Strengthened Director Duties of Care for Cybersecurity Oversight: Evolving Expectations of Existing Legal Doctrine

Brad Lunn[1]

It is difficult to identify when an existing order will change, and when the combined effects of multiple, seemingly independent forces will collude to bring about something new. We are reminded of this when a disruptive technology enters a new field. Existing practices give way to new realities and a return to the comfortable "old" way seems unimaginable. While corporate law practitioners have become comfortable with the substantial discretion provided directors under Delaware's interpretations of director duties and the business-judgment rule, a transformation of expectations concerning director oversight of cybersecurity and associated director liability is

[1] Brad Lunn is an executive in a leading Aerospace & Defense firm, and a founding member of the Defense Security Information Exchange (DSIE). An experienced board member, he served on a national governing body of the US Olympic Committee and was Audit Chair. He completed Harvard's flagship program on Corporate Governance and is chief executive of a non-profit organization focused on cyber-security oversight. Special thanks for the helpful advice of Professor Lynne Dallas of USD Law School. All errors are the author's alone.

currently underway. To date, board oversight of cybersecurity has been less than effective. The National Association of Corporate Directors' ("NACD") 2012 conference featured a presentation that described an "IT confidence gap" and noted most directors between age 60 and 65 spend a majority of their professional lives in the pre-digital era. The NACD presentation also disclosed that less than 1% of Fortune 500 directors have been or are currently chief information officers (CIO's) and that IT is highly technical and difficult for most directors to understand.[2] Moving forward, corporate directors are well advised to anticipate that emerging technology forces and corporate law precedent will pressure courts and regulators to require directors to oversee cybersecurity with vigilance similar to that expected of legal compliance professionals. In this new era, increased cybersecurity-oversight duties and director liability are certain to lead to dramatic and important changes in corporate law. Their time will come—the question is when and by what means.

I. The Importance of Cybersecurity to Corporations

Corporate law will evolve to respond to the threat of cyber-breaches. To see why, one only has to look at current events with cyber intrusions. Perhaps most notably, Target Corporation (NYSE:

[2] *Cybersecurity and the Board*, October 15, 2012, National Association of Corporate Directors, *available at* http://www.nacdonline.org (last visited Feb. 25, 2014).

TGT) suffered a massive data breach beginning in November of 2013, resulting in the loss of an estimated 70 million customer records including credit card information and emails. The event was followed by declines in revenue, falling stock prices, layoffs, moral problems and the replacement of the CEO.[3] The publicity of this event was widespread and persistent. Home Depot (NYSE: HD) also allowed customer data to be lost in September 2014 and in a company press release[4] noted the financial gross costs of about $62 Million covering the investigation, customer credit monitoring and legal expenses, although the additional damage to reputation and impact to the brand are difficult to calculate. An October 2014 cyber breach at JPMorgan Chase that is noted to affect 76 million households[5] highlights that that even financial firms who were long thought to be safe are in fact vulnerable to cyber crime. The Federal Reserve and the Department of Energy suffered cybersecurity breaches resulting in thousands of records being lost.[6] Similarly, Adobe

[3] Meagan Clark, *Timeline of Target's Data Breach and Aftermath How Cybertheft Snowballed For The Giant Retailer*, International Business Times, May 5, 2014, *available at* http://www.ibtimes.com, (last visited Oct. 18, 2014).

[4] Home Depot, The Home Depot Completes Malware Elimination and Enhanced Encryption of Payment Data in all U.S. Stores, Sept. 18, 2014, https://corporate.homedepot.com/.../Press%20Release.

[5] Jessica Silver-Greenberg, *JPMorgan Chase Hacking Affects 76 Million Households*, N.Y. TIMES, Oct. 2, 2014, *available at* http://dealbook.nytimes.com.

