Call for Chapters

Cyber Security and Supply Chain Management: Risks, Challenges, and Solutions

Editors:
Steven Carnovale, Ph.D. (Saunders College of Business, Rochester Institute of Technology)
Sengun Yeniyurt, Ph.D. (Rutgers Business School, Rutgers University)

Publisher:
World Scientific

Series Scope:
As supply chain management relies more and more on technology, key systematic vulnerabilities arise. This series will examine the front line of supply chain management as we transition into a new way of doing business. Thus, this series will examine topics such as: cyber security in supply chain management, supply chain privacy and fraud, supply chain risk management, blockchain, big data, 3-D printing, and so on.

Book Scope:
A recent IBM[1] study suggests that the average cost of a cybersecurity breach has risen over by 12% over the past 5 years and is estimated to cost over $3.9 million. In addition, in 2015 the overall cost [2] of cyber-attacks was an estimated $400 billion, which represents a 4-fold increase from 2013, and is expected to rise to $2Trillion by the end of 2019. Upon further scrutiny, what becomes clear is that the supply chain is often the core area of a firm's cyber security vulnerability. Take, for example, an extreme case of a cyber breach: Target. One of Target's suppliers was attacked and over 70 million pieces of customer information were stolen [3], which cost Target approximately $162 million [4].

The popular press is replete with examples just as extreme as this. Yet, much of the academic dialogue has yet to address this emerging area, which is in desperate need of research. So, the core topics we seek to address in this book include: cyber vulnerabilities in supply chain management, how firms can manage such cyber risk, cyber security challenges in procurement, manufacturing, and logistics, and many more. We expect that this book will bring together several experts from both industry and practice to shine light on this problem, and advocate solutions for firms operating in this brave new world.

Topics Submissions Should Cover:
- Connecting supply chain management to cyber security
- Core Cyber Vulnerabilities in Supply Chains
- The Legislative/SCM Interface: How Cyber Policy Impacts SCM
- Risk Management and Cyber Security
- Global Issues and Challenges in Supply Chain Cyber Security
- Cyber Security Challenges in Procurement
- Cyber Security Challenges in Manufacturing
- Cyber Security Challenges in Logistics
- Solutions to the Cyber Security Problem in Supply Chain Management

Submission Guidelines:

- All manuscripts are to be emailed with the subject line "Chapter Submission - Cyber Security and SCM" to the editors at scarnovale@saunders.rit.edu or yeniyurt@rutgers.edu by March 31st, 2020
- The editors expect to review the manuscripts within two (2) months and have a decision back to authors
    - Should a revision be invited, the Editors will expect to have the authors submit their changes within two (2) months.
- All manuscripts should be double spaced, with 12 point times new roman font
- Each manuscript should not exceed 30 pages, or 10,000 words, all manuscripts should be written in MS word and submitted accordingly.
- APA format for citations is appropriate

References:

[1] https://newsroom.ibm.com/2019-07-23-IBM-Study-Shows-Data-Breach-Costs-on-the-Rise-Financial-Impact-Felt-for-Years
[2] https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#524e26753a91
[3]http://www.forbes.com/sites/maggiemcgrath/2014/01/10/target-data-breach-spilled-info-on-as-many-as-70-million-customers/#18a1609d6bd1
[4]https://corporate.target.com/_media/TargetCorp/annualreports/2014/pdf/Target-2014-Annual-Report.pdf?ext=.pdf