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?

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
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

strengthens governance mechanisms by fostering multi-stakeholder collaboration (Galtung, 2011).

But how do these lofty ideas get translated into the complex, fast-paced, and oftentimes-messy corporate world? That is where the literature on polycentric governance, sometimes called the 'Bloomington School,' provides some insights, which are briefly discussed next before moving on to a suite of leading technical, budgetary, organizational, and managerial cybersecurity best practices.

3. How do we get there?

It is easy to throw up your hands when reading the slew of terrible news surrounding cybersecurity. When your toddler starts getting data breach notifications with offers of free credit monitoring, you know that something is amiss. Indeed, many practitioners are similarly not immune from this sense of apathy when it comes to cybersecurity—what can any of us do against the army of cyber-attackers that seem to be constantly coming after our Amazon passwords, bank details, and trade secrets? As it turns out, quite a lot. Before getting to the nuts and bolts, though, it is first worth couching this discussion within the literature on bottom-up empowerment known as polycentric governance, which grew from the tragedy of the commons.

You may recall at some point learning about the tragedy of the commons. This is the idea popularized by Professor Garrett Hardin in 1968 that predicts the overexploitation of scarce resources held in common, such as a village pasture—or for that matter many lakes, forests, and marine fisheries (Hardin, 1968). People tend to maximize their short-term personal interests ahead of the collective good. This is a dilemma in economic terms because an outcome exists that would make everyone better off if only people cooperated. But unfortunately, they often don't, a problem modeled as the prisoner's dilemma. What can be done about this? The classic solutions of nationalization and privatization each have their drawbacks. Nepal, for example, tried nationalizing its forests in the 1950s to stave off deforestation but actually wound up increasing it since local communities no longer had an incentive to be good stewards (Arnold & Campbell, 1986). Luckily there is a third way, an often overlooked solution to the tragedy of the commons that was part of the reason Professor Elinor Ostrom won the Nobel Prize in economics—the first woman to do so—in 2009: polycentric common property, which involves "group control over. . .[a] resource" leading to "the balancing of benefits and costs" through rules regulating joint use (Stevenson, 1991, p. 3).

The field of polycentric governance came of age in the domestic context during the 1970s and 1980s through a series of landmark field studies challenging the prevailing notion that the provision of public services, like police and education, was made better and more cost-effective through consolidation (Ostrom, Parks, & Whitaker, 1978). Scholars led by Professor Elinor Ostrom showed, for example, that small and medium-sized police departments outperformed their larger counterparts serving similar neighborhoods in major urban centers in measures of efficiency and cost (McGinnis, 1999). Later field work that she and others conducted on the provision of water resources in California, the design and maintenance of irrigation systems in Nepal, and the protection of forests in Latin America showed that, contrary to the conventional theory of collective action, many communities do in fact cooperate in the face of collective action problems (Ostrom & Nagendra, 2006; Shivakoti & Ostrom, 2002). These observations were consistent with laboratory experiments, which found that externally imposed regulations can crowd out voluntary cooperative behavior (Ostrom, 2010). In other words, this multi-level, multi-purpose, multi-functional, and multi-sectoral model has empirically demonstrated the benefit of norm entrepreneurs identifying and spreading best practices from the bottom up, challenging orthodoxy by demonstrating the benefits of self-organization, networking regulations 'at multiple scales,' and examining the extent to which national and private control can in some cases coexist with communal management (Ostrom, 2008). In the next section, I will translate what all this means for the task of mitigating cyber risk.

4. Mitigating cyber risk from the bottom up: Leaning in to a proactive cybersecurity posture

Polycentric regulation is not a 'keep it simple, stupid' response, but a multifaceted one in keeping with the complexity of the crises in cyberspace. This approach has its drawbacks, though, since not all aspects of polycentric governance easily apply to cyberspace. Given that the online community includes more than two billion users, the concept of self-organization, for example, is strained. Additionally, there are important drawbacks of polycentric regulation to be addressed, such as the fact that a highly fragmented system can lead to gridlock instead of innovation due, in part, to an insufficient hierarchy (Keohane & Victor, 2011). But the point is that viewing cybersecurity through this lens potentially takes the debate about how to address

cybersecurity challenges in a more productive direction by helping to eschew false choices, divisive top-down regimes, and all or nothing choices, as well as by challenging all relevant stakeholders to take action through a more inclusive conceptual framework. First and foremost on that list is business. After all, according to Frank Montoya, former U.S. National Counterintelligence Chief: ''We're an information-based society now. Information is everything. That makes. . .company executives the front line—not the support mechanism, the front line—in [determining] what comes'' (Gjelten, 2012). That puts managers in an unenvious, but vital position; not only do their decisions impact their own firm's operations, but also more broadly the competitiveness of the economy and the cause of national security. Heady stuff, and not necessarily what most signed up for. But that's where we're at, so let's dive in.