[6] Robert Lemos, *Federal Reserve, DOE Confirm Hackers Breached Servers, Stole Data*, EWEEK, Feb. 2, 2013, *available at*

Systems recently announced that approximately 2.9 million customer records containing credit card information were accessed forcing the company to reset all passwords.[7]

While consumer retail, financial and government entities suffer highly public cyber-breaches, other industry groups are not immune. Cybersecurity breaches can impact customers and suppliers, and cause intellectual property loss, identity theft, fraudulent transactions, damage to infrastructure (including electric utilities, water treatment, sewage treatment, industrial system control and even military readiness), and loss of classified and militarily sensitive information. Many companies are reluctant to disclose cyber-security incidents because doing so may impact their reputations, foster criticism, and increase liability for meeting increased threats.

II. Cyber Crime is Different

Cybercriminals can engage in behavior ranging from teenager nuisance hacking, creating annoying computer viruses, criminal extortion, and political hacking to government-sponsored espionage and all out cyber warfare. Those behind these acts are commonly intelligent, creative and

---

http://www.eweek.com/security/federal-reserve-doe-confirm-hackers-breached-servers-stole-data/ (last visited Feb. 25, 2014).

[7] *Adobe warns 2.9 million customers of data breach after cyber-attack*, THE GUARDIAN, Oct. 3, 2013, *available at* http://www.theguardian.com/technology/2013/oct/03/adobe-hacking-data-breach-cyber-attack (last visited Feb. 25, 2014).

persistent, so defenses must evolve. A cybercriminal, however, could transfer all funds out of a corporate bank account, access and steal corporate intellectual property, access confidential client records, steal and use customer credit card and banking files, alter corporate accounting records, access and adjust medical files, change grades, open flood gates at a dam, turn off municipal water pumps, or worse. While it's unlikely a common criminal could enter a building and take millions of customer records, a cybercriminal can leverage speed–of-light tools to their advantage, and hide for years in a cloak of distant unnamed servers in multiple jurisdictions, and erase a decade of brand building overnight. The very fact that these crimes occur regularly[8] and often involve enormous economic value makes it reasonable for corporate directors to pay close attention. Said another way, it might be challenging to assert that a reasonably informed board is unaware of today's substantial cybersecurity issues affecting organizations of all kinds.

III. A Complex Legal and Regulatory Environment

The legal profession is now recognizing that cyber threats are widespread and serious. The American Bar Association published its first handbook on cybersecurity in 2013. It states, "according to PriceWaterhouseCoopers, hacking

[8] The ABA Cybersecurity Handbook: A Resource for Attorneys, Law Firms, and Business Professionals 201-06 (Rhodes & Polley eds., 2013).

has become so prevalent that major organizations should assume that their systems have been compromised and proceed from that assumption in testing and improving their defenses."[9] While it is difficult to imagine that informed business professionals are not aware that cybersecurity events occur regularly, it is not difficult to appreciate that directors will find it difficult to monitor cyber-security risks, since they are not familiar with this difficult-to-understand subject. Difficulty, however, does not mean competent monitoring is not required. Just as financial controls were not universally understood by directors pre-Sarbanes Oxley and Enron, that lack of a firm grasp of financial controls did not mean oversight was not required, but rather that the oversight lacked adequate attention and expertise, which was later addressed through regulation and litigation.

Similarly, many important regulatory entities are now focused on cybersecurity. The Securities and Exchange Commission ("SEC") and the Federal Trade Commission ("FTC") have weighed in on cybersecurity regulation. Public companies are subject to certain mandatory disclosure requirements set forth in the Securities Act of 1933 and the Securities Exchange Act of 1934 and in regulations promulgated under such acts.[10] The Securities and Exchange Commission recently issued a bulletin providing guidance and

[9] *Id.* at 173.
[10] 17 C.F.R. §240. 10b-5.

