Security Polices from a CISO's Perspective

Carl Lochstampfor Jr.

Department of Cybersecurity, Old Dominion University,

CYSE 300 – Introduction to Cybersecurity, Professor Dr. Joseph Kovacic

September 14, 2025

Short Research Paper #2, Instructions:

You have been asked to design a security policy for a corporate information system consisting of on-premises web, application, and database servers. The database servers store very sensitive data that must be protected. Discuss five important issues that should be addressed in the security policy.

Perform research on information system security policies. Use the ODU library and/or appropriate Internet resources to perform content discovery. After you have completed reading through the research materials, write a 1–3-page paper describing the five important security policy issues.

Security Polices from a CISO's Perspective

Cyberattacks have more than tripled between 2023 and 2024, and they continue to increase at an alarming rate (Verizon Business, 2024). It also means that organizations are increasing their efforts to develop and refine their security policies to better protect both their customers who use their products and services, as well as the organizations' own data. In general, security policies employ a range of tools—including sub-policies, standards, procedures, and guidelines—to reinforce and protect networks and sensitive information from threat actors and unauthorized entities (King & Solomon, 2021, pp. 39-41). From the perspective of a Chief Information Security Officer (CISO), we can use two fundamental security philosophies to build our "master" or "macro" level organizational security policy: (1) the CIA Triad (Confidentiality, Integrity, and Availability) and (2) the NIST Cybersecurity Framework (CSF) (Nelson et al., 2022; Hashemi-Pour, 2023). A CISO is a senior officer in charge of management and leadership on information security issues for an organization (Nieles et al., 2017; Joint Task Force, 2020; Lochstampfor, 2025a & 2025b). The NIST CSF is a set of guidelines and best practices to help organizations manage and mitigate cybersecurity risks in a manner that aligns with their individual needs. In this paper, we will discuss **five key areas** that every organization's master security policy must cover with respect to the following three critical vulnerability attack vectors: on-premises Web, Application, and Database servers.

Challenge #1: User Access to Sensitive Data and Systems

Access Control Policies relate to Confidentiality, which is one of the pillars of the CIA Triad, because it emphasizes that only authorized users can access and view certain types of data (King & Solomon, 2021). A CISO must deploy those strict policies to help tighten control over who can access their web servers, application servers, and database servers. The policy must call for multi-factor authentication (MFA) on all user logins, implement privileged access management (PAM) to limit elevated permissions, and follow principles of least privilege. Thus, users are granted the minimal level of access they need based upon their roles and responsibilities. These guidelines are in accordance with the NIST CSF's Protect function; they are used to establish mechanisms that secure essential service delivery (Paulsen et al., 2016; Nelson et al., 2022).

Challenge #2: Rules for Using Company Resources

An **Acceptable Use Policy (AUP)** is a multifaceted document that outlines the organization's mission statement, defines acceptable and unacceptable uses of technology resources, and establishes employees' responsibilities regarding Internet and IT information security issues. The policy aims to protect the Availability and Integrity of the environment by providing rules for employees to follow, especially in a Bring Your Own Device (BYOD) environment, which may expose activities to unnecessary risks (Joint Task Force, 2020). AUP, alongside a Data Loss Prevention Policy (DLP), needs to specifically address both unauthorized software installation as well as the safe use of company data. Based on the NIST CSF Identify and Protect functions, the AUP can include monitoring devices that identify non-compliant actions and notify management within the organization (Paulsen et al., 2016; Nelson et al., 2022). Lastly, by educating users, CISOs can reduce the risk of incidents like data leaks and create a culture of responsibility, one that is also a source of pride in protecting their employer's and customers' data.

Challenge #3: Data Restoration and System Resilience

To maintain the second part of the CIA triad as a security objective, a CISO needs to ensure that systems and data are always available for legitimate use. A **Data Backup and Recovery Policy** helps ensure an organization can quickly recover data and technology services in the event of system failure or a cyberattack. The policy should include the frequency of backups, the location used to store data securely off-site, and how often backups should be tested for restorability (Joint Task Force, 2020). For example, by incorporating the NIST CSF Recover function, organizations can utilize automation tools to create and schedule routine, immutable backups (e.g., the 3-2-1 backup strategy): immutable backups are resistant to malicious modifications from malware and unauthorized personnel (Paulsen et al., 2016; Nelson et al., 2022). In on-premises deployments, it could mean air-gapped storage for critical databases, so that in the event of an incident, a CISO can bring operations back quickly and keep the business going with minimal downtime and consequences.

