

June 7, 2021

Dr. Henry Huang Co-authors a Study on the Economic Effects of Data Breaches

[Faculty](#), [Most Recent News](#) [yunews](#)



Dr. Henry (He) Huang

A recent study co-authored by Dr. Henry Huang, program director of the MS in Accounting and an associate professor of accounting at [Sy Syms School of Business](#), and Dr. Chong Wang, an assistant professor of accounting at Hong Kong Polytechnic University, and published by the American Accounting Association finds that there is a very real cost for companies that can't protect their customers' personal information. In addition to any reputational damage, the authors found that banks effectively apply a financial penalty to companies that have experienced data breaches. At issue are data breaches in which personal data, such as customer financial account information or social security numbers, is either stolen or inadvertently made public.

“We knew that data breaches were important, but wanted to find a way of quantifying their financial consequences,” says Dr. Huang. “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.”

Specifically, the researchers wanted to know whether companies that had experienced data breaches faced additional requirements when trying to secure bank loans. To that end, the researchers drew on data regarding 1,081 bank loans to publicly traded companies from 2003 to 2016: 587 loans were to companies that had experienced a data breach; 494 loans were to companies that had not.

To ensure they were seeing the impact of the data breach and not other factors, the researchers matched each company that had experienced a breach with another company that had similar characteristics but hadn’t experienced a breach. The results were clear: banks charged substantially higher interest rates to companies that had experienced a data breach, compared to companies that had not.

Several factors could make things worse. If the breach involved data on a lot of people, the effect was exacerbated. The effect was also exacerbated if the breach was the result of criminal hacking rather than a mistake. The effect was also more pronounced for companies in a subset of “vulnerable” industries: health, personal services, business services, computer, electronic equipment, and transportation.

Lastly, companies with good reputations for IT quality fared worse after a data breach because banks had to make a bigger adjustment to their assessment of the company’s security. In addition, banks also required more collateral and more covenants from companies that had experienced breaches. “However, we also identified remedial actions that mitigated the adverse impact of data breaches,” says Dr. Wang. Examples of these actions include retaining a third party to address the data breach and developing plans to improve IT security.

“One take-away message is that firms, especially those in vulnerable industries, should invest more in data security in order to avoid costly punishment in capital markets,” Dr. Wang says. “There are also valuable lessons here for accountants and auditors,” says Dr. Huang. “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.”

The study, “[Do Banks Price Firms’ Data Breaches?](#),” is published in *The Accounting Review*. The [American Accounting Association](#) is the largest community of accountants in academia. Founded in 1916, it has a rich and reputable history built on leading-edge research and publications. The diversity of the Association’s membership creates a fertile environment for collaboration and innovation, collectively shaping the future of accounting through teaching, research and a powerful network and ensuring the Association’s position as a thought leader in accounting.