With the technical, organizational, economic, and even professional costs of cyber insecurity becoming better appreciated, more managers are considering how best to protect their firms and themselves from the multifaceted cyber threat. Before moving on to best practices from each of these categories, though—which together may be couched as a comprehensive approach to cybersecurity due diligence—it may first be helpful to get some sense of how big of a problem cyber-attacks really are anyway. The problem is, no one really knows because of a lack of verifiable data and a common vocabulary on how best to talk about what we do know. Contested estimates place the global cost of cyber-attacks in the range of $400 billion to more than $2 trillion, which, if accurate, is a figure larger than estimates for the global illegal drugs market (Center for Strategic and International Studies, 2014). Regardless of the scale, though, it is true that cyber-attacks are a problem facing more individuals and organizations than ever, from First Lady Michelle Obama to average citizens in Ghana, along with the likes of Google down to local credit unions and even elementary schools (Baumhof, 2012; Galvin, 2013). Yet it is also true that neither these diverse stakeholders nor the nearly three billion Internet users worldwide are facing the same types of cyber-attacks. For example, firms with valuable intellectual property are targets for social engineering campaigns as well as advanced persistent threats (APTs) on their networks, potentially sponsored by nation states boasting tremendous patience and resources and carried out by sophisticated organized crime networks (McAfee Labs & McAfee Foundstone Professional Services, 2010). Firms today must conduct cyber risk assessments to determine their vulnerabilities in order to prepare for their most advanced attackers. This is no easy feat given the rapidly evolving cyber threat matrix, fragmented global regulatory landscape, and lack of consensus on the scope of the problem and what cybersecurity best practices should be deployed to better manage cyber-attacks (Fung, 2013). Insurance companies are among the best positioned to undertake such analyses, but they are also grappling with limitations on data and pricing structures (see Shackleford, 2012). Indeed, the situation is so complex that some insurance companies have refused to insure utilities operating the British electrical grid due to concerns over their latent cyber insecurity (Turk, 2014).

Effective cybersecurity requires engagement from every level of an organization, from the board of directors on down to the mailroom. Given both the prevalence of insider threats and how many organizations are now allowing their workers to connect their personal devices to professional intranets, it goes even beyond the workplace into employees' private lives. This section briefly discusses best practices ranging from addressing insecure supply chains and technical vulnerabilities in the Internet's architecture to personal and corporate cybersecurity management best practices.

4.1. Technical cybersecurity best practices

For much of its early history, a cadre of dedicated professionals and volunteers managed the Internet's communications and address system. As governance became more formalized, security has received greater attention, but vulnerabilities persist. Cyber-attacks are the result of a complex threat ecosystem to which these vulnerabilities contribute. Their effective management requires taking targeted measures at every level from securing hardware to code (Thaler & Aboba, 2008), but mitigation strategies are most efficiently introduced from the bottom up. Two examples are evident: supply chain management and protocol security.

First, circuits leave physical trapdoors, but as with code, most experts cannot easily identify flaws in a computer chip. Indeed, producing a microchip requires some 400 steps (Clark & Levin, 2009). And aside from manufacturing or design defects, some bugs may be purposefully implanted. A 2012 Microsoft report found malware being installed in PCs at factories in China, thus highlighting the insecurity of production lines (''Malware inserted on PC production lines,'' 2012). U.S. government reports have also cited supply chain concerns for hardware, finding components embedded with security flaws (Sternstein, 2011). Once compromised, hardware is

often in the hands of an unknowing user. Few hardware vulnerabilities are likely to be discovered and fixed, and even fewer are likely to be attributed to a particular cyber-attacker. This requires vigilance in supply chain management, such as requiring vendors to adopt best practices like the NIST Framework, which will be discussed.

Second, the Internet works through protocols that were, in many cases, created in an era when a relatively small number of academic and government researchers comprised the global pool of Internet users. As such, these protocols were frequently built on trust. Unfortunately, today that trust is oftentimes misplaced. Consider the Domain Name System (DNS). DNS is the Internet's address system that works as a phone book to map domain names to Internet Protocol addresses so that users only have to remember a name, such as www.indiana.edu, and not a string of digits to navigate to a website. Now consider that in August 2013, the *New York Times* online operations, along with an array of other organizations such as Twitter, were hacked, allegedly by the Syrian Electronic Army (Tsukayama & Lee, 2013). In this case, attackers hacked into an Australian domain name registry and managed to alter stored information there, allowing them to redirect users to a webpage sporting whatever information the Syrian Electronic Army wished to post. Unfortunately, such attacks are far from the exception and allow cyber-attackers to launch an array of exploits, including the ability to spoof legitimate websites to get customers to enter their personal credentials, potentially comprising both themselves and the targeted company's brand. Luckily, there's at least a partial fix available called the Domain Name Security Extensions (DNSSEC) protocol, which was proposed back in 1997 and revised in 2005. But because of the largely voluntary system of Internet governance, no organization mandated that DNSSEC be implemented. As a result, relatively few organizations have deployed it (Marsan, 2013). Has your business? If not, it may be worth looking into.

