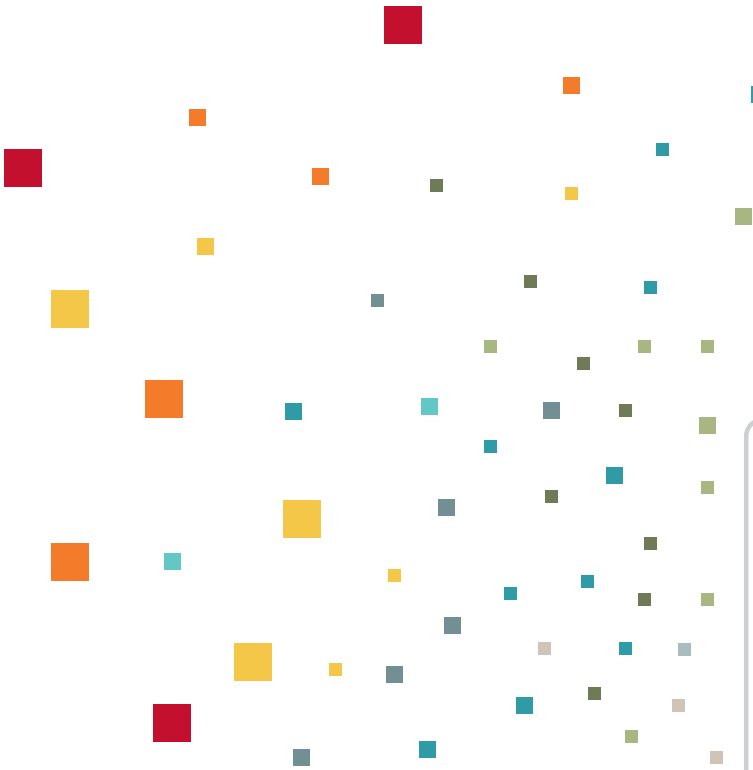
HOW CAN BOARDS AVOID CYBERSECURITY PAIN? A LEGAL PERSPECTIVE

PERRY E. WALLACE
PROFESSOR OF LAW AND DIRECTOR
JD/MBA DUAL DEGREE PROGRAM
WASHINGTON COLLEGE OF LAW
AMERICAN UNIVERSITY

RICHARD J. SCHROTH, PH.D
EXECUTIVE IN RESIDENCE AND EXECUTIVE DIRECTOR
KOGOD CYBERSECURITY GOVERNANCE CENTER
KOGOD SCHOOL OF BUSINESS
AMERICAN UNIVERSITY

WILLIAM H. DELONE, PH.D
KOGOD EMINENT PROFESSOR OF INFORMATION TECHNOLOGY AND EXECUTIVE DIRECTOR
KOGOD CYBERSECURITY GOVERNANCE CENTER
KOGOD SCHOOL OF BUSINESS
AMERICAN UNIVERSITY



AMERICAN UNIVERSITY
KOGOD SCHOOL OF BUSINESS
CYBERSECURITY GOVERNANCE CENTER
WHITE PAPER NO. 1 (EDITION 1)

ABOUT THE AUTHORS

Perry E. Wallace

Professor Perry E. Wallace received his undergraduate degree in electrical engineering and engineering mathematics from the Vanderbilt University School of Engineering. He received his law degree from Columbia University, where he was awarded the Charles Evans Hughes Fellowship. He is a tenured Professor of Law at the Washington College of Law of the American University, where he teaches corporate, environmental and international law.

Professor Wallace was for several years a senior trial attorney at the U.S. Department of Justice, handling cases involving environmental and natural resources law. He has also served as a securities and commercial arbitrator. Professor Wallace has served on numerous boards, commissions and councils over the years, including the U.S. Environmental Protection Agency's National Advisory Council for Environmental Policy and Technology, the Environmental Working Group and the Academic Council of the Institute for Transnational Arbitration.

Richard J. Schroth, Ph.D.

