Short Research Paper 2

Emmanuel Dade

Old Dominion University

Cybersecurity 300

Dr. Kovacic

September 13, 2025

Short Research Paper 2

The biggest issue that companies face today is protecting sensitive data. With corporate on-premises web, application, and database servers as the backbone of most corporate information systems, a clear security policy is paramount. In particular, there must be multiple layers of protection surrounding database servers with sensitive data to ensure that the risk of breaches and unauthorized access is minimized. Security corporate policy requires a three-part blend of technology, monitoring, and human behavior to be most effective. Therefore, there are five main issues that a corporate security policy needs to address: access control, secure configuration, monitoring and incident response, employee training, and data protection.

First, access control should be one of the pillars of any security policy. Ensuring that only those with authorized clearance can see or change data protects sensitive information. For example, studies show that strong access authentication and role-based access control significantly reduce insider threat and external breach risk (Omotunde & Ahmed, 2023). For a corporation, this means setting strict policies for who has access to what and ensuring that all privileges are provided on a “need to know” basis. For example, database servers should be restricted to only those administrators who need access for their daily operations while web and application servers can have tiered but structured access. Should such principles be woven into the corporate policy, sensitive data will always be protected from excessive unwanted exposure.

Second, policy must include secure configuration requirements. More often than not, many security issues occur based on misconfigured components, such as firewalls, web application filters, or databases. Research shows that secure configuration is one of the best defenses against cyber attacks yet remains underutilized (Ayedh, 2023). Thus, the corporation must pay careful attention to the required configurations stipulated by the security policy. For

example, any firewalls need to be fine-tuned to ensure they reject unwanted requests. Any application servers should be configured so that typical attacks do not gain any foothold—such as using stored procedures to prevent SQL injection vulnerabilities. These findings need to become policy practice to ensure that carelessness does not decrease security defenses.

Third, monitoring and incident response should be built into the corporate security policy framework. A software-based policy should never just try to prevent attacks without giving additional clarity on detection and response down the line. NIST has shown that organizations with incident response plans are more successful than those who do not (Cichonski et al., 2012). Therefore, the corporation security policy must include continuous monitoring of logs and suspicious user behavior. Furthermore, it should establish an incident response team trained to deal with various security issues. In such a way, even if attackers penetrate on-premises systems, they can be apprehended quickly enough to minimize any damage.

Fourth, employee training and awareness should serve as another foundation for corporate security success. While technical defenses are critical, they never succeed without human interaction. For example, many employees unwittingly become entry points for attacks through phishing. Studies in security related policy development indicate that training awareness increases compliance with policies and strengthens the organization’s overall posture (Ayedh, 2023). Therefore, a corporation's policy should require mandatory training annually and quarterly or monthly updates when threats change. In this way, employees will become more aware of how they use sensitive data and potentially become communication conduits for malware.

Finally, the corporation's security policy should include a specific element for data protection. For example, databases that hold sensitive information should have mandatory

encryption and auditing/intrusion detection. The more efforts made to make data useless as well as transient auditing capabilities added around it means that companies can deter nefarious intentions before they even begin. Omotunde & Ahmed (2023) note that when encryption is combined with auditing and intrusion detection services, exfiltration becomes far more difficult as there are now three layers of issues any potential attacker will have to deal with when simply trying to get data out of the system. This approach protects sensitive personal and financial information and protects a corporation's overall reputation when proper transparency exists.

In conclusion, when considering how to create a good security policy for corporate on-premises web, application and database servers, one must take a multi-faceted approach to security. By addressing access control, secure configuration efforts, monitoring/incidence response and need to train employees in awareness and safety, a corporation can create as much of a protective environment as possible while also mitigating possible attacks when they ultimately occur. In other words, sensitive database efforts should receive the strongest security protections; therefore, corporate policy must reflect such an idea to protect systems from attacks as well as develop good faith with customers in efforts at transparency over time.

References

Ayedh M, A. T., Wahab, A. W. A., & Idris, M. Y. I. (2023). Systematic literature review on security access control policies and techniques based on privacy requirements in a BYOD environment: State of the art and future directions. *Applied Sciences*, *13*(14), 8048.

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer security incident handling guide. *NIST Special Publication*, *800*(61), 1-147.

Omotunde, H., & Ahmed, M. (2023). A comprehensive review of security measures in database systems: Assessing authentication, access control, and beyond. *Mesopotamian Journal of CyberSecurity*, *2023*, 115-133.