CIS-481: Introduction to Information Security

InfoSec Chapter Exercise #3 - Option B

Team: ICE 3
Participants: Marvin Weaver, Kitrina Justus, Aaron Gordon, Brandon Crosier, Sam Steele

Logistics

A. Get together with other students on your assigned team in person and virtually.
B. Review the four options available and decide on only one to pursue as a team.
C. Discuss and complete this assignment in a collaborative manner. Don't just assign different problems to each teammate as that defeats the purpose of team-based learning.
D. Choose a scribe to prepare a final document to submit via Blackboard for grading, changing the file name provided to denote the number of your assigned **Team**.

Problem 1
In the United States, there is no single, uniform law that governs disclosure of data breaches. Instead, most states have passed piecemeal legislation with various covered elements and disclosure requirements. Companies can be (and are) held to entirely different compliance standards depending on which state an affected individual lives in. Kentucky is one of the last states to pass such legislation. Reference: https://www.bakerlaw.com/files/uploads/Documents/News/Articles/INTELLECTUAL%20PROPERTY/2015/Haggerty-Patrick-Article-May-2015-Bench-Bar.pdf

1. Who are considered covered entities (information holders) under the KY legislation? Who are explicitly excluded? Why do you think that KY chose to exclude these entities? *(5 points)*

   In the state of Kentucky the covered entities, information holders, are "any person or entity that conducts business in Kentucky." It is also any person or entity that is subject to HIPAA or GLBA. The law does not apply to any Commonwealth agency or any of its local government or political subdivisions. Kentucky excludes those entities because there is a separate breach notification law that any agency of the Commonwealth or nonaffiliated third party which includes, "any person that (a) has a contract or agreement with an agency; and (b) receives personal information from the agency pursuant to the contract or agreement."

2. What is the KY definition of PII? *(8 points)*

   PII stands for personally identifiable information. An individual's first name or first initial and last name in combination with any one or more of the following data elements, when the name or data element is not redacted: Social Security number; Driver's license number; or Account number or credit or debit card number, in combination with any required security code, access code, or password to permit access to an individual's financial account, counts as PII.

3. Would acquisition of encrypted data be considered a breach that would trigger notification requirements in KY? *(2 points)*

   No the acquisition of encrypted data wouldn't be considered a breach that would trigger notification requirements in KY because in KY the data acquired has to be unencrypted and unredacted for it to be considered a data breach.

BakerHostetler maintains a comprehensive comparison of the various state data breach laws at:
http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/Data_Breach_Charts.pdf
and an interactive map at: https://www.bakerlaw.com/BreachNotificationLawMap

4. Compare the summary of Kentucky's data breach law to California's in the various sections. Which of these do you think offers stronger protection to its citizens? Explain. *(4 points)*

   In Kentucky, the Attorney General or State Agency is not required, but if more than 1,000 persons must be notified at one time, then the information holder must notify all consumer reporting agencies. Notification is not triggered by only access. There is no explicit number of days that you are required to take action, but it must be done expediently and without unreasonable delay.

   In California, if more than 500 residents have been impacted by a breach, both the residents and the Attorney General must be notified. If it is specifically medical information the California Department of Health services must be notified of the breach within 15 business days. Like Kentucky, notification is not triggered by only access.

   Comparing the two states, California does a much better job of protecting its citizens in multiple areas. California's definition of personal information is much broader than that of Kentucky. California also covers a broader group of people with their definition of persons covered being "any person that (a) has a contract or agreement with an agency; and (b) receives personal information from the agency pursuant to the contract or agreement." Kentucky defines their persons covered as "any person who conducts business in Kentucky". There is also no explicit number of days for Kentucky to take action, but depending on the information accessed, California may require notification within 15 business days. Additionally, depending on the number of residents affects, California companies must report to the Attorney General while Kentucky companies do not, especially not at 500.

Companies are frustrated by the inconsistencies inherent in the piecemeal laws in 47 (and counting) states and have asked for one national law. Review the BakerHostetler blog post on this subject at: http://www.dataprivacymonitor.com/data-breach-notification-laws/dear-lawmakers-your-new-breach-notice-laws-should-address-these-issues/

5. If you were lobbying for national data breach legislation on behalf of a company, what would be your top three issues for the legislation to address? *(6 points)*

   Our top three issues are risk of harm, notification timing, and discovery. Risk of harm is most important because it would only notify individuals if there is a risk to their data, like if their Social Security number was stolen and posted on the internet. By only notifying individuals when there is an issue, it allows the individuals to know there is a serious issue and won't lead to notification fatigue.

   Notification timing is also important for much the same reason. By allowing the company time to investigate and see if there is cause for concern, it doesn't unnecessarily worry their customers. It also gives the organization time to develop a course of action for affected customers if it is determined that they are at risk.

   Discovery is important because a company that has been infiltrated needs to notify their affected parties of when the event occurred. By postponing the discovery until the company discovered something was wrong, they may be pushing the timeline too far forward for some affected individuals to find something wrong. For example, if a credit card was stolen, but the discovery wasn't until two weeks later, the customer would start looking at dates starting two weeks later, but they may miss something in those missing weeks.