**Data Center Security Redesign**

Toan Tran

CPSC 253

Prof. Franklin

November 11, 2024

**Abstract**

Due to weak security policies and inadequate management at ACME College, the break-in occurs. A restructuring plan for the data center are urgently needed. The carryout strategy should be able to fulfill security requirements and provide improvement; a safer and more convenient place for the business environment and give enough resources for research activities even with tight budgets. With administrative, technical, and physical control, this redesign proposal shall detect and prevent various threats and possibly mitigate risks and

**Administrative Controls**

To maintain order and a uniform workplace, knowing policies and procedures is a must because it is a framework for any organization that sketches out requirements and provides guidelines for all work activities with the goal of smooth operation. Michelle Rossevelt's written article, "Understanding Data Security Controls: A Comprehensive Guide, "provides that this organization's assets will be safe under a clear procedure of securing and maintaining systems and following up with multiple methods to mitigate risk, also highlighting policies and procedures (Rosselvelt, 2023). Human Resources Management can be seen as another approach allow companies avoiding or eliminating uncertainties which can resolve based on “the guide the behavior of individuals” (A Guide to Fundamental Security Control Types, 2024) and depend on how much involvement of the center manager with specified strategies.

**Access Control**

1. **Guidelines for acceptable use:** By maintaining a safe and secure environment, we can prevent future information leakages or misuse data. And verify that all new incoming
2. employees must sign contracts. These contracts outline a set of usage conducts and consequences for any violations. This process is a precautionary practice that provides signature documents for a lawsuit if needed.
3. **Security policies:** We should enforce rules and outline security practices for the data center to protect against compromised data. Emphasize the significance of students and employees staying alert about potential illegal network access and physical trespassing. By follow this policy, we may avoid a lot of troublesome.
4. **Incident Response:** We can establish base guidelines on response policy and follow resolve plans to ensure employees react as fast as possible to the incident, understand their duties and obligations in finding solutions to minimize damage, and allow flexible recovery methods.
5. **Least Privileges:** We should ensure employees can only access small amounts of resources that are enough to complete the tasks for their assigned jobs, doing so minimizes the potential of vulnerabilities and security breaches. These approaches prevent employees from doing things that exceed their abilities and privileges.

**Human Resources Management**

1. **Background Check:** We can perform a pre-employee investigation (social media, criminal records, etc.) to ensure that resume reports and answers during the interview on background questions are brutally honest to determine hiring acceptance. This process will help the data centers to minimize potential insider threats and will secure confidential and availability.
2. **Manager Role:** We should assign a manager role who holds sufficient power over management and comprehensive security in the research data center and is involved in
3. critical works, including reworking outdated policies and ensuring fewer authorized practices of those post-tested and transparent rules. Along with those given power, managers shall appoint regular meetings to update about recent data breach incidents to find optimal solutions to mitigate system databases and protect and evaluate research projects.

**Technical Controls**

Network monitoring plays a crucial role in technical control because it protects against multiple harming factors, including unverified individuals and network breakers. In addition, it can protect business websites and software identities, block malicious activities before they cause damage, and create a trusted place to store useful data among networks. According to Heilgenstein, the author of "Technical Security Control: Encryption, Firewalls & More,” claimed that “Technical security controls include any measures taken to reduce risk via technological means" (Heiligenstein, 2021). This seems to apply to threats at the system level, by using preventive, detective, and responsive patch management and password management, we assure integrity, confidentiality, and availability remain intact.

**Network Monitoring**

1. **Firewall Software:** We can embed network-based firewalls into all business center and research center technologies and server systems. We could launch hardware or software strategies to control incoming and outgoing traffic to prevent and block unauthorized access and overall familiar malicious content based on preset rules. Also, we needed to ensure log recording was enabled for investigation if necessary.
2. **IDS / IPS:** We can regulate intrusion detection systems and intrusion prevention systems 24-7 to continue monitoring the data center network system for suspicious activities, relying on predefined rules and patterns, and responding to potential suspicious breaches and policy violations. Snort is recommended in this case because it serves both purposes.

