Name : Selly Amelia Putri

Class : SIB 4C

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 access to buildings with a buzzer system - Restricted access to data centers and critical areas - Panic button alarms - Fencing and secure perimeters	- CCTV monitoring - Door, window, and motion sensors - Smoke detectors - Security patrols and monitoring	- Repair or replacement of damaged physical security equipment - Reissuance of lost badges and access cards - Maintenance and rapid replacement of malfunctioning equipment - Facility rental in case of severe damage to primary facility
Technical Controls	- Firewalls (network-based and host-based) - Anti-virus and anti-malware tools - Multi-factor authentication (MFA) for sensitive data - Encryption for sensitive student and staff records	- Log monitoring and analysis - Intrusion Detection Systems (IDS) - Security Information and Event Management (SIEM) - Network baseline analysis and anomaly detection	- Malware containment and system restoration - Patch management to resolve vulnerabilities - Data restoration from backups - Remediation and strengthening of systems post-incident
Administrative Controls	- Security awareness training for staff and students - Defined access control policies for staff roles - Regular policy updates and password policies - Asset management procedures for tracking equipment	- Regular audits and access log reviews - Monitoring and auditing of grading systems - Regular policy compliance checks - Regular risk assessments	- Incident response and recovery planning - Conduct forensic analysis post-incident to identify causes - Post-incident training to prevent future occurrences - Continuous improvement plans for security policies

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

	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 malfunction 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 stores = 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?

   Preventive physical controls are crucial in schools because they help create a safe and secure environment by reducing the risk of harm to students, staff, and school property. These controls:

   - Protect Students and Staff: By restricting unauthorized access, preventive physical controls help keep potentially dangerous individuals out of the school, safeguarding students and staff from physical threats.
   - Secure Valuable Equipment: Schools often house costly technological equipment, including computers and network servers. Physical controls like locked doors and surveillance reduce the likelihood of theft or damage to these assets.
   - Prevent Disruptions to Learning: When the school environment is secure, students and staff can focus on learning and teaching without safety concerns, contributing to a more productive educational atmosphere.
   - Support Cybersecurity Efforts: Protecting physical access to sensitive areas, such as data centers, is a foundational step in protecting digital assets from unauthorized access, which can be as crucial as virtual protections.

They are necessary to protect students from physical dangers, and to protect network and computer equipment from damage or theft.

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

   User training is indeed one of the most effective preventive administrative controls against social engineering attacks and ransomware. Additionally, these administrative controls can further strengthen a school's defenses:

   - Security Awareness Training: Regular training sessions that educate staff and students about social engineering tactics, such as phishing, baiting, and pretexting, are crucial. This helps individuals recognize suspicious emails, messages, and websites.
   - Clear Security Policies: Establishing comprehensive security policies, such as guidelines for handling sensitive information, data-sharing protocols, and acceptable use policies, helps to reinforce safe behaviors and reduce risks.
   - Strong Password Policies: Implementing policies that require strong, unique passwords and regular password updates helps prevent unauthorized access, which is often exploited in ransomware attacks.
   - Access Control and Role-Based Permissions: Limiting access to sensitive data and critical systems based on job roles reduces the potential attack surface for social engineering attacks, as only essential personnel have access to sensitive information.
   - Regular Phishing Simulations: Conducting periodic phishing simulations to test and reinforce training can help identify individuals who may need additional support and reinforce caution in digital interactions.
   - Incident Response Planning: Establishing a clear incident response plan ensures that staff know what steps to take if they suspect they've fallen victim to social engineering or ransomware. Quick response can limit damage and aid in recovery.

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

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

   Absolutely, a comprehensive data backup program is essential in mitigating the impact of ransomware attacks and avoiding costly payments. Here are the key practices to ensure effective prevention of lasting damage from ransomware:

   - Regular and Reliable Backups: Establish a consistent schedule for backing up all critical data to ensure that recent versions are always available. This reduces data loss if a ransomware attack occurs.
   - Offsite and Offline Backups: Store backups offsite and offline (isolated from the main network) to protect them from being encrypted by ransomware that may spread across the network.
   - Encouraging Network-Based Storage: Encouraging or requiring staff to save their work on centralized network servers rather than on local machines minimizes the risk of losing data stored only on personal devices.
   - Automated Backup Verification: Regularly verify the integrity of backups to ensure they are complete, accurate, and not corrupted. Automated testing can help confirm that backups will work correctly when needed.
   - Data Recovery Drills: Periodically run data restoration exercises to test the backup system's effectiveness and ensure a smooth recovery process. This prepares the team to act quickly in a real incident.
   - Access Controls for Backups: Limit access to backup systems to reduce the risk of backups being compromised. Only authorized personnel should be able to access and modify backup data.
   - Versioned Backups: Maintain multiple versions of backups, so if recent versions are corrupted or encrypted, previous uncorrupted versions can be restored.

A comprehensive program of reliable data backups will be very helpful. Encouraging or compelling staff to save there work on network servers, rather than locally, will also help prevent data loss.