clarifying operating risks that include cyber risks.[11] Under SEC requirements, newly described "disclosure controls" applying to both financial and nonfinancial information require Form 8-K to be filed with the SEC within two business days of an event's occurrence. The new requirement puts management on clear notice that events potentially having a material effect on the business or operations must be disclosed quickly. "These new rules, and proposed SEC rules accelerating reporting deadlines for filing required reports, place a new burden on reporting companies to develop and adopt adequate disclosure controls and procedures. The SEC expects each issuer to develop a process that is consistent with its business and internal management and supervisory practices. Thus, every reporting company should formalize and document the disclosure controls and procedures that it adopts as well as the methodology for evaluating those controls and procedures."[12] Given that computer systems are either central to a company's operating model, such as Amazon or eBay, or a substantial support system, such as banks or manufacturers, such systems can be both

[11] *Regulation Systems Compliance and Integrity*, Securities and Exchange Commission, Mar. 7, 2013, 17 CFR Parts 242 and 249, Release No. 34-69077, *available at* https://www.sec.gov/rules/proposed/2013/34-69077.pdf (last visited Feb. 25, 2014).

[12] James E. O'Connor, *Data Security & Privacy Law*, §10:4 , WestlawNext, Database updated June 2013.

financial and nonfinancial. Computer-system risks must be disclosed.[13]

The regulatory environment beyond the SEC has grown to include the FTC's oversight of identity theft, and its notable concept of "red flags." A recent law journal notes "One example of the regulatory landscape governing IT risk is the Federal Trade Commission's 'Red Flags Rule' requiring certain companies to implement an identity theft program. Under the rule, financial institutions subject to FTC oversight and all companies—both private and public—that extend credit to their customers must have a written plan in place to detect and respond to identity theft. The plan must identify the red flags inherent to a particular company's operations, such as scenarios in which there is risk for exposure of sensitive customer information or in which there are indicators that customer data may have already been breached."[14] Identity theft is only one of many

[13] *Id*. The actual text states "Any risk factors that would materially affect those computer system also will have a material effect on the business and operations of these companies. Based on the importance of computer systems to most businesses, companies are required to disclose the risks associated with installing, operating, maintaining and replacing or upgrading these systems, at least to the extent that these risks are unique in certain respects to the specific company or could have a materially adverse effect on the company's business. The risks to these computer systems include cybersecurity, and events related to its failure to protect such systems from internal and external threats. This disclosure obligation, coupled with the risks themselves, compel companies to do their best to limit such associated risks, both to systems they own directly and systems that a service provider may own or operate."

[14] Lawrence J. Trautman & Kara Altenbaumer-Price, *The Board's Responsibility for Information Technology Governance*, 28 J. MARSHALL J. COMPUTER & INFO. L. 313, 336 (2011).

different cybersecurity issues. The line between "required oversight" and simply good practice is increasingly uncertain.

A large firm operating in multiple jurisdictions faces more legal considerations in overseeing its cybersecurity. The American Bar Association notes numerous federal and state statutes and regulations relating to cybersecurity.[15] The federal statutes and regulations include the Electronic Signatures in Global and National Commerce Act, Federal Trade Commission Act, Gramm-Leach-Bliley Act, HIPPA, Homeland Security Act of 2002, and six others. States have many other requirements. The author identified 140 rules addressing obligations to provide security for credit card information, data disposal/destruction, the duty to encrypt personal information, security breach notification, SSN laws, and SSN policies. The legal landscape is complex indeed—heightening the importance of appropriate compliance.

IV. Negligence Theory and Cybersecurity

Negligence theory requires an analysis comparing duty to actual behavior deemed to breach the required level of care in the circumstances. A dated but famous case, *The T. J. Hooper*[16], set in the early 1930's, involved the

[15] The ABA Cybersecurity Handbook: A Resource for Attorneys, Law Firms, and Business Professionals 201-06 (Rhodes & Polley eds., 2013).
[16] *The T. J. Hooper*, 60 F.2d 737 (2d Cir. 1932).

sinking of a coal ship at sea. In *Hooper* the ship was not equipped with a recently developed technical innovation, namely radio systems that would have allowed the ship to know of an approaching storm and then simply maneuver to safe waters in advance of the approaching danger. The equipment was available and relatively inexpensive, yet it was not a universal or commonly implanted as standard equipment in those days. The operator of the ship argued that there was no standard in the industry that mandated such use of radios and that there was no common practice for the same. The judge in his opinion wrote "Courts must in the end say what is required; there are precautions so imperative that even their universal disregard will not excuse their omission."[17] While cybersecurity was not the subject of the *Hooper* case, the logic the court used has strong parallels to cyber oversight, in which dangers and technologies are evolving rapidly. Courts and regulators will not likely overlook these analogous situations.

