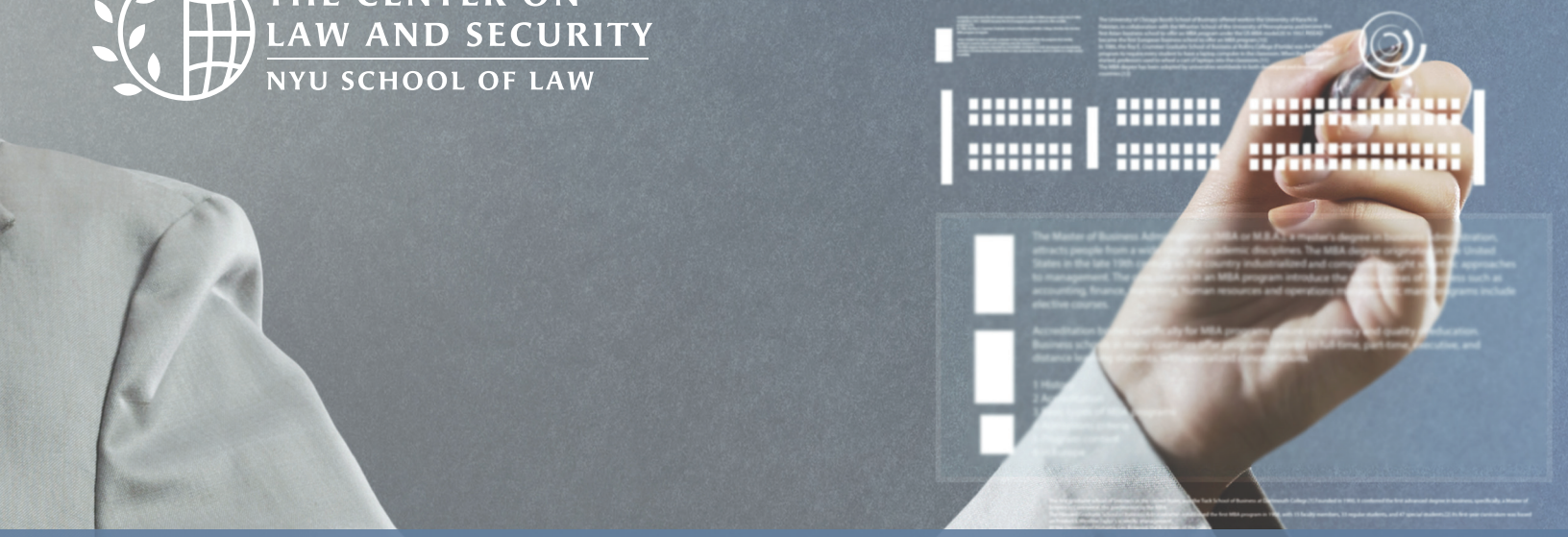
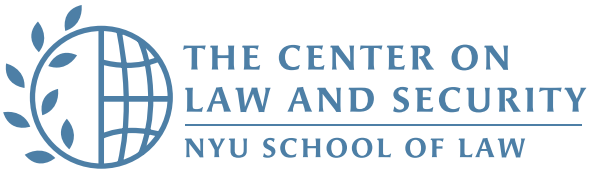
THE CENTER ON
LAW AND SECURITY
NYU SCHOOL OF LAW



From the War Room to the Board Room?

Effectively Managing Cyber Risk without Joining the Front Lines

Randal Milch and Zachary Goldman



From the War Room to the Board Room?

Effectively Managing Cyber Risk without Joining the Front Lines

Randal Milch and Zachary Goldman

June 2015

Copyright © Center on Law and Security 2015

All rights reserved. No part of the publication may be reproduced, stored in a retrieval system, translated, or transmitted in any form or by any means now or hereafter known, electronic or mechanical, without permission in writing from the copyright holder.

