# 5 Key Areas of a Corporate Security Policy

By Adam Haas

CYSE 300 15767

September 15th, 2023

Building a solid security policy to protect a company's network and information should be considered a primary goal in protecting systems and IT assets. Five major aspects to include in this policy are data encryption, firewall usage, a disaster recovery plan, logging, and using network intrusion detection software to ensure that systems stay functioning and are protected from unwanted access. This paper outlines why each of these topics are important additions to this critical policy.

One of the most important ways to secure a company's sensitive information and intellectual property is through data encryption. Using encryption inhibits unsanctioned access of private information and exposure. Keeping information secure while it is in storage and while it is being transferred is paramount to a security policy. The key to having effective encryption of data relies on every bit of ciphertext, all parts of the key, and the entirety of the plaintext being completely intertwined. This is achieved when no statistical correlation between ciphertext and plaintext can be found (Vacca, 2009/2014). Keeping all data encrypted on a network is one of the key first steps in developing a solid security policy.

Having a firewall protect the internal networked system is crucial in preventing unwanted access and attacks to a company's critical infrastructure. A firewall protects a system by segmenting the network into different areas. Separating the framework to keep distance between parts that need access to the internet from parts that are better suited operating on the internal network keeps a barrier shielding the inward sytem from the outward facing parts (O'leary & Springerlink (Online Service, 2019). Using firewalls is key to a security policy because it protects and separates areas of a company's critical infrastructure by keeping core systems apart from more vulnerable systems.

Disaster Recovery is critical to maintaining stability when unforeseen and unexpected circumstances take a company's critical IT infrastructure out of function, these risks include anything from natural disasters to malicious attacks. A component of a good security policy is having a solid disaster recovery plan dictating a strategy to handle the unexpected. The physical and digital environment is constantly changing, requiring businesses to continuously reassess their risks and vulnerabilities and implement creative plans that continuously adapt to these changes. Having a well planned strategy offers assurance of what to do when unanticipated scenarios occur which in turn helps to prevent catastrophic failures and shutdown. Organizations rely heavily on the IT department to understand, fix, and continue the function of systems when the disasters and disruption bring critical infrastructure out of function (Vacca, 2009/2014). A solid disaster recovery plan is critical to a security policy because it gives confidence and direction if unexpected situations occur.

Logging should be considered when developing IT infrastructure because it helps show the network's usage, providing information like who is using it and how the system is being utilized. Understanding IT traffic through logs is critical to understanding what is happening and what has already happened on a system. A solid, robust logging system helps to identify incoming attacks and debug network issues. Logs can help identify how attackers break into the system, the scope of systems affected, and how to fix the vulnerability. Logging can be a deciding factor in identifying where and how weaknesses are being exploited (Lockhart, 2004). Utilizing this tool in a security policy helps a company protect its system through documentation and transparency.

Another valuable tool to include in protecting IT systems is using network intrusion detection software. This software helps monitor traffic on networks for detection of suspicious

behavior. Utilization of this software can help identify attacks before they are able to reach their intended target and cause harm to a system's security. Some detection software monitors for byte patterns that have been previously identified with known attacks and other software analyzes packets that fall out of the normal network data patterns. Having a plan to use this type of software is helpful for companies to stay in front of attacks before they can be fully carried out (Lockhart, 2004). Network intrusion detection software is vital because it enables real time alerts and notifications when unusual traffic is taking place promoting the likelihood that attacks will be identified and dealt with before they have been fully executed.

Keeping a company's digital systems functioning and protected is becoming increasingly more important and challenging because of the development of new technologies and software. Encryption, firewalls, disaster recovery, logging, and intrusion detection are some of the principal ways to ensure digital safeguards and should be included in a company's IT toolbox. Having a strong well-conditioned security policy can make or break a company between success and failure.

Works Cited

Lockhart, A. (2004). *Network security hacks*. O'reilly.

O'leary, M., & Springerlink (Online Service. (2019). *Cyber Operations : Building, Defending, and Attacking Modern Computer Networks*. Apress.

Vacca, J. (2014). *Cyber security and IT infrastructure protection* (First). Steven Elliot. (Original work published 2009)