V. Negligence Theory and Foundational Corporate Law

The Third Restatement of Torts notes that the "Primary factors to consider in ascertaining whether the person's conduct lacks reasonable care are the foreseeable likelihood that the person's conduct will result in harm, the foreseeable severity of any harm that may ensue, and the burden of

[17] *Id.*

precautions to eliminate or reduce the risk of harm."[18] With respect to corporate law, the questions to ask include:

1) What exactly are the duties of a director?

2) What is expected of them under the law?

The Model Business Corporations Act ("MBCA"), which has been adopted by many states in some version, defines a standard of conduct for directors that requires them to act in good faith, act in the reasonable interests of the corporation, and become informed with respect to their oversight role. It also requires due care.[19] Corporate law looks to reasonable processes, not outcomes per se.[20] What is "reasonable" is a question of corporate law

[18] Restatement (Third) of Torts, Liability for Physical Harm §3 (P.F.D No 1, 2005), *available at* www.law.cornell.edu/wex/negligence (last visited Aug. 28, 2013).

[19] Model Business Corporations Act (MBCA), § 8.30, *available at* http://users.wfu.edu/palmitar/ICBCorporations-Companion/Conexus/ModelBusinessCorporations Act.pdf (last visited Feb. 25, 2014). The specific language states "(A) Each member of the board of directors, when discharging the duties of a director, shall act: (1) in good faith, and (2) in a manner the director reasonably believes to be in the best interests of the corporation. (B) The members of the board of directors or a committee of the board, when becoming informed in connection with their decision-making function or devoting attention to their oversight function, shall discharge their duties with the care that a person in a like position would reasonably believe appropriate under similar circumstances."

[20] *Id.* In the official notes at 110 "Section 8 30 sets forth the standards of conduct for directors by focusing on the manner in which directors perform their duties, not the correctness of the decisions made." In essence, the courts do not, as a rule, endeavor to hold a director accountable for bad outcomes, but rather a to reasonable process that went into making a reasonable decision under the circumstances at the time of the decision.

that accounts for the circumstances the board faces. The MBCA's official notes explain, "The phrase 'reasonably believes' is both subjective and objective in character. Its first level of analysis is geared to what the particular director, acting in good faith, actually believes—not what objective analysis would lead another director (in a like position and acting in similar circumstances) to conclude. The second level of analysis is focused specifically on 'reasonably.' While a director has wide discretion in marshaling the evidence and reaching conclusions, whether a director's belief is reasonable (i.e., could—not would—a reasonable person in a like position and acting in similar circumstances have arrived at that belief) ultimately involves an overview that is objective in character." [21] Boards and individual corporate directors are not expected to make perfect decisions, but rather to act reasonably under the circumstances. Corporate law refers to these duties as the duty of care and duty of good faith. The courts have also fashioned the "business judgment rule" ("BJR"), which is a presumption insulating directors from liability if they exercise good faith in the exercise of their judgment when just judgments turn out, in hindsight, to be harmful to the corporation.[22] "Delaware's default standard of review is the business judgment rule. The rule presumes that in making a business decision the directors of a corporation acted on an informed

[21] *Id.* at 112.
[22] *Potter v. Pohlad*, 560 N.W.2d 389, 392 (Minn. Ct. App. 1997).

