Harvard
Business
Review

Cybersecurity And Digital Privacy

The Devastating Business Impacts of a Cyber Breach

by Keman Huang, Xiaoqing Wang, William Wei, and Stuart Madnick

May 04, 2023

Anton Petrus/Getty Images

Summary. Cybersecurity risks are becoming more systematic and more severe. Although the short-term impacts of a cyberattack on a business are quite severe, the long-term impacts can be even more important, such as the loss of competitive advantage, reduction in credit rating, and increase in cyber insurance premiums. They should not be ignored. To address these concerns effectively, companies

need to: 1) Have a cybersecurity champion on the board to help set the tone for the organization, and 2) develop a long-term cybersecurity strategy, which should be a priority for every organization. **close**

Cyber risks are skyrocketing. The latest IBM Data Breach Report revealed that an alarming 83% of organizations experienced more than one data breach during 2022. According to the 2022 Verizon Data Breach Investigations Report, the total number of ransomware attacks surged by 13%, which is a rise equal to the last five years combined. The severity of the situation continues to be evident with the public disclosure of at least 310 cyber incidents that occurred in the past three months alone, according to January, February, and March data from IT Governance. These include OpenAI's ChatGPT, which exposed the payment-related and other sensitive information of 1.2% of its ChatGPT Plus subscribers due to a bug in an open-source library it used. Moreover, Samsung semiconductor has recorded three incidents where employees accidentally leaked company information when using ChatGPT.

Billions of Dollars Lost in Market Cap With a Ripple Effect Is Common

It is well known that a cyber incident can sink an organization's stock price, especially in the short term. Publicly traded companies suffered an average decline of 7.5% in their stock values after a data breach, coupled with a mean market cap loss of $5.4 billion. Even more concerning is the fact that it took 46 days, on average, for these companies to recover their stock prices to pre-breach levels, if they were able to do so at all.

Importantly, such an impact can reverberate throughout the entire supply chain, creating a ripple effect that can cause up to 26 times the loss for a company's business ecosystem. For example, a ransomware attack on ION Trading Technologies on

January 31 of this year sent financial institutions scrambling to confirm trades manually. Similarly, a security breach of a third-party supplier to Okta shaved about $6 billion off the company's market cap during the week the incident was made public. In other words, you are only as good as your weakest link.

Long-Term Impacts Are Emerging and Can Be More Significant Than Expected

Although fluctuations in stock prices may be a breeze for some executives to manage, the lasting effects of cyber incidents on companies are becoming more apparent.

First, a cyber incident will directly consume a company's resources, leading to an increased cost of doing business. In 2022, the global average cost of a data breach reached $4.35 million, while the number is more than double in the U.S., averaging $9.44 million. These expenses can include everything from ransom payments and lost revenues to business downtime, remediation, legal fees, and audit fees. For example, the audit fees for companies following data breaches can be about 13.5% higher than those for firms without breaches. While millions of dollars in losses can bankrupt a small company but not have much of an effect on a public company, the attackers are generally "smart" enough to cause more problems for the bigger companies. For example, ransomware attacks had a much bigger financial impact on the health care sector, with over $7.8 billion lost due to downtime alone in 2021.

Additionally, these costs can pass on to customers and investors, limiting a company's ability to maintain its market position. For example, 60% of organizations that have experienced data breaches have raised their prices. On average, companies

experiencing a significant data breach incident underperform the NASDAQ by 8.6% after one year, and this gap can widen to 11.9% after two years.

Furthermore, cyber risks can result in a credit-rating downgrade, impacting a company's ability and cost to secure financing. For instance, companies with weaker cybersecurity practices may face higher borrowing costs and increased financial risk, as Moody's announced in 2018 that it would evaluate companies' cybersecurity practices when assigning credit ratings. In fact, Moody's reduced Equifax's credit rating in 2019 following Equifax's data breach that occurred in 2017.

Don't Let Cybercrime Damage Your Bottom Line

It is clear that the ramifications of cyber incidents go beyond a short-term stock price reduction, and it is essential for executives to prepare for long-term impacts. A systematic response strategy and a proactive customer attitude — such as leading with already implemented cybersecurity measures, pivoting to planned improvements, and practicing fire drills — have proven to be effective in reducing the negative impacts of cyber incidents. To prepare for the long-term perspective, here are two critical efforts executives should undertake:

Put a Cybersecurity Champion on the Board

This is the first task executives should undertake to protect their companies. Having such a champion can not only help in responding to cyber incidents, but it can also keep cybersecurity as a strategic front and impart cybersecurity knowledge to the board.

Nowadays, cybersecurity is far more embedded into the operational landscape, including making cybersecurity a top priority for boards through effective communications and in

developing agile management processes. Beyond having a CIO or CISO sitting on the board to take responsibility for cybersecurity, a CEO or CFO with related expertise can also effectively reduce the cybersecurity risk and keep a company away from a cyber incident.

Develop a Long-Term Cybersecurity Strategy

The second critical effort that executives should undertake is adopting a long-term cybersecurity strategy, rather than a short-term, reactive approach. Although investing in cyber risk management may initially affect your revenue-generating resources in the short term, it will pay off in the long run.

A study of 5,882 U.S. hospitals found that those that *substantively* adopted and deeply integrated IT security into processes and structures, rather than simply being symbolic adopters, could effectively reduce 37.8% of data breaches. Businesses with better cybersecurity policies — such as those that have a dedicated CISO, conduct regular audits, and participate in threat-sharing programs — can recover their stock prices within seven days. Conversely, those with poor security posture may take much longer to recover, with an average of 90 days.

Cybersecurity should be an organization-wide priority, as employees are always the front line for mitigating cybersecurity risks. Cybersecurity should be part of every employee's job description. Consider again Samsung semiconductor's data breach incident, where employees submitted top-secret source code to ChatGPT for error fixing. This incident was not due to a technical weakness, but was rather a cultural and operational issue. A strong cybersecurity culture can help your employees avoid such an unintended cyber incident while allowing them to simultaneously capitalize on the benefits of cutting-edge digital innovations like ChatGPT.

...

Cybersecurity risks are becoming more systematic and more severe. Although the short-term impacts of a cyberattack on a business are quite severe, the long-term impacts can be even more important, such as the loss of competitive advantage, reduction in credit rating, and increase in cyber insurance premiums. They should not be ignored. In order for companies to address these concerns effectively, there needs to be a cybersecurity champion on the board to help set the tone for the organization and develop a long-term cybersecurity strategy, which should be a priority for every organization.

Acknowledgment: The research reported in this article was supported, in part, by funds from the NSFC 6217071254 and the members of the Cybersecurity at MIT Sloan (CAMS) consortium.

KH

Keman Huang is an Associate Professor at the Renmin University of China and a Research Affiliate at the MIT Sloan School of Management, where he works on cybersecurity management and strategy, innovation ecosystems, and big data analysis.

XW

Xiaoqing Wang is a Ph.D student majoring in information security at the School of Information, Renmin University of China. Her research interests include cybersecurity behaviors, innovations, and strategies.

WW

William Wei is the leader of the Multi-Cloud Working Group of Cloud Security Alliance (CSA) Greater China, and has over 20 years of cyber security experience. He was the General Manager of Trusteer Greater China, Senior Security Specialist of IBM Greater China, Head and Technical Director of Entrust Asia Pacific, and has Silicon Valley startup experience. His research interests include Edge computing, Zero trust, Secure access service edge (SASE), Extended detection and response (XDR) and cyber security culture, etc.

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.