Security Control Implementation Assessment

Elijah Olson

Southern New Hampshire University

Introduction

As an organization, ACME Company must continue assessing its infrastructure and make changes to transition into the new market that the company is projected to enter within the next several years. Since ACME Company is hoping to obtain federal government contracts over the next seven years it must prove that it has the infrastructure to maintain federal government standards for cybersecurity. To prove that ACME Company is capable of handling government contracts, the organization will implement a multi-layered approach to its enterprise security, beginning with an assessment of the organization's current infrastructure and hardware looking for areas of improvement. This report will include recommendations for ACME Company in areas of weakness within the three risk domains: people, process, and technology along with recommendations on how to remediate those weaknesses.

Threat Assessment

People

The first vulnerability identified within the risk domain of people would be roles and responsibilities not being properly divided among employees. Based on the definitions provided within the Inventory of Organization Hardware the workstations used by various employees are possibly being utilized by all employees instead of employees assigned to a single department. This could preclude that there are shared responsibilities between departments, for example, that someone working in HR is also assisting with responsibilities within Finance. This may mean that one employee has too much access to systems across boundaries that would allow them to misuse information or nefariously use their access for unintended purposes.

The second vulnerability identified within the risk domain of people would be the unlimited physical access that all individuals who enter the facility have to the campus. This falls under the domain of people because it is not inherently physical security becoming the problem but rather people taking advantage of the lack of security that becomes the problem. Currently, the facility has an open access policy at the front entrance which allows anyone to enter without authorization being checked. This allows them into the employee-only areas of the facility where employee workstations are accessible on both the first and second floor. This ability for any individual to enter the facility becomes a bigger concern once they bypass the employee cubicle area and reach the Information Technology (IT) closets. Neither closet on either floor has a lock on it which would allow anyone, an authorized employee or random stranger off the street, access to the equipment room. This creates a large security risk to the infrastructure of ACME Company because it would be very easy for anyone to disable the entire network by removing a single cable from the bottom floor closet. This simple act could disable operations for hours and cost the company thousands of dollars in lost revenue.

Process

The first vulnerability identified within the risk domain of process is the lack of a formal process for staff, vendors, and visitors to be identified and processed before being granted access to the facility due to their lack of physical security. Currently, there is no physical security control in place preventing anyone from accessing the main door of the facility. This lack of physical security control continues throughout the facility between floors and into infrastructure closets. Because there is no process in place requiring anyone to formally identify themselves before being granted access to areas of the facility meant for employees, currently, anyone would be able to move freely throughout the building. This constitutes a broken process because

someone with malicious intent would have free rein to access any part of the campus they wanted and perform any actions necessary. This also presents a safety risk for the employees because again, someone with intent to harm one of them could access the building freely and be able to find them without any interference.

The second vulnerability identified is that there is no process or procedure in place for the various servers utilized by ACME Company regarding how they are to be isolated and protected within the network infrastructure. According to the Current Organization Infrastructure Diagram, the Public Records Server is housed on the first floor and is connected directly to the Internet Router utilized by ACME Company's entire facility. There are two other servers located on the second floor, the Web Server, and the Authentication Server both connected haphazardly through a series of switches, hubs, and workstations. There is no standard procedure for how these servers are to be housed, or what types of connections should be utilized to connect them to the main router. Currently, there also is not any type of policy on what systems should be in place to protect access and connections to the servers.

Technology

The first vulnerability identified within the risk domain of technology is the current physical topology of the second floor. According to the Current Organization Infrastructure Diagram, ACME Company is currently utilizing a hub as the main connection point for the entire second floor. This is a poor decision because the hub is not a high-functioning piece of networking equipment, and if two transmissions are sent at the same time it can cause a traffic collision and prevent the traffic from being delivered. This issue is further compounded because from the main hub three computers are connected and from those computers they connect to another hub. The second hub acts as a connection point for the two servers that are housed on the

second floor. This is poorly designed because these will cause a high amount of traffic and given the issues hubs have with traffic, there will be issues with content not being delivered or being corrupted.

The second vulnerability identified is that according to the Current Organization Infrastructure Diagram, there is currently no VPN system in place for the remote employees to utilize for access to on-site resources. Without the use of a VPN for remote employees, all communications sent by the remote employees will be done in clear text and could be viewed by anyone who intercepts that traffic (Nord VPN). This exposes ACME Company to the potential to have their proprietary data, customer Personally Identifiable Information (PII) or employee PII exposed due to an unsecured connection.

Implementation Approach

People

To remediate the first vulnerability identified that there alludes to the presence of employees sharing responsibilities between departments and therefore individual employees may have too great of access to the system the recommendation is to implement the concept of separation of duties. To accomplish this the first step that needs to be taken is to clearly define what each department's responsibilities entail, what areas they cover, and how far their reach extends. Once the department's responsibilities have been defined then ACME Company can go within each department and clearly define each job function within that department and clearly define its responsibilities including its scope. Once individual job roles and responsibilities have been clearly defined and the scope has been developed it becomes much simpler for the IT Department to then tailor the system access to their needs. It should also be ensured that within a

single department, no one individual has the full authority to carry out a task that should have dual authorization, the example given by NIST is with the use of payroll within the finance department, the person authorizing the payroll for ACME Company should not be the same individual responsible for signing the paychecks (NIST). This meets the requirements for separation of duties and will reduce the likelihood that one individual has too great of access and misuses their system privileges (NIST).

