TechXplore

Firms perceived to fake social responsibility become targets for hackers, study shows

May 5 2020, by Shannon Roddel

Credit: CC0 Public Domain

Data breaches have become daily occurrences. Research firm Cybersecurity Ventures reveals that in 2018 hackers stole half a billion personal records—a 126 percent jump from 2017—and more than 3.8 million records are stolen in breaches every day, including recently the

World Health Organization.

What corporate leaders may not realize is that strides they are making toward social responsibility may be placing a proverbial target on their backs—if their efforts appear to be disingenuous, according to new research from the University of Notre Dame.

A firm's social performance, as measured by its engagement in socially responsible or irresponsible activities, affects its likelihood of being subject to computer attacks that result in data breaches, according to "Too Good to Be True: Firm Social Performance and the Risk of Data Breach," forthcoming in Information Systems Research from Corey Angst, professor of IT, analytics and operations at Notre Dame's Mendoza College of Business.

There is evidence that not all hackers are motivated by money and that at least some target what they dislike. Recent hacks against the WHO, due to its actions or alleged inactions related to the coronavirus pandemic, are a case in point, according to Angst.

"Recent hacking activity, including 25,000 email addresses and passwords allegedly from the National Institutes of Health, WHO, Gates Foundation and others being posted online, is supported by our findings," Angst said. "What is most surprising is that firms that are 'bad actors' regarding corporate social responsibility are generally no more likely to be breached than firms that are good. In fact, the opposite is true."

The study shows firms that are notably poor at corporate social responsibility, or CSR, are no more likely to experience a data breach, while a strong record of CSR in areas peripheral to core firm activities, including philanthropy and recycling programs, results in an elevated likelihood of breach.

"Delving into this latter finding, our results suggest firms that simultaneously have peripheral CSR strengths alongside major concerns in other areas are at increased risk of breach," Angst said. "This reality for firms with seemingly disingenuous CSR records suggests that 'greenwashing' efforts to mask poor social performance make firms attractive targets for security exploitation. Some perpetrators can 'sniff out' firms' attempts to give the appearance of social responsibility, and, consequently, these firms are more often victimized by malicious data breaches."

The team conducted its research by compiling a unique dataset consisting of publicly available information on data breaches at 189 firms spanning 2005 to 2010 and included external assessments of their CSR and other firm-specific factors.

"Corporate leaders need to understand that hackers are seeing through weak attempts at CSR," Angst advised. "They are taking matters into their own hands and acting as corporate disciplinarians by breaching the technology infrastructure of firms that they deem to be promoting themselves as good corporate citizens when in fact there are blemishes under the surface. When firms portray themselves as 'holier-than-thou,' any small misstep could trigger an attack."

More information: Adjerid, Idris and D'Arcy, John and Angst, Corey M. and Glavas, Ante, Too Good to Be True: Firm Social Performance and the Risk of Data Breach (May 4, 2020). D'Arcy, J., Aderid, I., Angst, C. M., and Glavas, A. Forthcoming. "Too Good to Be True: Firm Social Performance and the Risk of Data Breach," *Information Systems Research*, pp. 1-45.. papers.ssrn.com/sol3/papers.cf … ?abstract_id=3592518

Provided by University of Notre Dame

Citation: Firms perceived to fake social responsibility become targets for hackers, study shows (2020, May 5) retrieved 25 April 2024 from https://techxplore.com/news/2020-05-firms-fake-social-responsibility-hackers.html