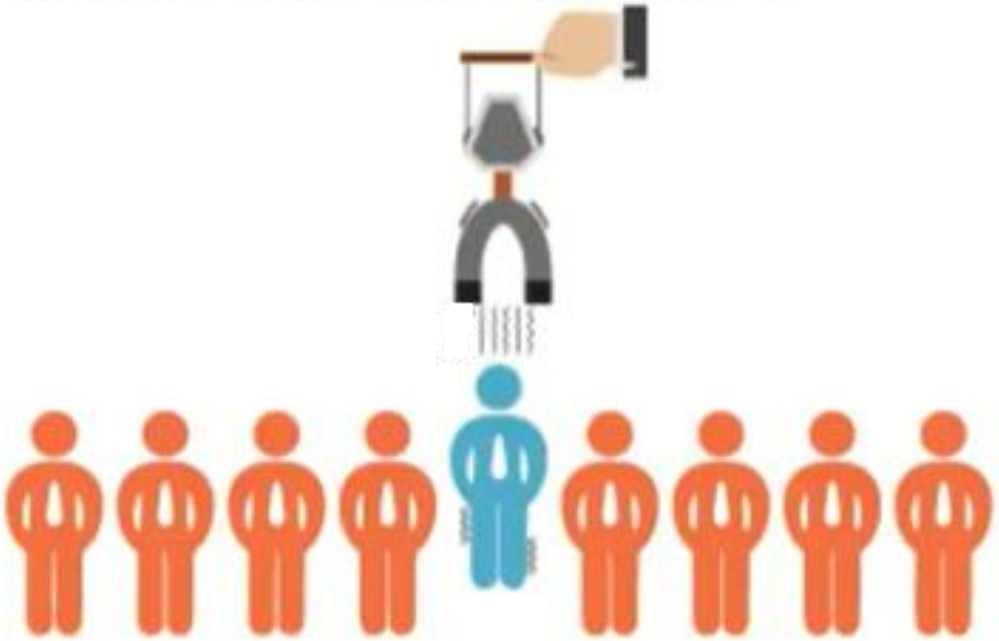
- Hardware
- Software
- People
- Services
- Information

Social engineering..

- The main goal of social engineering is to gain access to certain information systems, organizations, or other places that kept valuable assets without authorization by deceiving authorized personnel to give access to them.

What is social engineering

- **Social Engineering:** Psychological manipulation of people into performing actions or Disclose (declare) confidential information.



Motivation for Social Engineering

- Economic profit or financial gain
- Personal interest
- Revenge
- External pressure
- Politics

THANK YOU

ANY QUESTION?