Editorial: Cybersecurity

Chris McPhee, Editor-in-Chief

Michael Weiss, Guest Editor

From the Editor-in-Chief

Welcome to the April 2017 issue of the *Technology Innovation Management Review*. This month's editorial theme is **Cybersecurity**, and I am pleased to welcome **Michael Weiss**, Associate Professor in the Department of Systems and Computer Engineering and the Technology Innovation Management (TIM; timprogram.ca) program at Carleton University in Ottawa, Canada.

In May, we examine the theme of **Lean and Global** with Guest Editor **Stoyan Tanev**, Associate Professor of Innovation & Design Engineering at the University of Southern Denmark.

For future issues, we are accepting general submissions of articles on technology entrepreneurship, innovation management, and other topics relevant to launching and growing technology companies and solving practical problems in emerging domains. Please contact us (timreview.ca/contact) with potential article topics and submissions.

Chris McPhee
Editor-in-Chief

From the Guest Editor

The articles in this special issue mirror some of the recent developments in cybersecurity. The Internet of Things and Internet-enabled medical devices are changing the security landscape: i) cyber attacks can be carried out on a much larger scale by levering devices that have less computing power and are, therefore, harder to protect against cyber-attacks, and ii) attacks can also affect humans lives directly through medical devices that are accessible via the Internet and embedded into the human body. A third area explored by the articles is the connection between cyber security and big data.

In the first article, **Mikko Hypponen**, Chief Research Officer at F-Secure, and **Linus Nyman**, Assistant Professor at the Hanken School of Economics in Helsinki, Finland, highlight the importance of security engineering for manufacturers building devices for the Internet of Things (IoT). Building on Hypponen's law, which asserts that "Whenever an appliance is described as being 'smart', it's vulnerable.", the authors offer recommendations to help manufacturers and consumers address the vulnerabilities of smart devices. They also highlight the importance of legislation in securing the Internet and its connected devices.

Next, **Mackenzie Adams**, Co-Founder and Creative Director at SOMANDA Inc., examines individual privacy in the IoT, specifically as it relates to big data. Drawing on evidence from recent big data breaches, the authors assert that the collection of data from IoT devices, and subsequent customization based on the collected data, create vulnerabilities in individual data privacy. The article examines the complexity of tackling technological and legislative challenges in protecting individual privacy. The authors position these issues in terms of the future implications of the IoT and the loss of privacy.

Then, **Ahmed Shah** and **Michael Weiss** from Carleton University; **Ibrahim Abualhaol** from Larus Technologies; and **Mahmoud Gad** from the VENUS Cybersecurity Corporation, describe the creation of a prototype system for monitoring real-time Border Gateway Protocol (BGP) traffic for security threats. By combining

Editorial: Cybersecurity

Chris McPhee and Michael Weiss

modes of exploratory analysis and automated analysis, the system enables security analysts to discover new anomalies and validate detection rules.

Finally, **Aida Alvarenga** and **George Tanev** from the Technology Innovation Management program at Carleton University propose a cybersecurity risk-assessment framework that integrates value-sensitive design. Using the field of medical devices as a case domain in which to ground their framework, the authors review the relevant literature through the perspective of using security initiatives as a value proposition that could be communicated to the medical device manufacturer’s stakeholders. To illustrate how it can be applied to a device and used to select the risk controls that bring the most value to the device’s key stakeholders, they apply their framework to the theoretical case of an insulin pump.

We hope that you enjoy reading this issue and will learn about some of the recent trends in cybersecurity.

Michael Weiss
Guest Editor

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 nearly 20 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.

Michael Weiss holds a faculty appointment in the Department of Systems and Computer Engineering at Carleton University in Ottawa, Canada, and is a member of the Technology Innovation Management program. His research interests include open source, ecosystems, mashups, patterns, and social network analysis. Michael has published on the evolution of open source business, mashups, platforms, and technology entrepreneurship.

Citation: McPhee, C., & Weiss, M. 2017. Editorial: Cybersecurity. *Technology Innovation Management Review*, 7(4) 3–4.
http://timreview.ca/article/1065

Keywords: cybersecurity, Internet of Things, IoT, Hypponen’s law, vulnerabilities, smart devices, security engineering, privacy, big data, legislation, anomaly detection, real time, exploration, automation, risk assessment, medical devices, value proposition