It might also be worth considering encrypting data both in transit and at rest. Surveys have shown that certain technologies, like firewalls and anti-virus software, are now widely diffused security technologies. Encryption, perhaps surprisingly, is still less common. By guarding data internally and forcing thieves to decrypt it, encryption helps protect both intellectual property and the long-run competitiveness of economies. But it is not perfect. Typically, though, attackers focus on compromising the underlying code rather than the mathematical algorithms at its core, meaning that open source encryption and other products hold the potential for securing online communication (Shane & Perlroth, 2013). However, there is no magic bullet here, and addressing technical vulnerabilities is just the first step in enhancing organizational cybersecurity.

4.2. Personal cybersecurity best practices

In many ways, personal cybersecurity is the foundation on which cyber peace is built. Without an informed and engaged online community, malicious actors will continue to take advantage of unknowing or apathetic users to perpetuate crimes and launch cyber-attacks. Internet use comes with both rights and responsibilities. More public- and private-sector campaigns are needed to educate users about best practices starting at an early age, potentially equating good cybersecurity citizenship with good hygiene such as the importance of washing hands. Luckily, much can be done to make it less likely that you will be one of the approximately 12.6 million annual U.S. victims of fraud or identity theft. For example, according to one study, the most common password remained '123456,' whereas the tenth most common was 'abc123' (Coursey, 2010). Putting in the effort that it takes to create strong passwords can not only save time and money—the average victim of identity theft in 2011 reportedly spent 12 hours and $365 to fix the problem—but it can also enhance the overall level of cybersecurity by, for example, making it less likely that your computer will become just another zombie in a nefarious botnet. Other personal cybersecurity best practices are listed in Table 1.

Unfortunately, many businesses do not mandate cybersecurity education for their workers, and few of those that do audit their programs for effectiveness or have cybersecurity included as part of an overarching enterprise risk management strategy that is regularly updated and communicated throughout the organization. Therefore, I attempt to summarize the arena of corporate cybersecurity best practices next.

4.3. Corporate cybersecurity best practices: The benefits of being proactive

The private sector is at the front line of enhancing cybersecurity. As with individuals, it is in firms' best interests to take cybersecurity seriously to protect their intellectual property and reputations and safeguard their customers' personally identifiable data. The strategic management literature has shown that cybersecurity should be viewed as a 'value creator' supporting e-business (Cavusoglu, 2004). To reduce their risk exposure, firms should adopt a proactive, systemic approach to cybersecurity through three steps. First, companies should regularly conduct cyber risk assessments and invest in enhancing security consistent with their risk exposure. This first step

Table 1. Top 10 Personal Cybersecurity Best Practices

1. Install antivirus and antispyware software, like Microsoft Security Essentials or Symantec Endpoint, and use auto update.
2. When using public Wi-Fi, use browsers like TOR to make it more difficult for hackers to spy on you.
3. Keep all software and operating systems up to date by selecting auto update—especially Windows, but also programs like Adobe Reader, Flash, and Java, which are often convenient backdoors that can be closed through frequent updates.
4. Use strong passwords of at least 14 characters; keep them secret, and change them often. Consider starting with a favorite sentence, and then just take the first letter of each word. Add numbers, punctuation, or symbols for complexity.
5. Never turn off your firewall; it's an important software program that helps stop viruses and worms.
6. Use flash drives cautiously. They are easily infected: In fact, the biggest breach of U.S. military systems to date was due to a flash drive.
7. Encrypt sensitive information on your computer with programs like Identity Finder.
8. Be conscious of what you click on, both in emails and on the Web. When in doubt, ignore or reply and double check before accessing attached files.
9. Be on the lookout for 'HTTPS'—do not use banks or other sensitive websites that do not have the 'S,' which means that the site is encrypted.
10. Try not to bank on your mobile device, and consider using a separate secure Wi-Fi connection or other computer for personal computing at home.

could include requiring data encryption, air gapping vital systems, and conducting regular penetration testing with third party audits. Second, managers should assess their insurance coverage as part of a comprehensive risk mitigation effort, making use of cost-benefit analysis to determine whether additional protection is warranted. Third, firms should analyze their cybersecurity organization to ensure that it is optimized for coordination and information sharing, both within the company and with relevant industry groups and public-private partnerships. This third step serves both to help better inform policymakers and to protect their own company against known threats. Some degree of centralization is important, whether through a Chief Information Security Office (CISO) or an analogous position (Ponemon Institute, LLC, 2011). For example, when Sony was breached in 2011—leading to one of the largest data breaches in history to that point—it did not have a CISO. It does now. As losses mount, investors will likely stop treating cyber-attacks as a corporate nuisance, and start treating them as the serious threat that they are to the survival of firms and, at a macro level, the long-term competitiveness of knowledge economies built on innovation. What else can firms do? They should consider the realms of budgetary and organizational best practices.

