Assignment Week 2 – ISO 27002

Master – Cyber Security and Resilience

Group 4 - St. Pölten University of Applied Sciences

Flita-Vasile Adrian – cr221504

Adithyan Shyni Manoj – cr221506

Rakesh Vijayan – cr221515

Alen Marian Varkey Vanisseril– cr221509

Course: Information Security Management

Lecturers: Peter Schoenegger, Simon Tjoa

Semester: WS 2022

St. Pölten, 19.10.2022

Topic: Security Awareness

NOTE: For the Slides set, please refer to File "ISM_Group_4_Assignment_Week_2_ISO_27002_Security_Awareness_Presentation.pptx".

Topic: Asset Management / Asset Clustering

On college and university campuses, asset tracking has undergone a complete transformation. Higher education institutions are realizing that providing great physical and virtual resources that fulfill their students' learning needs will help to ensure the sustainability of the college and contribute to the success of their students. There are many more resources available to employees, instructors, and students than just a computer and a printer. And here is where having an asset tracking and management platform can help with asset management.

Something that has worth for a company is referred to as an asset. The value, whether it be a computer, piece of sporting equipment, car, or dormitory furniture, and its shape, rely on the organization and its stakeholders. The management of numerous assets, structures, and pieces of equipment is under the purview of colleges and universities. These resources could be dispersed across numerous buildings on a single campus or in various places off-campus. Regardless of where these assets are, they need to be monitored and cared for. To ensure that the assets are continually usable and do not disrupt the learning environment, this also entails keeping up with service requests and maintenance schedules.

Inventory of the assets that are security-relevant:

- Laboratories equipment
- Servers
- Online platforms
- IT department equipment
- Students and Staff cards

Ownership of assets:

- Laboratories equipment should only be used by the students of the University, Teachers and only if there is an emergency by the IT department.
- Servers must be used only by the authorized personnel.
- Online platforms must be used only by the employees of the University.
- IT department equipment must be used only by the members of the department
- Students and Staff cards must be use by the people they are assigned to.

Acceptable use of assets:

- Laboratories equipment must not be used at home and should be used only for educational purposes.
- Servers are must not be used at home and should be used only for educational purposes and hosting online activity of the university.
- Online platforms are used to keep a connection with employees and for educational purposes (e.g. study at home).
- IT department equipment are used for creating a secure educational environment for all of the university employees and some.
- Student and staff cards must be used only if students want to study independently and use university resources when they finished their courses.

Return of the assets

- Online platforms access is restricted after the employees leave their jobs and for students also when they finish their studies.
- IT department equipment must be handled back after leaving the job place.
- Students and staff cards must not be available after leaving the job of finishing the studies.

The CISO benefits of the ability to:

- compile accurate information about assets to analyze performance
- schedule preventative maintenance
- download reports in a digital format to a computer, smartphone or tablet
- customize reports to see data that is most important to him/her.
- access a cloud-based platform that is accessible anytime, from anywhere
- know the history and changes to an asset, whether it was an update to the cost or depreciation or whether a classification or field was added
- meet audit requirements

All the assets mentioned above have a direct link with the scope of the organization and with their protection and accurate risk management the university could provide education in a safe way.

Topic: Security zone concept

The physical situation of St. Poelten University of Applied Sciences includes University Assets such as University Campus, University Buildings etc. Which are Located at Campus-Platz 1, 3100 St.Poelten.

The Infrastructure Includes:

- Five lecture halls with room for up to 215 people
- 24 seminar rooms
- Ten multimedia labs
- Seven computer rooms
- An assembly hall for up to 500 people
- A canteen that seats approximately 170 persons
- 225 parking spaces
- A library with roughly 50,000 items

For this infrastructure The St. Poelten University of Applied Sciences has Implemented the Following Security Facilities for Physical Security:

Lights
Flickering lights may not be placed at the top of your security priority list, but it is a minor detail that can greatly impact the occurrence of crime on campus. Well lit areas are proven to reduce crime rate, and also are necessary to obtain good security footage from existing security cameras.

Access Control Systems
It can be difficult to keep track of who is entering and exiting college buildings. With access control systems, only those with an authorized card or fob would be able to access secured areas.

Security Cameras
Monitored security cameras can prevent crimes from happening in the first place. If an incident occurs, they also provide an opportunity to gather evidence to understand the event, and prevent it from happening again.

Reinforce Doors & Windows
Security lights, cameras, on-campus police and access control systems all have their place in a well-rounded security plan. However, these security measures overlook the event of forced entry and need to provide a physical barrier to prevent break-ins.
Riot Glass, Inc's new Gen II framing system is designed to be easily implemented on existing glass structures. This system is an affordable way to strengthen your windows and glass doors with almost no visible change.

Smoke detection and fire prevention system
A smoke detector is an electronic fire-protection device that automatically senses the presence of smoke, as a key indication of fire, and sounds a warning to building occupants. Commercial and industrial smoke detectors issue a signal to a fire alarm control panel as part of a building's central fire alarm system.

