# Uncovering the Financial Fallout of Cyber-Attacks

Professor Karen Hogan

JUNE 2024

doi.org/10.33548/ SCIENTIA1036

BUSINESS, ECONOMICS & FINANCE

Scientia

# Uncovering the Financial Fallout of Cyber-Attacks

In our increasingly digital world, cyber-attacks pose a significant threat to corporations with their potential to disrupt operations, damage reputations, and ultimately impact shareholder value. Because these attacks are getting more sophisticated, companies need to protect both their own systems and be aware of what potential threats might exist as a result of doing business with their suppliers and partners. **Professor Karen Hogan** from Saint Joseph's University in the USA is an expert on the complex relationship between cyber-attacks and shareholder wealth. Her comprehensive research provides valuable insights into how companies and investors can navigate this treacherous landscape.



## An Evolving Threat

Cyber-attacks have emerged as the top concern for companies worldwide, with the potential to cause significant fluctuations in corporate value. And it's not just a case of attacks increasing – many of these attacks now originate from vulnerabilities in supply chain networks, meaning that a single weak link can have cascading effects across multiple companies.

To illustrate how severe this threat is, Professor Karen Hogan from Saint Joseph's University in the USA points to the 2013 cyber-attack on Target, one of the largest retailers in the USA. During this attack, hackers gained access to Target's systems through a vulnerability in the network of one of its suppliers. This gave them access to huge volumes of customer credit card information and personal data. Unsurprisingly, this incident created significant financial losses and reputational damage for Target as a business, and highlights not only the financial consequences of cyber-attacks but also the damage caused by the loss of customer trust.

## Unravelling the Financial Impact

To shed light on the financial consequences of cyber-attacks, Professor Hogan and her team conducted an in-depth analysis of cyber data breaches using a proprietary dataset from Advisen Ltd., a leading provider of data and technology solutions for the insurance industry. This unique dataset contained information on nearly 4,000 publicly traded companies that experienced cyber events between 1990 and 2019.

By examining the characteristics of these breaches and the frequency with which they happened, the team aimed to identify patterns and trends to help companies and investors get a better understanding of cyber-attacks and mitigate the risks presented by them.

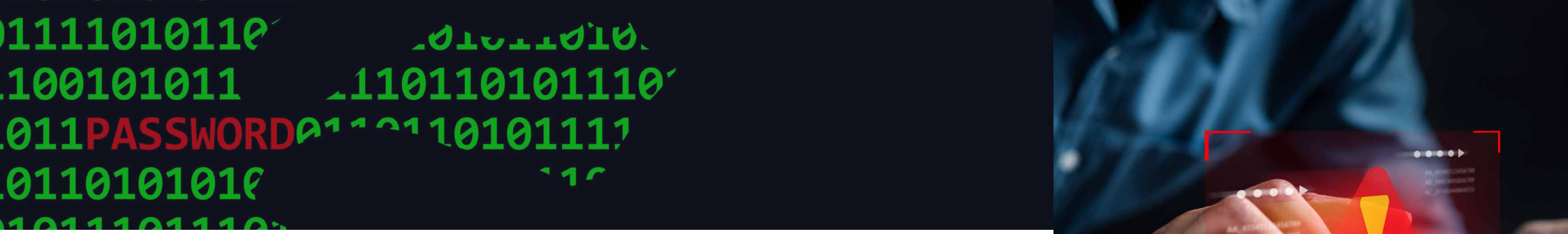
## Industries Under Siege

One of the key findings from the team's research was that certain industries are more vulnerable to cyber-attacks than others. The service, finance, and retail trade sectors experienced a higher frequency of cyber events compared to other industries. The vast amounts of sensitive customer data that these industries handle make them a very attractive target for cybercriminals.

Using a method called event study analysis, which involves calculating the impact of a certain event on stock prices, Professor Hogan and her colleagues assessed the short-term impact of cyber-attack announcements on stock prices. They found that companies experienced significant negative returns in the days following the disclosure of a cyber-attack. However, the magnitude of these negative returns was smaller compared to earlier studies. The team surmised that this reduction in negative returns might be due to increased awareness, improved communication with stakeholders, and better mitigation strategies.

Interestingly, companies in industries with a higher frequency of cyber events, such as finance, saw larger drops in stock prices compared to those in less frequently targeted industries. This suggests that investors may be more sensitive to cyber risks in these sectors.