Cybersecurity best practices do not necessarily come cheap. Still, it may be worth spending a bit more; as recently as 2008, most "organizations allocated 5 percent or less of their overall IT budget to information security" (Richardson, 2008). However, it is worth noting that companies keep track of their security budgets in different ways. At Microsoft, the push to enhance cybersecurity is team-driven and staffed by engineers from different groups, so the cost is diffused. Company size and geography also matter (Gordon, Loeb, Lucyshyn, & Richardson, 2006). Companies in emerging economies, for example, tend to spend relatively more than their developed-nation counterparts (PwC, 2010). Still, the Ponemon Institute estimates that more than $45 billion in investments are needed to secure private firms operating critical infrastructure alone (Engleman & Strohm, 2012). But it is not as simple as spending more in cybersecurity; infinite investment will not breed investment security. Rather, a cost-benefit analysis at the firm level is central to identifying enterprise risks and determining the best tools, including organizational best practices, to manage cyber-attacks.

Regarding organizational best practices, leadership from the top is a necessary but insufficient prerequisite to cybersecurity success. Just 13% of respondents to a 2012 PwC survey made the survey's 'leader cut'—a label used to identify respondents that measured and reviewed security policies annually and had either an information security strategy or a CISO reporting to management (PwC, 2011). In fact, up to 80% of small firms reportedly lack cybersecurity policies at all (Homeland Security News Wire, 2011). Such bleak statistics call into question the potential for the private sector to lead the drive to promote a positive cyber peace, even as success stories like Microsoft show the innovative potential for bottom-up change. Still, there are a range of best practices that businesses can adopt to better mitigate their cyber risk, as is discussed in Table 2.

Moreover, it is vital that firms identify their most valuable intellectual property and put together a plan for how to protect it from technical and human risks, as well as come up with a strategy for how to communicate that risk mitigation plan both internally as well as with regulars and shareholders (see Touhill & Touhill, 2014).

Overall, though, it is vital that firms take a proactive, and not a reactive, approach to cybersecurity.

Table 2. Top 10 Corporate Cybersecurity Best Practices

1. Do everything in Table 1, articulated as part of an overarching enterprise risk mitigation strategy with cybersecurity as one component. Ensure that the plan is regularly updated and communicated as part of an employee cybersecurity education campaign.
2. Segment networks and air gap vital systems from the public Internet.
3. Use the NIST Framework, or at least be able to articulate why you are not using it.
4. Assess current cyber risk insurance coverage as part of a larger conversation on cyber risk mitigation.
5. Consider joining private or public-private cyber threat information sharing organizations such as an Information Sharing and Analysis Center (ISAC).
6. Localize local administrator privileges to make it more difficult to log in as an administrator.
7. Ensure that all operating systems and approved software packages are being updated automatically.
8. Secure your supply chains to the extent possible, such as by requiring NIST Framework compliance for all vendors.
9. Have an incident response plan in place that lays out what parties are responsible for working with law enforcement and affected consumers.
10. Be proactive! Build in these and other cybersecurity best practices from the start of a new product or service; don't leave them as an afterthought.

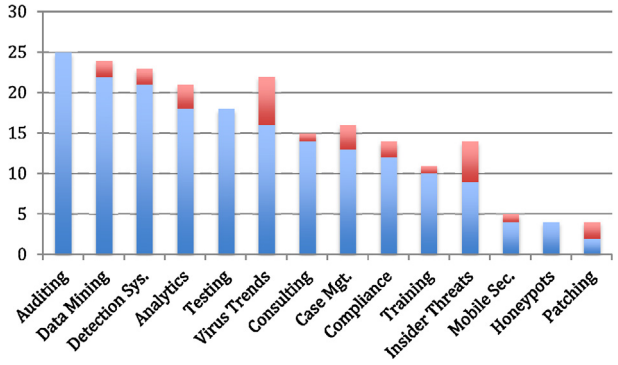
The emerging field of proactive cybersecurity is complex, encompassing a range of activities also referred to as 'active defense.' While 'hacking back' is often a highly visible point of contention when discussing the role of private sector active defense, it is just one facet of the larger proactive cybersecurity movement, which includes technological best practices including real-time analytics, cybersecurity audits promoting built-in resilience, advanced threat intelligence sharing, and active detection techniques like honeypots (Craig, Shackelford, & Hiller, 2015). To get a sense of leading proactive best practices, the offerings of 26 leading cybersecurity firms were surveyed and compiled together in Figure 1. The most widespread practices across surveyed companies are on the left side of the chart, while practices on the right side are less common. It should be noted that that these findings do not represent definitive industry norms, emerging or otherwise. There are hundreds, if not thousands, of firms offering cybersecurity solutions worldwide—so many that some have even questioned whether a cybersecurity bubble is brewing. Still, these findings do represent an industry snapshot (as of October 2014) that offers some telling data points about the areas in which these cybersecurity firms are focusing their efforts.

