جامعة الحسين التقنية
Al Hussein Technical University

Information Security Management

J/618/7447
10203300

جامعة الحسين التقنية
Al Hussein Technical University

Topic 1: INFORMATION SECURITY PRINCIPLES

Eman Alzyoud
School of Computing and Informatics
Eman.Alzyoud@HTU.EDU.JO

جامعة الحسين التقنية
Al Hussein Technical University

Table of content:

- What an ISMS Concepts and definitions .
- Impact of information security threats.
- The need for, and benefits of, information security .

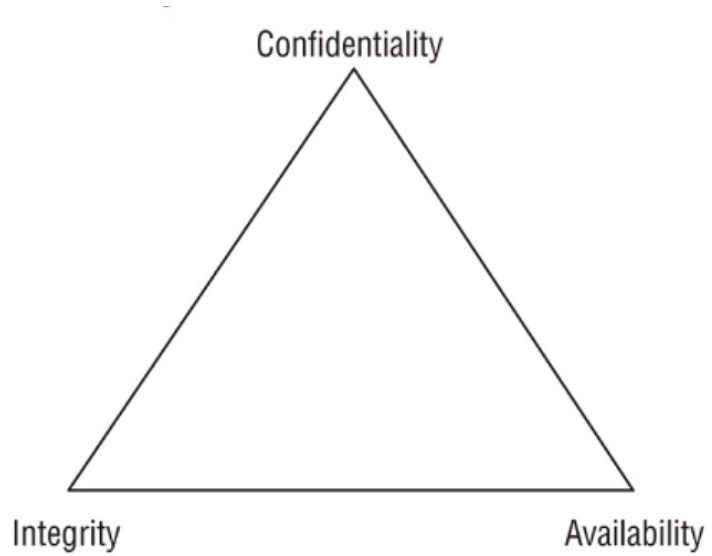
جامعة الحسين التقنية
Al Hussein Technical University

ISMS concepts and principles

- An information security management system (ISMS) is a set of policies and procedures for systematically managing an organization's sensitive data. The goal of an ISMS is to minimize risk and ensure business continuity by proactively limiting the impact of a security breach.

- Confidentiality, integrity, and availability (CIA) are typically viewed as the primary goals and objectives of a security infrastructure.

- Security controls are typically evaluated on how well they address these three core information security tenets. Vulnerabilities and risks are also evaluated based on the threat they pose against one or more of the CIA Triad principle .



CIA Triad

جامعة الحسين التقنية
Al Hussein Technical University

CIA Triad principle

- **Confidentiality.** The property that information is not made available or disclosed to unauthorized individuals, entities or processes (ISO/IEC 27000)

Information must be applicable only to a limited number of individuals because of its nature, its content or because its wider distribution will result in undesired effects, including legal or financial penalties or embarrassment. Restricting access to information to those who have a 'need to know' is good practice. Controls to ensure confidentiality form a major part of the wider aspects of information assurance management.

- **Availability.** The property of being accessible and usable upon demand by an authorized entity (ISO/IEC 27000)

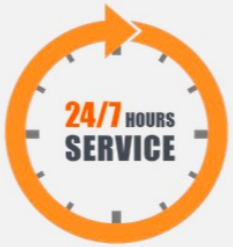
Information that is not available when and as required is not information at all but irrelevant data.

- **Integrity.** The property of accuracy and completeness (ISO/IEC 27000)

Information is only useful if it is complete and accurate, and remains so. Maintaining this aspect of information (its integrity) is often critical and ensuring that only certain people have the appropriate authority to alter, update or delete information is another basic principle of IA(information Assurance).

Confidentiality

- Data at rest (whole disk, database encryption)
- Data in transit (IPSec, TLS, PPTP, SSH)
- Access control (physical and logical)



Availability

- Redundancy
- Backups
- Resiliency

Integrity

- Hashing (data integrity)
- Configuration management (system integrity)
- Change control (process integrity)
- CRC functions cyclic redundancy check
- Access control (physical and logical)

جامعة الحسين التقنية
Al Hussein Technical University

Why do companies need ISMS?

