Topic 3 Discussion 2

Outline one recent incident where failure to adhere to information governance (in favor of budget) resulted in significant financial loss. Explain how the article you selected relates to informational governance.

Hello Class,

The 2024 National Public Data breach serves as a stark example of how neglecting information governance in favor of budget constraints can lead to substantial financial losses.

The 2024 National Public Data breach, which compromised an estimated 2.7 billion records, exemplifies a scenario where budgetary limitations likely led to a weakening of information governance practices, resulting in significant financial losses(360 Privacy, 2025). National Public Data, a company tasked with managing sensitive background check information, became a target for cybercriminals. The sheer scale of the breach, involving billions of records, suggests a potential systemic failure in data protection and management, often a direct consequence of underinvestment in information governance.

Information governance is the overarching framework that dictates how an organization collects, stores, uses, protects, and disposes of its information assets(Blade Technologies, 2024). In the context of the National Public Data breach, a lapse in governance could manifest in several ways:

* Inadequate Data Classification and Inventory **-** Without proper classification, the organization might not have accurately identified or prioritized the protection of its most sensitive data, leaving vast amounts of personal information vulnerable.
* Weak Access Controls **-** Budgetary pressures might have led to insufficient investment in sophisticated access management systems, allowing unauthorized parties to gain entry.
* Insufficient Data Minimization and Retention Policies **-** Holding onto more data than necessary, or for longer than required, increases the attack surface. A robust governance framework would enforce strict data minimization and retention schedules.
* Delayed Security Updates and Patching **-** Cost-cutting measures could have resulted in a backlog of essential security updates, leaving systems exposed to known vulnerabilities.

The financial ramifications for National Public Data, though not fully detailed in the provided snippets, would undoubtedly be substantial. These typically include regulatory fines for non-compliance with data protection laws (such as GDPR or CCPA, depending on jurisdiction), the cost of forensic investigations, expenses related to notifying affected individuals, potential legal fees from lawsuits, and the immeasurable cost of reputational damage. As the IBM Cost of a Data Breach 2024 report indicates, the average global breach cost has reached USD 4.88 million, a figure that could be significantly higher for a breach involving billions of records(Bonderud, 2024). The incident underscores that while budgets are important, a foundational commitment to information governance is paramount to preventing such devastating financial and operational impacts.

References:

360 Privacy. (2025, September 5). *National Public Data Breach: Analyzing the Aftermath - 360 Privacy*. 360 Privacy. https://360privacy.io/articles/national-public-data-breach-analyzing-the-aftermath

Blade Technologies. (2024). *Exploring the National Public Data Breach: What Went Wrong? | Blade Technologies*. Bladetechinc.com. https://www.bladetechinc.com/news/exploring-the-national-public-data-breach

Bonderud, D. (2024, August 13). *Cost of a data breach in 2024 for the financial industry*. IBM. https://www.ibm.com/think/insights/cost-of-a-data-breach-2024-financial-industry