

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 task 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

****TASK 1****

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:

****ANSWER****

	Preventive	Detective	Corrective
Physical Controls	<ul style="list-style-type: none"> • Lock buzzer access to school building • admin only access to data center and network facilities • panic button alarms 	<ul style="list-style-type: none"> • CCTV monitoring • door, window, and motion • sensor alarms 	<ul style="list-style-type: none"> • Repair of physical damage • rapid replacement of damaged or malfunction critical equipment • maintain spare parts inventory
Technical Controls	<ul style="list-style-type: none"> • network firewalls or IPS • host-based firewalls and anti-virus • multifactor authentication for access to sensitive data stores • encryption of student record data • network application control • comprehensive data and OS backup • robust patch management 	<ul style="list-style-type: none"> • monitoring of access and other logs • network security monitoring • IDS functionality • host log collection and analysis • using SIEM tools 	<ul style="list-style-type: none"> • patch management • malware containment and removal • data and disk image restoration from backup
Administrative Controls	<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • grade audits • log review 	<ul style="list-style-type: none"> • continuity planning • incident response planning • incident response training • forensic analysis • post-incident user training

****TASK 2****

Reflection Questions

****QUESTION 1****

1. Why are preventive physical controls important in schools?

Because it helps to prevent physical security breaches and also it is important to protect students from physical danger.

****QUESTION 2****

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

User and Employee training is the single most important preventive control for stopping social engineering attacks and preventing the ransomware campaigns.

****QUESTION 3****

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

Data backups of files and records are essential to prevent lasting damage from ransomware attacks.