Data Breach prevention policy

All across the world people's data is being exposed. This is an ongoing problem worldwide and I want to propose a policy to prevent data breaches. The data breach prevention policy was created to protect people's personal information. I will explain what data breaches are and why my policy is essential in cyberspace. A data breach is when unauthorized users gain access to confidential information. Data breaches happen because of a weakness in technology and user behavior. As technology continues to advance there are more exploits in which data can slip through. Technology companies are valuing convenience over security, as many new devices lack encryption. Hackers take advantage of this because they know many new products lack security testing. Understanding how data breaches occur is essential to protect yourself. Data breaches occur for a variety of reasons, some examples include outside criminals, stolen devices, accidental insiders, and malicious insiders. To get more in-depth, an accidental insider involves an employee using another employee's computer to read data without proper authorization. Even though the data wasn't shared this is still considered a data breach because an unauthorized user gained access. A malicious insider is a person who shares data purposely with the intent to cause harm. A malicious insider usually has the proper authorization to look at data, but they use it for negative reasons. Lost or stolen devices can also cause data breaches, as sensitive information could be on these devices. Malicious outside criminals are hackers who use numerous schemes to gather information from a server. Malicious outside criminals use schemes like phishing attacks, brute force attacks, and malware. Phishing attacks are when hackers send fake emails posing as people or organizations you may trust. But in reality, they are trying to trick you into giving out personal information. Brute force

attacks are when hackers use software features to guest your password. Malware involves criminals using spyware to steal personal data without being detected. Data breaches can be extremely damaging as they can affect a business's reputation and finances. Now that you understand what data breaches are, I will explain my policy. Most organizations have a data breach prevention policy to safeguard their confidential data. A data breach prevention policy consists of guidelines related to an organization that prevents data leakage and unauthorized access. The policy goes over procedures to access and share data, the type of data that needs to be protected, data security methods, encryption, and data access control. To make an effective data prevention policy you must know the data architecture and potential risk within an organization. You must be able to identify sensitive data by order of importance, locate where the data is stored, classify data sources, determine user roles, track data movements, and determine how data security information will be saved. Data security solutions implement data protection protocols in the data breach prevention policy. These technical tools help monitor, detect, and prevent data leakage across an organization's data footprint. Various data security solution methods help prevent data from being lost. These methods include data discovery and classification, data exfiltration detection, incident response, monitoring, and analysis checks. Data discovery and Classification are used to scan information stacks and detect sensitive data with advanced technologies. Data exfiltration detection is when security platforms protect devices from data leaks by monitoring and controlling data transfer and access. Incident response is when Data loss prevention platforms implement guidelines to reduce unauthorized data access. These platforms monitor data streams and restrict suspicious activity. Enforcing

Data Breach prevention policy

a data breach prevention policy is essential to keep a business successful. Implementing a data breach prevention policy with a data security platform improves cyber security and shields sensitive data from outside risk. The data breach prevention policy fits perfectly with the national cybersecurity policy. Data breach prevention is the main policy that aligns with the national cybersecurity policy, as it ensures all information is kept secure. It protects confidential information among different nations that should be kept inside. The data breach prevention policy prevents foreign allies from gathering confidential information about our country. Without the data breach prevention policy, our data would be exposed throughout different nations. Which could put our country at extreme risk financially. Other nations would take advantage of our data and use it to their advantage. In the scholarly articles I read they all saw the data breach prevention policy as essential in today's cyber space. The protection of private data is key to ensuring good cybersecurity. The articles explained how without a data breach prevention policy nobody's data would be secure. Scholarly articles explained the importance of not only establishing proper guidelines within your organization but also following through with procedures to keep data secure.

Scholarly articles

"Exploring Data Security Management Strategies for Preventing Data Breaches - ProQuest." *Www.proquest.com*, www.proquest.com/openview

Kongnso, Fedinand. “Best Practices to Minimize Data Security Breaches for Increased Business Performance.” *Walden Dissertations and Doctoral Studies*, 1 Jan. 2015, scholarworks.waldenu.edu/dissertations

Fathima, Afrah;Ahmed, Badiuddin. “Making Data Breach Prevention a Matter of Policy in Corporate Governance.” *International Journal of Scientific Engineering and Technology*,