**Components of a Security Policy for a Corporate Information System**

Mike Green

Old Dominion University

CYSE-300

Dr. Joseph Kovacic

May 28, 2023

First and foremost, the CIA (Confidentiality, Integrity, Availability) triad needs to be addressed. To keep sensitive data confidential while also maintaining the integrity of various types of data, the security policy needs to include security controls that differentiate who can or cannot view or alter it. These security controls should include aspects like data encryption, data cryptography, access controls for different types of data, data classification standards for implementation of these access controls, security and protection of the physical systems/devices that contain this data (could change depending on if data is primarily stored in the cloud/some type of cloud service), proper disposal of outdated/unneeded data, and employee information security training to help further guarantee the security of sensitive data. Regarding on-premises web servers, the security policy is going to differ a bit since web servers typically aren’t made to store data. The security policy should involve aspects like strong authentication methods for accessing user accounts, regular updates & patches to ensure that there are minimal vulnerabilities, some type of firewall for traffic control to the server, utilization of encrypted protocols for network communication, server monitoring to track activity that could be deemed a security risk, user access controls, and employee training to further ensure the security and protection of the server. Lastly, application servers operate differently than web servers, but they do utilize similar ways to ensure security of the applications used within the corporation while also serving as the host for these applications. Security policies for an application server includes aspects like strong authentication methods for accessing user accounts, server hardening for reducing vulnerabilities that may be present in the server, regular updates and patches to further reduce vulnerabilities, firewalls for traffic control, user access controls, backing up of data in case anything happens that compromises the server (could apply to all servers really), encrypted protocol utilization for secure server/network communication, and employee training, once again, to further guarantee server security.

For the Availability component of the CIA triad, multiple methods/practices should be utilized to ensure the maximum uptime for each server. Load balancing is a method that helps ensure uptime by distributing incoming network traffic across multiple servers or distributing incoming network traffic across the available resources on a server. Another method, monitoring systems/tools, can be used to track the utilization of server resources and network traffic; and they can be configured to notify whoever is responsible for administering the server of anything occurring that likely shouldn’t be occurring. The security measures mentioned above (data security, traffic control, data encryption, etc.) are guaranteed ways to ensure server uptime as well since any compromise to those aspects could lead to the server being attacked or shut down. Lastly, Disaster Recovery Planning is, objectively, one of the best ways to ensure server uptime; a corporation NEEDS to plan for any disaster that could occur whether that be a natural disaster, a malicious attack, or any type of catastrophic event. If there is no plan, then there is no recovery.

Acceptable use/end-user behavior is another critical aspect that needs to be addressed because, at the end of the day, the user is the greatest liability when it comes to the security of a network. Acceptable use encompasses what the user should be doing, should not be doing. Regarding what the user should be doing, user responsibilities come into play. This is where the corporation should clearly define what is expected of authorized users i.e., following regulations, procedures, policies, security measures, for handling sensitive data, for the occupation itself, etc. Regarding what the user should not be doing, this is where consequences for failing to comply come into play; disciplinary actions or complete termination can be waged for any employee who fails to comply or decides not to comply with any of the user responsibilities that have been stated.

This may be encompassed by everything aforementioned, but incident response is also extremely important for any security policy. When talking about incident response in the security policy, there are several aspects that should be clearly defined, but only a few are going to be outlined here. Incident identification and reporting is important because this is where the policy defines how to spot an incident that may be a threat, and how/who it should be reported to. Without this, it would be difficult to manage risk within a corporation. Relating to that, incident categorization is important in determining how the appropriate parties should react to that threat; this essentially helps to prioritize risk by classifying threats according to how dangerous/severe they are. Lastly, none of the above could be implemented on a corporation-wide level without proper employee training. Every aspect of a security policy needs some type of employee training to improve awareness of certain situations while also decreasing the chances of these incidents occurring and decreasing the chances of these incidents flying under the radar.

References

Exabeam. (n.d.). The 12 Elements of an Information Security Policy - Exabeam. *Exabeam*. <https://www.exabeam.com/explainers/information-security/the-12-elements-of-an-information-security-policy/>

*Minimum Security Standards | University IT*. (n.d.). Uit.stanford.edu. Retrieved May 28, 2023, from <https://uit.stanford.edu/guide/securitystandards#security-standards-applications>

Read “Computers at Risk: Safe Computing in the Information Age” at NAP.edu. (n.d.). In *nap.nationalacademies.org*. <https://nap.nationalacademies.org/read/1581/chapter/4#53>

‌University of Delaware. (2018). *Managing data confidentiality*. Udel.edu. <https://www1.udel.edu/security/data/confidentiality.html>

University, C. M. (n.d.). *Web Server Security Guidelines - Information Security Office - Computing Services - Carnegie Mellon University*. Www.cmu.edu. <https://www.cmu.edu/iso/governance/guidelines/web-server.html>

‌

‌

‌