Research reveals massive failures in US cybersecurity laws

February 19 2024, by Dan Tran

Credit: Unsplash/CC0 Public Domain

In the world of advancing technology, cyberattacks have been on the rise, causing a potential risk of stolen personal data across 400 million users. In response, governments in all 50 states have introduced breach

notification laws (BNLs) mandating that companies notify a consumer if their data has been breached.

In a recently published paper for *The Review of Law & Economics*, Brad Greenwood, an information systems professor at the Donald G Costello College of Business at George Mason University, finds that BNLs have had little to no effect on overall security and protection.

Greenwood's co-author was Paul M. Vaaler of the University of Minnesota.

The researchers used data from the Privacy Rights Clearinghouse (PRC), an organization that arranges details on data breaches in firms since 2005. The PRC data includes information on breached firms, locations, causes, and the number of compromised records. The researchers used a two-way fixed effects design, also known as "difference-in-differences" estimates.

This is to evaluate the impact of BNLs on data breach event counts and magnitudes in different U.S. states from 2005 to 2019. With the use of alternative data from the FTC's Consumer Sentinel Network Data Book, they also investigated the impact of BNLs on follow-on counts and magnitudes of fraud and identity theft.

The resulting findings indicate no evidence for a decrease in data breach incidents or longer-term decrease in data misuse after breaches. Greenwood says, "The lack of significance is so striking, that you would expect at some point we would be getting random significance." This suggests that BNLs may not have achieved their intended goals of decreasing the number of data breaches.

Greenwood suggests some of the reasons for BNL failure. The goal of the BNLs is to incentivize companies into investing more into

cybersecurity, so as to avoid the reputational damage that results from breach disclosure.

But Greenwood says the force of that incentive is blunted by a "general numbness" in the public mind about cybersecurity failures. To motivate companies to take serious action, "there must either be an economic payoff to do so or an economic penalty for failing to do so," he says.

Greenwood and his co-author suggest a few possible alternatives or additions to BNLs. One suggestion involves the Federal Trade Commission assigning a cybersecurity score to all U.S. companies above a certain size, making it easier for people to compare companies on the basis of their cybersecurity performance.

Greenwood adds that "federal legislation might mandate minimum security protocols, such as the well accepted standards from NIST, which would establish at least a legal floor for expected behavior."

Another possible alternative would be changes to the current legal liability regime. Right now, the standard of material harm for claimants is high, making it harder for companies to be sued. "The case law is kind of evolving on this. Courts are beginning to recognize that the time people have to spend cleaning up cybersecurity messes is harm, it's billable. But it's still a fairly narrow window [to establish material harm]."

"The future is clearly uncertain with regard to consumer protections," Greenwood concludes. "But the one thing we know for sure is that the current regime of protection isn't working for anyone but cybercriminals themselves."

More information: Paul M. Vaaler et al, Do US State Breach Notification Laws Decrease Firm Data Breaches?, *Review of Law &*

Economics (2023). DOI: 10.1515/rle-2023-0038