Ultimately though, as Professor Andrew Murray has argued, "The market functions—but only so far!" with regards to enhancing cybersecurity (Murray, 2006, p. 200). Policymakers, then, also have a role to play when it comes to enhancing cybersecurity, especially when this is considered an example of a market failure. Given the rapidly changing technological environment, though, it is a difficult task for many jurisdictions. Still, many nations have tried. The final section introduces the global legal environment of cybersecurity law and policies focusing on efforts by the U.S. and the European Union to enhance private-sector cybersecurity and with it advance the cause of cyber peace.

5. The global legal environment: Get to know the NIST framework

Just as no nation is an island in cyberspace, no firm operates in a legal vacuum. Among the most influential jurisdictions currently crafting cybersecurity

Figure 1. Snapshot of Proactive Cybersecurity Practices



Source: Craig et al. (2015, p. 758)

policies impacting the global legal environment are the U.S. NIST Framework and the EU's cybersecurity policy, each of which is briefly discussed in turn.

In February 2013, President Obama issued an executive order that, among other things, expanded public-private information sharing and tasked the National Institute for Standards and Technology (NIST) with establishing a voluntary 'cybersecurity framework' comprised partly of private-sector best practices that companies could adopt to better secure critical infrastructure (The White House, 2013). The Framework version 1.0, *Framework for Improving Critical Infrastructure Cybersecurity*, was released in February 2014. It harmonizes consensus standards and industry best practices to provide, its proponents argue, a flexible and cost-effective approach to enhancing cybersecurity that assists owners and operators of critical infrastructure in assessing and managing cyber risk.

The Framework provides a voluntary procedure to map cybersecurity best practices, determine the overall state of an organization's cyber risk management practices, and structure roadmaps for organizations to mitigate those risks. This framework is important since, even though its critics argue that it helps to solidify a reactive stance to the nation's cybersecurity challenges (Armerding, 2014), it is arguably spurring the development of a standard of cybersecurity care in the United States that plays into discussions of due diligence (Shackelford, Proia, Martell, & Craig, 2015). Although the NIST Framework has only been out for a relatively short time, some private-sector clients are already receiving the advice that if their "cybersecurity practices were ever questioned during litigation or a regulatory investigation, the 'standard' for 'due diligence' was now the NIST Cybersecurity Framework" (Verry, 2014). Indeed, more companies are requiring NIST Framework compliance for all suppliers and potential partners, something that more firms are undertaking. For example, in early 2015 Bank of America announced "that it is using the Framework and will also require it of its vendors[,]" while "QVC is announcing that it is using the Cybersecurity Framework in its risk management" (The White House, 2015). Over time, the NIST Framework not only has the potential to shape a standard of care for domestic critical infrastructure organizations but also could help to harmonize global cybersecurity best practices for the private sector writ large given active NIST collaborations with a number of nations including those in Europe.

The same month that President Obama empowered NIST to create the cybersecurity framework, the European Commission issued a communication that set out a proposal for boosting cybersecurity within the European Union (Christopher, 2014). Among much else, this regime would require many firms with some nexus to e-commerce to invest in cybersecurity technologies, develop procedures to prove compliance to national and EU regulators, and undertake enhanced cyber risk mitigation measures such as regular penetration testing to better manage attacks. In so doing, this development could cause any firm providing online services in Europe to "fundamentally have to change the way its business operates" (Ashford, 2013). It could also help define a Europe-wide cybersecurity duty of care for covered industry. Given that the size of the EU's economy is comparable if not larger than that of the United States, this new EU regime could have substantive network effects extending to the many global businesses that operate in EU nations. Moreover, U.S.-EU policymakers are in regular discussions, meaning that the NIST Framework could be influential in shaping EU efforts in this space and could even help shape a global duty of cybersecurity care (Christopher, 2014). Thus, the NIST Framework is worth paying attention to if for no other reason than it's quickly becoming the benchmark against which a baseline cybersecurity posture is measured, which can include negligence litigation following a data breach.

