June 2, 2021

Breached companies facing higher interest rates and steeper collateral requirements

A study found that companies dealing with data breaches later faced increased scrutiny from banks.

By Jonathan Greig | June 2, 2021

Companies are now being penalized financially by banks for data breaches, according to a new study from the American Accounting Association.

In a new report, titled "Do Banks Price Firms' Data Breaches?" the organization found that banks are punishing companies that lose customer financial account information or social security numbers through data breaches with substantially higher interest rates and steeper requirements for collateral and covenants.

The researcher behind the report analyzed data on 1,081 bank loans to publicly traded companies from 2003 to 2016. Of the 1,081 bank loans, 587 went to companies that had dealt with a data breach and 494 went to companies that had not.

Henry Huang, co-author of the study and an associate professor of accounting at Yeshiva University, said he wanted to find a way of quantifying the financial consequences of breaches.

The researchers matched companies in similar industries to see whether those that had been breached saw differences in how banks dealt with them. The report showed a clear link between higher interest rates and data breaches, with those that suffered more disastrous breaches faced even tougher treatment from banks.

But banks did make a distinction between the companies that had been hacked by criminal groups and those that had lost control of customer data through accidents or mistakes.

The financial penalties were harsher for certain industries, like healthcare, business services, computer, electronic equipment, and transportation. Surprisingly, companies that were known for having well-regarded IT departments faced even harsher treatment from banks after breaches because "banks had to make a bigger adjustment to their assessment of the company's security."

"We also wanted to learn which variables come into play. For example, we learned there are things companies can do to mitigate damage after a data breach," Huang said, mentioning actions like hiring security companies to address the attack and building out IT security systems.

"There are also valuable lessons here for accountants and auditors. It highlights the consequence of different types of data breaches in different industries, the importance of safeguarding confidential information, and the value of remedial actions after a breach," Huang added.

Cybersecurity experts like Lamar Bailey, senior director of security research at Tripwire, explained that insurance rates and loan rates are all based on risk.

He compared it to the credit scores and driving records banks use for consumers, noting that the higher interest rates breached companies face is "totally valid."

"I would love to see a public security risk score so consumers can decide if they want to do business with this company or give them any personal data," Bailey told ZDNet.

Panorays founder Demi Ben-Ari explained that since companies are being held accountable for data breaches through data privacy regulations, it's not

surprising that banks are taking a similar approach by charging risky organizations higher interest rates.

"The message is clear: organizations are responsible for protecting the data of their customers. To prevent cyber incidents, it's essential for companies to thoroughly assess and continuously monitor their own cyber posture as well as that of the third parties with which they do business," Ben-Ari said.

"Clearly, investing in such processes pays in the long run."