Name : Rizqi Zamzami Jamil

Class : SIB-4C

NIM : 2141762089

Lab - Security Controls Implementation

Objectives

- **Analyze security needs of an organization.**
- **Recommend security controls based on organizational needs.**

Background / Scenario

In this lab, you will recommend security controls based on the needs of the Greenville Public School system.

The school system consists of one high school, one middle school, and three elementary schools. The district serves about 2500 students, has a staff of 210 teachers, 220 administrators and support staff, and 25 maintenance staff. The internet point of presence and data center is housed in the high school, which also houses the administrative offices. The schools are interconnected to the high school over a redundant fiber optic network. The data center houses all of the required servers in one location.

Your company has been hired to analyze the physical security and cybersecurity of the Greenville school system. An incident recently occurred in which a high school student obtained a teacher's credentials and logged into the administrative network. The student altered his grades, deactivated CCTV cameras, and obtained phone numbers for students.

The director of security for the district recently left her job and the position had not been filled. Security had been implemented by a number of consultants and employees and had not been well documented. Your tasks is to propose security controls that should be implemented and analyze the current system to see if it utilizes those controls. The superintendent and school board have compiled the following list of security concerns. You will use as a starting point for your analysis:

- A wide range of computers, with aging hardware and software, are located haphazardly throughout the district, many in classrooms and learning labs.
- Some school districts nationally have faced lawsuits due to loss of parental information because of data breaches.
- Another school district in the state had to shut down until systems were restored after a ransomware attack encrypted data held on a number of computers in the district network.
- Academic records have been accessed and altered by students.
- A parent who was not authorized to see his child gained access to an after-school activity on school grounds that the child attended.
- The library server in the data center had been unplugged by cleaning staff in the past.
- Student information was disclosed by an administrative employee in response to a malicious email.

Required Resources

- Device with internet access

Instructions

Part 1: Review security controls

Review the definitions of the security control types and functions below.

Security controls can be divided into three types:

1. **Physical security controls** - implemented to control physical access to people, equipment,

facilities, and information.

2. **Technical security controls** - implemented to protect hardware and software systems and the information that these systems transmit, process, or store.
3. **Administrative security controls** - are policies, procedures, rules, and guidelines that are followed by personnel in order to achieve the security goals of an organization.

Security controls are viewed as having three functions:

1. **Preventive** - stop security threats from occurring
2. **Detective** - identify unauthorized activity
3. **Corrective** - address unwanted activity by restoring systems to normal CIA status

Part 2: Complete a security controls grid

You will now complete the grid by recommending specific measures for each of the empty boxes in the grid. You will recommend both general security and cybersecurity measures, systems, or activities. Assume that the school district has no security in place at the present time.

Record your answers in the table below:

	Preventive	**Detective**	**Corrective**
Physical Controls	**Answer** 1. Access card systems 2. Door locks and security gates 3. Fencing around perimeter 4. Secure server rooms with restricted access 5. Security barriers at entry points 6. 6. Proper lighting systems	**Answer** 1. CCTV surveillance systems 2. Motion detectors 3. Security guards on patrol 4. Visitor logs and check-in systems 5. Environmental monitors (temperature, humidity) 6. Access attempt logs	**Answer** 1. Backup power systems 2. Spare equipment storage 3. Equipment repair services 4. Alternative facilities 5. Emergency response equipment 6. Physical damage repair procedures
Technical Controls	**Answer** 1. Firewalls and network segmentation 2. Antivirus software 3. Data encryption 4. Strong password requirements 5. Multi-factor authentication (MFA) 6. Access control systems	**Answer** 1. Intrusion Detection/Prevention Systems (IDS/IPS) 2. Log monitoring systems 3. Network traffic monitoring 4. Security audit tools 5. File integrity monitoring 6. User activity monitoring	**Answer** 1. System backups and recovery 2. Disaster recovery plans 3. System restoration procedures 4. Incident response plans 5. Data recovery tools 6. System rollback capabilities
Administrative Controls	**Answer** 1. Security policies and procedures 2. Regular security awareness training 3. Background checks for employees 4. Access management procedures 5. Change management policies 6. Acceptable use policies	**Answer** 1. Regular security audits 2. Performance reviews 3. Activity reports and monitoring 4. Compliance monitoring 5. Security assessments 6. Policy violation monitoring	**Answer** 1. Incident response procedures 2. Business continuity plans 3. Disaster recovery procedures 4. Employee disciplinary procedures 5. Policy review and updates 6. Security awareness retraining

Blank Line, No additional information

Reflection Questions

1. Why are preventive physical controls important in schools?

Answer:
Preventive physical controls protect students, staff, and assets by blocking unauthorized access and ensuring a safe learning environment.

2. What preventive administrative controls are most effective against social engineering, including vectors that spread ransomware?

Answer:
Effective controls include security awareness training, clear procedures, phishing simulations, and verification protocols to prevent unauthorized access and malware spread.

3. What is essential to preventing lasting damage from ransomware attacks while saving money on ransomware payments for restoration of data?

Answer:
Regular, secure data backups and tested restoration processes are essential to recover data without paying ransoms.