Hardware Firewall
A hardware Firewall is a physical appliance that is deployed to enforce a network boundary. All network links crossing this firewall, which enables it to perform inspection of both inbound and outbound and outbound network traffic and enforce access controls and other security policies

Topic: Supplier Relationship

Suppliers are used for two main reasons

1. You want them to do work that you have decided not to do internally.
2. You can't easily do the work as well or as cheaply as the suppliers.

In the policy, the University should identify and require information security controls that specifically address external parties gaining authorized access to the organization's information (contractors, service providers). Controls should also specify the processes and procedures to be followed when third-party contractors work within the University or when service provider/hosting arrangements exist.Suppliers should be managed throughout the lifecycle of a relationship with them, from initial contract and security review to monitoring SLAs and performance agreements once they are engaged to perform services and/or provide solutions.

Hardware / Equipment

Firewall/Routers

Firewall can me Hardware firewall or Software Firewall
By choosing Cyberbrom, Ciso ASA 5505 like hardware firewall Wenders needs to Ensure the provided system can handle the concurrency load and service leave agreement to upgrade or replace if the suggested devices do not meet the requirements. Audits, Compliance, Service levels, Service Capacity everything needs to monitor and review by the supplier

Switches
Example : S3900-48T6S-R - 48-Port Gigabit

- Switches are chosen based on the level of security and capability to manage vlan etc stated by the supplier, which is legally binding through the purchase / Service Level Agreement with the supplier (Information Classification / Rules of Engagement).
- The supplier must ensure that the product meets the specifications.
- If the supplier declares that its products meet certain security standards, these standards ensure a certain level of security.

- Audits, Compliancequirement.
- If the university relies on cloud instances, the cloud server authority may ensure that a security breach does not occur on the physical server itself and that no data is lost.

Fire extinguisher

Example : Amerex B500 5lb ABC Fire Extinguisher

- As per the contract from the university supplier should recommend and ensure the quality of the fire extinguisher placed in the university datacenter.
- Supplier should do a training class for each staff how to use the fire extinguisher

Fire Alarm

Example : ekey set IN 2.0 E DRM 1

- As per the university service level agreement should be placed between university and supplier.
- Suppliers should periodically check and ensure the devices are in good condition in the service level agreement.

Software :

Operating system

Operating system (Microsoft / Red Hat / Suse Linux)

- Service level agreement and security level should be signed with Microsoft operating system license purchase from the supplier
- Service level agreement supplier responsibility to update the new version release and knowing the changes to the university.
- Supplier should arrange the training to the staff at the level of new major update in UI level
- If the open source Operating used in university server admin should update himself and get attend the training from the open source programs.

Library management System

Example : ResourceMate, Koha

- Suppliers should be aware of the limitation and capacity of the software. Suppliers should sign the service level agreement, maintain the relation by sharing knowledge and make the bug fixes in software.
- For the open source software employee level education and training should be content to meet the gnu level agreement.

Erp Softwares:
Example Geniuserp:

The service provider agrees to perform and complete the following IT support services in a professional and timely manner, including maintenance, checkup, and update.

- Install, monitor, and maintain the software, as well as its systems, applications, codes, and programs;
- Meet and exceed the client's customer service expectations by being responsive and accommodating.
- Conduct monthly inspections to ensure that the software is up to date and efficient.

Access control; Particularly for sensitive information, precise definition, management, and monitoring are required. Awareness training for both internal and external staff who handle or interact with this data is required.

Topic: Control design and measurement of effectiveness

Policies for Information Security
Control
A set of information security policies should be defined, approved by management, published, and distributed to employees and relevant third-party stakeholders.
Implementation
Information Security policy shall be created and improved following the PDCA cycle. This policy must adhere to all applicable laws, regulations, and standards. It is also consistent with Universities' business objectives and is based on the current information security threat environment. The information security policy defines a) the ISMS's segmented areas and how information security is approached in these areas, as well as b) the ISMS's roles and responsibilities.

Management Responsibilities
Control
Management should require all employees to use information security in accordance with the ISM that has already been implemented.
Implementation
Management should demonstrate its support for the information security policy, procedures, and controls. Before granting access to an organization's confidential data, information security roles should be defined. And they should be provided with the information security expectations of the University. Employees and students should achieve a level of awareness regarding their role in the organization. Compliance with employment, contract, or agreement terms and conditions, including the organization's information security policy and appropriate working methods.

Threat Intelligence

Control

To generate threat intelligence, information about information security threats should be collected and analyzed.

Implementation

Information about existing and emerging threats is collected and analysed for performing informed actions to prevent the threats from causing harm to the organization, so that the impact of threat can be reduced.

Information Transfer

Control

For all types of transfer facilities within the organization and between the organization and other parties, information transfer rules, procedures, or agreements should be in place.

Implementation

The organization should develop and communicate to all relevant interested parties a topic-specific policy on information transfer. The classification of the information involved should be reflected in the rules, procedures, and agreements to protect information in transit. Transfer agreements should be established and maintained where information is transferred between the organization and third parties to protect information in all forms in transit.

Disposal of unused data

Control

Unused data should be disposed seculey when no longer required.

Implementation

A process is defined for securely disposing of unused data based on the classification of the information contained within it. An external contractor with the necessary certifications could carry out this process. The disposal of each piece of sensitive media must be documented.

.