6. Conclusion

Today the international community is at the point of determining how governance of cyberspace should develop in the 21st century. The strategies and practices assumed in the short-term will impact how this fast-evolving body of law and policy is shaped and systems are secured. Policymakers and managers alike should consider not only what serves short-term interests but also the shared long-term interest of building a secure, interconnected, and robust cyberspace for the world's existing 2.5 billion Internet users and the billions more to come.

There are market, ethical, and legal reasons for firms to invest in cybersecurity best practices and thereby further cyber peace. Therefore, given the central role of the private sector in managing cyberattacks in the United States and around the world, the role of businesses in fostering cyber peace should not be underestimated. Working together through polycentric partnerships, and with the leadership of engaged individuals and institutions, we can mitigate cyber conflict by laying the groundwork for a positive cyber peace that respects human rights, spreads Internet access along with best practices, and strengthens governance mechanisms by fostering multi-stakeholder collaboration. Over time, a set of

guiding principles of cyber peace may be developed in the same vein as the UN Global Compact. Ultimately, it is up to boardrooms just as much as governments to help foster a global culture of cybersecurity; but in order to do that, we need you!

References

Armerding, T. (2014). *NIST's finalized cybersecurity framework receives mixed reviews*. Retrieved January 31, 2014, from http://www.csoonline.com/article/2134338/security-leadership/nist-s-finalized-cybersecurity-framework-receives-mixed-reviews.html

Arnold, J. E. M., & Campbell, J. G. (1986). Collective management of hill forests in Nepal: The community forestry development project. *In Proceedings of the conference of common property resource management* (pp. 425—454). Washington, DC: National Academy Press.

Ashford, W. (2013, February 19). *How will EU cyber security directive affect business?* Retrieved February 19, 2013, from http://www.computerweekly.com/news/2240178256/How-will-EU-cybersecurity-directive-affect-business

Atwood, J. B. (2003). The link between poverty and violent conflict. *New England Journal of Public Policy, 19*(1), 159—165.

Baumhof, A. (2012, February 8). Credit unions and the evolving cybercrime landscape. *Credit Union Times*. Retrieved February 8, 2012, from http://www.cutimes.com/2012/02/08/credit-unions-and-the-evolving-cybercrime-landscap

Bucktin, C. (2014, June 10). Spies can listen to your iPhone microphone even if it is switched OFF, experts reveal. *Mirror*. Retrieved June 25, 2014, from http://www.mirror.co.uk/news/technology-science/technology/spies-can-listen-your-iphone-3670347

Cavusoglu, H. (2004). Economics of IT security management. In L. J. Camp & S. Lewis (Eds.), *Economics of Information Security: Vol. 12. Advances in Information Security* (pp. 71—83). New York: Springer US.

Center for Strategic and International Studies. (2014, June). *Net losses: Estimating the global cost of cybercrime*. Retrieved June 25, 2015, from http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf

Christopher, J. (2014, February 4). EU eying NIST framework with 'great interest'. *Inside Cybersecurity*. Available at https://insidecybersecurity.com

Clark, W. K., & Levin, P. L. (2009, November/December). Securing the information highway. *Foreign Affairs*. Retrieved June 25, 2015, from https://www.foreignaffairs.com/articles/united-states/2009-11-01/securing-information-highway

Coursey, D. (2010). Study: Hacking passwords easy as 123456. *PCWorld*. Retrieved January 21, 2010, from http://www.pcworld.com/article/187354/Study_Hacking_Passwords_Easy_As_123456.html

Craig, A. N., Shackelford, S. J., & Hiller, J. S. (2015). Proactive cybersecurity: A comparative industry and regulatory analysis. *American Business Law Journal, 52*(4), 721—787.

Dilanian, K. (2010, September 14). Privacy group sues to get records about NSA-Google relationship. *Los Angeles Times*. Retrieved September 14, 2010, from http://articles.latimes.com/2010/sep/14/business/la-fi-nsa-google-20100914

DuBose, M. (2011, April 18). Electronic Interview with Michael DuBose, head of cyber investigations at Kroll Advisory Solutions and former chief of the Computer Crime & Intellectual Property Section, Criminal Division, Department of Justice, in Washington, D.C

Engleman, E., & Strohm, C. (2012, January 31). Cybersecurity disaster seen in U.S. survey citing spending gaps. *Bloomberg Business*. Retrieved January 31, 2012, from http://www.bloomberg.com/news/articles/2012-01-31/cybersecurity-disaster-seen-in-u-s- survey-citing-spending-gaps

Evers, T. (2010). Doing business and making peace. UI Occasional Papers (No. 3). Retrieved June 25, 2015, from http://www.ui.se/upl/files/48638.pdf

Fort, T. L., & Schipani, C. A. (2003). *The role of business in fostering peaceful societies*. New York: Cambridge University Press.