The Center on Law and Security
New York University School of Law
139 MacDougal Street
New York, NY 10012
212.992.8854

CLS@exchange.law.nyu.edu
www.lawandsecurity.org

Corporations seeking to manage the asymmetric cyber threat environment face a range of pressures. The current unstable legal landscape makes management's day-to-day approach to the persistent and mounting challenge all the more difficult. Companies face an increase in activity by the plaintiffs' bar and inconsistent regulatory attention by the various government agencies involved in cybersecurity. Amidst this uncertainty, however, the obligations of boards of directors in the management of corporate risks—including cyber risks—remain clear. Despite the novelty of the cyber threat, the framework laid out in the *Caremark* case and its progeny continues to provide a stable source of guidance as boards engage with the challenges of managing digital threats. Rather than mandating that board members become cybersecurity experts themselves, the well-established framework for public company governance demands that boards oversee effective processes to identify and mitigate cyber risks within a company.

I. Introduction

The series of large retail data breaches in 2014 and 2015 have focused the attention of senior corporate leaders on the ways in which companies are—or need to be—governing and mitigating their cyber risk. Boards of directors are paying greater attention because of both the reputational risks and the prospect of material litigation losses for the companies involved in significant breaches (to say nothing of the harms generated by the breaches themselves). Some board members, like Target Chairman and CEO Gregg Steinhafel, and Amy Pascal, co-Chairman of Sony Pictures Entertainment, also have stepped down in the aftermath of significant cyberattacks.

With those breaches have come shareholder-related litigation, alleging—either through a derivative action or a stock-drop case—that the company's directors and employees (and their insurers) bear liability in some respect for the breach. With the prospect of director liability comes the frequent suggestion that directors should become deeply knowledgeable about cybersecurity in order to fulfill their legal duties to their company's shareholders.

But just as evidence shows that many cyber incidents could be prevented by adhering to "basic, boring security practices,"[1] directors can and should meet their fiduciary obligations in response to cyber threats by adhering to basic governance standards. In other words, directors should work to ensure that appropriate corporate processes are in place, rather than becoming cyber-warriors themselves. It is at this point a commonplace that a high-functioning board should embrace a diversity of talents among directors and it makes sense that experience with information management and security would find its way onto a board's list of desirable backgrounds for potential new members. But there is no legal requirement—nor should there be—to develop deep board expertise in cybersecurity in order to meet the directors' obligations. Instead, a board should stick to its proper role: making a good-faith effort to undertake reasonable oversight of a firm's cybersecurity efforts, just as it does with all other material risks to the corporation.

II. The Role and Importance of the Private Sector in Cybersecurity

There are many facets of the cybersecurity challenge and some of the most vexing revolve around how private companies can most effectively manage cyber risk. The hack of Sony Pictures Entertainment in 2014 demonstrated that nation-states would target the commercial interests of private companies for coercive political purposes. The North Korean Government did so in a way that had broad applicability to a range of industries beyond entertainment by destroying significant amounts of data, releasing sensitive information (including internal emails), and threatening the outlets for Sony's products—namely the theaters that intended to show the satirical movie *The Interview*.

But the vast majority of cyberattacks are commercially motivated, may require little in terms of resources or technical sophistication, and seek credit card or other personal information that can be monetized rapidly, or intellectual property that can short-cut years of expensive research and development.[2] This dynamic exposes

[1] Verizon, 2015 Data Breach Investigations Report (2015), at 56.
[2] *Id.* at 31-34.

virtually all commercial entities to cyber risk,[3] and puts many of the world's most valuable companies squarely in the cross hairs of sophisticated hackers, some of which are backed by the resources of nation-states.[4] Moreover, private companies own most of the infrastructure over which malicious cyber activities traverse, complicating the possibilities for a coherent strategic response and limiting the role that government may take in defending American companies.

While there certainly is a role for the U.S. Government in improving cybersecurity—ranging from increased sharing of threat information to using diplomatic or criminal sanctions—the private sector is, fundamentally, on its own to manage cyber risk.

