Hackers targeting companies that fake corporate responsibility

October 1 2020

Credit: CC0 Public Domain

A new study suggests some hackers aren't just in it for the money but instead are motivated by their disappointment in a company's attempts to fake social responsibility.

"There is emerging evidence that the hacking community is not homogenous, and at least some hackers appear to be motivated by what they dislike, as opposed to solely financial gain," said John D'Arcy, a co-author and professor of management information systems (MIS) at the University of Delaware. "Recent hacks against the World Health Organization, due to its actions (or supposed inactions) related to the COVID-19 pandemic, are a case in point."

D'Arcy and his coauthors, interested in exploring whether a firm's corporate social performance (CSP) impacts their likelihood of being breached, studied a unique dataset that included information on data breach incidents, external assessments of firms' CSP and other factors. The results, published on Sept. 18 in the *Information Systems Research* paper "Too Good to Be True: Firm Social Performance and the Risk of Data Breach," were intriguing.

The key to these results, D'Arcy explained, lies in understanding the difference between two different types of corporate social responsibility efforts: those that are more minor and peripheral (like recycling programs or charitable donations) versus those that involve social responsibility being embedded throughout the firm's core business and processes (like diversity initiatives and producing eco-friendly products).

Companies only participating in peripheral efforts and not more deeply embedded ones are sometimes called "greenwashing," attempting to give the appearance of social responsibility without infusing such practices throughout their entire organization. According to D'Arcy's research, firms that do this are more likely to face problems from hackers.

"An example of a firm that has been accused of greenwashing is Walmart," D'Arcy said. "This is because Walmart has touted its investments in charitable causes and environmental programs, but at the same time has been criticized for providing low wages and neglecting

investments in employees' physical and psychological working environment."

The study found that hackers of all kinds—from internal disgruntled employees to external hacktivist groups—can "sniff out" these actions that only give the appearance of social responsibility. To an even further extent, when companies not only are trying to improve their image but also are using these actions to mask poor overall CSP, they are especially likely to be breached.

"Consequently, these firms are more likely to be victimized by a malicious data breach for these reasons," D'Arcy said. "Firms may be placing a proverbial target on their back, in an information security sense, by engaging in greenwashing efforts."

Conversely, the study found that when firms that engage in more embedded and meaningful forms of corporate responsibility, they are more likely to see solely positive outcomes. In this case, that means fewer hacks and data breaches.

"These same internal and external hackers are likely to see such embedded CSP efforts as genuine attempts at social responsibility (in other words, the company is 'walking its talk' when it comes to social responsibility) and thus they will be less likely to target these firms for a computer attack that results in a breach," D'Arcy said.

What lessons should companies take from this research? D'Arcy warned that companies should be cautious about promoting peripheral CSP efforts if they have otherwise poor records on corporate social issues.

"What was once accepted as meaningful CSP activity may no longer appease certain stakeholders," he said. "And in this era of increased information transparency and greater expectations of the firm's role in

society, engaging in only peripheral actions may result in stakeholder backlash. Firms need to be cautious about promoting their CSP activities unless they can defend their actions as embedded in core practices and as authentically motivated."

More information: John D'Arcy et al, Too Good to Be True: Firm Social Performance and the Risk of Data Breach, *Information Systems Research* (2020). DOI: 10.1287/isre.2020.0939