Fung, B. (2013, September 30). How Britain's new cyberarmy could reshape the laws of war. *The Washington Post*. Retrieved September 30, 2013, from https://www.washingtonpost.com/news/the-switch/wp/2013/09/30/how-britains-new-cyberarmy- could-reshape-the-laws-of-war/

Galtung, J. (2011). Peace, positive and negative. In D. J. Christie (Ed.), *The encyclopedia of peace psychology* (Vol. 2, pp. 758—762). Oxford: Wiley-Blackwell.

Galvin, T. (2013, March 13). Why Michelle Obama should disclose details of data theft. *USA Today*. Retrieved March 13, 2013, from http://www.usatoday.com/story/tech/2013/03/13/michelle-obama-celebrity-hack-data-theft/1984821/

Gjelten, T. (2012, May 8). Bill would have businesses foot cost of cyberwar. *NPR*. Retrieved May 8, 2012, from http://www.npr.org/2012/05/08/152219617/bill-would-have-businesses-foot-cost-of-cyber-war

Global Reporting Initiative. (2015). *Sustainability Disclosure Database*. Retrieved from http://database.globalreporting.org/

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Richardson, R. (2006). 2006 CSI/FBI computer crime and security survey. *Computer Security Institute*. Retrieved June 25, 2015, from http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf

Hardin, G. (1968). The tragedy of the commons. *Science, 162*(3859), 1243—1248.

Homeland Security News Wire. (2011, October 25). *80% of U.S. small businesses have no cyber security policies in place*. Retrieved October 25, 2011, from http://www.homelandsecuritynewswire.com/80-us-small-businesses-have-no-cyber-security-policies-place

Keohane, R. O., & Victor, D. G. (2011). The regime complex for climate change. *Perspectives on Politics, 9*(1), 7—23.

King, M. L., Jr. (1957). Non-violence and racial justice. *The Christian Century, 74*(6), 165—167.

Kupchan, C. A. (2012). *How enemies become friends*. Princeton, NJ: Princeton University Press.

Lyons, S. (2014, November 12). Typewriters are back, and we have Edward Snowden to thank. *The Washington Post*. Retrieved June 25, 2015, from https://www.washingtonpost.com/posteverything/wp/2014/11/12/typewriters-are-back-and-we-have-edward-snowden-to-thank/

Malware inserted on PC production lines, says study. (2012, September 13). *BBC News*. Retrieved September 13, 2012, from http://www.bbc.com/news/technology-19585433

Marsan, C. D. (2013, January 29). 5 years after major DNS flaw is discovered, few US companies have deployed long-term fix. *Network World*. Retrieved January 29, 2013, from http://www.networkworld.com/article/2163092/lan-wan/5-years-after-major-dns-flaw-is-discovered-few-us-companies-have-deployed-long-term-fix.html

McAfee Labs & McAfee Foundstone Professional Services. (2010). Protecting your critical assets: Lessons learned from "Operation Aurora" [White paper]. Retrieved March 1, 2010, from http://www.wired.com/images_blogs/threatlevel/2010/03/operationaurora_wp_0310_fnl.pdf

McGinnis, M. D. (1999). *Polycentricity and local public economies: Readings from the workshop in political theory and policy analysis*. Ann Arbor, MI: University of Michigan Press.

Murray, A. (2006). *The regulation of cyberspace: Control in the online environment*. Oxon, UK: Routledge-Cavendish.

Ostrom, E. (2008). *Polycentric systems as one approach for solving collective-action problems* (Ind. Univ. Workshop in Political Theory and Policy Analysis, Working Paper Series No. 08-6, 2008). Retrieved June 25, 2015, from http://dlc.dlib.indiana.edu/dlc/bitstream/handle/10535/4417/W08-6_Ostrom_DLC.pdf?sequence=1

Ostrom, E. (2010). Beyond markets and states: Polycentric governance of complex economic systems. *American Economic Review, 100*(3), 641—672.

Ostrom, E., & Nagendra, H. (2006). Insights on linking forests, trees, and people from the air, on the ground, and in the laboratory. *Proceedings of the National Academies of Sciences, USA, 103*, 19224.

Ostrom, E., Parks, R. B., & Whitaker, G. P. (1978). *Patterns of metropolitan policing*. Cambridge, MA: Ballinger Publishing Co.