III. Diverse Pressures Shaping Corporate Responses

In this environment, with estimates of the value stolen through cyber theft at hundreds of billions of dollars each year,[5] companies face pressures from various sources as they attempt to take a strategic approach to managing the threat.

A. The Asymmetric Nature of the Cyber Threat

One of the most important strategic dynamics distinguishing the cyber threat from other sources of risk to companies is the potential for truly asymmetric threats. While many cyber threats are relatively simple (even if a good number of companies have yet to embrace the basic cyber-hygiene that will address them), even the best-resourced and most sophisticated companies find themselves consistently out-gunned. With nation-states either directly involved in, or illicitly supporting, the theft of sensitive information for commercial purposes,[6] there is not necessarily a direct relationship between resources companies devote to security and the extent to which their most important data is truly safe. No company, in other words, is immune from the threat.

This structural feature of the threat landscape, unique to cybersecurity, presents a fundamentally new challenge for companies because they are generally not accustomed to contending with determined criminal adversaries that have the resources and expertise of nation-states available to them.

This asymmetric vulnerability means that the cybersecurity threat can be managed, but not solved, and the fact that perfect security is impossible also shapes the obligations of boards. It means they should be evaluated on how well they superintend processes designed to minimize loss and mitigate the effects of loss and not on whether their company avoids a loss altogether.

B. The Government is Not The Answer

Part of the challenge facing companies that seek to manage cyber risks is the fragmented government approach to the matter. Companies cannot sit back and expect the government to meaningfully mitigate their cybersecurity shortcomings and cyber risk. To the contrary, some government agencies are focused on pursuing corporate victims in post hoc determinations that their cybersecurity practices were inadequate or that their cyber-risk disclosures were deficient or inaccurate. Other arms of the government are tasked with protecting national security and pursuing cyber criminals; helping company victims by directly defending their networks and other digital assets is not their primary mission.

Certain regulatory agencies, like the Federal Trade Commission (FTC), have focused on bringing civil suits

[3] As then-FBI Director Robert Mueller once put it, "I am convinced that there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again." Robert S. Mueller, III, Director, U.S. Fed. Bureau of Investigations, Remarks at the RSA Cyber Security Conference (Mar. 1, 2012), http://www.fbi.gov/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies.

[4] For instance, on May 19, 2014, a grand jury in the Western District of Pennsylvania indicted 5 Chinese military hackers for the theft of trade secrets from, among others, Westinghouse, U.S. Steel, and Alcoa. The alleged purpose of the cyber-espionage was to use the stolen information to assist the vicitms' Chinese competitors. Press Release, U.S. Dep't of Justice, Office of Public Affairs, U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage (May 19, 2014), http://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

[5] Ellen Nakashima & Andrea Peterson, *Report: Cybercrime and espionage costs $445 billion annually*, Wash. Post, June 9, 2014.

[6] *See* U.S. Office of the Nat'l Counterintelligence Exec., Foreign Spies Stealing US Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and industrial Espionage, 2009–2011 5 (2011), http://www.ncsc.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf.

against companies that have been the victims of a breach in an effort to incentivize them to devote more resources to cyber defense. But the FTC has done so with an uncertain mandate currently subject to litigation, and it has been roundly criticized for penalizing companies after the fact, without first publishing regulations clearly outlining its expectations for their behavior.[7] The Federal Communications Commission (FCC) also has claimed jurisdiction and is striving to catch up to the FTC[8] by announcing several multi-million dollar fines in the past year.[9] State attorneys general, too, have been active in bringing actions against companies that have been the victims of data breaches.[10] And New York State's Department of Financial Services has taken a typically forward-leaning approach to addressing the cyber vulnerabilities of banks under its jurisdiction, through potential regulation aimed at the cyber risks attendant with third party relationships, among other measures.[11]

The Securities and Exchange Commission (SEC) has required appropriate disclosures of cyber risks and material breaches for the general population of companies.[12] It has also made clear that, for investment companies and investment advisors for whom it serves as the primary substantive regulator, the corporate victim of the attack should take into account its obligations under the federal securities laws as it endeavors to prepare for, detect and respond to cyber attacks.[13] While the SEC has not yet brought enforcement actions, the potential for these proceedings remains.

Finally, the national security-related agencies also are involved in addressing the cybersecurity threat, but generally are not charged with protecting private companies. The NSA and CYBERCOM collect intelligence; work to protect military and other national security networks; conduct military and intelligence operations abroad; and, on a limited basis, share information with the private sector in the United States. The FBI, in its capacity as America's main domestic intelligence agency, participates in similar activities on our shores, while its criminal investigation division (as well as that of the Secret Service) investigates cybercrime for the purposes of prosecution. The Department of Homeland Security, meanwhile, is charged with protecting most civilian government networks and critical infrastructure. While the relevant legal authorities define critical infrastructure broadly, cooperation is generally voluntary, and the resources of DHS are limited.

No agency, then, has the protection of companies as its primary mandate, and this void is all the more apparent for companies that are not classified as critical infrastructure. At bottom, after a breach at this point government agencies can be allies, adversaries, or both.

C. Sources of Direct Liability

Companies also have been sued regularly in the aftermath of breaches. Some suits allege that victim companies, like Target, negligently failed to adopt adequate security measures exposing business partners, such as banks, to loss.[14] Other companies, including Premera Blue Cross,[15] have been sued in consumer class actions on the basis of various legal theories, including negligence.

---

[7] *See FTC v. Wyndham Worldwide Corp.*, 10 F. Supp. 3d 602 (D.N.J. 2014). For criticism of the FTC's approach *see, e.g.*, *Hacking Victims Become Federal Targets*, Wall St. J., Aug. 19, 2014, http://www.wsj.com/articles/wsj-hacking-victims-become-federal-targets-1408318038.

[8] Indeed, one apparent effect of the FCC's recently announced Open Internet rules is to oust the FTC from any jurisdiction over internet service providers. *See* Brendan Sasso, *Net Neutrality Has Sparked an Interagency Squabble Over Internet Privacy*, Nat'l J., Mar. 9, 2015, http://www.nationaljournal.com/tech/the-future-of-broadband/net-neutrality-has-sparked-an-interagency-squabble-over-internet-privacy-20150309.

[9] Malathi Nayak, *U.S. FCC imposes $25 million fine on AT&T over customer data breach*, Reuters, Apr. 8, 2015, http://www.reuters.com/article/2015/04/08/us-at-t-settlement-dataprotection-idUSKBN-0MZ1XX20150408.

[10] *See, e.g.*, *California v. Citibank, N.A.*, No. RG13693591 (Alameda Cnty. Ct. filed Aug. 29, 2013).

[11] *See* N.Y. State Dep't of Fin. Serv., Rep. on Cyber Security in the Banking Sector: Third Party Service Providers (April 2015), http://www.dfs.ny.gov/reportpub/dfs_rpt_tpvendor_042015.pdf; Letter from Benjamin M. Lawsky, Superintendent of Financial Services, N.Y. State Dep't of Fin. Serv. (Mar. 26, 2015), http://www.dfs.ny.gov/about/press2015/pr150326-ltr.pdf.

[12] Division of Corp. Fin., U.S. Sec. & Exch. Comm'n, CF Disclosure Guidance: Topic No. 2, Cybersecurity (2011), https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm. Suits alleging liability for a decline in the value of the company's stock following a cyber attack may become significant and their outcome will often hinge on the quality of disclosure.

[13] Div. of Inv. Mgmt., U.S. Sec. & Exch. Comm'n, IM Guidance Update No. 2015-02, Cybersecurity Guidance 2 (2015), http://www.sec.gov/investment/im-guidance-2015-02.pdf.

[14] *In re* Target Corp. Customer Data Security Breach Litig., No. 14-md-02522-PAM, 2014 WL 7192478 (D. Minn. Dec. 18, 2014).

[15] Elise Viebeck, *Premera Blue Cross sued over data breach*, The Hill, Mar. 27, 2015, http://thehill.com/policy/cybersecurity/237181-premera-blue-cross-sued-over-data-breach.

As case law accumulates, the standards of care to which companies must adhere will emerge. But until the legal landscape stabilizes, direct liability arising out of cyber incidents will remain an unpredictable source of risk for companies.

IV. From the War Room?

Boards, too, are starting to face liability in the form of shareholder derivative suits (most notably in the Target and Wyndham Hotels cases) focusing attention on the legal obligations of boards with respect to the management of cyber risk. It is important to note that, despite the sophistication of some threat actors, a substantial proportion of cyber harm that befalls companies derives either from lapses in established procedure, or relatively simple methods of compromise (such as phishing attacks).

In this context, it is important properly to conceptualize the role of the board of directors in managing a company's cybersecurity risk. While strategic level cyber threats to companies are relatively new, the legal framework governing how boards should interact with management to solve problems and guide companies is well-established. The real challenge comes in adapting the obligations described in the venerable *Caremark* framework to the cybersecurity challenge in a way that protects companies without fragmenting the company's approach to the problem.

The legal standard governing the duty of care of boards of directors was articulated in *In re Caremark International, Inc. Derivative Litigation*.[16] A board's obligation to manage risks of all kinds amounts to a duty to "exercise a good faith judgment that the corporation's information and reporting system is in concept and design adequate to assure the board that appropriate information will come to its attention in a timely manner as a matter of ordinary operations…"[17] There is no reason that the board's obligations would be any different in the new and evolving cyber context than in the context of other, more established risks.

Indeed, a company's failure to prevent losses, even large ones, does not mean that the board failed in its duty to "supervise or monitor corporate performance."[18] This is as true in the cyber context as in any other, and for good reason. It is a board's role to set reasonable—and even reasonably ambitious—goals for management in every material area of the business. But perfection is not the expectation in either the board's goal setting or in management's execution.[19] The peculiarities of the cyber threat reinforce the need for the forgiving boundaries of the business judgment rule: the novelty and rapid evolution of the threat make it difficult for any entity to stay ahead of the perpetrators, particularly perpetrators with the assets of a nation-state.

The board role, then, is to ensure that company management has established processes designed to understand the firm's unique vulnerabilities and has created specific procedures to reduce the likelihood that those vulnerabilities turn into losses. This includes ensuring that the management has taken reasonable and appropriate measures to:

- understand the assets that a company has at risk, its data retention policies and practices, and its sources of vulnerability, which should shape its cybersecurity strategy;
- combat the "simple" problems that often cause so much cyber harm (such as by mandating employee training and implementing fundamental security measures like two-factor authentication, encryption, and frequent password changes or more secure alternatives to passwords);
- institute defenses based on industry best practices that raise the cost of an attack, so hackers abandon the attempt and move on to less well-defended targets;
- decrease the amount of time required for detection so breaches can be stopped before they do significant harm;

[16] *In re* Caremark Intern. Inc. Derivative Litigation, 698 A.2d 959 (Del. Ch. 1996).
[17] *Id.* at 970.
[18] *Id.* at 961 ("Neither the fact that the board . . . did not accurately predict the severe consequences to the company that would ultimately follow from the deployment by the company of the strategies and practices that ultimately led to this liability, nor the scale of the liability, gives rise to an inference of breach of any duty imposed by corporation law upon the directors…")
[19] *See, e.g.*, *In re* Heartland Payment Sys., Inc. Sec. Litig., No. 09-cv-1043, 2009 WL 4798148, at *5 (D.N.J. Dec. 7 2009) ("The fact that a company has suffered a security breach does not demonstrate that the company did not 'place significant emphasis on maintaining a high level of security.'").

