Data Center Security Plan

Christopher D. Contreras

California State University, Fullerton

College of Engineering & Computer Science

CPSC 253: Cybersecurity Foundation and Principles

Professor Michael Franklin

April 10, 2025

Background and Purpose

This paper aims to create a security plan to secure and protect both ACME College data centers adequately. ACME College currently has budget and space limitations, which causes them to use the research data center as a backup to their business data center. Due to recent events indicating possible security breaches, ACME is fully committed to protecting and securing its data by justifiable means. This plan will implement aspects that cover administrative, technical, and physical controls to reduce security risks.

Administrative Controls

For any organization to have reasonable security policies and procedures, they must be implemented to guide action or behavior that can lead to security breaches. Therefore, proactively enhances security in an organization and reduces risk. In NIST public 800-53 Revision 5 section, they state the following, "Policies and procedures contribute to security and privacy assurance. Therefore, security and privacy programs must collaborate on the development of [these] policy and procedures." (SP 800-53 Rev. 5) Furthermore, the implementation of proper role control is necessary to ensure that unauthorized individuals can affect aspects that concern confidentiality, integrity, and availability. The Information Security Risk Management for ISO states, "The protection of information and associated assets – information security – is therefore overtaking physical asset protection as a fundamental corporate governance issue. The responsibility for information security in an organization must be clearly defined, and the roles and responsibilities of all staff must be clearly understood." (Calder & Watkins, 2010, p. 25).

Policies and Procedures

- *Role-Based Access Policy*

- Clearly defines who gets access to which system and why.
- It prevents anyone from having access to the business or research system based on their job title.

- *Acceptable Use Policy*
  - This ensures no misuse of research and business systems, including the equipment.
  - Set behavioral rules regarding students, faculty, and anyone granted access to the data center.
- *Security Awareness Training*
  - Educates the user on the importance of securing the data center and how they can implement that information into their role.
  - It helps reduce leaving the door open or unauthorized logging.
- *After-Hour Access Procedure*
  - Anyone needing access to the data center after hours must have preapproval, sign in, log in, and state their purpose.
  - This controls and documents unexpected after-hours visits.
- *Incident Response and Reporting Policy*
  - Provides a proper way to report any suspicious activity or security breaches.
  - Ensure that any sign of breach has been handled correctly in terms of investigation and resolution.

Role and Responsibilities

- *Data Center Manager*
  - Responsible for overseeing security development and managing the day-to-day.

- Implements access controls and coordinates with security regarding access during the day and after hours.

- *Faculty and Research Staff*
  - Use the system for authorized purposes only.
  - Follow policies and may request access to systems with proper justifications.
- *Security Guards*
  - Monitor physical access to the data center 24/7
  - Maintain security logs and respond to unauthorized access alerts.
  - Requires security guards to do multiple walks through the entirety of their shift

Technical Controls

An organization's framework is an essential part of security and focuses on protecting its systems, network, and data through technological measures. Despite not usually being used to prevent physical measures like armed robbery, it's part of the security aspect, but it is more about internet security. In network security, as IBM stated, "Network security is the field of cybersecurity focused on protecting computer networks and systems from internal and external cyber threats and cyberattacks." (IBM, n.d.). Therefore, it assists with protecting the work environment and operating systems. The NIST describes systems as follows: "System security requirements define the protection capabilities provided by the system, the performance and behavioral characteristics exhibited by the system, and the evidence used to determine that the system security requirements have been satisfied." (NIST, n.d.). Furthering the idea of protecting the data center, which ACME College views as a company asset.

Network Security

- *Firewall Configuration*

- Blocks internal and external traffic.
- Protect the data center from inbound and outbound traffic.

- *Intrusion Detection and Prevention System*
  - Monitor for suspicious activity throughout the entire network.
  - It helps with blocking and preventing threats.
- *Encrypted Network Traffic (TLS/SSL)*
  - Used to transmit data in transit, especially since it is a backup data center.
- *Network Access Control*
  - It prohibits devices and users from connecting to the network if they are not authorized.
  - Prevents unmonitored devices from gaining access.
- *Virtual LAN(VLAN)*
  - Separates the research systems from business systems while being on the same network.
  - Mitigates the lateral movements when a breach occurs.

System Security

- *Multifactor Authentication (MFA)*
  - Adds a second layer of verification when accessing a sensitive system (business data)
  - Reduces the risk of unauthorized access, even if they have internal credentials
- *Patch Management and Automatic Updates*
  - Allows the system to be up to date with new security patches
  - Reduces attacks that are known to work on older models
- *Audits Logging and Log Review Tools*

- Tracking who logs in and what's going on in systems allows for suspicious behavior to be detected

Physical Control

For any organization, the first line of defense is established by physically restricting access to a sensitive area, usually mitigating risk by preventing damage. Usually, physical control will deter any physical threats and prevent them from causing break-ins or thefts. The US Army describes it as, "Physical security describes security measures designed to deny unauthorized access to facilities, equipment, and resources and to protect personnel and property from damage or harm (such as espionage, theft, or terrorist attacks). Physical security involves using multiple layers of interdependent systems, including CCTV surveillance, security guards, protective barriers, locks, access control, perimeter intrusion detection, deterrent systems, fire protection, and other systems designed to protect persons and property." (Department of the Army, 2001, p. 1-1). Through these forms of physical control, an organization can prevent breaches, affecting what the CIA triads stand for.

