3-2 Activity: Incident Report Components

Joshua Merren

Southern New Hampshire University

CYB 320: Incident Response and Investigation

Professor Noah Nicholls

12 November 2024

The FEMA data breach primarily resulted from excessive data sharing due to inadequate data handling protocols, underscoring a significant lapse in the agency's adherence to data minimization principles (Newman, 2019). FEMA provided more information than necessary, including sensitive details like bank account numbers and home addresses, which were optional for the contractor's task. This incident underscores the need for a robust data governance framework specifying who can share data. The lack of practical training and management in data protection contributed to this oversight. For example, sharing full banking details for disaster survivors was unnecessary and posed a high risk of financial fraud if mishandled. This breach indicates a critical need for enhanced training programs focusing on data privacy and security for all FEMA employees handling sensitive information.

The data compromised in the FEMA breach included susceptible information that put the disaster survivors at significant risk (Abrams, 2019). Critical personal information leaked included banking details, such as bank account numbers and home addresses that could expose physical locations to malicious entities, and other personally identifiable information (PII) like full names and birth dates. An example of how this data could be misused includes potential phishing attacks where criminals could use detailed information to craft convincing, personalized scams. Such exposure also raises serious concerns about the survivors' physical security, as the disclosure of home addresses could lead to unwanted physical intrusions or harassment.

The Inspector General's report recommended that FEMA implement stricter data minimization practices and improve oversight and control of data sharing with external contractors to ensure compliance with established data protection standards (Abrams, 2019). These recommendations seek to establish a more secure environment for handling sensitive information and suggest a dynamic data governance system within FEMA that can adapt to

evolving threats and vulnerabilities. Additionally, updating contractual agreements to include strict data security clauses and conducting regular audits on data processes would ensure that data mishandling does not recur. If implemented effectively, these measures would significantly mitigate risks and reinforce FEMA's commitment to safeguarding personal information.

Adopting CIS Controls such as Continuous Vulnerability Management and Data Protection would play a pivotal role in rectifying the data breach's root causes and enhancing FEMA's overall security posture (Newman, 2019). Continuous Vulnerability Management involves conducting regular scans and assessments to identify and address vulnerabilities before attackers can exploit them. Implementing Data Protection controls would involve setting up robust encryption protocols for data at rest and in transit and strict access controls to ensure that only authorized personnel have access to sensitive information. These measures would not only prevent similar future breaches but also help build a resilient infrastructure capable of protecting sensitive data against emerging cyber threats.

References

Abrams, L. (2019, March 22). FEMA data leak exposes personal info of 2.3M disaster survivors. *BleepingComputer*. https://www.bleepingcomputer.com/news/security/fema-data-leak-exposes-personal-info-of-23m-disaster-survivors/

Newman, L. H. (2019, March 23). FEMA leaked data from 2.3 million disaster survivors. *WIRED*. https://www.wired.com/story/fema-leaked-the-data-2-million-disaster-survivors/