Cyber Security Assessment
and Management
Bruno Sousa, bmsousa@dei.uc.pt
2024/2025

Assignment #1
Risk Management

November 01th @ 23:59 (soft deadline)

OBJECTIVE:

Understand the process of analyzing, evaluating, and planning risk management activities. **This assignment can be done individually or in groups of two.** Parts of the exercise are identified as specific for groups of two.

CONTEXT:

Following the risk management frameworks and methodologies discussed in the classes, define a risk management plan for a retail company. The company has multiple stores, geographically distributed in different countries, and a management and control center responsible for supply chain operations and centralized information storage. Additionally, the company also provides a delivery service. The clients purchase the products using a web application and the closest store that can assure the delivery provides the service. A high-level architecture of the system is presented in the figure.

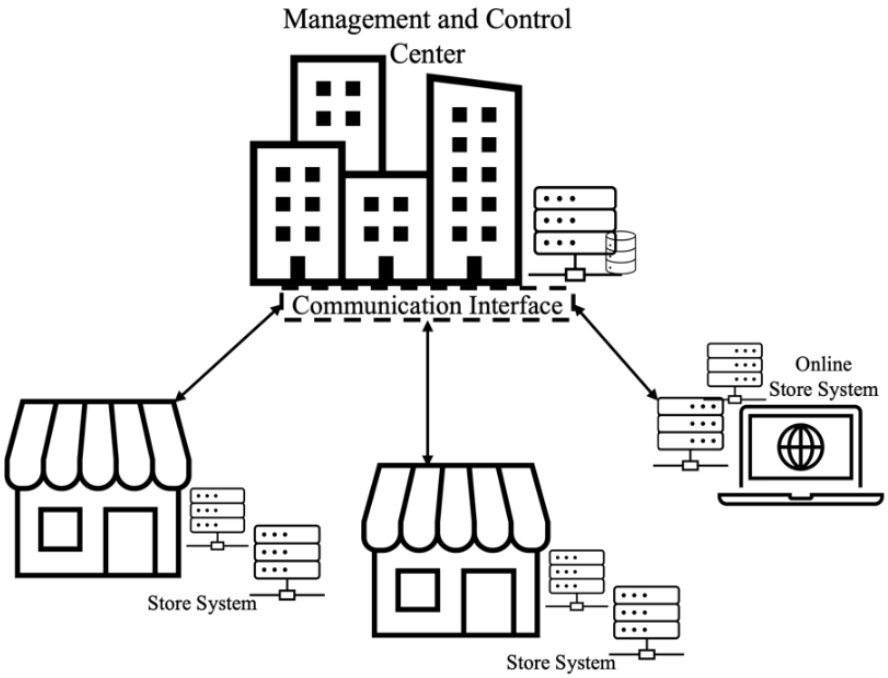

Figure 1 - High-level architecture of the company store.

The system to be considered handles the following set of functionalities:

- Business information storage and sharing
- Supply chain support to multiple stores in different countries

- Stock and delivery management **(for groups only)**
- Supplier' information storage (e.g., delivery method, type of goods, etc) **(for groups only)**
- Clients' information storage (e.g., payment data, delivery addresses, etc)
- Employee information: managers, technical personnel, and other staff
- Promotions information (e.g., start and end of campaigns, discount rates, conditions)

Besides the computer system necessary to implement those functionalities, you should consider the management of the physical assets required in your analysis. Whenever you make relevant assumptions, you should clearly state them.

Your risk management plan shall include the following steps:

1. **System categorization**, including system description, boundaries definition, and the risk tolerance (or risk appetite) analysis:
    a. you should assume that the organization already has in place some security measures and policies that contribute to an initial organizational structure that is ready to withstand attacks against the system.
    b. during the system categorization and description, you should describe an initial structure that already considers some security mechanisms, policies, and controls (e.g., network segmentation, access control policies, etc.).
2. **Risk identification and assessment**, including asset valuation, threat assessment, vulnerability assessment.
3. **Risk control strategies**, including examples of security controls to implement, and a monitoring and re-assessment plan.

While the first step should consider multiple stores, each with on-premises systems, to avoid repetitive tasks, steps 2 and 3 **should consider only one of those stores** and cover all the assets and controls necessary to implement the listed functionalities.

After the risk management analysis is completed, discuss how a malicious attack on the management and control center would affect the normal operation of the stores and how the controls and security measures implemented would help reduce its impact. The analysis should consider **at least two scenarios** regarding the magnitude of the intrusion resulting from the attack.

This analysis should include the following information:

- Security properties that can be affected with the attacks;
- The possible impact on the business (e.g., consider easiness of performing such attacks);
- The risk for the organization and **at least two** countermeasures that can mitigate the risk.

For groups: the online store of the company should also be covered during the risk management analysis. This includes all three phases (system categorization, risk identification and assessment, and risk control) of the process. The analysis should consider the stock information and online delivery management infrastructure, and the suppliers information.

DELIVERABLE:

A detailed report on the process conducted to define the obtained risk management plan and discussion on the attack on the management and control.

The report must also include information regarding the approach that was followed for risk assessment, and the limitations of the approach and how it could be improved/enhanced.

READINGS:

- Slides of theoretical classes
- Whitman, M., & Mattord, H. (2017). Principles of Information Security (6 ed). Cengage Learning. **(Chapter 5)**
- Schumacher, M., Fernandez-Buglioni, E., et al (2006). Security Patterns: Integrating security and systems engineering. John Wiley & Sons. **(Chapter 6)**
- NIST SP 800-39, Managing Information Security Risk Organization, Mission, and Information System View