Business Horizons (2016) **xxx**, xxx—xxx

ELSEVIER

Available online at www.sciencedirect.com

ScienceDirect

KELLEY SCHOOL OF BUSINESS
INDIANA UNIVERSITY

www.elsevier.com/locate/bushor

GUEST EDITORS' PERSPECTIVE

Cybersecurity in 2016: People, technology, and processes

Michael Parent [a,*], Brian Cusack [b,*]

[a] *Telfer School of Management, University of Ottawa, 55 Laurier Avenue East, Ottawa, ON K1N 6N5, Canada*
[b] *Auckland University of Technology, 55 Wellesley Street East, Auckland 1142, New Zealand*

You have been, are being, or will be hacked. It's that simple, that certain, and that daunting. For most organizations today, it's no longer a matter of if, but when. As James Comey, director of the Federal Bureau of Investigation (FBI), bluntly stated in a *60 Minutes* interview in 2014: "There are two kinds of big companies in the United States. Those who've been hacked by the Chinese and those who don't know they've been hacked by the Chinese" (Cook, 2014).

According to the National Association of Corporate Directors (NACD), from 2014 to Q2 2015, companies reported over 2,429 data breaches affecting more than 1.25 billion records, at a hard (out-of-pocket) cost of over $150 per record. For individual firms, this typically means costs of $5.85 million for a single security incident (CompTIA, 2015; Owen & Bondi, 2016). And it is only going to get worse. The forthcoming, aptly-named Internet of Things (IoT) will see well over 10 billion internet-connected devices by 2020—more than the current number of computers, smartphones, tablets, and wearables combined (Adler, 2013), providing hackers with untold gateways into the world's networks and databases.

The Ponemon Institute reports that it takes an average of three months for financially vigilant firms to discover they have been hacked, an average of seven months for most organizations, and even years for others; meanwhile, it may take hackers just minutes to compromise a network (Kennedy, 2016; Osborne, 2015). A compilation of some of the largest hacks in recent history attests to this. Following is a miniscule sample of the many large breaches (Dingman, Silcoff, & Greenspan, 2015):

- Target — December 2013: 110 million records
- TJX — January 2007: 94 million records
- JP Morgan — August 2014: 83 million records
- The Home Depot — September 2014: 56 million records

We are witnessing a new dawn in cybercrime: a layer cake, if you will, of criminals eagerly seeking out networks and data. The bottom layer—in more ways than one—are the so-called *script kiddies*: hackers who troll the internet for attack scripts and then copy-paste them into attacks of their own. Not terribly sophisticated; but then again, a recent report calculated that over 652,000 distributed denial-of-service (DDoS) attacks occurred in a seven-day period (Graphic News, 2015). The next layer consists mainly of criminals, who have become increasingly enamored of *ransomware*: encrypting companies' data and offering to sell back the decryption key at a high price (Dingman, 2016). Organized crime and terrorists occupy the next

* Corresponding authors
E-mail addresses: michael.parent@telfer.uOttawa.ca (M. Parent), brian.cusack@aut.ac.nz (B. Cusack)

0007-6813/$ — see front matter
http://dx.doi.org/10.1016/j.bushor.2016.08.005

two tiers, using attacks to hide money-laundering activities or to gain valuable intelligence against people, places, and infrastructures. At the top of the cake are APTs: Advanced Persistent Threats, or sovereign hacking. According to Comey, most APTs come from two countries: the People's Republic of China (PRC) and the Democratic People's Republic of Korea (DPRK, or North Korea). In this case, the perpetrators are not looking for credit cards or personal information, but rather for patents, new drug discoveries, proprietary information, financial data (like forthcoming mergers or acquisitions), intellectual property, or even national secrets.

Any way you look at it, the news and prognoses are grim. Data breaches have paradoxically become commonplace crises and organizations are lagging in responding, adapting, and adopting protective measures. Reaction windows are now measured in minutes, not hours, much less days. As we like to say when briefing managers: "Hope is no longer a strategy."

In soliciting articles for this issue, we sought to go beyond the conventional and beyond the dramatic. There seems to be a widespread culture of shared negative experiences surrounding cybersecurity. Contributing to alarmist discourses does little to reassure managers and even less to encourage constructive research. Our goal was to provide clear and cogent perspectives that might facilitate positive information exchanges.

If one thing is clear, it is that cybersecurity is more than just a technical issue. It involves unique alchemies between technologies, people, and processes—the latter in the form of overarching regulations and laws. As such, we have divided the articles into these three sections, starting with two articles on the most important element: people.