The recommendation to remediate the second vulnerability identified constituting the potential for people to misuse the current lack of physical security throughout the ACME Company facility the recommendation is to implement electronic security locks, CCTV, and security guards. The reason for the recommendation to implement electronic security locks is to add a layer of physical security in areas that have physical barriers that currently have no locks and should only be accessed by authorized personnel. Examples of areas that these locks should be implemented in would be the IT closets housing network infrastructure equipment and employee-only areas of the building. It would also be recommended to install an electronic security lock at the front door and set it up on a timer system so that there is still open access during work hours for business needs. The electronic security locks that would be recommended to install are keycard-based locks that would require an employee to tap their badge against a keycard reader which would be installed against the door to be granted access to a secured area (Kisi).

The secondary recommendation for the second vulnerability is a passive security measure which is to install a CCTV system within the campus. Installing a CCTV system on the ACME Company campus will make individuals who might be considering entering areas they do not belong in or planning nefarious actions think twice before following through with their actions.

This recommendation pairs with the third recommendation which is to institute a security guard presence on the ACME Company campus. Having a physical security guard present within the facility and on company grounds will show that the organization is monitoring the facility and there are individuals on site who can take swift action if the need arises. The security guards can monitor the CCTV systems for any suspicious activity. These guards are also able to watch for potential tailgating with the electronic security lock system and verify that only people with working employee IDs can gain access. The security guards would also be able to follow an established protocol for processing visitors to gain access with an escort to employee-only areas of the facility as the need arises.

Process

The recommendation to remediate the first vulnerability found under the risk domain of process which is that ACME Company currently lacks a formal process for identifying employees, vendors, and visitors for entry to the facility due to the lack of physical security is to first implement the recommendations for implementing physical security controls and second establish a formal process for identification. The first recommendation for the formal process of identification for employees is to issue all employees an official ACME Company work identification badge that should include details about their employment such as full name, employee ID number, department, and employee photo. The recommendation for the identification of vendors is to gain an official list of all vendor staff that are going to be accessing ACME Company property so that an identification badge can be issued for them. This badge should include the vendor staff photo, full name, name of vendor, and period of validity. The vendor badges should remain on-site at the security desk and vendors should be required to check in with the security guards to be issued their ID upon check-in and required to turn it in

upon checking out of the building. The recommendation for identification of visitors is for all visitors to be required to stop at the security desk so that the guards may inspect their acceptable photo ID which includes driver's licenses, state ID, tribal ID, and passports. The security guard is to record the visitor's full name, ID number, reason for visit, and destination into an electronic log before issuing the visitor a visitor pass and calling for their escort from their destination if in a secure area.

The recommendation to remediate the vulnerability identified which is that there is currently no policy or procedure in place regarding how the servers used by ACME Company are to be isolated or protected is to standardize a policy so that all servers are uniform in technology utilized for isolation and protection unless specific exceptions apply requiring higher protection requirements. One recommendation for the new server policy would be that all servers must be contained behind a firewall. The servers may have individual firewalls or utilize a shared firewall if the security requirements are equal. It is then recommended that a uniform policy be implemented regarding what technologies be utilized for what can connect the servers to the internet router so that a minimum standard of networking technology is required. Currently, the second-floor servers are daisy-chained through two hubs and three workstations which does not provide a reliable connection for the servers. There needs to be an established policy stating what the minimum required network technologies allowed to be utilized for connecting servers to the internet router are and completely forbidding the servers to be connected through workstations.

Technology

The recommendation to remediate the first vulnerability found under the technology risk domain caused by the current network configuration of the second floor is to reconfigure the layout of the second-floor topology to replace the hubs with switches and re-route the Servers to

be directly connected to a switch instead of being connected through the workstations. The recommendation is to replace the IT Main Hub with a networked switch which can be labeled Second Floor Main Switch. This switch should connect to two additional switches, the first would be labeled IT Department Switch, and the second would be Server Switch. The workstations for the IT Department would all be connected directly to the IT Department switch and any additional workstations that need to be added later would have space to be included in this switch. The Server Switch would be dedicated only to the two servers housed on the second floor, the Web Server, and the Authentication Server. Since the servers would be connected directly to switches instead of hubs and workstations, they would have a higher rate of reliability.

The recommendation to remediate the second vulnerability that was identified which is the potential exposure of sensitive information by remote employees due to the lack of VPN utilization is to implement the use of VPN technology to create a secure connection for all remote employees. Utilizing a VPN for remote work would encrypt all traffic between the remote employees and ACME Company's facilities making working more secure (Nord VPN). This is especially important if the employees who are working remotely are working off of a public Wi-Fi network which has a great potential to be monitored by threat actors (Nord VPN).

Conclusion

After having reviewed both the Inventory of Organization Hardware and the Current Organization Infrastructure Diagram for ACME Company multiple vulnerabilities were located for the risk domains of people, process, and technology. After identifying the vulnerabilities within each domain, a unique recommendation to remediate each vulnerability was made which would allow ACME Company to successfully mitigate the risk. The risk assessment performed, along with following through with the recommended mitigation steps will assist ACME

Company with implementing a multi-layered approach to security. Increasing their standards towards a multi-layered approach will put ACME Company in a much greater standing to pick up contracts with the federal government on the timeline set forth by the organization.

References

Kisi. *Keycards for Access Control Systems*. Retrieved September 04, 2023 from https://www.getkisi.com/keycard-access-systems

NIST. *Separation of Duty (SOD)*. Retrieved September 04, 2023 from https://csrc.nist.gov/glossary/term/separation_of_duty

Nord VPN. *Pros and Cons of VPN*. Retrieved September 04, 2023 from https://nordvpn.com/blog/pros-and-cons-of-vpn/