basis, in good faith and in the honest belief that the action taken was in the best interests of the company. This standard of review reflects and promotes the role of the board of directors as the proper body to manage the business and affairs of the corporation. Unless one of its elements is rebutted, the court merely looks to see whether the business decision made was rational in the sense of being one logical approach to advancing the corporation's objectives. Only when a decision lacks any rationally conceivable basis will a court infer bad faith and a breach of duty."[23] A party claiming damages against a board of directors' decision must rebut presumption that board's business judgment was an informed one.[24] Determination of whether a board of directors' business decisions is informed "turns on whether the directors have informed themselves, 'prior to making business decision, of all material information reasonably available to them.'"[25] This important holding demonstrates an affirmative duty to become informed. Furthermore, the court goes on to say, "Under the business judgment rule there is no protection for directors who have made unintelligent or unadvised judgment. A director's duty to inform himself in preparation for a decision derives from the fiduciary capacity in which he

[23] *In re Trados Inc. Shareholder Litigation*, 73A.3d 17 (Del. Ch. Aug. 16, 2013).
[24] *Smith v. Van Gorkom*, 488 A.2d 858 (Del. Supr. 1985).
[25] *Id.* at 872.

serves the corporation and its stockholders."[26] This is powerful language.

A case called *Caremark*[27] introduced the concept of "red flags" to director oversight. In *Caremark* the defendant company had a history of legal-compliance issues and faced derivative litigation plaintiffs believed breached director duty. The court noted that the "Board of directors may not satisfy obligations to monitor corporation's activities, which was part of its duty to be reasonably informed regarding corporation's affairs, without members assuring themselves that information and reporting systems exist in the organization that are reasonably designed to provide to senior management and to the board itself timely, accurate information sufficient to allow management and the board, each within its scope, to reach informed judgments concerning both the corporation's compliance with law and its business performance."[28]

---

[26] *Id.* at 872.

[27] *In Re Caremark Intern. Inc. Deriv. Lit.,* 698 A.2d 959 (Del.Ch.1996).

[28] *Id.* at 960, §10. The court also gave substantial insight into its reasoning that reflects upon the notions of court oversight of business decisions and the emphasis on process versus outcomes. It said "a director's duty of care can never appropriately be judicially determined by reference to the content of the board decision that leads to a corporate loss, apart from consideration of the good faith or rationality of the process employed. That is, whether a judge or jury considering the matter after the fact, believes a decision substantively wrong, or degrees of wrong extending through "stupid" to "egregious" or "irrational", provides no ground for director liability, so long as the court determines that the process employed was either rational or employed in a good faith effort to advance corporate interests. To employ a different rule-one that permitted and "objective" evaluation of the decision' world expose directors to substantive second guessing by ill-equipped judges or juries, which would, in the long-run, be injurious to investor interests."

So while *Caremark* introduces the concept of "red flags," legal doctrine evolves from what could be called a "director passive" model, which allows directors to wait until red flags clearly appear, to what might be termed a "director active" model, which requires that an information-gathering system be used to discover problems requiring board attention. *Stone v. Ritter*, an important case embodying this concept, was tried and appealed in Delaware in 2006. The *Stone* court held that "… Caremark articulates the necessary conditions predicate for director oversight liability: (a) the directors utterly failed to implement any reporting or information system or controls; *or* (b) having implemented such a system or controls, consciously failed to monitor or oversee its operations thus disabling themselves from being informed of risks or problems requiring their attention. In either case, imposition of liability requires a showing that the directors knew that they were not discharging their fiduciary obligations. Where directors fail to act in the face of a known duty to act, thereby demonstrating a conscious disregard for their responsibilities, they breach their duty of loyalty by failing to discharge that fiduciary obligation in good faith." [29] Additionally, and for clarity on this crucial point of law, Justice Holland opined "In this appeal, the plaintiffs acknowledge that the directors neither "knew nor should have known that violations of law were occurring," i.e., that there were no "red flags"

[29] *Stone ex rel. AmSouth Bancorporation v. Ritter*, 911 A.2d 363, 365 (Del. 2006).

before the directors. Nevertheless, the plaintiffs argue that the court of chancery erred by dismissing the derivative complaint which alleged that "the defendants utterly failed to implement any sort of statutorily required monitoring reporting or information controls that would have enabled them to learn of problems requiring their attention."[30] The opinion reiterated that, for directors, good faith and the duty to be informed are linked. "In the absence of red flags, good faith in the context of oversight must be measured by the directors' actions 'to assure a reasonable information and reporting system exists' and not by second-guessing after the occurrence of employee conduct that results in an unintended adverse outcome."[31] Corporate directors need to note the critical requirement that requires their active engagement as a condition of fulfilling their legally mandated duties.

