4-1 Worksheet Activity Summation of Privacy Laws #3

Joshua Merren

Southern New Hampshire University

CYB-260-11229 Legal and Human Factors of Cyb C-3

Professor Jimmy Harvey

27 May 2024

The OPM data breach, discovered in 2015, was a significant security incident where attackers accessed and stole highly private information from the Office of Personnel Management (OPM). This breach included sensitive details from SF-86 forms used for government security clearance background checks and fingerprint data of millions. The breach originated in 2013 but was only detected two years later due to ineffective security measures at OPM. Initially, the attackers gained entry using a contractor's credentials linked to OPM, which should have been safeguarded better. Once inside, they exploited weaknesses in OPM's security systems. One of them is the need for two-factor authentication. This essential security measure requires a password and a second form of identification to access sensitive systems.

After gaining access, the attackers installed malicious software to create backdoors and navigate OPM's network undetected. These backdoors allowed them to steal data over an extended period without being noticed. The breach's detection was too late; by then, massive amounts of data had been stolen. The response to the breach could have been better because of internal politics and a lack of adequate security tools, which delayed the prompt addressing of the breach. It was a failure in the technology used and the organizational response to the breach that led to such a significant loss of sensitive information. The aftermath involved investigations, resignations of top officials, and a reevaluation of security practices at OPM.

Two significant laws relate directly to the OPM data breach. The Privacy Act of 1974 is crucial as it governs federal agencies like OPM, mandating them to safeguard personally identifiable information (PII) effectively. This law emphasizes the need for robust data management and security protocols, which OPM failed to implement adequately, leading to the

breach. Similarly, the Federal Information Security Management Act (FISMA) requires federal agencies to develop, document, and enforce comprehensive information security protections. OPM must follow FISMA's guidelines, particularly regarding security controls such as two-factor authentication. The breach could have been mitigated if OPM had adhered to FISMA's stringent security requirements. Both these laws set the standards for data protection and outline the consequences of non-compliance, which, in this case, included the massive loss of sensitive data.

The jurisdiction of the Privacy Act of 1974 and FISMA is strictly applicable to federal agencies, making their relevance to the OPM breach direct and significant. These laws are specifically designed to guide federal entities in handling and securing data, directly implicating how OPM manages its cybersecurity. The clear jurisdictional mandate provided by these laws required OPM to adhere strictly to prescribed data security measures. Unfortunately, the agency's failure to comply with these legal requirements contributed to the severity of the breach. By understanding the jurisdictional scope of these laws, it is clear that OPM was under a legal obligation to protect the data that was ultimately compromised. Compliance with these laws is not optional but a critical requirement for federal agencies, emphasizing the need for strict adherence to prevent data breaches.

The Privacy Act of 1974 and the Federal Information Security Management Act (FISMA) impose specific reporting obligations on federal agencies like OPM in case of a data breach. These laws required OPM to notify the affected individuals and relevant authorities, potentially including the public, depending on the extent of the breach. Reporting under these statutes involves several steps, such as identifying the breach's scope, notifying all potentially

affected stakeholders, and taking remedial actions to mitigate future risks. Such reporting is crucial for maintaining transparency and trust between the public and federal agencies. It also plays a vital role in regulatory compliance, ensuring that oversight bodies are informed and can take appropriate actions. Moreover, reporting can help understand what went wrong and how similar incidents can be prevented, making it a critical component of post-breach management.

Implementing specific CIS controls could have significantly minimized the risk and impact of the OPM breach. Inventory and Control of Enterprise Assets is vital for maintaining a precise and updated inventory of all assets, which helps detect unauthorized changes or access. 'Access Control Management' involves rigorous monitoring and control of who can access sensitive information, which could have prevented the misuse of stolen credentials. The 'Data Protection' control emphasizes encrypting sensitive data and controlling access, which could have made unauthorized access much harder for the attackers. Finally, 'Incident Response Management' is crucial for a timely and effective response to security incidents. Enhancing this control allowed OPM to detect and respond to the breach more quickly, possibly containing the damage. Together, these controls form a robust framework for defending against cyber attacks, and their proper implementation and monitoring are vital to safeguarding sensitive information.