The first article—by Dang-Pham, Pittayachawan, and Bruno—considers how and when security advice is shared by employees. Research supports the efficacy of security-centric cultures. However, more often than not, managing security is seen as a top-down exercise, where a lack of compliance is met with disciplinary action. The authors analyze some of the underlying personal and structural causes impeding security cultures, asserting they are more circular than hierarchical, and offer some practical insights for both researchers and managers who wish to develop and sustain peer-managed security cultures in their organizations.

The role of Chief Information Security Officer, or CISO, is a recent creation in organizations. The second article—by Hooper and McKissack—outlines the responsibilities of this role, its place in the organization, and the type of leadership it demands if it is to succeed.

The Technology subsection of the issue presents the next three articles, each dealing with different technological considerations related to security. Lutui's article is our only piece on digital forensics and is eerily reminiscent of the FBI's recent desire to unlock a domestic terrorist's phone, the subject of court action against Apple Inc. Lutui presents a forensic model that is both contemporary and concise. In doing so, he provides a sound overview of digital forensics for those who might not be familiar with the field. While the tool he presents is still in its infancy, it holds much promise for investigators as smartphones and smart devices proliferate. The two other articles in this subsection—by co-editor Cusack and his colleague Ghazizadeh; and Mills, Watson, Pitt, and Kietzmann—discuss the risks inherent in nascent technologies: the cloud and single sign-on failures for the former and the growing field of wearables for the latter. In both cases, we deal with security issues at the cutting edge of technology. However, the authors also all make the point that while the technologies might be new and their imperatives different, the principles underlying sound security policies and practices still apply—now more than ever.

Finally, Crowley and Johnstone conclude the special issue section with an overview of the legal and technical issues surrounding data security. As they so aptly state, "nothing in cyberspace may be private." The article explores the tension between privacy and disclosure using the recent Microsoft E-Mail and Apple iPhone cases. Crowley and Johnstone echo some of the points made by earlier authors in the subsections on people and technology. Although the Apple case has been resolved, it nevertheless allowed legislators, law enforcement authorities, privacy advocates, equipment manufacturers, and end-users to comment on and gain insight from each other.

With the vastness, visibility, and velocity of data breaches increasing exponentially, managers are left with a complex challenge that spans across the organization, not just their information technology (IT) divisions. Cybersecurity is a critical, cross-functional issue that affects everyone and every organization, directly and indirectly. The six articles presented in this special issue, we believe, collectively merge the human, technological, and regulatory environments, offering intriguing insights and ideas for both research and practice as this discussion evolves.

References

Adler, E. (2013, December 7). Here's why 'the Internet of Things' will be huge, and drive tremendous value for people and business. *Business Insider*. Retrieved May 1, 2016, from http://www.businessinsider.com/growth-in-the-internet-of-things-2013-10

CompTIA. (2015). *Trends in Information Security*. Retrieved May 10, 2016, from https://www.comptia.org/resources/trends-in-information-security-study

Cook, J. (2014, October 6). FBI Director: China has hacked every big US company. *Business Insider*. Retrieved May 15, 2016, from http://www.businessinsider.com/fbi-director-china-has-hacked-every-big-us-company-2014-10

Dingman, S. (2016, May 20). Ransomware in real time: How hackers infiltrate secured systems. *The Globe and Mail*. Retrieved May 30, 2016, from http://www.theglobeandmail.com/technology/ransomware-in-real-time-how-hackers-infiltrate-secured-systems/article30111818/

Dingman, S., Silcoff, S., & Greenspan, R. (2015). Hacked: The escalating arms race against cybercrime. *The Globe and Mail*. Retrieved December 12, 2015, from http://www.theglobeandmail.com/report-on-business/hacked-the-escalating-arms-race-against-cybercrime/article21305464/?page=all

Graphic News. (2015, October 27). Cyber smokescreen to steal data. *Graphic News*. Retrieved from http://www.graphicnews.com/en/go/pages/33616/TECHNOLOGY_Destructive_cyber_assaults

Kennedy, J. (2016, April 25). Data breaches take minutes to happen, but weeks to discover. *Silicon Republic*. Retrieved May 16, 2016, from https://www.siliconrepublic.com/enterprise/verizon-data-breach-report-2016

Owen, D. R., & Bondi, B. J. (2016, March 16). Defending data — A director's cybersecurity duty. *NACD Directorship Boardroom Intelligence*. Retrieved May 1, 2016, from https://www.nacdonline.org/Magazine/Article.cfm?ItemNumber=25613

Osborne, C. (2015, May 19). Most companies take over six months to detect data breaches. *ZDNet*. Retrieved May 16, 2016, from http://www.zdnet.com/article/businesses-take-over-six-months-to-detect-data-breaches/