As a practical matter, it is important to distinguish between a breach of the duty of care and the duty of loyalty or good faith. The liability for director breach of the duty of care can be limited in the articles of incorporation, but no such exculpation is possible for a breach of the duty of loyalty or good faith.[32] A finding that directors breached their duty of loyalty or good faith can have a direct impact on director liability.

---

[30] Palmiter and Partnoy, Corporations 607 (2010).
[31] *Stone ex rel. AmSouth Bancorporation v. Ritter*, 911 A.2d 971 (Del. 2006).
[32] Jeffrey D. Bauman, *Delaware General Corporation Law* 352 (2011).

Systematic disregard of important information by act or omission is not insulated in certain situations. "The widely cited *Caremark* decision analyzed the circumstances in which directors might be held personally liable for failures to exercise sufficient oversight over corporate affairs. That decision articulated a standard of liability keyed to whether the plaintiff demonstrates '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 exists.'" [33] Such rulings suggest that a board cannot wait for a red flag, and that it has an affirmative obligation to be well informed. While a director is entitled to rely on management reports, if such reports are inconsistent with what a reasonable director knows to be true, directors are not entitled to rely on reports they reasonably suspect are inaccurate. The concept of boards using a reasonable "information or monitoring system" supports the basics of corporate governance, specifically directors' duty to be well informed, particularly on factors that in and of themselves should grab reasonable directors' attention. Corporate legal doctrine requiring directors to have an information system allowing them to gather needed information aligns to negligence theory in terms of reasonable foreseeability; thus, the governance and negligence doctrines fit together

[33] Gorris, Hamermesh et al., *Delaware Corporate Law and the Model Business Corporations Act A study in symbiosis*, Widener Law School Legal Studies Research Paper Series no. 11-15, March 25, 2011 SSRN.

naturally. The business-judgment rule noted earlier provides protection for corporate directors who exercise their duties in good faith—if they act on an informed basis. To overcome the BJR presumption, a successful plaintiff must prove defendants' actions were grossly negligent. Gross negligence in the corporate context requires showing "reckless indifference" or "deliberate disregard,"[34] which may include acts and omissions caused in part by not having a reasonable system to inform directors of important information, which we know includes cybersecurity matters.

In another early warning of changes to come, the successful corporate law firm of Wachtell, Lipton, Rosen and Katz ("WLRK"), which has vigorously defended corporate clients for years commonly arguing against activist-oriented corporate governance agendas and practices, supports the notion that the board should "… determine the company's risk appetite (financial, safety, reputation, etc.), set state-of-the-art standards for managing risk and monitor the management of those risks,"[35] and to "set state-of-the-art standards for compliance with legal and regulatory requirements, monitor compliance and respond appropriately to "red flags."[36] Notably, WLRK also foresaw the possibility of boards being held to an expanded standard of care. "To date our

[34] O'Connor, *supra* note 12.
[35] Memorandum, *The future of Corporate Governance and the Board of Directors*, Nov. 17, 2010, Wachtell, Lipton, Rosen & Katz.
[36] *Id.* at 2

courts, even in cases involving multi-billion-dollar losses by financial institutions, have continued to adhere to the customary Caremark-case standard for determining whether directors have met their duties of care. Earlier this year, however, the European Commission, in a consultation paper seeking comments on options to improve corporate governance in financial institutions, suggested strengthening 'legal liability of directors via an expanded duty of care.' And the possibility that higher standards of care could eventually be imposed not only on directors of financial institutions, but on directors of all corporations, is real. Specialized committees, use of expert consultants, tutorials and expanded director education programs will go a long way to enable boards to meet even a strengthened duty of care."[37]

