Fdic data breach: ethics involved in handling a data breach

INTRODUCTION

This essay is on the data breach incident that occurred at the Federal Deposit Insurance Corporation (FDIC), a United States Government Agency that provides deposit insurance for commercial banks and financial institutions in the US. There were many data breaches that took place in FDIC from 2015 to 2016 [1] , this essay is going to focus on one particular incident that occurred on October 2015, also known as the Florida Incident [2] .

A Data breach can be defined as a security issue where there is intentional or unintentional disclosure of sensitive, confidential or private information through unauthorized access of such data [3][4]. Private Information includes Personally Identifiable Information (PII) such as name, social security number(SSN), credit card number, fingerprint, Digital Identity etc., which can be used to identify the identity of an individual

In the case of the FDIC data breach, the former employee who worked as a Bank Secrecy Act Specialist had copied around 1, 200 documents with 100, 000 files onto her personal USB device containing customer data reports including data of 40, 000 individuals with over 10, 000 SSNs, bank transaction reports, Suspicious Activity reports, and other sensitive agency related data prior to her departure from the company. [9]

This activity was tracked by the FDIC's Information Security and Privacy staff (ISPS) who monitor such incidents using a Data Loss Prevention tool(DLP), one month after the incident took place. It is found that the employee had

turned in an encrypted USB while exiting the Agency. But the ISPS determine that it is not the same device that was used for copying the files. The Employee initially denies the existence of a secondary device but later verifies that there was indeed another personal USB device involved in the breach which was held in the possession of the Employee's Attorney.

The Data Breach Management Team (DBMT), a part of the ISPS team responsible for evaluating and determining the proper course of action to be carried out in the case of breach of sensitive data suggest to the Chief Information Officer (CIO) who is the primary decision maker for handling security issues, to classify the incident as a breach a month after it has been identified, on the grounds that a threshold of 10, 000 individuals' information had been compromised.

Furthermore, this incident isn't reported to the Congress: the FDIC's higher authority and to the affected individuals for four months since the breach occurred since it was uncertain whether to classify the data breach as a ' Major Incident' though there were grounds to classify it as a major incident earlier on. The CIO states that delay in making this decision is attributed to the fact that clear guidelines weren't available on the FDIC's Data Breach Handling Guide, though it was found that proper criteria was present in order to classify the incident correctly but were not followed through by the CIO and the management.

The USB is retrieved two months after the breach from the employee, until which time the data was vulnerable to external threats. The employee is made to sign a declaration stating that she no longer was in possession of

any other sensitive information and that no FDIC or customer related confidential data was dispersed from the USB device.

The purpose of taking up this case is to analyze the decision-making process when it comes to classifying and responding to a security breach and the time taken to notify the affected individuals.

A REVIEW OF THE LITERATURE ON THE SUBJECT

The FDIC data breach incidents were first declared to the general public by The Federal Times [5] and The Washington Post [7] , who report that 44, 000 FDIC customers were affected in five major data breach incidents that occurred due to employees copying sensitive files onto personal storage devices over the course of two years.

The particular case of the Florida incident is well documented in the Audit report [2] by FDIC's Office of Inspector General (OIG) which gives the detailed report of the breach along with the timeline of incidents that happened.

The decision-making process involved and the response to the events are given in detail in both the Audit report [8] and Memorandum [9] prepared by the OIG.

MAIN PARTICIPANTS AND ACTIONS

PRIMARY PARTICIPANTS

The Former Employee

The Employee unlawfully copied the sensitive data despite company policy on to their personal storage device while exiting the Agency.

The Employee withheld sensitive data by denying to provide the original device used to copy the confidential files.

The CIO

The Chief Information Officer takes over a month to classify the incident as a data breach and takes over four months to report it to Congress, due to which the affected customers are not informed earlier of their data being compromised.

The CIO states lack of clear guidelines present for the delay in decision making and breach notification.

SECONDARY PARTICIPANTS

The ISPS Staff

The ISPS Staff report that a huge quantity of data was transferred on a removable media nearly one month after the first instance of file transfer using the Data Loss Prevention tool.

They also identify that the device turned in was not the actual device used for copying the files.

The DBMT Staff

The Data Breach management Staff initiates meetings with the Employee to retrieve the files and determine the possible course of action that needs to be taken to quarantine the spread of sensitive data.

The DBMT attributed to the delayed decision making as they did not effectively asses the risk of harm to affected customers. [8]

IMPLIED PARTICIPANTS

The Financial Institutions under FDIC

The Commercial Banks and financial institutions, the direct customers of FDIC whose data files had been copied on to the storage device.

Customersof the Financial Institutions

The customers of the Banks under FDIC are indirectly affected by the breach since their PII had been exposed via the data files.

REDUCED LIST

The DBMT staff, though responsible for analyzing the incident and determine what course of action to take, are not the final decision-makers; instead, they give their inputs to the CIO who has more control of the actions to be taken.