Challenge #4: Handling a Security Breach

An **Incident Response Policy** is crucial for the Detect, Respond, and Recover areas of the NIST CSF. The policy formalizes a strategy for containing incidents, including on-premises servers (e.g., distributed denial-of-service attacks) that are involved in breaches. The phases of the policy should include detection, containment, eradication, and recovery, as well as post-incident analysis and clear communication between all relevant parties (Nelson et al., 2022; Paulsen et al., 2016). Additionally, a robust Incident Response Policy helps protect the Integrity of an organization by empowering it to respond swiftly and prevent threat actors from tampering with and erasing critical data and important digital evidence for tracking down unauthorized users. As a CISO, running tabletop and simulation exercises can help their teams rehearse for the real thing, minimizing the impact on them and how quickly they get back up.

Challenge #5: Employee Education and Awareness

Human error is a significant contributor to data breaches. Thus, CISOs will schedule training and continual education on an ongoing basis. An **Employee Security Awareness and Training Policy** can address human weaknesses that can compromise the entire CIA Triad (e.g., being duped into acting against your own best self-interest because of social engineering tactics) (Joint Task Force, 2020). The policy must include the requirement for periodic training sessions on topics such as recognizing phishing emails, password hygiene, and simulated gaming exercises to test one's learning (Lochstampfor, 2025a & 2025b). Consistent with NIST's security framework functions Protect and Detect, continuous monitoring embedded with AI/ML features helps an organization remain compliant with government regulations and ordinances while adapting to new or emerging threats (e.g., Zero-Day attacks) (Paulsen et al., 2016; Nelson et al., 2022). By focusing on the workforce as the first line of defense, CISOs can help minimize incidents and improve the overall security posture of an organization.

References

Hashemi-Pour, C. (2023). *What is the CIA Triad? Definition, Explanation, Examples*. (W. Chai, Editor) Retrieved from TechTarget, September 12, 2025, from https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA

Joint Task Force. (2020). Security and privacy controls for information systems and organizations (NIST Special Publication 800-53, Revision 5). National Institute of Standards and Technology. https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

Kim, D., & Solomon, M. G. (2021). Fundamentals of information systems security (4th ed.). Jones & Bartlett Learning.

Lochstampfor, C. (2025a). Protecting availability of your systems: A CISO's perspective (Unpublished manuscript). Department of Cybersecurity, Old Dominion University, CYSE 200T: Cybersecurity, technology, and society. https://sites.wp.odu.edu/locky/2025/06/30/protecting-availability-of-your-systems-a-cisos-perspective/

Lochstampfor, C. (2025b). Human factors: A CISO's response to human error & threats (Unpublished manuscript). Department of Cybersecurity, Old Dominion University, CYSE 200T: Cybersecurity, technology, and society. https://sites.wp.odu.edu/locky/it-cyse-200t-2/

Nelson, A., Rekhi, S., Souppaya, M., & Scarfone, K. (2022). Incident response recommendations and considerations for cybersecurity risk management: A CSF 2.0 community profile (NIST Special Publication 800-61r3). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r3Links to an external site.

Nieles, M., Dempsey, K., & Pillitteri, V. Y. (2017, June). An introduction to information security (NIST Special Publication 800-12, Revision 1). National Institute of Standards and Technology. https://csrc.nist.gov/pubs/sp/800/12/r1/final

Paulsen, C., & Toth, P. (2016). Small business information security: The fundamentals (NISTIR 7621, Revision 1). National Institute of Standards and Technology. https://csrc.nist.gov/pubs/ir/7621/r1/final

Verizon Business. (2024, June). 2024 Data Breach Investigations Report. Retrieved September 12, 2025, from https://www.verizon.com/business/resources/reports/dbir/#top-takeaways