- A good ISMS is vital for organizations today. It can provide a much-needed overview of where things stand regarding information security and the tools to make sure it remains strong. Picture an organization's data as a castle, encompassed by thick walls that protect its valuable content from unwanted intrusions.

- There is no doubt that organizations are facing a flood of threats to their intellectual assets and to their critical and sensitive information. High-profile cyber attacks and data protection compliance failures have led to significant embarrassment and brand damage for organizations – in both the public and private sectors – all over the world.

- Data or information is right at the heart of the modern organization. Its availability, integrity and confidentiality are fundamental to the long-term survival of any 21st-century organization

جامعة الحسين التقنية
Al Hussein Technical University

Patterns over time in incidents and breaches

- The annual Verizon Data Breaches Report * gathered data from 80,000 data breaches (which occurred in a 12-month period) across the world to conclude that 700 million compromised records were the cause of financial losses of some $400 million. Matters are worse in every subsequent year.

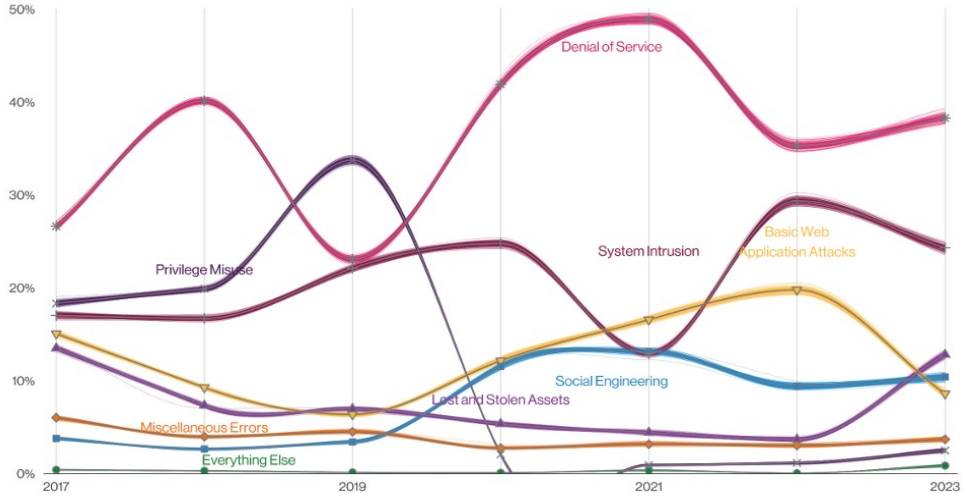


Figure 1. Patterns over time in incidents

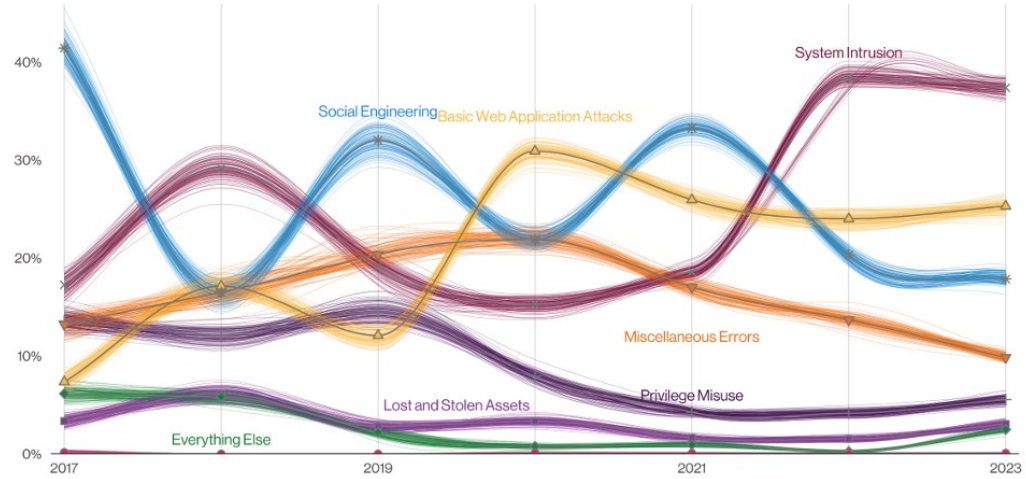


Figure 2. Patterns over time in breaches

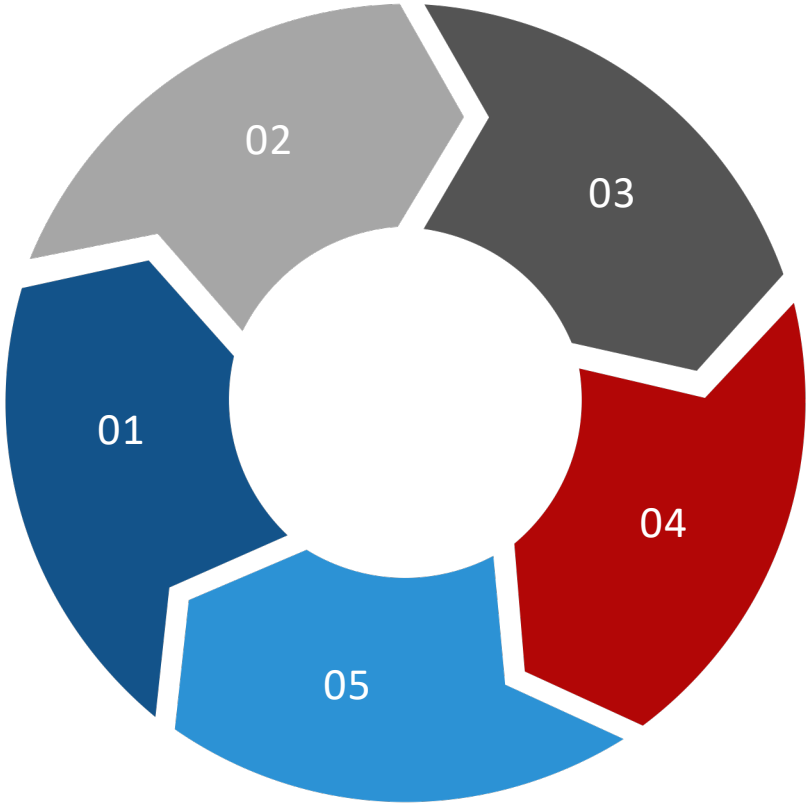
*https://www.verizon.com/business/resources/reports/dbir/

IMPACT OF INFORMATION SECURITY THREATS

It is worth understanding the risks to which an organization with an inadequate ISMS exposes itself. These risks fall into five categories:

Damage to operations

Financial impact



Damage to reputation

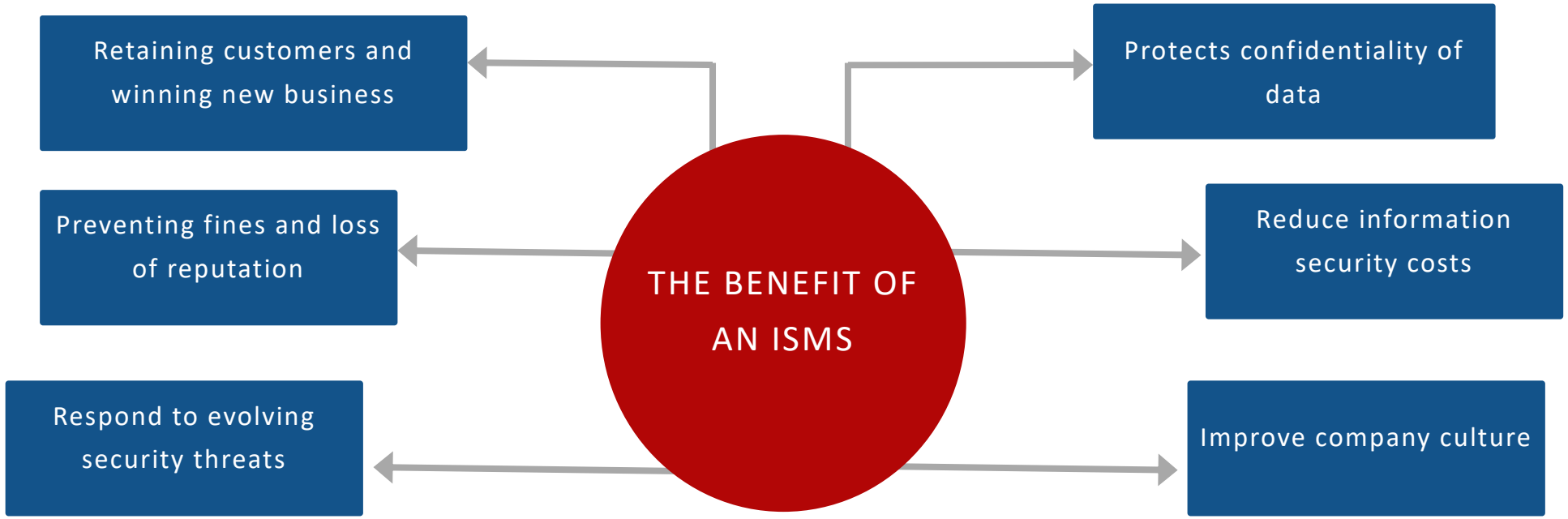
Third-party risk

legal consequence

9

جامعة الحسين التقنية
Al Hussein Technical University

THE BENEFIT OF AN ISMS



جامعة الحسين التقنية
Al Hussein Technical University

HOW DOES AN ISMS WORKS?

جامعة الحسين التقنية
Al Hussein Technical University

Project Mindset

Implementing ISMS is a Project (takes around 6 months depend on the organization)

The Project plan of the organization is completed prior to the establishment of a project dedicated to the ISMS, as well as phases of monitoring and improvement are activated only when the location of system components has been finalized. In each phase, it is usual that security controls are also implemented sequentially .

We will integrate the ISMS into existing processes.

We will Involve all the stakeholders in the organization.

Grant support from your management

جامعة الحسين التقنية
Al Hussein Technical University

Steps for ISMS

Planning

-Understanding the organization
-Leadership and approval of the ISMS project
ISMS scope
- Information security policies
- Risk management process
- Organizational structure of information security
- Statement of applicability (SOA)

Implementation

- Design of security controls (P&P)
- Implementation of security controls
- Document management process
- Communication plan
- Training and awareness plan
- Operations management
- Incident Management

Monitoring

-Monitoring, measurement, analysis and evaluation
- Internal audit
- Management review
- Treatment of problems and non-conformities
- Continual improvement

جامعة الحسين التقنية
Al Hussein Technical University

A Standards Approach to Building An Information Security Management System (ISMS)

Building ISMS using a recognized standard, such as ISO 27001, can help organizations ensure that their ISMS is comprehensive, effective, and meets industry-specific requirements and best practices.

ISO 27001 is the international standard for creating and maintaining an ISMS and provides a set of guidelines and requirements for establishing, implementing, maintaining, and continually improving an ISMS. It covers a wide range of information security controls, including physical, technical, and organizational measures. It helps organizations identify and assess their information security risks and implement mitigation controls.

With ISO 27001, organizations can achieve certification that their ISMS meets the highest regulatory standards. Some organizations will only work with companies that can demonstrate they have been certified to ISO 27001 or other approved frameworks.

جامعة الحسين التقنية
Al Hussein Technical University

Reference

- Alexander, D., Finch, A., Sutton, D. and Taylor, A. (2020) Information Security Management Principles BCS. 3rd edn. BCS The Chartered Institute for IT.

- Calder, A. and Watkins, S. (2019) IT Governance: An International Guide to Data Security and ISO27001/ISO27002. 7th edn. Kogan Page.

- Chapple, Mike - CISSP Official Study Guide (2021, Sybex). 9th edn.