Access Controls

- *Security Guards*
  - On-site personnel will monitor and respond to any suspicious activities.
  - It is essential to ensure everyone follows the policies and procedures through supervision.
- *CCTV Cameras*
  - They are positioned in every area to monitor everything in real time and after any incident.

- It is essential to learn from mistakes and improve the areas where security weakness is seen.

❖ *Facial Scanner*

- Biometrics access is required to enter the data center room, as it is a valuable asset.
- It is tough to manipulate a biometric scanner.

❖ *Badge Swiper*

- Some form of access control is required for all the rooms around the data center, which still presents a strong form of security that limits access.

❖ *Entrance logs*

- It requires anyone who enters to record whether they came in and whether they work at the facility or not. This allows for monitoring who comes in day-to-day.

Physical Security Measures

❖ *Bollards at Main Entrance*

- It prevents any vehicle from crashing into the building and causing any infrastructural damage.

❖ *Motion Sensors*

- Alerts security guards when any unauthorized movements happen during the day and after hours.

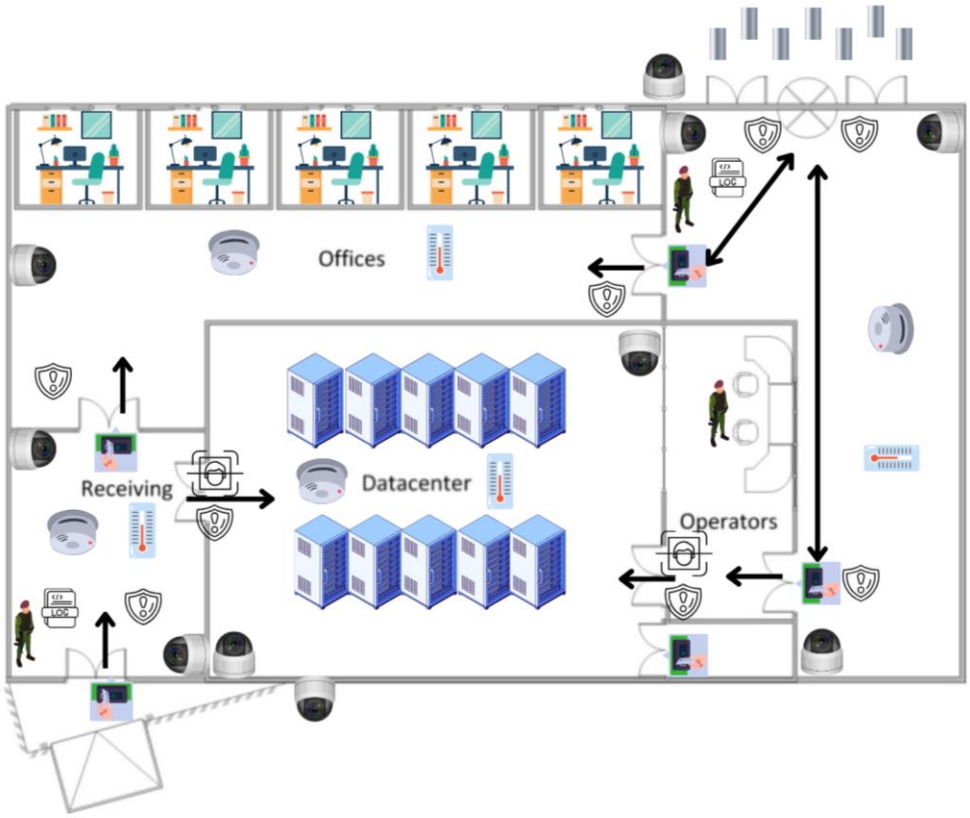
❖ *Environmental Controls*

- Smoke detectors and temperature detectors are installed throughout the building to ensure the safety of staff and data servers.
- Prevents any catastrophic event from occurring within the rooms.

Conclusion

Through administrative, technical, and physical control, ACME College will be able to create a fully secure data center by allowing access to its research data and protecting its critical business data, which allows for operational function. Overall, the security plan created is done through effective and trusted sources, which justifies why everything is needed and essential for security.

Data Center Layout



Reference

Calder, A., & Watkins, S. (2010). *Information security risk management for ISO 27001/ISO 27002*. IT Governance Publishing.

IBM. (n.d.). Network security: The practice of protecting networks and their components from cyber threats. *IBM*. https://www.ibm.com/think/topics/network-security

National Institute of Standards and Technology. (n.d.). System security requirement. *NIST Computer Security Resource Center*. https://csrc.nist.gov/glossary/term/system_security_requirement

National Institute of Standards and Technology. (2020). *Security and privacy controls for information systems and organizations* (SP 800-53 Rev. 5). *U.S. Department of Commerce*. https://doi.org/10.6028/NIST.SP.800-53r5

Department of the Army. (2001). *Physical security* (FM 3-19.30). *Headquarters, Department of the Army*. https://irp.fas.org/doddir/army/fm3-19-30.pdf