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	• Locked buzzer access to school buildings • Admin-only access to data center and network facilities • Sprinkler systems • Panic button alarms • Backup power for critical systems • Regular equipment maintenance	• CCTV monitoring • Door, window, and motion sensor alarms • Smoke detectors • Vulnerability assessment and PenTesting • Outdoor lighting	• Repair of physical damage • Rapid replacement of damaged or malfunctioned critical equipment • Maintain spare parts inventory • Reissue lost badges and access cards • Temporary facility rental
Technical Controls	• Network firewalls or IPS • Host-based firewalls and anti-virus • Multifactor authentication for access to sensitive data • VPN access for work at home • System hardening of networking devices • Encryption of student record data • Network application control • Comprehensive data and OS backup • Robust patch management • Card-based building access control • DNS proxy	• Monitoring of access and other logs • Network security monitoring • IDS functionality • Host log collection and analysis • Honeypots • AAA or other logging • SIEM • Network baselining and trend analysis	• Patch management • Malware containment and removal • Data and disk image restoration from backup

	Preventive	Detective	Corrective
Administrative Controls	• Employee badging • Cleaning of data center and network facilities only under supervision • Registration of all guests and guest badging • Hiring special security staff • Password strength and renewal policies • Security awareness training for all personnel and students • Access control policies and groups based on role • Asset management policies and procedures	• Grade audits • AAA log review	• Continuity planning • Incident response planning • Incident response training • Forensic analysis • Post-incident user training

Reflection Questions

1. Why are preventive physical controls important in schools?

   Answer: They are necessary to protect students from physical dangers, prevent unauthorized access to facilities, and safeguard network and computer equipment from damage or theft.

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

   Answer: **User training** is the single most important preventive control for stopping social engineering attacks and preventing ransomware campaigns. Regular security awareness and phishing simulations are also highly effective.

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

   Answer: A **comprehensive backup program** with reliable and frequent data backups is crucial. Ensuring that staff store their work on secure, network-based servers rather than local machines also helps in preventing data loss in the event of an attack.