4-1 Short Paper: Impact of a Data Breach

Michael Singletary

IT-412, 17EW1, SNHU

Introduction

The aircraft manufacturing company that experienced a data breach resulting in the loss of government contract-related employee records, bank account numbers, and blueprints is demonstrative of the seriousness of data security in business. This scenario is increasingly common as hackers more directly and indirectly target vulnerable computer systems for attack. While many of these attacks are not specifically catered to the organization that is affected, data security standards must be upheld to ensure that sensitive information is protected both from targeted and more broad attempts at unauthorized access of their systems. Laws at both the state and federal level set standards for what types of data should be protected and how, including consequences of failing to properly protect this data.

Violations

This aircraft manufacturing company violated a number of laws and regulations when it allowed this employee to insecurely allow unauthorized access to their systems and network. First, the company was not in compliance with the Federal Information Security Management Act of 2002 (FISMA), specifically the NIST Special Publication 800-53 which sets the standards for baseline security policies to protect sensitive information. (U.S. Dept. of Commerce, 2013). These standards require certain levels of security, action plans, and accreditation reviews that evaluate the security posture of the company to ensure compliance and a high security posture. These controls would have significantly mitigated this threat.

Additionally, FISMA requires that organizations working with the federal government and storing data related to its contracts must maintain certain security controls that protect the data on their systems. The aircraft manufacturing company was lacking certain controls that prevented its employee from opening and utilizing remote access protocols, protected by only a

simple password, that allowed them to work from home more easily. According to the Federal Information Processing Standards Publication 200 (FIPS), referenced by FISMA, companies contracting with the federal government must implement certain minimum security controls including access control policies. (NIST, 2006). Implementing these controls would have prevented the employee from initializing their own remote access solution, or at least required a stronger authentication method.

Finally, the aircraft manufacturing company is required by the State of California to notify affected persons of this data breach. A large number of personally identifiable information (PII) data was accessed in this data breach, putting their identities at risk for theft and fraud. The State of California requires that companies affected by breaches like this notify affected persons as quickly as reasonably possible so that they may take efforts to mitigate the effects of this breach. (California, 2017).

Prevention

Although breaches like this are incredibly difficult to prevent every time, there are a number of controls that a company may implement to significantly decrease their possibility or to mitigate the loss of sensitive information if a breach occurs.

First, this company should implement system access controls that prevent non-administrative users from being able to install services or open ports that expose their computer systems and the network to incoming network connections. In addition, network administrators at the company should implement a software-based firewall at the router level that filters out unauthorized connection attempts to the network from the internet. This would also prevent remote access connections from being allowed on the network.

Second, password creation and maintenance standards should be implemented. These controls would define secure requirements for each password, requiring selections that include things like capital letters, symbols, and numbers, and also require that they be changed frequently and that old passwords may not be reused.

Last, simple data encryption standards should be implemented that require sensitive information like employee records, social security numbers, and bank account information are stored only in an encrypted format. This would prevent data breaches from yielding useful information to the attackers, better protecting those affected by the breach from identity theft or fraud.

Conclusion

While companies are increasingly facing a larger amount of threats targeting sensitive information that can be leaked for fun or profit, there are a number of steps that these companies can take to mitigate these threats and the impacts to the company and its employees and customers. Simple security controls defined by both state and federal laws, as well as industry standards, help protect these organizations from breaches or limit the usefulness of the data obtained from a breach. By not following these laws and standards, the aircraft manufacturing company unnecessarily placed itself, its employees, and the nation at risk in the event of a data breach like the one that occurred.

References

California Legislative Information (2017, January 1). Accounting of Disclosures. *California Legislative Information*. Retrieved from http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.29

National Institute of Standards and Technology. (2006, March). Minimum Security Requirements for Federal Information and Information Systems. *Federal Information Processing Standards Publication*. Retrieved from http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf

U.S. Dept. of Commerce. (2013, April). Security and Privacy Controls for Federal Information Systems and Organizations. *NIST Special Publication 800-53.* Retrieved from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf