Key Security Policies for Protecting Corporate Information Systems

Adeline Harris

School of Cybersecurity, Old Dominion University

CYSE300: Introduction to Cybersecurity

Professor Kovacic

February 2, 2025

In a modern world dependent on technology and the Internet, physical protection alone of on-site security is not enough. It is of vital importance that a cybersecurity system be set for any and every corporation. This paper is an outline of a security policy for a corporation and the reasoning behind the specific policies, focusing on five key issues: data protection, access control, network security, software security, and incident response.

In a corporation with on-site web applications and database servers, security measures are taken to reduce and/or protect sensitive data stored in database servers, prevent unauthorized access to web applications and database servers, ensure secure communication between system components, establish incident response and recovery mechanisms, and comply with industry regulations and best practices. To properly meet these security needs, a system that allows uninterrupted data flow, limits access, is regularly checked and updated, and follows security regulations is a major goal of the security personnel. This requires the security team to implement end-to-end encryption using strong cryptographic algorithms (e.g., AES-256, TLS 1.2/1.3) to protect data both at rest and in transit (National Institute of Standards and Technology, 2018). The Equifax breach was an exploitation of data at rest, involving the personally identifiable information of customers (Kabanov & Madnick, 2021a). Data protection ensures that data transmission and storage are secured to prevent interception or tampering. HTTPS should be installed for all web applications to secure these pages (OWASP, 2021). A cryptographic system should randomly generate keys and convert all passwords into keys using appropriate password-to-key derivation functions (OWASP, 2021). Encryption keys should be securely stored using a hardware security module (HSM) or a key management system. Data protection builds on the requirement that there is no unauthorized access to the network and, therefore, the data. A very common breach risk is the parties that can access the information. It is advisable that role-based access control with limited

privileges be established, granting access only to authorized devices, users, or processes (National Institute of Standards and Technology, 2018). In light of only authorized users or devices gaining access, a deny-all-by-default setting should be set up in the system (OWASP, 2021). Limiting access to data and processes reduces the risk of information leakage. For authorized personnel, a multi-factor authentication system with biometric keys, where applicable, is required for access. This reduces the risk of third parties gaining access by brute force or acquiring an access key. Setting up a system with end-to-end encryption and limited access, along with a multi-factor authentication requirement, requires regular access log checks to detect unauthorized access and remove access for parties who are no longer authorized.

The network in the corporation should be segmented and secured to prevent database servers from being accessed or exploited in the event of a breach. Multiple firewalls should be set up, with at least one firewall per segmented subnet; this reduces the risk of sensitive information being compromised. In addition to the firewalls, intrusion detection and prevention systems should be implemented to monitor network traffic (National Institute of Standards and Technology, 2018). In the Equifax breach, the network was not properly segmented, and there was no intrusion detection or prevention system monitoring network traffic, which allowed the hackers to remain undetected for months (Kabanov & Madnick, 2021a). Protective technology is advised to be used to prevent such instances and enhance the resilience of systems and assets. These technologies should be consistent with related policies, procedures, and agreements (National Institute of Standards and Technology, 2018). Access to data and servers must be restricted to authorized applications. The security software should be checked regularly, with update checks done frequently, and updates and patches installed promptly upon release. With software updated, it is important to check for vulnerabilities and run penetration tests regularly. All unused dependencies and unnecessary

features are to be removed from the systems, and only components and packages from officially signed sources should be used to prevent modified malicious components (OWASP, 2021). The main cause of the Equifax breach was a vulnerability in Apache Struts within the web application that was not updated when the patch was released (Kabanov & Madnick, 2021a). Endpoint detection and response tools help monitor threats in the system (National Institute of Standards and Technology, 2018). As these steps and procedures are put in place, an incident response plan must be developed, and all staff must be trained in proper procedures to prevent operational disruptions. All information and data should be backed up offsite as part of the disaster recovery plan, with separate encryptions.

In an age of technology, cybersecurity plays an important role in corporate security, and policies should be implemented with staff trained on procedures and patch management policies employed by the IT department of the corporation.

References

Kabanov, I., & Madnick, S. (2021b). Applying the Lessons from the Equifax Cybersecurity Incident to Build a Better Defense. *MIS Quarterly Executive*, *20*(2). https://aisel.aisnet.org/misqe/vol20/iss2/4/

National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. *Framework for Improving Critical Infrastructure Cybersecurity*, *1.1*(1). https://doi.org/10.6028/nist.cswp.04162018

OWASP. (2021). *OWASP Top Ten*. Owasp.org; OWASP. https://owasp.org/www-project-top-ten/