Dr. Richard Schroth is a trusted private advisor and thought leader to business around the globe. He is Executive Director of The Kogod Cybersecurity Governance Center at American University and an Executive in Residence. Honored as one of the Top 25 Consultants in the World by *Consulting Magazine* and his peers, Richard is the Managing Director of the Newport Board Group's Global Technology Strategy, Innovation and Cyber Practice and the Axon Global Cyber Alliance, where he actively leads world-class teams of cyber professionals and board level advisors seeking to minimize the serious nature of cyber risk.

Dr. Schroth is energetically engaged in the cutting-edge of global private sector cyber initiatives including areas of M&A cyber diligence, board policies for cyber risk and advanced cyber business strategy. He is a private confidant to Fortune 500 boards, executives, private equity firms, national professional associations and Economic and Trade Consular Offices. Richard is a full board member of the National Association of Corporate Directors, an NACD Board Leadership Fellow and member of the NACD Board Advisory Services where he leads strategy sessions with Boards on cyber and related risk issues around the world.

Former Senior United States Fulbright Scholar, Dr. Schroth was nominated as a Fellow in the American Academy of Arts and Sciences for his distinguished career and contributions as a thought leader in business, technology, and Cyber-Counter Intelligence. Dr. Richard Schroth received his Doctorate from Indiana University, a M.S. from the University of Illinois, post-bachelors work at Texas A&M and holds a B.S. from Western Illinois University. Dr. Schroth has been honored as The Distinguished Alumnus of all the universities where he has graduated.

William H. DeLone, Ph.D

William DeLone is an Eminent Professor of Information Technology at the Kogod School of Business at American University and Executive Director of the Kogod Cybersecurity Governance Center. Professor DeLone earned a B.S. in mathematics from Villanova University; an M.S. in industrial administration from Carnegie-Mellon University; and a Ph.D. in Computers and Information Systems from the University of California, Los Angeles. His dissertation studied the successful use of computers and information systems by small businesses. He has served as Acting Dean, Senior Associate Dean, and Chair of the Department of Information Technology. He also served as Chair of American University's Strategic Planning Steering Committee.

Professor DeLone's primary areas of research include the assessment of information systems' effectiveness, risk and value, e-government and public value and the management of global software development. Professor DeLone has published in the top information systems journals and lectured and consulted on information systems at universities in London, Paris, Rome, Venice, Warsaw, Galway, Singapore, Kuwait, Leipzig & Saarbrucken in Germany, and Guatemala.

ACKNOWLEDGEMENTS

The Kogod Cybersecurity Center would like to recognize our sponsor FINRA, whose financial support made this report possible.

The authors would like to acknowledge the contributions of Israel Martinez, National Practice Partner of the Newport Board Group's Cyber Practice and CEO of Axon Global along with Patrick Von Bargen, co-founder of 38 North Solutions, who reviewed and commented on earlier versions of the report.

Introduction

The relentless acceleration and changing complexity of cybercrime against corporations rank among the greatest corporate governance challenges of our times. Our aim in this executive report is to encourage corporate boards to devise, implement, and strengthen proper and effective corporate cybersecurity governance strategies.

To this end, we present the relevant legal concepts, principles and issues in this area, ultimately identifying concrete best practices, standards and guidelines in establishing and maintaining a high quality cybersecurity governance strategy. We focus this report on the law and legal principles because they loom large in cybersecurity governance and there is a scarcity of consolidated information where board members can find an independent and assembled overview of the legal landscape.

Why is Cybersecurity Governance Important?

Public awareness and concern about cybercrime and other cyber threats are growing daily, as a result of numerous high-profile data security breaches at large retail companies, banks, and the federal government. Moreover, concerns that these problems reflect a rapidly expanding trend have been expertly verified in numerous professional reports and studies, including the well-known Verizon Risk Team's annual *Data Breach Investigations Report*.[i]

Other prominent studies merit attention. For example, in the Ponemon Institute's *2015 Cost of Data Breach Study*[ii] (the Ponemon Report), researchers found that, in the case of U.S. companies, "[t]he average cost for each lost or stolen record containing sensitive and confidential information increased from $201[the previous year] to $217. The total average cost paid by organizations increased from $5.9 million [the previous year] to $6.5 million."[iii] Further, the Ponemon Report reached the following critical conclusions:

- Data breach costs are at an all-time high;
- The total average organizational cost of data breach has increased in 2015;
- Malicious or criminal attacks continue to be the primary causes of data breach;
- Malicious attacks are most costly;
- The more churn (loss of existing customers) experienced by an organization, the higher the per capita cost of data breach;
- Detection and escalation costs are at record highs;
- Notification costs increased slightly;
- Post data breach costs have increased; and
- Lost business costs grew.[iv]

Against this general background, it is no surprise that corporate leaders are concerned about this problem. In a 2014 survey of nearly 500 company directors and general counsel, "data security" was the top area of governance that "keeps [directors] up at night," and it was the second most important area for in-house counsel, after regulatory compliance.[v]

Cybersecurity Governance: What's at Stake?

The National Association of Corporate Directors (NACD) has identified several areas of vulnerability for businesses in terms of asset loss:

- Business plans, including merger or acquisition strategies and bid information;
- Trading algorithms;
- Contracts with customers, suppliers, distributors, and joint venture partners
- Employee log-in credentials;
- Information about company facilities, including plant and equipment designs, maps, and future plans;
- Product designs;
- Information about key business processes;
- Source codes;
- Lists of employees, customers, contractors, and suppliers; and
- Client data.[vi]

Intellectual property impairment or loss as a result of cyber incidents deserves special mention. Perhaps the most emphatic and insightful expression of its importance comes from the website of the U. S. Department of Justice's Computer Crime and Intellectual Property Section (CCIPS):

> CCIPS's enforcement responsibilities against intellectual property crimes are … multi-faceted. Intellectual Property (IP) has become one of the principal U.S. economic engines, and the nation is a target of choice for thieves of material protected by copyright, trademark, or trade-secret designation.
>
> The fact that a major federal law enforcement agency places such a high value and priority on protecting the intellectual property of U.S. companies speaks volumes about the key position of these special assets in the economy.[vii]

A final concern that directors and officers must take into account in managing a corporation is "regulatory risk." This concept has been defined as follows:

> The risk that a change in laws and regulations will materially impact a security, business, sector or market. A change in laws or regulations made by the government or a regulatory body can increase the costs of operating a business, reduce the attractiveness of investment and/or change the competitive landscape.[viii]

The present period is one in which the regulatory risk involving cybersecurity must be characterized as "high." Cybersecurity breaches can cause catastrophic harm to individuals, organizations, and society itself. **Nevertheless, there is no comprehensive regulatory scheme in place to address this threat. The current patchwork of "piecemeal" measures is inadequate.** ***Simply stated, this is a time for the exercise of vision by corporate directors and other leaders.***

Government Enforcement Actions; Applicable Laws

Below we highlight the subjects, legal grounds, and strategies employed by governmental agencies to address the growing cybersecurity threat. *We also highlight strategies that companies can adopt to prevent and respond to government scrutiny.*

Federal Trade Commission (FTC)

Using one or more of its legal authorities, *the FTC has vigorously pursued a number of investigations and enforcement actions under three categories: (1) big data, (2) mobile technologies, and (3) securing sensitive data.*

A recent decision by the Third U.S. Circuit Court of Appeals has confirmed that, in the event of cybersecurity intrusion, the FTC has the authority to investigate a company and file charges against it for failure to protect customers from theft of their data. The FTC may have jurisdiction over claims that firewalls were insufficient, that cybersecurity software was antiquated, and that proper data security procedures were not implemented or followed. Apart from suffering reputational damage, a FTC claim can subject a company to expensive fines. There is also a heightened risk that FTC claims will encourage class action and shareholder lawsuits.

Securities and Exchange Commission (SEC)

The SEC has been interested in cybersecurity governance for a number of years, but *it has substantially increased its compliance and enforcement activities in keeping with the vastly increased need for such a regulatory enhancement.*

For example, according to recent news reports, the SEC is investigating an extensive program of cyber-related financial fraud, based on research conducted by FireEye, Inc., a cybersecurity firm. [ix] To the extent the news reports are true, such an enforcement initiative may be an indication of the agency's future direction and the ever-widening scope of its cyber-related activities.

It is safe to assume that the agency's efforts in this area will be *intensified and expanded*. This was underscored by SEC Chair Mary Jo White at a March 26, 2014 "Cybersecurity Roundtable," where she stated that "[t]his is a global threat. Cyber threats are of extraordinary and long-term seriousness."[x]

FINRA

The Financial Industry Regulatory Authority, Inc. (FINRA) *is a private, non-governmental corporation that assists the SEC in regulating member brokerage firms and exchange markets*. FINRA is classified as a self-regulatory organization (SRO), and the SEC is the government agency with ultimate regulatory authority over it. *Thus, it is not a government agency, but it is a regulator.*

FINRA encourages firms to take a "risk management-based approach" to cybersecurity. The following formulation of the term "risk management" was developed by the National Institute of Standards and Technology (NIST):

> Risk management is the process of identifying, assessing, and responding to risk. Particularly within critical infrastructure, organizations should understand the likelihood that a risk event will occur and the resulting impact. With this information, organizations determine the acceptable level of risk for IT and digital assets and systems, expressed as their risk tolerance.
>
> With an understanding of risk tolerance, organizations can prioritize systems that require attention. This will enable organizations to optimize cybersecurity expenditures. Furthermore, the implementation of risk management programs offers organizations the ability to quantify and communicate changes to organizational cybersecurity. Risk is also a common language that can be communicated to internal and external stakeholders.[xi]

Against this background of investigation, evaluation and assessment, FINRA has proceeded with significant enforcement activities.

U.S. Department of Justice

The "Computer Crime and Intellectual Property Section" (CCIPS) of the U. S. Department of Justice (DOJ) Criminal Division is responsible for implementing the Department's national strategies in combating computer and intellectual property crimes worldwide. The Justice Department also issued a set of "Best Practices for Victim Response and Reporting of Cyber Incidents."[xii]

State Laws and State Attorneys General

At the state level, government officials have enacted laws and undertaken enforcement actions to address cyber threats. Unfortunately, there is no uniformity among these laws and initiatives. Therefore, this legal "patchwork" is a "moving target" that directors should monitor carefully. In this regard, the National Conference of State Legislatures' comment on the status of *active state security breach laws* is directly on point:

> Forty-seven states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring private or government entities to notify individuals of security breaches of information involving personally identifiable information.
>
> Security breach laws typically have provisions regarding who must comply with the law (e.g., businesses, data/ information brokers, government entities, etc.); definitions of "personal information" (e.g., name combined with SSN, driver's license or state ID, account numbers, etc.); what constitutes a breach (e.g., unauthorized acquisition of data); requirements for notice (e.g., timing or method of notice, who must be notified); and exemptions (e.g., for encrypted information).[xiii]

One potential enforcement matter that illustrates how major cases evolve concerns an

investigation by certain state attorneys general of the financial firm J. P. Morgan Chase. As one reviews the various laws and enforcement activities at the state level, it is clear that the state law "patchwork" of activities is obviously beneficial—especially where efforts are vigorous—but *the larger national picture of cybersecurity enforcement is not uniform at present*.

The above section paints a picture of increasing regulation and litigation by federal and state agencies and should be a matter of increasing concern and attention of corporate executives and boards.

Risk Area: Private Litigation

First, it is crucial to note that *many private lawsuits are commenced after a government agency has charged a company with a cybersecurity violation—especially if the government eventually wins, but even if there is merely a settlement. Why? One reason is that where the government has chosen to go forward with charges, there is at least an implicit assumption that there has been a thorough preliminary investigation by an expert agency, in which substantial incriminating evidence has been uncovered. The impact of such government action can be not only psychological, but also reputational and even legal*.