**System Monitoring**

1. **Anti-virus:** By implementing anti-virus in all devices, we can detect and quarantine malicious viruses from software, protect data against cyber-attacks and malware, and alert about accessing malicious catchy websites. This provides an additional layer securing integrity and confidentiality. Bitdefender is a good choice $63.99 for 10 devices.
2. **Password Manager:** We should add password manager, so that our employees don’t have to worry about forgetting their password ever again and protect confidentiality. Password manager itself already generate a strong unique password that will take forever for the cybercriminal to crack. It is also worth noting that password manager nowadays often come along with build-in strong AES encryption and two-factor authentication. This protects our privacy information and minimize the risk of using the same password. NordPass currently have a good deal $1.24/month.
3. **Patch Management:** We should ensure software updates regularly to fix vulnerabilities and improve security. As for regular computer updates, our staff can take a conscious approach, like when they perform data search tests for compatibility, so we should wait for a week to avoid unnecessary corruption, as new release patches tend to be unstable and have the possibility to introduce unknown error.

**Physical Controls**

By implementing access control, environment control, and infrastructure protection, we can enhance physical security measures. According to the “A Guide to Fundamental Security Control Types” blog on the Packetlabs website, we can regulate an “organization's security infrastructure, ensuring that areas with access to sensitive assets are protected from intrusions, theft, vandalism, and natural disasters” (A Guide to Fundamental Security Control Types, 2024). With the help of biometric security measures, personnel guards, and surveillance protection systems we can avoid uncertain situations and activities and provide constant monitor; to decrease the possibility of violating integrity and availability of the sensitive valuable data.

**Access Control**

1. **Iris and Thumb Scanners:** We should set up iris scanners for both research center entrance doors. This search center access is only permitted for search staff and managers, business employees and students shall not enter. The thumb scanners shall be located at the main center entrance and the receiving entrance. Other than that, we needed to ensure these restriction centers should be in lock mode, especially off-hours. Iris is the most expensive but should in demanding, $1500 - $3000 and thumb scanners could range between $200 - $500.
2. **Card Swipe Security:** We should be able to card swipe to open at other doors after verifying ID at entrance doors when entering the data centers. An ID card swipe at the business office's entrance will determine whether the staff or employees' authority is enough to enter an off-limit area. We could implement A RFID Reader Sonew card reader provide a solid price $59. Along with the camera, we can ensure that nobody shall hack into it before coming near a physical card reader machine.
3. **Door Lock:** We need to make sure that we have a backup plan so that only our boss and our managers can hold the keys. The door lock shall be set up in a way that it will automatically show the keyhole to open after a power outage occurs. We should do that to limit the potential the physical break-ins and insider threats.

**Surveillance and Monitoring**:  We should deploy surveillance cameras near each entrance: a lot around the data center, and some along the business hallways. Alarm systems linked with cameras that have motion sensor functionality shall trigger whenever someone either by accident or with suspicion enters off-limited zones during on-hours /off-hours. These cameras make it easier to trace evidence with sound record scenes and incident logs. We should get the Hanwha Vision SND-7011N Surveillance camera for $97, affordable and fits budgets.

**Environmental Controls**

1. **Server Room Air Conditioner:** We should leave the air conditioner power-on for offices to filter air because there are no windows in the rooms and turn it off when leaving but since the data centers need cool temperature air conditioner should be active 24/7, and help reduce humidity levels, and keep the comfort when working in a complete closed space and keep data servers run smoothly, limited system crashing and prevent from overheating. 1 or 2 Tripp Lite by Eaton Portable AC Unit for Server Rooms - 12,000 BTU, a little pricy $ 997.99 should be sufficient.
2. **Fire suppression:** We should have fire suppression in place just in case natural stuff happens, like electric leakages, overheating causing fires, etc. We should have staff check fire suppression frequently to ensure that is not outdated and replace them. By having those, we can minimize damage to the data center.
3. **Power generation:** We should have a backup plan for power outages to prevent data corruption and ruining the server network since the server database needs to continually update and run or else it may corrupt whole computer systems.