Professor Hogan and her colleagues also found that cyber-attacks varied over time and showed periods of increasing and decreasing activity. Criminals tended to focus on specific industries, types of information, access sources, and countries. Popular targets included personal identity details, financial data, and health information. Attacks most commonly occurred via servers, websites, phone communications, and laptops.




## Long-term Effects of Cyber-Attacks

Professor Hogan's team also looked beyond immediate stock price reactions to explore the longer-term consequences of cyber-attacks. One key finding was that companies with a history of more breaches did not necessarily experience a negative impact on sales following a new attack. This could indicate that these companies have developed effective response strategies and are better equipped to handle the fallout from cyber incidents. However, the team did find that companies in the finance industry tended to experience slower sales growth following a breach compared to other industries, emphasizing the importance of industry-specific factors in determining the long-term financial impact of cyber-attacks.

## Key Insights for all Stakeholders

The team's findings will be of great interest to both companies and investors. For companies, the increasing frequency and sophistication of cyber-attacks highlight the need for top-class cybersecurity measures and swift incident response plans. This means not only investing in technical solutions but also fostering a culture of cybersecurity awareness throughout an organization and its entire supply chain. Creating this culture could involve collaborating with suppliers and partners to establish common security standards, conducting regular security audits and assessments, and sharing intelligence on emerging threats.

For investors, the findings highlight the importance of considering a company's cybersecurity track record and preparedness when making investment decisions. By incorporating these factors into their analysis, investors can better assess the potential risks and returns associated with their investments.

## Firm Foundations for Future Digital Defence

Professor Hogan and her team highlight the importance of continued research in this rapidly evolving field. Future studies could explore the effectiveness of specific cybersecurity measures in mitigating the financial impact of attacks or examine how regulatory frameworks and disclosure requirements shape corporate responses to cyber threats.

Along with developing and implementing strategies to protect themselves and their suppliers, companies also need to communicate transparently with investors about their cybersecurity efforts and the potential impact of cyber risk on their business. By demonstrating a proactive and resilient approach to managing cyber risk, companies can build trust with investors and other stakeholders, even in the face of an uncertain and ever-evolving threat landscape.

As cyber-attacks continue to evolve and become more sophisticated, ongoing collaboration between researchers, industry experts, and policymakers is going to be vital for developing new strategies to protect companies and investors from financial repercussions. Professor Hogan and her team have laid the foundation for a deeper understanding of this complex issue, paving the way to a more secure and resilient financial future for companies and investors alike.




For investors, the findings highlight the importance of considering a company's cybersecurity track record and preparedness when making investment decisions.

## MEET THE RESEARCHER

**Professor Karen Hogan,** Department of Finance, Haub School of Business, Saint Joseph's University, Philadelphia, PA, USA

Professor Karen Hogan received her BS in Finance from LaSalle University and her PhD in Business and Economics from Lehigh University. She is the Brian Duperreault Endowed Chair in Risk Management and Insurance and a Full Professor of Finance at Saint Joseph's University. Professor Hogan's research focuses on corporate finance, governance, and risk management, with a particular emphasis on the insurance industry and cybersecurity. She champions women in cybersecurity leadership and has published over 40 peer-reviewed journal articles. Professor Hogan has received several awards for her teaching and research, including the Tengelmann Award, the highest honour bestowed by Saint Joseph's University. She is actively involved in university service and has held leadership positions such as Department Chair and Academic Coordinator for the Executive MBA program.

### CONTACT

hogan@sju.edu

https://directory.sju.edu/karen-hogan

### KEY COLLABORATORS

Gerard T Olson, PhD, Villanova University

Jackson D Mills, PhD, University of Alabama

Peter A Zaleski, PhD, Villanova University

### FUNDING

Chubb Insurance for funding the Saint Joseph's University

Brian C. Duperreault '69 Chair for Risk Management and Insurance Endowment

### FURTHER READING

KM Hogan, G Olson, J Mills, P Zeleski, A Comprehensive Analysis of Cyber Data Breaches and Their Resulting Effects on Shareholder Wealth, *International Journal of the Economics of Business*, 2023, 30(1), 51–78. DOI: 10.1080/13571516.2023.2168994

KM Hogan, GT Olson, Governance and corporate control in the United States, *Corporate Law & Governance Review*, 2021, 3(2), 41–52. DOI: 10.22495/clgrv3i2p4

KM Hogan, A global comparison of corporate value adjustments to news of cyber-attacks, Journal of Governance & Regulation, 2020, 9(2), 34–44. DOI: 10.22495/jgrv9i2art2

SJU

Find out more at **scientia.global**