Ponemon Institute, LLC. (2011, March). *Annual study: U.S. cost of a data breach*. Retrieved June 25, 2015, from https://www.fbiic.gov/public/2011/mar/2010_Annual_Study_Data_Breach.pdf

PwC. (2010). *Trial by fire: What global executives expect of information security—in the middle of the world's worst economic downturn in thirty years*. Retrieved June 25, 2015, from http://www.pwc.com/gx/en/information-security-survey/pdf/pwcsurvey2010_report.pdf

PwC. (2011, September). *Eye of the storm: Key findings from the 2012 global state of information security survey*. Retrieved June 25, 2015, from http://www.pwc.se/sv/bank-kapital/assets/2012-global-state-of-information-security-survey.pdf

Richardson, R. (2008). *CSI computer crime & security survey*. Retrieved June 25, 2015, from http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf

Shackelford, S. J. (2012). Should your firm invest in cyber risk insurance? *Business Horizons, 55*(4), 349—356.

Shackelford, S. J. (2016). *Managing cyber attacks in international law, business, and relations: In search of cyber peace*. New York: Cambridge University Press.

Shackelford, S. J., Fort, T. L., & Prenkert, J. D. (2014). How businesses can promote cyber peace. *University of Pennsylvania Journal of International Law, 36*(2), 353—431.

Shackelford, S. J., Proia, A. A., Martell, B., & Craig, A. N. (2015). Toward a global standard of cybersecurity care? Exploring the implications of the 2014 cybersecurity framework on shaping reasonable national and international cybersecurity practices. *Texas International Law, 50*(2), 305—355.

Shane, S., & Perlroth, N. (2013, September 6). Legislation seeks to bar N.S.A. tactic in encryption. *New York Times*. Retrieved September 6, 2013, from http://www.nytimes.com/2013/09/07/us/politics/legislation-seeks-to-bar-nsa-tactic-in-encryption.html?ref=technology&_r=2&

Shivakoti, G., & Ostrom, E. (2002). *Improving irrigation governance and management in Nepal*. Oakland, CA: ICS Press.

Sternstein, A. (2011, July 7). Threat of destructive coding on foreign-manufactured technology is real. *Nextgov*. Retrieved July 7, 2011, from http://www.nextgov.com/cybersecurity/2011/07/threat-of-destructive-coding-on-foreign-manufactured-technology-is-real/49363/

Stevenson, G. G. (1991). *Common property economics: A general theory and land use applications*. New York: Cambridge University Press.

Thaler, D., & Aboba, B. (2008, July). What makes for a successful protocol? *IETF*, Network Working Group, RFC 5218. Retrieved June 25, 2015, from https://tools.ietf.org/html/rfc5218

Touhill, G. J., & Touhill, C. J. (2014). *Cybersecurity for executives: A practical guide*. Hoboken, NJ: Wiley.

Tsukayama, H., & Lee, T. B. (2013, August 28). How the Syrian electronic army and other hacker groups are attacking news web sites. *The Washington Post*. Retrieved August 28, 2013, from https://www.washingtonpost.com/business/economy/how-the-syrian-electronic-army- and-other-hacker-groups-are-attacking-news-web-sites/2013/08/28/bda8f464-1032-11e3-8cdd-bcdc09410972_story.html?wpmk=MK0000200

Turk, V. (2014, February 27). Energy firms' cybersecurity is so bad they can't get insurance. *Motherboard*. Retrieved June 25, 2015, from http://motherboard.vice.com/read/energy-firms-cybersecurity-is-so-bad-they-cant-get-insurance

United States Institute of Peace. (n.d.). *Rule of Law, GLAS*. Retrieved February 10, 2014, from http://www.usip.org/ruleoflaw/index.html

Verry, J. (2014, February 25). Why the NIST cybersecurity framework isn't really voluntary. *Pivot Point Security*. Retrieved February 25, 2014, from http://www.pivotpointsecurity.com/blog/nist-cybersecurity-framework/

Weart, S. R. (1998). *Never at war: Why democracies will not fight one another*. New Haven, CT: Yale University Press.

Wegener, H. (2011). Cyber peace: A concept of cyber peace. In H. I. Touré and Permanent Montoring Panel on Information Security (Eds.), *The Quest for Cyber Peace* (pp. 77—85). Retrieved June 25, 2015, from https://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-PDF-E.pdf

The White House, Office of the Press Secretary. (2013, February 12). Executive order on improving critical infrastructure cybersecurity [Press release]. Retrieved February 12, 2013, from https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity-0

The White House, Office of the Press Secretary. (2015, February 13). Fact sheet: White House summit on cybersecurity and consumer protection [Press release]. Retrieved June 17, 2015, from https://www.whitehouse.gov/the-press-office/2015/02/13/fact-sheet-white-house-summit-cybersecurity-and-consumer-protection

Whitehouse, S. (2010, July 27). Sheldon speaks in senate on cyber threats [Web log post]. Retrieved July 27, 2010, from http://www.whitehouse.senate.gov/news/speeches/sheldon-speaks-in-senate-on-cyber-threats