**Infrastructure Protection**

1. **Security Guards:** Hire 2 security guards to guard during off-hours, their duty is to prevent theft from stealing or damaging physical assets or data. They should stand at both ends during on-hours to verify ID cards when someone arrived to ensure unauthorized individuals shall not enter data centers. They might check the records in operation room if they found something wrong along and with staff if serious. We shall offer a salary of range of $18 to $20 per hour for each guard.

**Conclusion**

Throughout administrative, technical and physical securing methods for ACME College, we can now assuming business and research assets is safe from outsider and insider threat. By implementing those taking in account to those controls we’re able to provide significant improvements to research center. Still, continuous check and monitor, and balance access to ensure this those rules keeps those efficiencies and help detect and prevent those uncertainties.

**Data Center Redesign Figure**

A diagram of a building

Description automatically generated

**References**

*A guide to fundamental security control types*. Packetlabs. (n.d.).

https://www.packetlabs.net/posts/a-guide-to-fundamental-security-control-types.

Amazon.com: RFID Reader Outdoor Wiegand Waterproof Door Access Management Smart Card Door Access Control Door Entry Access Control panel(id): Electronics. (n.d.).

https://www.amazon.com/Outdoor-Wiegand-Waterproof-Management-Control/dp/B07RHJ855C

Devasia, A. (2024, June 3). *Biometric access control system price: Full Guide (2024)*. Safe and Sound Security.

https://getsafeandsound.com/blog/biometric-access-control-system-price/#:~:text=Iris%20scanners%20are%20typically%20the,suitable%20for%20high%2Dsecurity%20environments.

Heiligenstein, M. X. (2023, July 14). *Technical security controls: Encryption, Firewalls & More*. Firewall Times.

https://firewalltimes.com/technical-security-controls.

*NordPass password manager: Zero password stress. forever.* Securely Store, Manage & Autofill Passwords. (n.d.-a).

https://nordpass.com/affiliates/cybernews-deal-2/?coupon=cybernewspass&utm\_medium=affiliate&utm\_term&utm\_content=7a093c701ab54a93b9502a582ae60e89bafe&utm\_campaign=off644&utm\_source=aff41342&aff\_free

Samsung SND-7011N 3MEGAPIXEL network dome camera, 3mm lens. (n.d.-b).

https://www.surveillance-video.com/camera-snd-7011n.html

*Stay safe with the most consistently top-rated antivirus of the last 10 years (and counting) pick the perfect plan for your needs.* Stay Safe with the Most Consistently Top-Rated Antivirus of the Last 10 Years (and Counting) Pick the perfect plan for your needs. (n.d.-a).

https://www.bitdefender.com/pages/consumer/en/new/cl-offer-premium?pid=nonb&cid=ppc%7Cc%7Cgoogle%7C60off&&s\_kwcid=AL%216076%213%21721117912976%21b%21%21g%21%21antivirus&gad\_source=1&gclid=Cj0KCQiA0fu5BhDQARIsAMXUBOIR5DjYDZisRuxrZ2DWeRzxFHGamyQJzXJeJq7gxztALEOt9m34c4AaAuREEALw\_wcB&gclsrc=aw.ds

*Tripp Lite by Eaton Portable AC unit for Server Rooms - 12,000 BTU (3.5 kW), 120V: Dell USA*. Dell. (2024, November 21).

https://www.dell.com/en-us/shop/tripp-lite-by-eaton-portable-ac-unit-for-server-rooms-12000-btu-35-kw-120v/apd/a7220654/power-cooling-data-center-infrastructure?tfcid=91049735&dgc=ST&gacd=9684992-1102-5761040-266906002-0&SA360CID=71700000117208879&gad\_source=4&gclid=CjwKCAiArva5BhBiEiwA-oTnXYYCYsfAdopCdcVeCqTiwXjDI4bWrqdwfJv5iEpoViNIBZ4vTdraORoC3vMQAvD\_BwE&gclsrc=aw.ds

*Understanding Data Security Controls: A comprehensive guide*. Newsoftwares.net Blog. (2024, June 21).

https://www.newsoftwares.net/blog/understanding-data-security-controls.

Wilson, M. (2023, May 23). *Data Center Physical Security Best Practices*. Nlyte.

https://www.nlyte.com/blog/data-center-physical-security-best-practices.