Second, note that where external parties, such as consumers or other contracting parties, sue the corporation for injuries allegedly inflicted, they often "raise the stakes" greatly by bringing the suit as a "class action." This means that although only a few persons may actually initiate the lawsuit, its ultimate plaintiffs are both those "named" persons and also "all others similarly situated" who may have been harmed by the governance failure. *Obviously, in the event of a victory, the monetary damages recovered by the plaintiffs from the corporation must be sufficient to compensate the entire class, which can be catastrophic for some companies. Finally, when shareholders sue, the lawsuit is often against the directors and officers for failure to live up to their duties and causing injury to the "corporation and shareholders as a whole." These lawsuits, known as "shareholder derivative suits," are initiated by the shareholders but brought on behalf of the corporation, and any relief awarded would go to the corporation.*

It is important to note that private companies whose corporate financing strategies include the use of private equity or venture capital firms should expect to meet high-level standards in their organization and operations. Today, *this applies increasingly to cybersecurity governance policies and practices*.

In an era of increasingly stringent cybersecurity consciousness, as well as government enforcement and private litigation, any private company—and any such company's directors and managers—must be prepared to adopt high cybersecurity governance standards. Similarly, private equity and venture capital firms must do the same.

Given the pervasive role of law, regulation and litigation in the cybersecurity area, it should come as no surprise that *the role of legal counsel is critical to companies faced with cyber threats and other cybersecurity challenges*.

Legal Duties and Liabilities for Cybersecurity Governance Imposed Directly on the Board of Directors and Officers

Certain corporate law concepts govern *standards of conduct and liability* for officers and directors. We apply these concepts to cybersecurity governance. In corporate law, the fiduciary duty concept derives from the basic legal obligation of directors to "manage and direct the business and affairs of the corporation." The concept also applies to officers and anyone else who is delegated authority by the board of directors. It gives a simple command to all these fiduciaries:

> Carry out your assigned duties *properly, in the corporation's and the shareholders' best interests*, and if you do not do so, you may be sued by either the shareholders or a corporate representative and held *personally liable* for economic injuries that come to the corporation or the shareholders because of that failure of duty.

In fact, there are several fiduciary duties that guide the conduct of directors and officers, but *the most pertinent ones for cybersecurity governance analysis are the fiduciary duty of care (FDC) and the fiduciary duty of oversight or monitoring (FDOM). Essentially, these duties mean what they say in plain English, and while they would appear to set fairly strict, high standards, in reality they only require minimum good conduct*. Only the most egregious conduct will cause liability. Nonetheless, they are important because, when liability is assigned, it is often of considerable quantum in the monetary sense. Further, *even where directors and officers win a lawsuit using defenses such as the business judgment rule (BJR), there may be serious reputational damage, employee morale problems and other challenges that reduce sales and hurt the company's position in the competitive markets*.

Director/Officer liability may also arise based on the plain language of a statute or rule. Section 11 of the Securities Act of 1933 is an example. Section 11 makes directors expressly liable for misrepresentations or omissions of "material" facts in registered public offerings. Again, we have here yet another instance in which a corporate governance process was of such great overall significance to the American economy and society that Congress deemed it necessary to require an especially high level of quality in director performance through the device of express individual duties and liabilities.

Legal Duties and Liabilities for Cybersecurity Governance Imposed Directly on the Corporation

Here we focus on instances of legal liability imposed directly on the business entity, such as the corporation itself. *We emphasize that the corporation is a "separate legal entity" – that it alone is the business. In these situations,, when there are violations of law, the business is legally liable, not the directors and officers (who enjoy "limited liability")*. On the other hand, *there are two well-known exceptions to this limited liability that can render directors, officers and others liable along with the corporation for the violation in question:*

- **Direct or Active Participation**, in which a director or officer directly or actively participates in a violation of law (including by way of supervision) and is thus held individually liable along with the corporation; and
- **"Piercing the Corporate Veil,"** in which a court grants a plaintiff's request that the usual protection of limited liability (the corporate "veil" of protection) be ignored or set aside and that individual directors, officers or shareholders be held liable along with the corporation. This is a rarely granted remedy, but it may be imposed when the corporate protections are abused and there has been a "basic injustice" done to a party outside the corporation. (It does not apply to injuries to shareholders).

The fundamental point of this section is that *directors and officers should never simply assume that they will enjoy the protections of limited liability automatically and inevitably*. Understanding these exceptions is crucial to their body of knowledge and comprehension about serving successfully and effectively as directors and officers of a corporation.

