# Nama : Winda Umi Fatimatus Sa’diyah

# NIM : 2141762055

# Absen : 19

# 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** | - Install access control systems (e.g., key cards, biometric scanners) to restrict entry to buildings.<br>- Use security cameras in critical areas like entrances and hallways.<br>- Install sturdy locks and security barriers for server rooms and data centers. | - Deploy motion detectors and video surveillance systems with real-time monitoring to identify unauthorized access.<br>- Conduct regular patrols or use security personnel for random checks. | - Develop and practice emergency response plans for physical security breaches.<br>- mplement a rapid repair or replacement strategy for damaged security equipment. |
| **Technical Controls** | - Use firewalls and intrusion prevention | - Monitor network traffic using | - Create a robust data recovery plan |

| | | | |
|---|---|---|---|
| | systems (IPS) to block unauthorized access.<br>- Implement endpoint protection and antivirus software on all devices.<br>- Enable multifactor authentication (MFA) for accessing critical systems. | intrusion detection systems (IDS) and log analysis tools to identify anomalies.<br>- Employ real-time alert systems to notify IT staff of potential breaches. | that includes regular system backups.<br>- Use automated patch management to quickly address vulnerabilities and prevent re-exploitation. |
| **Administrative Controls** | - Develop and enforce an information security policy that outlines user responsibilities.<br>- Provide comprehensive security training for staff and students to raise awareness of social engineering and phishing scams.<br>- Implement access management policies to limit permissions based on role. | - Conduct regular security audits and risk assessments to identify gaps in procedures.<br>- Use incident reporting mechanisms to document and evaluate security events. | - Establish an incident response team to handle breaches or attacks.<br>- Perform post-incident reviews and update policies and training based on findings to improve future responses. |

*Blank Line, No additional information*

Click **Show Answer** to show an example answer.

| | **Preventive** | **Detective** | **Corrective** |
|---|---|---|---|

| | | | |
|---|---|---|---|
| Physical Controls | • locked buzzer access to school buildings<br>• admin only access to data center and network facilities<br>• sprinkler systems<br>• panic button alarms<br>• backup power for critical systems<br>regular equipment maintenance | • CCTV monitoring<br>• door, window, and motion sensor alarms<br>• smoke detectors<br>• vulnerability assessment and PenTesting<br>• outdoor lighting | • repair of physical damage<br>• rapid replacement of damaged or malfunction critical equipment<br>• maintain spare parts inventory<br>• reissue lost badges and access cards<br>• temporary facility rental |
| Technical Controls | • network firewalls or IPS<br>• host-based firewalls and anti-virus<br>• multifactor authentication for access to sensitive data stores<br>• VPN access for work at home<br>• system hardening of networking devices<br>• encryption of student record data<br>• network application control<br>• comprehensive data and OS backup<br>• robust patch management<br>• card-based building access control<br>DNS proxy | • monitoring of access and other logs<br>• network security monitoring<br>• IDS functionality<br>• host log collection and analysis<br>• honeypots<br>• AAA or other logging\<br>• SIEM<br>• Network baselining and trend analysis | • patch management<br>• malware containment and removal<br>• data and disk image restoration from backup |
| Administrative Controls | • employee badging<br>• cleaning of data center and network facilities only under supervision<br>• registration of all guests and guest badging | • grade audits<br>• AAA log review | • continuity planning<br>• incident response planning<br>• incident response training<br>• forensic analysis<br>• post-incident user training |

| | Preventive | Detective | Corrective |
|---|---|---|---|
| | **● hiring special security staff**<br>**● password strength and renewal policies**<br>**● security awareness training for all personnel and students**<br>**● access control policies and groups based on role**<br>**● asset management policies and procedures** | | |

Blank Line, No additional information

## Reflection Questions

1. Why are preventive physical controls important in schools?

   - Preventive physical controls are crucial in schools as they help create a safe learning environment, ensuring the protection of students and staff from unauthorized access and potential harm. They also safeguard critical infrastructure, including computers and servers, from physical damage, theft, and tampering, which can disrupt school operations and compromise sensitive data.

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

   - Implementing robust security awareness programs and training sessions for both staff and students is vital to combat social engineering. Policies that establish clear protocols for verifying identities, avoiding suspicious links, and handling sensitive data can prevent attackers from exploiting human vulnerabilities. Regular simulations of phishing attacks and scenario-based training can also prepare individuals to recognize and respond to threats effectively.

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

   - Maintaining a thorough data backup strategy is essential. Regular, automated backups stored securely offline or in the cloud ensure that critical data can be restored without resorting to paying ransoms. Additionally, promoting centralized data storage practices and implementing versioning to keep multiple copies of files can minimize data loss and accelerate recovery after an attack.