Chapter 8
Cybersecurity Disclosure and Corporate Reputation:
Rising Popularity of Cybersecurity in the Business World

Arpita Lenka
CHRIST University (Deemed), India

Madhurima Goswami
CHRIST University (Deemed), India

Harmandeep Singh
CHRIST University (Deemed), India

Harsha Baskaran
Compose Corner, India

ABSTRACT

This chapter emphasizes the importance of cybersecurity for a corporation as today's organizations are more vulnerable than ever and their enemies are in the form of viruses and malware. The work provides evidence that cybersecurity can have an impact on brand value, market value, and overall corporate reputation. It focuses on depicting the global scenario with reference to cybersecurity disclosures by corporations and how it is important in today's digitized era where data is the most valuable and vulnerable asset. With rapid digitalization, cybersecurity has become a major concern for all businesses, especially when there is financial and reputational damage to cybersecurity breaches and incidents. Even in the absence of clear cybersecurity laws and regulations, corporations are opting for voluntary disclosure. Existing literature explains this as an attempt to mitigate any potential risk or occurred risk through increased transparency which will build the trust of all stakeholders.

INTRODUCTION

Digitalisation is not a new word as it has been used for several decades now. "Digitalisation" is the "process of transforming from an analog to a digital format," which refers to the conversion of analog texts, photos, or sounds into a digital format that can be processed by a computer, according to Gartner's IT Glossary (Blieberger et al. 1996, p. 18). This definition would have sufficed if we were in the early 2000s. Unfortunately, the Covid-19 pandemic of 2020 showed the world the actual definition of digitalisation when that was the only way to survive and thrive. Digitalisation is using digital technologies to change a business model and provide new revenue and value-producing opportunities. It is the process of moving to a digital business (Gartner IT Glossary, 2019).

An online global survey of executives was conducted by Mckinsey (2020). From July 7 to July 31, 2020, a total of 899 C-level executives and senior managers representing a wide range of geographies, industries, firm sizes, and functional specialisations responded to this online survey. From the responses received, it was estimated that adoption of digital technologies by companies for supply chain and customer interaction was accelerated by 3-4 years due to the Covid-19 pandemic. Places like North America took the most significant stride towards digitalisation, with 60% of its products and services now entirely or partially digital.

Digitalisation has not only helped with survival, but it has also enabled opportunities to make businesses better and more efficient. That is why spending $2 trillion by businesses on digital transformation in 2019 does not come as a surprise. At a CAGR (Compound Annual Growth Rate) of 20.9%, it is predicted that the global market for digital transformation will increase from $1.79 trillion in 2022 to $6.78 trillion in 2029 (Fortune Business Insights, 2022). The insane amount of investment makes sense when it directly contributes to the company's growth. Companies with higher levels of digital maturity reported revenue growth of 45% compared to 15% for companies with lower levels (Deloitte, 2020). 45% of businesses suffering declining revenues as a result of COVID-19 stated they are putting more of a focus on digital transformation (McKinsey, 2020).

Digitalisation is doing wonders for businesses across the globe. Unfortunately, there is no rose without a thorn. Businesses have a sharp and poisonous thorn to deal with before they reap the benefits of digitalisation, that is, cybersecurity risks. Public Safety Canada (2014) defines cybersecurity as "The body of technologies, processes, practices and response and mitigation measures designed to protect networks, computers, programs and data from attack, damage or unauthorised access to ensure confidentiality, integrity, and availability." According to DHS (2014), it is "The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorised use or modification, or exploitation."

A decade ago cybersecurity was an alien concept. Businesses didn't consider it to be a significant factor in their business environment that could affect their strategic position. A majority of businesses had an "it won't happen to me" mindset and were unwilling to completely rethink their strategies to counter this possible danger (James, 2021). The scenario has completely changed now. With the emergence of big data, the shortage of skilled professionals to run and implement big data is not the only challenge that is faced by organisations. Security of such data is also stressful ("Companies Are Satisfied With Business Outcomes From Big Data and Recognize Big Data as Very Important to Their Digital Transformation, Accenture Study Shows | Accenture," 2014). Since COVID-19, the number of attacks has surged five-fold (Williams et al., 2020).

13 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/cybersecurity-disclosure-and-corporate-reputation/324922

Related Content

JomMachineLearning: Bringing Artwork Nearer With DesignLab
K.M. Liow, P.S. Joseph Ngand H.C. Eaw (2021). *International Journal of Business Strategy and Automation (pp. 54-71).*
www.irma-international.org/article/jommachinelearning/276457

SERVQUAL-Based Evaluation of Service Quality in Turkish Health Industry With Fuzzy Logic
Hasan Dinçer, Serhat Yüksel, Yaar Gökalpand Serkan Eti (2021). *Interdisciplinary Perspectives on Operations Management and Service Evaluation (pp. 213-233).*
www.irma-international.org/chapter/servqual-based-evaluation-of-service-quality-in-turkish-health-industry-with-fuzzy-logic/264102

Intermediation and Innovation Contests on the Internet: Lessons from the Study of Two Platforms
Isabelle Liotardand Valérie Revest (2017). *Global Intermediation and Logistics Service Providers (pp. 104-122).*
www.irma-international.org/chapter/intermediation-and-innovation-contests-on-the-internet/176034

Integrating Industry 4.0 Technologies Into Lean Thinking for the Development of Efficient, Low-Carbon Processes
Antonio Sartal, Fernando León-Mateosand Roberto Bellas (2023). *Lean Thinking in Industry 4.0 and Services for Society (pp. 1-28).*
www.irma-international.org/chapter/integrating-industry-40-technologies-into-lean-thinking-for-the-development-of-efficient-low-carbon-processes/316695

Gamesy: Using Game Mechanics to Boost Intrinsic Motivation in School
B. W. Waweru, P. S. Joseph Ngand H. C. Eaw (2021). *International Journal of Business Strategy and Automation (pp. 36-52).*
www.irma-international.org/article/gamesy/282520