CIS-481: Introduction to Information Security

InfoSec Chapter Exercise #3 - Option B

Team: 1

Participants: Zack Graas, Jacob Forcht, Trevor Hagel

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)*

According to Patrick Hagerty under Kentucky legislation, the information holders are "any person or entity who conducts business in Kentucky " (Hagerty 1) and excluded entities are "any person or entity subject to HIPAA and GLBA.6 (...) [also] any agency of the Commonwealth or any of its local governments or political subdivisions".(Hagerty 1) So every entity and person who does business in Kentucky is classified as an information holder. People and entities excluded from this are ones that are subject to HIPPA, GLBA.6, and any agency of the commonwealth. We think the entities that are excluded because of HIPPA and GLBA.6 are excluded due to the fact that they already have federal laws governing data breaches so they don't need the Kentucky state laws also applied to them. We think the entities that were excluded due to being a part of any agency of the commonwealth were because that these agencies already have their own laws applying to them. Patrick Hagerty supports this by stating: "There

is a separate breach notification law applicable to any agency of the Commonwealth and nonaffiliated third parties"(Hagerty 1-2).

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

According to Patrick Hagerty when talking about Kentucky's definition of personally identifiable information:

> "which is defined as "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: (1) Social Security number; (2) Driver's license number; or (3) 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."10 The law only applies to unencrypted and unredacted computerized data—it does not apply to paper records." (Hagerty 2)

So in Kentucky personal identified information is comprised of several components: social security numbers, driver's license numbers, financial account numbers accompanied with means to access it such as passwords, and credit card and debit card numbers with the information required to use it such as a PIN number. Kentucky specifically defines PII as first name or first initial with the last name in addition to one of the previously listed components. An example of this would be J. Smith 4040-40-4040 this is what is classified as personally identified information in Kentucky.

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

According to Hagerty in regards to encrypted data breaches:

> "The law defines a 'breach of the security of the system' as the 'unauthorized acquisition of unencrypted and unredacted computerized data that compromises the security, confidentiality, or integrity of personally identifiable information maintained by the information holder(...)"(Hagerty 2)

Hagerty mentions only unencrypted data when stating the law's definition of a "breach of the security system" therefore encrypted data would not result in a breach and would not require notification under Kentucky's current laws.

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)*

California:

- Definition of “Personal Information” is Broader: Users must use an username/email along with a password with a security question to allow access to their online account to get the information of medical, license plate registration, and health insurance. Medical information included their Social Security, mail address, and phone number.
- Require Risk-of-Harm Analysis: None
- Require a Notice to Attorney General: Any person who notifies more than 500 people that they have been breached by a single security threat, then they must complete an Attorney General’s Breach Form and have to attach a copy of the notification letter that include the affected residents
- Requires Notification with in a Time Frame: For clinics, the Medical Information Breach Notification statute could apply. The statute states that the licensees must notify the patients no later than 15 business days after any unauthorized access.
- Permit a Private Cause of Action: Customer injured by violations of general breach can make a civil actions to recover any damages.
- Encryption Safe Harbor: Applies if the information is not encrypted or encrypted if the key allows unauthorized party to load the data.

Law Map Information

- Personal Information: Social Security Number, Drive License Number, Passport Number, Account Number, Username/Password combination, Medical/Health Information, Biometric data
- People Covered: State agencies, people, and businesses; Clinics and other medical agencies
- Encryption Trigger: Applies if the information is not encrypted or encrypted if the key allows unauthorized party to load the data. Trigger upon notification of unauthorized acquisition of confidential information.
- Specific Requirements: Follow these specific headings: 1. What Happened; 2. The Information that was involved; 3. What things are they doing; 4. What can you do; 5. For More Information
- Timing: Without Unreasonable Delay
- Penalty/Private Right of Action: Allow for civil action to recover data that’s more than $100 and less than $750.
- Other Provisions: Any person who notifies more than 500 people that they have been breached by a single security threat, then they must complete an Attorney General’s Breach Form and have to attach a copy of the notification letter that include the affected residents
-

Kentucky:

- Definition of “Personal Information” is Broader: None
- Require Risk-of-Harm Analysis: Required if unauthorized acquisition of computerized data which is compromised through the security of the personal information maintained by the information holder.
- Require a Notice to Attorney General: None
- Requires Notification within a Time Frame: None
- Permit a Private Cause of Action: None
- Encryption Safe Harbor: activated when unauthorized acquisition of unencrypted computer data.

Law Map Information

- Personal Information: Social Security Number; ID/Driver License Number; Account Number for Banks
- People Covered: Any person or business that holds information and the business must be conducted in Kentucky
- Encryption Trigger: Only applies unauthorized computer data; Applies if the information is not encrypted or encrypted if the key allows unauthorized party to load the data. Trigger upon notification of unauthorized acquisition of confidential information.
- Specific Requirements: None
- Timing: Without Unreasonable Delay
- Penalty/Private Right of Action: None
- Other Provisions: If more than 1,000 people get notified at once, the holder must notify all customer agencies and credit bureaus that collect files on a nationwide basis without unreasonable delay.

We believe that California protects their citizens more than Kentucky because they have a wide variety of protections and trigger to notify people if their information is being stolen. Also, they have a lot more laws and protections than Kentucky. For example, California have to notify their Attorney Generals if their information was breached and Kentucky doesn’t have any to notify if their information is breach beside the government.

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)*

If I were a lobbyist for national data breach legislation, I would want the legislation to address notification timing, notification method, and risk of harm. As a company, it is easiest in terms of man hours and policy setting to do everything in a unified manner rather than have to vary the approach state to state. I think that notification timing should have two timeframes. One within thirty days stating that a breach occurred, and another within ninety days stating the exact risk of harm that the customer should expect from the breach. The first notification should be able to be delivered by any method, but the second should be by mail as well as a secondary method. This tiered system will allow users to be notified of a breach quickly, as well as maintain their interest for learning more about their risk of harm in a secondary notification which when delivered by mail gives the company and customer a solid paper trail of exact risk and notification timeframe. I also think that in the name of transparency the risk of harm notification should be required even if an investigation concludes that the breach will not result in any harm. It is best for the consumer to know all the facts that are available at the time.

Sources

Hagerty, Patrick. *A Primer on Kentucky's Notification Law*. https://www.bakerlaw.com/files/uploads/Documents/News/Articles/INTELLECTUAL%20PROPERTY/2015/Haggerty-Patrick-Article-May-2015-Bench-Bar.pdf.