- evaluate means, including cyber-insurance or liability sharing contract clauses, to mitigate financial exposure when incidents occur;
- establish efficient and effective documented processes to manage incidents once breaches are detected; and
- stay abreast of the evolving legal and technical landscape to ensure a dynamic rather than static approach to cybersecurity.

While management's efforts will necessarily be technically detailed, the board's contribution need not be. As long as the board undertakes in good faith to understand the nature of cyber risk that the company faces and creates an information and reporting system to ensure management and the board are sufficiently apprised of that risk and significant breaches, "the level of detail that is appropriate for such an information system"[20] is reviewed under the "director-protective business judgment rule."[21] In fact, meeting the duty of good faith "cannot be thought to require Directors to possess detailed information about all aspects of the operation of the enterprise. Such a requirement would…be inconsistent with the scale and scope of efficient organization size in this technological age."[22]

Boards of directors, therefore, need not become cyber warriors themselves—rather, they must ensure that the corporation's cyber warriors are adequate to the task.

V. To the Board Room...

If directors should not themselves become the company's cyber experts, how should they engage with the issues in ways that meet their legal obligation to protect the strategic interests of the company? To fulfill its legal obligation to provide "reasonable oversight" of the company's cybersecurity measures, a company's board should focus on ensuring high levels of integrity in at least the following three processes:

1. Articulating the Goal

Boards must make a good faith effort to create a reasonable information and reporting system for the firm's cybersecurity efforts. The content of those efforts will vary greatly based on the industry; the position of the company in that industry; the type of data the company possesses; and a range of other factors. The board's role is to ensure that management has appropriately elevated the importance of digital security within the organization. The board should also ensure that management has created a robust system of reporting to the board with respect to the kinds of corporate assets that are vulnerable; the cyber threats to the company; and how management is prepared to handle those cybersecurity challenges. The board should also ensure that the corporation's team responsible for managing digital security is adequately structured and resourced to deal with the threat in that company's specific context.

The board need not (and, indeed, cannot) demand perfect security. But it can, and should, require management to articulate a vision of appropriate and defensible security for the corporation and to demonstrate that it has created and implemented a plan for achieving that vision.

2. Board Structure

Boards must ensure that they are adequately structured to oversee management's approach to cybersecurity threats and vulnerabilities. As a matter of routine, it makes little sense for the board as a whole to be responsible for overseeing the cybersecurity measures taken by the company; as with many complex matters, a board committee will likely be a more efficient overseer. If a committee is in charge, whether it should be a standing or separate committee will depend on the relative importance of the cyber threat compared to other threats the firm faces as well as the size of the company and its board. Standing audit or risk committees that deal with all of the material risks to the firm are sensible starting places for oversight. The responsible committee must ensure that senior management regularly reports on cybersecurity regardless of whether there are particular breaches

[20] Caremark, *supra* note 16, at 970.
[21] *Id.* at 967.
[22] *Id.* at 971 ("Generally where a claim of Directorial liability for corporate loss is predicated upon ignorance of liability creating activities within the corporation . . . only a sustained or systematic failure of the board to exercise oversight—such as an utter failure to attempt to assure a reasonable information and reporting system exits—will establish the lack of good faith that is a necessary condition to liability. Such a test of liability—lack of good faith as evidenced by sustained or systematic failure of a Director to exercise reasonable oversight—is quite high.").

or incidents to manage. These reports must include status updates on management's execution of its plan to prevent, ameliorate and respond to cyber issues. The committee should insist that the most senior responsible officers of the company (CISO, CIO and General Counsel at a minimum) are present for the periodic reports. The committee and corporate officers should then periodically apprise the full board on where the company stands regarding cyber risk and preparedness.[23]

In the event of a serious incident, a special board committee may be appointed to handle the matter and (should it become necessary) review any shareholder demands on behalf of the board. Because all companies have idiosyncratic cybersecurity concerns depending on their data assets, process-based vulnerabilities, and predictable harms, director education about cybersecurity can and should be a natural by-product of receiving reports on the firm's particular cyber issues.

