Business Horizons (2016) **59**, 539—548

Available online at www.sciencedirect.com

ScienceDirect

KELLEY SCHOOL OF BUSINESS
INDIANA UNIVERSITY

www.elsevier.com/locate/bushor

Business and cyber peace: We need you!

Scott J. Shackelford

Kelley School of Business, Indiana University, 1309 E. Tenth Street, Bloomington, IN 47405-1701, U.S.A.

KEYWORDS
Cybersecurity;
Cyber-attack;
Due diligence

Abstract Rarely does a day seem to go by without another front page story about a firm being breached by cyber-attackers. Even experts in the field are far from immune from the unsustainable status quo. For example, Jim Lewis of the Center for Strategic and International Studies has said: "We have a faith-based approach [to cybersecurity], in that we pray every night nothing bad will happen." This is a difficult starting point to consider an appropriate end game. Still, it is something that firms must do since infinite investment cannot breed infinite security. This article takes lessons from the burgeoning field of cyber peace studies and applies them to private sector cyber risk mitigation strategies. With members of the C-suite on down to mailroom clerks worrying about the next attack and looking over their shoulder after a breach occurs, who wouldn't welcome some peace of mind?
© 2016 Kelley School of Business, Indiana University. Published by Elsevier Inc. All rights reserved.

1. Introduction

> 'Cyber peace' to me would be an entire weekend without my Blackberry going off.
>
> — *Kroll Advisory Solutions Managing Director Michael DuBose* (2011)

Remember the good old days of the roaring late 1990s? U.S. GDP growth was humming along at almost 5%, Cher's *Believe* was topping the charts, no one was glued to smartphones—if one even had a cell phone it was likely a Nokia featuring picture messaging for the first time—and cyber-attacks were still something done mostly by teenage hackers with too much time on their hands. My, how times change. The world in 2015 is a much more complicated place—the number of Angry Birds iterations alone boggles the mind—and the issue of cybersecurity has become especially problematic for managers, so much so that some firms are going back to a time before the late 1990s and are reintroducing typewriters to better protect their consumers and invaluable intellectual property (Lyons, 2014). In an era when smartphones can be turned into microphones for purposes of eavesdropping even when they are turned off, the dangers of cybersecurity illiteracy and the necessity of building a global culture of cybersecurity are self-evident (Bucktin, 2014). But defining and promoting the cause of cyber peace is easier said than done with many managers left unsure about where to put that next dollar of investment (e.g., deciding whether to go with biometrics or an employee cyber hygiene

E-mail address: sjshacke@indiana.edu

0007-6813/$ — see front matter © 2016 Kelley School of Business, Indiana University. Published by Elsevier Inc. All rights reserved.
http://dx.doi.org/10.1016/j.bushor.2016.03.015

education), how to reorganize to better mitigate the risk of cyber-attacks, and what to do when things go wrong. Although it is beyond the scope of this brief article to answer all of these questions, a range of cybersecurity best practices are discussed along with how they fit together to promote the cause of cyber peace.

Indeed, rarely does a day seem to go by without another front page story about a firm being breached by cyber-attackers. Even experts in the field are far from immune from the unsustainable status quo. For example, Jim Lewis of the Center for Strategic and International Studies has said: ''We have a faith-based approach [to cybersecurity], in that we pray every night nothing bad will happen'' (Dilanian, 2010). This is a difficult starting point to consider an appropriate end game. Still, it is something that firms must do since infinite investment does not breed infinite security. This article takes lessons from the burgeoning field of cyber peace studies and applies them to private sector cyber risk mitigation strategies. It is structured as follows: First, cyber peace itself is defined in the context of how businesses can promote peace generally, and then how that goal can be attained by working together. Next, a range of proactive cybersecurity best practices is discussed before finally considering the global cybersecurity legal environment. With managers and even members of the C-suite looking over their shoulder after a breach, who wouldn't welcome some peace of mind?

2. Defining 'cyber peace'

How does business foster peace generally? Five ways which are related to the cybersecurity context are evident (Evers, 2010; Shackelford, Fort, & Prenkert, 2014). The first pertains to peacemaking, such as negotiations to resolve a conflict in Nicaragua in which business people actively participated in the settlement process (Kupchan, 2012). The second arena is promoting economic development and job growth—an important feat given the extent to which cyber-attacks are costing jobs (Whitehouse, 2010). Studies by both the United Nations and the World Bank suggest that there is a strong correlation between poverty and violence (Atwood, 2003). The third way that businesses promote peace is by furthering good governance and the rule of law since countries that govern pursuant to the rule of law tend to be more peaceful than those that do not (United States Institute of Peace, n.d.). Relatedly, economic freedom has been shown to correlate with peace in a series of studies; so too has democracy (Weart, 1998). The fourth contribution businesses can make to peace comes in the sense of how the company is a community unto itself as well as being part of a larger community. Fifth, companies that are respectful of local customs, norms, religions, and traditions will have an impact greater than ones that are abusive, exploitative, and insulting (Fort & Schipani, 2003).

Of course, many businesses fail to live up to these ideals, such as by contributing to local corruption, exploiting disempowered communities, and extracting local political or even tribal divisions to extract concessions. But putting such behavior aside, the point is that many businesses can and do promote peace around the world, whether they realize it or not. More firms are adopting the practice of sustainability reporting—for instance, through such frameworks as the Global Reporting Initiative (GRI)—or are implementing the Guiding Principles on Business and Human Rights into their operations. In fact, nearly 8,000 organizations have submitted more than 25,000 GRI reports as of June 2015, making the framework the dominant sustainability-reporting standard for international business (Global Reporting Initiative, 2015). Less appreciated, though, is the invaluable role that businesses are playing in furthering the cause of cyber peace.

A trifecta comprised of the Vatican, the World Federation of Scientists, and the International Telecommunication Union (ITU), a UN agency specializing in information and communication technologies, did some of the early work on the concept of cyber peace, defining 'cyber peace' in part as ''a universal order of cyberspace'' built on a ''wholesome state of tranquility, the absence of disorder or disturbance and violence. . .'' (Wegener, 2011, p. 82). Although certainly desirable, such an outcome is politically and technically unlikely, at least in the near term. That is why cyber peace is defined here not as the absence of conflict—a state of affairs that may be called negative cyber peace (King, 1957)—but rather as the construction of a network of multilevel regimes that promote global, just, and sustainable cybersecurity by clarifying the rules of the road for companies and countries alike to help reduce the threats of cyber conflict, crime, and espionage to levels comparable to other business and national security risks (see Shackelford, 2016). To achieve this goal, a new approach to cybersecurity is needed that seeks out best practices from the public and private sectors to enhance cybersecurity due diligence. Working together through polycentric partnerships, different parties can mitigate the risk of cyber war by laying the groundwork for a positive cyber peace that respects human rights, spreads Internet access along with best practices, and

Download English Version:

https://daneshyari.com/en/article/5108932

Download Persian Version:

https://daneshyari.com/article/5108932

Daneshyari.com