Branden Barnes

CS 465

9/22/2024

Security and Privacy Policies and Regulations

Q1. Find an information security (or cybersecurity) policy of a utility company and briefly list some of its key features in the context of what you have learned in this module:

The Noth American Electric Reliability Corporation's (NERC) Critical Infrastructure Protection (CIP) standards is a policy for large utility companies. Key features include: Sabotage reporting, asset identification and classification, policy and governance, personnel and training, network security, physical security of cyber assets, systems security controls, cyber security incident response, recovery plans, change and vulnerability management, protection of BES cyber system information, control center communications, supply chain security, physical security of key substations. The purpose of these cybersecurity regulations is to force companies and organizations to protect their systems and information from cyberattacks.

Q2. Look into the security rule of HIPAA and summarize the technical safeguards that it recommends (or enforces) as part of security standards:

"The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity." The Health Insurance Portability and Accountability Act of 1996 required the Secretary of the U.S. Department of Health and Human Services (HHS) to implement the technical safeguards to protect privacy and security of health information. HHS separated standards into two categories, Privacy Rule and

Security Rule. The most valuable asset of this standard is the defense of Electronic Protected Health Information. Safeguards are categorized into three parts, Administrative, Physical, and technical. Administrative safeguards consist of security personnel designated to implement security policies and procedures. When security management process is assessed, information access management is created, along with, workforce training and evaluation. Physical safeguards include facility access and control and workstation and device security. Technical safeguards include access control, audit control, integrity control, and transmission security.

Q3. All educational institutions have to comply with FERPA. Use web resources to write a brief summary of the security implications of FERPA from the institution's perspective:

"(FERPA) does not require educational institutions to adopt specific security controls, security threats can pose a significant risk for student privacy. Educational institutions should take appropriate steps to safeguard student records." If institutions do not follow guidance's with cyber security policies, breaches of educational data can lead to a violation of FERPA which will imply legal consequences. Institutions should follow the U.S. Department of Education's Integrated Data Systems and Student Privacy guide. To comply with FERPA institutions should understand the importance of data quality and security, maintain a record of each request for access to PII, ensure the security of PII in its essential components; physical security, network mapping, authentication, intrusion detection, etc..

References

Certrec. (2023, September 26). *What are NERC CIP standards and why are they important for power utilities?*. LinkedIn. https://www.linkedin.com/pulse/what-nerc-cip-standards-why-important-power-utilities-certrec#:~:text=The%20NERC%20CIP%20standards%20are,operators%2C%20and%20regional%20transmission%20organizations

Data security: K-12 and higher education. Data Security: K-12 and Higher Education | Protecting Student Privacy. (n.d.). https://studentprivacy.ed.gov/data-security-k-12-and-higher-education#:~:text=While%20the%20Family%20Educational%20Rights,steps%20to%20safeguard%20student%20records.

Mooney, G. (2024, February 5). *What is Ferpa and what are the necessary security controls?*. Progress Blogs. https://www.progress.com/blogs/what-is-ferpa-and-what-are-the-necessary-security-controls

(OCR), O. for C. R. (2022a, October 20). *Combined text of all rules*. HHS.gov. https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/combined-regulation-text/index.html

(OCR), O. for C. R. (2022, October 20). *Summary of the HIPAA security rule*. HHS.gov. https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html