The ISPS team report the data breach incidents through their Data Loss Prevention tool. Since they don’t contribute to the decision making, they need not be included in this list.

The Financial Institutions under FDIC and the customers of these institutions can be excluded since they did not participate in the data breach.

The CIO is a key member in the decision-making process. He is responsible for deciding whether the incident was a major breach of data and to report it to the higher authority within a specific time period.

Thus, based on these statements, all participants excluding CIO and the former employee can be excluded from the list of key participants.

LEGAL CONSIDERATIONS

In this case, one of the legal issues to be considered is Cyber Law through the violation of FDIC's security policy by the former employee, who despite security rules used a personal storage device to copy sensitive files. Another law to be considered is the Data Protection Act, where a company must ensure that adequate security measures are in place so that sensitive data is not compromised or misused. In our case, the Agency could have disabled the access of systems using removable media following multiple data breach incidents that happened to the company in the past. Security Breach Notification Law can is also applicable since it took four months to notify the customers affected by the data breach, during which time the customer's personal data was vulnerable to external threats.

POSSIBLE OPTIONS FOR PARTICIPANTS

PRIMARY PARTICIPANTS

The Former Employee

- Could have followed company policy and not transferred sensitive agency data onto a personal device.
- Could have returned the original USB used for copying the files once the security incident was reported.

The CIO

- Could have classified the incident as breach once it was known that a substantial amount of PII was copied onto the USB.
- Could have followed the recommendation of the DBMT team and followed the criteria provided in the Data Breach Handling guide to classify the incident as a major data breach earlier on, allowing for early breach notification and effective risk mitigation to be facilitated.

POSSIBLE JUSTIFICATIONS FOR ACTIONS

The Employee

- Denied the existence of the original USB for fear of legal actions against her.
- Thought the use of a secondary device would not be detected.

The CIO

The CIO can justify his actions by stating that:

- There was a need for extensive analysis of the evidence and evaluation of risk of harm as the reason for not concluding the incident as a data breach earlier on.

- The lack of proper guidelines provided in the Data Breach Handling guide lead to the delayed classification of the breach as a ‘ Major Incident’.

KEY STATEMENTS

“…The ISPS determine that it is not the same device that was used for copying the files…”

“…The Employee initially denies the existence of a secondary device…”

“…to classify the incident as a breach a month after it has been identified…”

“…This incident is reported to the higher authorities and to the affected individuals, four months after the breach occurred…”

“…though it is found that proper criteria were present in order to classify the incident correctly…”

“.. The USB is retrieved two months after the breach, till which time the data was vulnerable to external threats…”

QUESTIONS RAISED

Should there have been more safety measures in place given that similar cases of a data breach had occurred within the agency in the past?

Could more clear guidelines have been established for the incident to be classified as a breach earlier on?

Should the CIO have reacted more quickly in declaring the breach as a major incident given the PII of over 10, 000 individuals was compromised?

Could there have been a more efficient analysis of risk impact undertaken so that the FDIC customers could have been notified immediately?

ANALOGIES EMPLOYED

There have been many cases where unauthorized access to data have happened leading to a security breach and organizations delaying response in notifying the affected individuals.

A similar case to the FDIC data breach is the one that happened to Equifax, a credit monitoring agency when hackers gained access to their customer records through a software portal. The company didn't notify this breach to the public for two months restricting the customers to take alternate measures to protect their data. [10]

The famous case of the Uber data breach is of significance since the company only made the breach public after a year of the incident. They reportedly paid 100, 000 dollars to the hackers to destroy the data which caused concern as there is no way to verify if the data had been thoroughly destroyed [6].

Since in our case, the data breach was due to an insider, the Ofcom data breach shares some similarity where it was found out that a former employee had been collecting potentially sensitive third-party data over the

course of 6 years before leaving the company and tried to selling it to Ofcom's competitor. [11]

CODES OF ETHICS UTILIZED

For this case, the ACM codes of Ethics [12] can be applied to address the actions of the former employee who breached the following code of ethics,

- [1. 3] Be honest and trustworthy, by hiding the existence of the actual personal storage device for two months since the security violation was identified.
- [1. 6] Respect Privacy, by breaking company security policy by unlawfully copying sensitive data that contained private and PII of over 40, 000 individual.
- [1. 7] Honour Confidentiality, by copying confidential company data.

The Data Processing Management Association DPMA codes of ethics [13] can be applied to the CIO while making decisions regarding breach notification,

- Protect the privacy and confidentiality of all information entrusted to me. Use my skill and knowledge to inform the public in all areas of my expertise.
- Never misrepresent or withhold information which is germane to a problem or situation of public concern nor will I allow any such known information to remain unchallenged.

