Editorial: Cyber-Resilience in Supply Chains

Chris McPhee, Editor-in-Chief
Omera Khan, Guest Editor

From the Editor-in-Chief

Welcome to the April 2015 issue of the *Technology Innovation Management Review*. The editorial theme of this issue is **Cyber-Resilience in Supply Chains**, and I am pleased to welcome our guest editor, **Omera Khan**, Professor of Operations Management at the Technical University of Denmark.

We hope you enjoy this issue of the TIM Review and will share your comments online. In May, we will be publishing a general, unthemed issue, which will be followed by an issue on **Cybersecurity** in June.

For future issues, we welcome your submissions of articles on innovation management, entrepreneurship, and other topics related to the launching and growing of technology companies. Please contact us (timreview.ca/contact) with article topics and submissions, suggestions for future themes, and any other feedback.

Finally, some of our readers may be interested to know that La Salle – Ramon Lull University in Barcelona, Spain, will be holding a doctoral consortium on the theme of "Digital Innovation" from July 2nd to 3rd, 2015. The deadline for the submission of abstracts is April 30th. For details, please see the Innova Institute blog: tinyurl.com/lbtp5qp

Chris McPhee
Editor-in-Chief

From the Guest Editor

It is my pleasure to be the invited guest editor for this month's issue on Cyber-Resilience in Supply Chains. Our growing interconnectivity in cyberspace has exposed us to new and greater vulnerabilities, and we have recently witnessed the catastrophic damage that cyber-attacks can cause to a firm's reputation and shareholder value. Supply chain cyber-resilience can be defined as the capability of a supply chain to maintain its operational performance when faced with cyber-risk.

Response measures to cyber-risks are being developed and researched, and the World Economic Forum has been at the forefront of advocating for the importance of addressing cyber-resilience. However, few if any, methods are currently robust enough to support cyber-resilience in supply chains.

Supply chain cyber-resilience has received less attention compared to cyber-risk, security, and resilience generally. An explanation for this could be because naturally we view information technology (IT) as solely responsible for cyber-related issues. This compartmentalization of disciplines is at the heart of the problem and must be overcome to achieve supply chain cyber-resilience. Cyber-attacks are crippling the world's most sophisticated supply chains, thereby causing losses that run into billions of dollars, but a disconnect between IT professionals and supply chain professionals means that determining accountability for this risk could take far longer than tackling the issue itself. A more coordinated approach between IT and supply chain professionals, led by an organizational culture that seeks to build resilience rather than just react to cyber-attacks, may have higher chances of survival as it adapts and aligns to a dynamic defense strategy against a growing threat.

The aim of the collection of articles presented in this issue is to highlight the significance of this topic and develop a shared understanding of the definition, theory, and managerial implications of cyber-risk and cyber-

Editorial: Cyber-Resilience in Supply Chains

Chris McPhee and Omera Khan

resilience in supply chains. And, in doing so, the issue seeks to develop an agenda for future research that provides solutions to the challenges of developing a supply chain cyber-resilience strategy, the tools and methods to respond to cyber-breaches in the supply chain, and case studies of best practice.

In the first article, **Omera Khan** and **Daniel Alberto Sepúlveda Estay**, a Professor and a PhD Student from the Technical University of Denmark, set the scene by developing a research agenda for future research after exploring the critical frameworks that exist in the supply chain risk management domain. The article concludes with prescriptions for academics and practitioners that must be taken to expand our understanding of supply chain cyber-resilience.

Next, **Luca Urciuoli**, Associate Research Professor in the Zaragoza Logistics Center in Spain, describes the challenges of implementing information and communication technologies to support the resilience of complex global supply chains, which could have an adverse effect if not addressed correctly. The article sheds light on the managerial strategies to improve cyber-resilience such as combining current technologies and services to achieve cyber-resilience.

In the third article, **Adrian Davis**, Managing Director of the Europe, Middle East, and Africa (EMEA) region at (ISC)2 in the United Kingdom, provides practical solutions to the challenges of achieving supply chain cyber-resilience, suggesting an information-centric approach to protect information early on in the supply chain. The key point here is to integrate information into the procurement cycle to build cyber-resilience, and a list of actions is provided to facilitate this.

Then, **Hugh Boyes**, Principal Fellow at WMG at the University of Warwick, United Kingdom, applies a model for cybersecurity for both product and service supply chains that is adapted from the Parkerian hexad to explore the security and trustworthiness facets of supply chain operations that may impact cyber-resilience. This model is particularly relevant to complex, time-critical, and cyber-physical systems and is currently being documented for use in the construction industry.

In the fifth article, **Lars Jensen**, CEO and Co-Founder of CyberKeel, an international maritime cybersecurity company based in Copenhagen, Denmark, explores cyber-resilience challenges in the maritime industry, which, as this article reveals, has seen a significant increase in levels of cyber-attacks. After describing the nature and characteristic of cyber-threats, the article argues for an urgent response by the maritime industry to rapidly develop a set of best practice guidelines to reduce the risk profile and increase cyber-resilience.

Finally, **Richard Wilding**, Professor and Chair of Supply Chain Strategy at Cranfield School of Management in the United Kingdom, and **Malcolm Wheatley**, a Visiting Fellow at Cranfield School of Management, answer the question "how can I secure my digital supply chain?" by providing insights into understanding and addressing the challenges of securing the supply chain. The authors identify five areas that chief executives and directors of manufacturing and supply chains must focus on securing.

We hope you enjoy reading this month's issue on supply chain cyber-resilience. The articles in this issue present us with an introduction and explanation of the nature of supply chain cyber-resilience, and in doing so, they provide both academics and practitioners with key insights and challenges that may help them to address the growing threat from cyberspace.

Omera Khan
Guest Editor

Editorial: Cyber-Resilience in Supply Chains

Chris McPhee and Omera Khan

About the Editors

Chris McPhee is Editor-in-Chief of the *Technology Innovation Management Review*. He holds an MASc degree in Technology Innovation Management from Carleton University in Ottawa, Canada, and BScH and MSc degrees in Biology from Queen's University in Kingston, Canada. Chris has over 15 years of management, design, and content-development experience in Canada and Scotland, primarily in the science, health, and education sectors. As an advisor and editor, he helps entrepreneurs, executives, and researchers develop and express their ideas.

Omera Khan is a Full Professor of Operations Management at the Technical University of Denmark. She works with leading organizations on a range of supply chain and logistics issues and is advisor to many universities developing courses in logistics, supply chains, and operations management. She has led and conducted research projects commissioned by government agencies, research councils, and companies in supply chain resilience, responsiveness, sustainability, and the impact of product design on the supply chain. Her latest area of research focuses on cyber-risk and resilience in the supply chain. Omera is an advisor to many organizations and provides specialist consultancy in supply chain risk management. She is a highly acclaimed presenter and is regularly invited as a keynote speaker at global conferences and corporate events. She has published her research in leading journals, contributed to several book chapters, and is lead author of *Handbook for Supply Chain Risk Management: Case Studies, Effective Practices and Emerging Trends*. She founded and was Chair of the Supply Chain Risk and Resilience Research Club and the Product Design and Supply Chain Special Interest Group. She has also been a visiting professor at a number of leading business schools.

Citation: McPhee, C., & Khan, O. 2014. Editorial: Cyber-Resilience in Supply Chains. *Technology Innovation Management Review*, 5(4) 3–5.
http://timreview.ca/article/884

Keywords: supply chains, cyber-resilience, resilience, cybersecurity, cyber-attacks, cyber-risk