Call for contributions:

The Economic Cost of Cybersecurity Threats

An edited collection to be published by Palgrave-Macmillan

Co-edited by:
Thomas Walker, PhD
Marcus Walker, co-CEO
Rajesh Kumar Tharumar, BSc
Victoria Kelly, BSc

The John Molson School of Business at Concordia University kindly invites contributions to the edited book collection, entitled *The Economic Cost of Cybersecurity Threats*, to be published by **Palgrave-Macmillan**.

ABOUT THE BOOK

The world recognizes the importance of cybersecurity threats; The World Economic Forum (WEF) has designated cybersecurity risks a leading global concern since 2015 (Global Risk Report 2015 - 2023[1]). Despite this, digitization has unprecedented reach ushering in an age of convenience, efficiency, and innovation. A conservative 2022 estimate of the global average cost of a cybersecurity breach is 4.45 million USD (IBM 2023[2]). The economic cost of a breach is a complex paradigm: some damages are direct, such as those which stem from a breach's negative effects on operational or business continuity, costs related to data recovery, and those associated with the notification to concerned parties and regulatory bodies; other costs are indirect such as reputational damages, disruption of supply lines, and insurance premiums, to name but a few.

Our book will explore the various types of cybersecurity threats affecting the world today and the best practices recommended by various global regulatory bodies. The economic cost of these threats is then examined within the context of best practices and regulatory requirements with detailed policy analysis and case studies. Finally, we examine the mechanics of cybersecurity threat assessments, the costs and advantages of cybersecurity insurance. By focusing on new developments in academic research, industry practices, and regulatory policies, the book aims to provide valuable insights for practitioners, policymakers, academics, and students alike.

We aim to provide a comprehensive and integrated perspective on how threats have evolved despite advisories and adaptations to address and mitigate them. The educational features of the book, such as case studies and expert analysis, provide readers with a deep understanding of the topic and how it can be applied in practice. Global institutions and other entities can benefit from the book's practical guidance on the existing limitations and the evolving threat of cybersecurity, making it a valuable resource for professionals looking to make a positive impact in their field. Additionally, the book's comprehensive coverage of the latest developments in the field of cybersecurity will enable readers to stay ahead of the curve and make informed decisions about how to integrate these concepts into their operations. Academics and researchers will also benefit from the book's clear and concise organization, which facilitates easy comprehension and enables readers to stay up to date with the latest developments in the field.

CALL FOR CONTRIBUTIONS

The editors invite contributions from the international community of scholars and practitioners at the interface of cybersecurity risk management, corporate risk management, risk mitigation, policymaking, entrepreneurship, and financial development research. They welcome contributions that review and analyze emerging risks in cybersecurity, business and policy approaches, and adaptations in different key locations

[1] The Global Risk Report is published by the World Economic Forum (https://www.weforum.org/). The last annual report was published in January 2023. The report explores the most severe risks that affect the global landscape over three different time frames 1) current, 2) short term (2 years or less), and 3) long term (greater 2years but less than 10 years).

[2] The report published in 2023 is the 18th annual edition and is based on an independent study by the Ponemon Institute. Their report is based on data breaches in 553 organisations globally between March 2022 and March 2023.

through financial and economic lenses. Moreover, because the main aim of the text is to examine a broad range of business and policy solutions emerging today, the co-editors invite chapters that adopt an interdisciplinary or transdisciplinary approach and that incorporate new concepts or tools beyond the academic fields of business administration and risk management, including the applied, natural, and social sciences. Authors are encouraged to consider the geographic coverage and scalar relevance – at the local, regional, national, and supranational levels – of their contributions. Case studies or comparative studies (between different solutions, applications in different industries, or variations between regions) are also most welcome.

Submitted chapters must be original and exclusively prepared for the book, with no part of the article having been published elsewhere. Finally, although the book can be used as a reference book in academic courses, it is not explicitly organized as a textbook

POTENTIAL TOPICS FOR CHAPTERS

1. **Open access networks, cloud computing, and air-gapped systems**
   1.1 Overview and importance of different architectures
   1.2 Best practices
      NIST framework (USA)
      ISO/IEC 27001 (global)
   1.3 Other guidelines

2. **Different types of cybersecurity threats**
   2.1 Hacking
   2.2 Malware
   2.3 Phishing
   2.4 DDOS attacks
   2.5 Social engineering
   2.6 Technological barriers

