Data Breach Notification Law: Policy Analysis Paper #3

Antonio Shields

School of Cybersecurity, Old Dominion University

CYSE 425W: Cybersecurity Strategy and Policy

Prof. Lora Pitman

April 20, 2023

In continuing the discussion on the Data Breach Notification Law, the first paper focused on introducing the data breach notification law in some of its domestic and international variations. The second paper focused on the political implications and governmental impact of establishing and enforcing the data breach notification law both domestically and internationally. This paper will focus on how data breaches impact society, specifically affected individuals and breached companies, leading to the creation of the data breach notification laws that are in place today.

The data breach notification law in its different variations, was at its basis, established to mandate companies and businesses to notify impacted individuals that the personal information the company or business was entrusted to utilize and keep secure, had been accessed by unauthorized means. The notifications are intended to inform the impacted individuals of the data breach, when the breach occurred, what was taken, and actions needed to be taken by the impacted individuals to protect themselves in case the stolen information is used. In 2014, the Bureau of Justice Statistics reported that in the United States, 17.6 million residents were victims of identity theft, where 37% of the victims were unsure of how their information was stolen, 45% were informed by the breached financial institution, and 19% discovered their information was compromised when they noticed fraudulent activity on their statements (Labrecque et al., 2021, p. 560). Risk Based Security reports that in 2020, there were 3,932 breaches that were publicly reported where 37 billion records worldwide containing personal information were stored or exposed by hackers (Madan et al., 2022, p. 1). It should be noted that in 2014 all 50 states did not have data breach notification laws in place with the last state, South Dakota, going into effect in 2018, but these two statistical examples show that many individuals are impacted by data breaches and steadily increasing. The effects a data breach can have on affected individuals are

oftentimes associated primarily with the financial impact it could have, but data breaches can affect an individual emotionally and mentally as well.

In 2015 when the Office of Personnel Management (OPM) suffered a data breach that affected millions of government employees, their families, friends, and anyone used as a clearance reference, caused an emotional uproar on Twitter (Bachura et al., 2022, p. 882). The emotions categorized during a two-month period of observation of tweets regarding the OPM data breach were Anxiety, Anger, and Sadness (Bachura et al., 2022, p. 886). The results showed that as the breach first became public knowledge, more people were anxious about the breach compared to anger and sadness, although anger stayed relatively high throughout (Bachura et al., 2022, p. 889). As more details of the breach were revealed over the month and understanding of what occurred increased, the anxiety about the situation decreased as anger and sadness increased, with anger being the highest emotion displayed (Bachura et al., 2022, p. 889). As more time passed since the initial announcement of the breach, sadness about the situation became the highest emotion with anger decreasing slightly and anxiety being low. (Bachura et al., 2022, p. 889). The results showed that emotions changed as the details of the incident were revealed more in-depth.

Some of the mental or psychological effects that have been reported to arise from data breaches are anxiety, depression, post-traumatic stress disorder (PTSD), and paranoia (Kilovaty, 2021, p. 18). According to Kilovaty (2021), “Further psychological research has confirmed the prevalence of diagnosable mental disorders resulting from data breaches, such as Major Depressive Disorder, Panic Disorder, Agoraphobia, and more.” (p. 19). When data breaches occur, the fear of how the personal information that was taken will be used, the process of securing the platforms that were compromised, which can range from changing passwords to

making new accounts to getting new cards depending on the type of breach, can be a daunting task. Trust issues may also arise due to a data breach because the impacted individual may never trust that breached company or business again and the impacted individual may be hesitant to give personal information to other companies or businesses in the future. Data Breaches of personal information could also result in harassment, stalking, microtargeting, or doxing of affected individuals, which could contribute to paranoia and fear concerns (Kilovaty, 2021, p. 43).

The other impacted party when a data breach occurs is the company or business itself. When a data breach occurs, the company or business that was breached will have to assess the incident, figure out what was taken, address the vulnerability, and depending on what state and/or countries they conduct business in, be required to notify the individuals whose data was compromised according to the appropriate data breach notification laws. Public notification of a data breach of a company or business, according to Madan et al. (2022), "can lead to fines from regulators, customer turnover, loss of reputation, and legal costs." (p. 1). If it can be proven that a breached company or business did not protect consumer data privacy to the best of its ability, the Federal Trade Commission (FTC) can bring about charges (Labrecque et al., 2021, p. 560). According to Labrecque et al. (2021), "The FTC is tasked with protecting consumers from deceptive and unfair businesses, which includes consumer data privacy, providing best practice guidelines for businesses, and monitoring and acting on illegal and/or risk business practices in the U.S like data breaches." (p. 560). Customer turnover can result from loss of confidence and trust in the company or business following a data breach. Impacted individuals may be skeptical to continue doing business with a company that compromised their information and may prefer taking their business somewhere else in search of more reliability and dependability. The

reputation of a company or business after a data breach will sustain damage, but full transparency during the incident and after the incident to demonstrate that steps were taken to address the breach and mitigation strategies were applied to prevent future breaches from occurring can assist in repairing their image over time. Legal costs from a data breach can come from lawsuits brought by the affected individuals either separately or through a class action lawsuit and can impact the company's or business's bottom line if required to pay damages. From an employee perspective, resignations, firings, or layoffs may occur if the data breach effects are significant enough. In the OPM data breach incident mentioned earlier, OPM Director Katherine Archuleta resigned from her position following the acknowledgment of 21.5 million background investigation data records being compromised (Bachura et al., 2022, p. 883).

Data breach notification laws aim to keep companies and businesses honest and transparent when breaches occur, to notify the impacted individuals in a timely manner, and assist in protecting the impacted individuals from the potential data breach effects. From the first data breach law that was enacted in California in 2002 to now, the laws have been established in locations that at one time did not have a law and amended in other locations when the scope of the law requires modification. As more research continues to be conducted on the data breach effects on impacted individuals, some of the currently less acknowledged emotional and mental effects will be considered and the laws will be improved to provide support resources for those effects that are currently not supported.

References

Bachura, E., Valecha, R., Chen, R., & Rao, H. R. (2022). The OPM data breach: An investigation of shared emotional reactions on Twitter. *MIS Quarterly*, *46*(2), 881–910. https://doi.org/10.25300/misq/2022/15596

Kilovaty, I. (2021). Psychological data breach harms. *North Carolina Journal of Law & Technology*, *23*(1), 1–66. https://doi.org/10.2139/ssrn.3785734

Labrecque, L. I., Markos, E., Swani, K., & Peña, P. (2021). When data security goes wrong: Examining the impact of stress, social contract violation, and data type on consumer coping responses following a data breach. *Journal of Business Research, 135*, 559–571. https://doi.org/10.1016/j.jbusres.2021.06.054

Madan, S., Savani, K., & Katsikeas, C. S. (2022). Privacy please: Power distance and people's responses to data breaches across countries. *Journal of International Business Studies*, 1–24. https://doi.org/10.1057/s41267-022-00519-5