Guidelines & Best Practices

Over the years, "best practices" standards and guidelines for cybersecurity governance have been issued by various organizations. The most widely recognized and adopted guidelines are those published in the National Institute of Standards and Technology (NIST) Voluntary Framework. Other organizations that have published useful guidelines are the American Bar Association (ABA) Initiatives, U.S. Department of Homeland Security, FINRA, U.S. Department of Justice, and National Association of Corporate Directors (NACD). NACD has developed five principles for corporate directors:

1. Directors need to understand and approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue;
2. Directors should understand the legal implications of cyber risks as they relate to their company's specific circumstances;
3. Boards should have adequate access to cybersecurity expertise, and discussions about cyber-risk management should be given regular and adequate time on the board meeting agenda;
4. Directors should set the expectation that management will establish an enterprise-wide cyber-risk management framework with adequate staffing and budget; and
5. Board-management discussion of cyber risk should include identification of which risks to avoid, accept, mitigate, or transfer through insurance, as well as specific plans associated with each approach.[xiv]

This executive report, a summary of our more comprehensive legal Research Paper, has attempted to provide, from a legal perspective, some guidance that will assist boards of directors in carrying out their mandate to "manage and direct the business and affairs" of the corporation (and their officers and legal counsel as well), as regards cybersecurity matters, in a manner that is both productive for the corporation and shareholders and protective for the directors.

The Conclusion of the legal Research Paper ends with the following observation: **Good cybersecurity governance is no longer an "option." It is now a mandate.**

Finally, we caution that this publication does not purport to be, nor should it be taken as, actual, specific legal advice or counsel. Readers are urged to consult with their own legal counsel when dealing with particular legal issues that might arise in the conduct of their business operations or that they may identify after reviewing this report.

For more information visit **www.kogod.american.edu/cybergov**.

To contact the Center, email cybergov@american.edu or phone William DeLone at 202-885-1959.

[i] See, e.g. "2014 Data Breach Investigations Report," Verizon Risk Team, available at https://dti.delaware.gov/pdfs/rp_Verizon-DBIR-2014_en_xg.pdf.

[ii] "2015 Cost of Data Breach Study: United States," p.1-, Ponemon Institute Research Report, May 2015, available at http://public.dhe.ibm.com/common/ssi/ecm/se/en/sew03055usen/SEW03055USEN.PDF.

[iii] Id.

[iv] Id. at 1-3.

[v] See, "The Emergence of Cybersecurity Law," p. 4, February 2015, Indiana University Maurer School of Law/Hanover Research, available at http://info.law.indiana.edu/faculty-publications/The-Emergence-of-Cybersecurity-Law.pdf.

[vi] "Cyber-Risk Oversight," Director's Handbook Series, 2014, NACD, page 6.

[vii] "About the Computer Crime and Intellectual Property Section," U. S. Department of Justice, Criminal Division, available at http://www.justice.gov/criminal-ccips.

[viii] "Regulatory Risk," Investopedia, available at http://www.investopedia.com/terms/r/regulatory_risk.asp

[ix] Sarah N. Lynch and Joseph Lynn, "SEC hunts hackers who stole emails to trade corporate stocks," Jun 23, 2015, Reuters, available at http://www.reuters.com/article/2015/06/23/us-hackers-insidertrading-idUSKBN0P31M720150623.

[x] Mary Jo White, "Opening Statement at SEC Roundtable on Cybersecurity," March 26, 2014, Securities and Exchange Commission, available at http://www.sec.gov/News/PublicStmt/Detail/PublicStmt/1370541286468.

[xi] "Improving Critical Infrastructure Cybersecurity, Executive Order 13636, Preliminary Cybersecurity Framework," National Institute of Standards and Technology (NIST), available at http://www.nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf.

[xii] "Best Practices for Victim Response and Reporting of Cyber Incidents" U.S. Department of Justice, April, 2015, available at http://www.justice.gov/sites/default/files/criminalccips/legacy/2015/04/30/04272015reporting-cyber-incidents-final.pdf

[xiii] National Conference of State Legislators, available at http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

[xiv] Id. at 3.