Alex Smetana

CIS260

04/22/2022

For this assignment, you will assess the civil liability risk of a database. This will require doing a little research to come up with a figure. There is no one correct answer here - it's an estimate based on previous penalties and fines levied, so you will need to find previous settlements and extrapolate. Be sure to cite your sources and explain how you arrived at your result. Assume this database contains CHD and PII - 320,000 records worth.

How much liability risk is here in PII, fines and penalties, assuming Wisconsin law applies?

In Wisconsin, a data breach is defined as "Personal information acquired by an unauthorized person, excluding certain good faith acquisitions." Data breaches carry a very high risk and can hurt the reputation of a company.

PII information is defined as the following under Wisconsin:

- Social Security number.
- Driver's license number or state identification card number.
- Financial account, credit card, or debit card number or any security code, access code, or password that would permit access to an individual's financial account.
- DNA profile or Unique biometric data.

In a database that has over 320,000 records worth of CHD and PII has a very high liability risk. Anyone who is found in violation of a data breach must notify the consumer within a timely matter or 45 days. Violations may result in civil penalties or other remedies.

"Whoever is concerned in the commission of a violation of this chapter for which a forfeiture is imposed is a principal and may be charged with and convicted of the violation." Fines will vary based on the degree of the data breach. For example, a violation of HIPPA or PCI will carry its own consequences.

Overall, the Liability risk of a 320,000 PCI database cannot be understated. It is huge and the more PII included, the higher the Liability risk. Ultimately, fines and lawsuits are to be expected in the event of a data breath that exposes PII information.

How much risk is here for PCI fines, and what other threats are present?

A database that contains CHD and PII - 320,000 records worth is classified as a PCI Level 2 Compliance. Violating PCI guidelines can vary depending on the amount of time a

business is found. You can expect financial penalties from $5,000-$10,000 per month for violating PCI compliance guidelines. One to three months of being non-compliant, translates anywhere from $10,000 - $5,000. Four to six months can result to $50,000 - $25,000. Seven or months translates to $100,00 -$50,000. These all vary depending on the size.

In the event of a data breach, the fines present are astronomical. A fine can range anywhere from $50-$90 per cardholder data exposed, depending on the severity of the information. With 320,000 records worth a of data the fines can vary drastically. Assuming a worst-case scenario, where all the information is exposed can be very expensive. At $50-$90 per cardholder equates to $16,000,000,000 - $228,000,000 in fees.

On top of the fees, the threat of lawsuits and loss of reputation is present. You can expect a loss in business if the company manages to stay in business all things considered. If a bank discovers that your company isn't PCI compliant, you can be denied the right to process transactions. Actions must be taken to remain PCI compliant and prevent any sort of fees as it can cripple any business.

In conclusion, a business will face fees for: PCI DSS Penalties for Non-Compliance, costs of reissuing cards, legal costs, Investigations and Audits, and Fraud Presentation Technologies.

If a class action lawsuit were brought again the organization, how much would a settlement likely cost?

Unfortunately, with a data breach happens, lawsuits are going to happen. Lawsuits are expensive and when dealing with the exposure of cardholder data, it the fees will rack up. If your found to be non-compliant with PCI, the lawsuit severity will increase

An example, in a Target data breach, loss the credit card data of over 40 million customers. The company spent almost $150 million dollars in a lawsuit with over 47 attorneys to settle the issue. Another example is Equifax, which was held responsible for the loss of over 147 million personal data back in 2017. Unfortunately, they had to pay more than $550 million.

Using these two case studies as a basis, a full data breach with 320,000 records breached, would add up in $1,00,000 – $1,200,00 ballpark range in fees. However, the fees could drastically vary significantly more or less depending on the severity of the data breach. After the fact, forensic investigations an audit will be needed. These fees can add up and be costly for your business. Regardless of the actual number, it depends on the severity of the data breach. Lawsuits are expensive and will hurt even the most prestigious business.

Resources

https://lewisbrisbois.com/privacy/US/Wisconsin/data-breach

https://docs.legis.wisconsin.gov/statutes/statutes/134/98

https://datcp.wi.gov/Documents/IDTheftDataBreach607.pdf

https://www.pcidssguide.com/what-are-the-pci-compliance-fines-and-penalties/

https://rubygarage.org/blog/price-of-pci-dss-non-compliance