3. Cyber Strategy

Once these structures are in place, what is the role of the board with respect to the contents of the company's cyber plan and strategy? In the first instance, the board must ensure that cybersecurity matters are part of the company's Enterprise Risk Management (ERM) process. The board must ensure that the cyber plan is articulated in an official corporate policy document and that it includes ways to manage cyber risks both in advance of any breaches (in a way that will decrease the likelihood of a significant incident) and once a breach or other event occurs.

The plan must also demonstrate a sophisticated understanding of the current regulatory and liability landscape as well as best practices in the relevant industry sector. Given the uncertain legal landscape previously discussed, creating the right cybersecurity structure for both pre-incident protection and post-incident response may be the best way to lower the regulatory and litigation risks to the company.

[23] The Wyndham shareholder derivative action is instructive on this point. *See Palkon v. Holmes* No. 2:14-cv-01234 (SRC), 2014 WL 5341880 (D.N.J. Oct 20, 2014). Although the action was dismissed because the board was found to have adequately investigated and rejected the underlying claims, the court remarked that, in light of *Caremark*'s "utter failure" standard (see *supra* note 22), because "security measures existed when the first breach occurred" and the Wyndham "Board addressed such concerns numerous times," the weakness of the underlying claims was "noteworthy." *Id.* at note 1.

VI. Conclusion

Risks emanating from cyber space pose a significant threat to some of the most economically important companies in the United States. Firms are struggling to manage an asymmetric conflict, in which the technical, financial, and intelligence resources of nation-states are arrayed against those of individual companies. Boards of Directors must, of course, be engaged in the subject. But their role is generally to ensure that management is focused, resourced, and aligned with the board's objectives in order to execute the cyber mission well. How this task is executed in practice can be immensely complicated and is constantly evolving, but the general principles are well-established. Cybersecurity concerns are migrating from the war room to the board room and the board should—by design—oversee the battle from behind the front lines.

Acknowledgments

The authors wish to thank Sarvenaz Bakhtiar, Raj De, Judi Germano, and Meg Henry for their comments and assistance on this paper.

Randal Milch '85 is a distinguished fellow at the Center on Law and Security and a member of the Center's Board of Advisers. Randy was most recently executive vice president and strategic policy adviser to Verizon's chairman and CEO. He served as the company's general counsel from 2008 to 2014, and head of public policy from 2012 to 2014. Before 2008, Milch was general counsel of several business divisions within Verizon. Earlier in his career, Milch was a partner in the Washington, D.C. office of Donovan Leisure Newton & Irvine. He clerked for Clement F. Haynsworth Jr., chief judge emeritus of the Court of Appeals for the Fourth Circuit.

Zachary Goldman '09 is the Executive Director of the Center on Law and Security, where leads the Center's programs on cybersecurity, intelligence oversight, and financial sanctions, among others. Before joining the Center, Goldman was a special assistant to the Chairman of the Joint Chiefs of Staff at the U.S. Department of Defense, a policy advisor in the Treasury Department's Office of Terrorism and Financial Intelligence, and an attorney with Sullivan & Cromwell LLP. Goldman is a Term Member of the Council on Foreign Relations, and has published widely on national security strategy, financial sanctions, counterterrorism, cybersecurity, and U.S. foreign policy. He is co-editor, with Samuel Rascoff of *Intelligence Oversight: A Global View*, forthcoming from Oxford University Press.

The Center on Law and Security (CLS) is a non-partisan multidisciplinary research institute at NYU School of Law focused on promoting informed dialogue and conducting groundbreaking research on the most important national security, legal, and strategic questions of the post-9/11 era. The Center is focused on national security law issues, including cybersecurity; intelligence oversight; comparative national security law; and the relationship between national security law and national security strategy.