THREEALTERNATIVEPROPOSALS THAT COULD PROVIDE ETHICAL SOLUTIONS

PESSIMISTIC

The former Employee could have easily misused the sensitive data by selling the information to a competitor or published it to the public within the one month it took to identify the data breach. Furthermore, it took a month more to declare the incident as a data breach and two more months before the device was retrieved by which time the data could have fallen into the wrong hands. The delay in notifying the customers affected and inefficient risk impact analysis prevented enforcing alternate measures to protect data immediately after the data breach was identified.

OPTIMISTIC

This incident could be used to identify flaws in the FDIC's data loss prevention system and aide in updating the company's security policy. Since the delay in identifying the data breach was found to be due to a large number of security incidents bombarding the DLP tool, new criteria can be defined to identify breaches earlier. The lack of stringent regulations and poor breach response can also be addressed and rectified.

COMPROMISE

One of the ethical duties of any organization is to ensure personal data of its customers is secure from any sort of threat and to provide early notification in case any breach or leak of data has occurred. On this note, FDIC should update its security systems to be more efficient in identifying security threats and implement proper guidelines and provide a clear outline of criteria for classifying and handling security breaches to be more effective and timely in notifying its customers about a potential security threat. Establishing key response metrics and documenting of decisions in relation

to previous data breaches could also help save time while dealing with data breaches.

ETHICAL THEORY THAT HAD THE MOST INFLUENCE ON MY CONCLUSION

Based on the analysis of the scenarios, an ideal ethical solution can be bought out by compromise. The FDIC should agree to implement better guidelines to ensure effective decisions are made at an earlier stage of identification of a security issue. They should also make sure proper risk mitigation factors are in place and that the customers are notified at the earliest once a major data breach is identified.

CONCLUSION

Handling data breaches can be quite tricky for organizations as often there are difficulties in establishing guidelines and criteria for handling breaches. It is important to note that organizations are often bombarded with large quantities of security alerts on a daily basis. It is the prime responsibility of an organization to implement updated security measures to protect customer data and it’s their ethical duty to inform affected individuals promptly once a data threat is identified. This applies for the case of the FDIC data breach, hence rectifying these issues can improve the ethics of decision making involved in handling data breaches and early notification to customers thereby ensuring the protection of sensitive data.

REFERENCES

[1] us-dgs. com. (2017) .” What we can learn from the FDIC”. [online]. Available at: https://us-dgs. com/dgs-blog/2017/5/30/what-we-can-learn-from-the-fdic

[2] FDIC OIG (2017). “ Office of Audits and Evaluations Report No. AUD-16-004AUD”.[online]. Available at: https://www. fdicoig. gov/sites/default/files/publications/16-004AUD. pdf

[3] CyberScout (2018) .“ Difference between a data breach, compromise, leak or a breach of trust?” [online]. Available at: https://cyberscout. com/education/blog/does-anyone-really-know-the-difference-between-a-data-breach-compromise-leak-or-a

[4] Techopedia. com.” Definition of Data Breach”[online]. Available at: https://www. techopedia. com/definition/13601/data-breach

[5] Federal Times(2016).” Congress investigating October FDIC data breach”[online]. Available at: https://www. federaltimes. com/2016/04/28/congress-investigating-october-fdic-data-breach/

[6] The BBC(2017).” Uber concealed huge data breach”.[online]. Available at: https://www. bbc. com/news/technology-42075306

[7] The Washington Post. (2016).” Inadvertent cyber breach hits 44, 000 FDIC customers[online]. Available at: ” https://www. washingtonpost. com/news/powerpost/wp/2016/04/11/inadvertent-cyber-breach-hits-44000-fdic-customers/? utm_term=. b9507c27833e

[8] FDIC OIG(2017).” Office of Information technology and Cyber Report No. AUD-17-006AUD0”.[online]. Available at: https://www. oversight. gov/sites/default/files/oig-reports/FDICOIG-17-006AUD. pdf

[9]FDIC OIG(2018).” The FDIC’s Response, Reporting, and Interactions with Congress Concerning Information Security Incidents and Breaches”.[online]. Available at: https://www. fdicoig. gov/publications/fdic%E2%80%99s-response-reporting-and-interactions-congress-concerning-information-security

[10] J. Kevin Foster(2018).” What are the Ethical Implications of the Equifax Data Breach”.[online]. Available at: https://johnkevinfoster. com/equifax-data-breach/

[11] Welivesecurity. com(2016).” Ofcom experiences major data breach thanks to former employee”.[online]. Available at: https://www. welivesecurity. com/2016/03/11/ofcom-experiences-major-data-breach-thanks-former-employee/

[12] ACM. org(2018)” ACM Code of Ethics and Professional Conduct”.[online]. Available at: https://www. acm. org/code-of-ethics

[13] Data Processing Management Association(2011).” Code of Ethics(1981)”.[online]. Available at: http://ethics. iit. edu/ecodes/node/4027