3. **The cost of cybersecurity failures**
   3.1 Direct financial losses
      Operational
      Subsequent litigation
   3.2 Indirect losses
      Reputational damages
      Loss of competitive advantages
   3.3 Opportunity costs
      Long term repercussions
      Overhaul of IT systems
      Stakeholder confidence
      Recovery of lost data
      Settlements with affected parties

4. **Cybersecurity risk management**
   4.1 Risk assessment
   4.2 Incident planning
   4.3 Addressing market volatility

Financial planning
4.4 Managing stakeholder reactions
Business continuity planning
Interaction of cybersecurity risk and other risks
Alternate access and/or operational infrastructure
4.5 New oversight mechanisms
4.6 Capital investment in IT infrastructure

5. **Cybersecurity insurance**
   5.1. Current assessment methodology
   5.2. Cost vs benefits of cyber insurance

IMPORTANT DATES

- Abstract and CV submission deadline – **February 12, 2024**
  Selection of abstracts and notification to successful contributors – **February 29, 2024**
  After February 2024, the publisher's release forms will be forwarded to successful contributors
  Full chapter submission – **May 31, 2024**
  Revised chapter submission – **July 31, 2024**
  Manuscript delivery – **September 30, 2024**
  Publication (tentative date) – **Late Fall 2024**

GUIDELINES FOR CONTRIBUTORS

Submissions should be written in English using a non-technical writing style. The contributions may include diagrams/illustrations in order to present data, or photographs/figures (all in black & white) to better illustrate the topic of discussion. Submitted chapters should be original and exclusively prepared for the present book. **No part of the article should be published elsewhere**. Chapters must not exceed 7,000 words (including all references, appendices, biographies, etc.), must use 1.5-line spacing and 12 pt. Times New Roman font, and must use the APA 7th edition reference style. Researchers and practitioners are invited to submit abstracts of no more than 500 words, a bibliography for their proposed chapter, and a CV. Abstract submission are expected by **February 12th, 2024**. Submissions should be sent by email to cyber.econ@concordia.ca.

Authors will be notified of the status of their proposals and will be sent complete chapter guidelines. Full chapters are expected to be submitted by **May 31st, 2024**.

Please note there are no submission or acceptance fees for the manuscript.

ABOUT THE EDITORS:

Thomas Walker

Thomas Walker holds a BSc in Management Information Systems from the Technical University of Darmstadt, Germany, and an MBA and PhD degree in Finance from Washington State University. Prior to his academic career, he worked for several years in the German consulting and industrial sector at such firms as Mercedes Benz, Utility Consultants International, Lahmeyer International, Telenet, and KPMG Peat Marwick. His research interests are in emerging risk management, corporate finance, venture capital, sustainability & climate change, fintech, corporate governance, securities regulation and litigation, insider

trading, and institutional ownership, and he has published over 70 articles, book chapters, and edited books in these areas. He is the lead editor of seven books on sustainable financial systems, sustainable real estate, sustainable aviation, environmental policy, emerging risk management, innovations in social finance, and water risk management. Dr. Walker currently serves as the principal investigator on research grants by the Social Sciences and Humanities Research Council (SSHRC), the Autorité des marchés financiers, and the Global Risk Institute. In 2018, he founded the Emerging Risks Information Center (ERIC, https://emerging-risks.com) which conducts targeted research on environmental, technological, and societal risks that affect our world today. In 2021, he became the inaugural director for the Jacques Ménard/BMO Center for Capital Markets at Concordia University and the Concordia University Research Chair in Emerging Risk Management (Tier 1).

Marcus Glenn Walker

Marcus Glenn Walker is a partner and co-CEO of Dragon Data Solutions, a German software firm that specializes in transportation solutions for cargo shipments by land, sea, and in the air. He is an expert in artificial intelligence (AI) and sustainability and has published with the ERIC team on several occasions in the past. He currently cooperates with the team on creating an AI solution that will increase the efficiency and thereby reduce the emissions of medium and long-haul truck shipments.

Rajesh Kumar Tharumar

Rajesh Kumar Tharumar is an MSc candidate at the John Molson School of Business, Concordia University where he studies Finance. He currently serves as a research associate in the Department of Finance at Concordia University. His research interests include risk management, emerging risks, corporate finance, and sustainable finance.

Victoria Kelly

Victoria Kelly is a Research Associate at the Emerging Risks Information Center (ERIC) at Concordia University in Montreal. With the Center, Victoria has contributed to several publications in the field of sustainability. Victoria holds a BSc in Biology and an additional major in Irish Studies and is currently a first-year master’s student in History and Irish Studies where her research focuses on public health management.