SECURITY & PRIVACY

A Cyberattack Doesn't Have to Sink Your Stock Price

by Keman Huang and Stuart Madnick

August 14, 2020

px photography/Getty Images

Over 60% of the Fortune 1000 had at least one public data breach over the last decade, according to a Cyentia Institute research report. On an annual basis, it is estimated that one in four Fortune 1000 firms will suffer a cyber loss event. There is an estimated cyber attack every 39 seconds. As is often stated, "it is not a matter of *if*, but *when* you will suffer a cyber attack." Are you prepared?

A hack can sink a company's stock price and leave investors fuming. In the wake of the Capital One hack, which was publicly reported in July 2019, the company's stock price dropped nearly 6% immediately in after-hours trading, losing a total of 13.89% over two weeks. Likewise, following the announcement of the Equifax breach back in early September of 2017, the company saw a similar negative reaction from the stock market with its stock price plunging from $142.72 to $92.98 in just one week. What is worse, its market share dropped significantly in 2017 and has struggled to recover ever since.

Getting hacked doesn't have to be a disaster, however. The JP Morgan Chase breach in 2014, for instance, didn't impact its stock growth negatively, in fact, its stock actually rose slightly. These counterintuitive outcomes indicate that many factors determine the fallout from data breach incidents. They also show that there are steps a company can take to not only mitigate reputational damage, but sometimes even end up improving their position. Our research and review of more than 14 published studies revealed that the consequences of a data breach incident may differ depending on the industry, firm size, the type of information exposed, and the response strategy. Here we will focus on the firm's response strategy, the area that the company has the most control over.

How to Respond When You're Hacked

Let's start with what not to do. First off, don't try to hide that it happened. Strategies such as hiding the existence of the incident or finding excuses to minimize the organization's responsibility can result in even worse consequences. One example is when Uber paid hackers through its bug bounty program to cover up a data breach incident in 2016. When the incident was publicly disclosed in 2017, it resulted in significant damage to Uber's reputation, and a $148 million fine from the Federal Trade Commission in 2018. And while many companies trot out the CEO to say "I am deeply sorry for what has happened" or fire the chief security officer, neither acts will likely be much help.

So what *should* you do? There are two key pieces of advice: 1) Lead with what you did right to prepare for this eventuality, and 2) then pivot to how you're going to improve even more.

Lead with the cybersecurity measures already in place. Our analysis shows that both customers and the stock market are reassured by a CEO who immediately and effectively communicates about the cybersecurity mechanisms the company already has in place. Broadcasting that a serious investment was made before a hack shows that the company took security, and especially the privacy of its customers, seriously. Even if these measures didn't ultimately thwart the attack, discussing them up can mitigate some of the damage: data encryption can guarantee confidentiality, a backup system can help to speed up recover, and network segmentation can isolate the incident to reduce the magnitude of the impact. If you're reading this and you haven't been hacked yet, now would be a good time to double check security measures like these.

Pivot to planned improvements. Immediately after the breach, remedial actions should be taken and publicized, such as announcing a big increase in budget to further improve corporate cybersecurity capability. Hiring more cybersecurity professionals to enhance internal cybersecurity capabilities can also contribute to maintaining customers' trust. For example, after the JP Morgan Chase breach, the company released extensive information on the attack and doubled its investment in security.

On top of internal improvements, it is wise to publicly offer all customers a monitoring service, such as LifeLock, to help avoid any potential abuse of their data, such as identity theft. Doing so — and advertising that you're doing it — makes clear that customers are in good hands and are going to be taken care of. Together, these post-breach recovery strategies helped organizations to reduce or eliminate short-term negative stock price drop, according to our analysis.

Prepare Now

These immediate and well-planned responses are critical to restoring confidence. But even though you may not always be able to prevent a cyberattack, you can prepare for it. All too often we have seen CEOs immediately make statements to the press — only to backtrack within hours or days — making it seem like the company does not know what it is doing. Of course, this seriously reduces confidence in the company.

Our research affirmed the importance of cyberattack fire drills to address this. These involve having top management, often including the board, participate in a simulated cyberattack to develop and practice response procedures and communications strategies. We have run several such fire drills with companies: We introduce a series of events — sometimes as video clips as might be reported on the news — and have the executives respond to each event, after which we assess what worked well, what did not, and what additional training and preparation is needed before a real event occurs. If your company is not already practicing cyberattack fire drills, it should do so as fast as possible.

Importantly, a cyberattack is a crisis, but it can also be an opportunity. Leaders should recall Winston Churchill's guidance, "never waste a good crisis." While a cyberattack brings the targeted company into the spotlight, it also provides free publicity for the company to showcase their responsibility and efforts to protect stakeholders, customers, suppliers, and the community. That is why a well-rehearsed action plan and communication strategy is so important. Instead of blaming the cybersecurity team or gullible employees, organizations should turn those incidents into opportunities to improve and optimize their business by increasing transparency, enhancing cybersecurity maturity, and improving competitive position.

The best case outcome is to reduce, or even eliminate, the cyber-incident's short-term negative impact (such as on stock price) through a systematic response strategy and proactive customer attitude. Then turn the experience into a trigger for expanded organizational learning to create positive long-term impact and digital innovation. This should be the mission for every organizational leader. If all these things are done, and done well, the company can emerge better, stronger, and smarter.

Acknowledgement: This research was supported, in part, by funds from the members of the Cybersecurity at MIT Sloan (CAMS) consortium.

Keman Huang is a Research Scientist at the MIT Sloan School of Management, where he works on cybersecurity management and policy, innovation ecosystems, and big data analysis.

Stuart Madnick is the John Norris Maguire (1960) Professor of Information Technologies in the MIT Sloan School of Management, Professor of Engineering Systems in the MIT School of Engineering, and Director of Cybersecurity at MIT Sloan (CAMS): the Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity. He has been active in the cybersecurity field since co-authoring the book *Computer Security* in 1979.

This article is about SECURITY & PRIVACY

⊕ Follow This Topic

Comments

Leave a Comment

Post Comment

0 COMMENTS

Join The Conversation

POSTING GUIDELINES

We hope the conversations that take place on HBR.org will be energetic, constructive, and thought-provoking. To comment, readers must sign in or register. And to ensure the quality of the discussion, our moderating team will review all comments and may edit them for clarity, length, and relevance. Comments that are overly promotional, mean-spirited, or off-topic may be deleted per the moderators' judgment. All postings become the property of Harvard Business Publishing.