The legal parallels between the *Caremark* and *Stone v. Ritter* precedents and expansion of regulatory controls into the cybersecurity realm are well aligned. While boards and directors are not expected to be cybersecurity experts, they are expected to oversee firm imperatives similar to financial controls, legal compliance, and other matters. In this modern era, cybersecurity issues faced by any organization are reasonably foreseeable. Directors are required to make decisions on a well-informed basis and to have an appropriate information system on which to base

[37] *Id*. at 3

decisions and judgments. Recall that boards cannot wait until red flags emerge; the existence of red flags indicates that oversight is needed—having been detected in some fashion they are no longer simply a reasonably foreseeable risk exposure.

VI. Cybersecurity Red Flags

So, what is a cybersecurity red flag? Examples include a pattern of penetrations or similar cyber events, a stated or known targeting of the firm, and perhaps even the possession of certain "cyber assets" of such value that it is reasonable to presume they will be actively targeted. The combinations are almost endless.

A. Hypothetical Scenario

Let's place ourselves in a situation of our own design. You are a director for ABC Company and are on the audit committee. ABC is a successful public company. The board has not received a briefing on cybersecurity as a part of its oversight, nor is cybersecurity discussed in the busy agenda. Cybersecurity is not on the annual board agenda. The CEO advised the board that outsiders accessed the company's network and early indications suggest information was stolen. He also noted that it seems like the same group that has accessed the system the last three times over two years but nothing was stolen in those events. You were not previously aware of these "other" incursions. What are the governance issues here? (Ignore for a

moment the issues that result from the fact that these cyber events and related risks were not disclosed in company filings, as you were unaware of them.)

Did the board act reasonably in discharging its duties? Did the board exercise appropriate oversight, or become adequately informed on these matters? Was the event reasonably foreseeable? Did the fact that the CEO thought the same group was involved in penetrations previously over a period of time give a reasonable person reasonable doubt that the systems were still secure? What if the CIO believed the company would be penetrated again unless certain actions were taken, but such actions were not implemented? How does this affect the situation? How does the value of what was stolen enter the equation? Would your opinion change if you learned that the information stolen affected 10 million people likely to suffer issues of identity theft and financial losses for years? What if the information stolen provided key insights into how banks protect their communications and transactions globally, or it was sensitive military data giving adversaries an advantage in battlefield conflicts for the next two decades? Let's say the cyber issues immediately preceded a substantial stock price reduction and are threatening future revenues?

The answers, and thus oversight, are complicated and circumstance driven. What is

reasonable depends on the circumstances, so it is not sufficient to assume there is a "one size fits all" cyber-oversight approach. Clearly the value of what's being protected or the impact of its loss has a role in deciding what is reasonable under the circumstances.

A few questions the board's counsel will likely ask: what was the board's duty to oversee cybersecurity, and what evidence exists that oversight was performed reasonably? Is it reasonable that the board did not have cyber oversight on the agenda given a history of intrusions and the presence of valuable cyber-assets? Would a reasonable board inquire about cybersecurity in these circumstances, and if so, how would a sufficient inquiry be accomplished?

B. Reasonable Cyber Oversight

The question directors should ask is "what should we do under the circumstances?" What will it take to fulfill the directors' duties of care, loyalty and duty to act on an informed basis? How does a board avoid creating systematic, sustained or otherwise negligent acts or omissions in how it performs oversight? Recall that courts focus on the process used by the board to reach a decision, rather than the decision or outcome itself. For the company's directors to avoid liability, a court will need to find that the board used a rational process, that the decisions were made on a well-informed basis, and that decisions were an outcome of that

reasonable process under the circumstances faced by the firm and its board. Boards and management should not assume this is simple. Risk management in general is difficult and cyber risk management is foreign to many directors. A Harvard Business Review article notes, "Risk management focuses on the negative-threats and failures rather than opportunities and successes. It runs exactly counter to the "can do" culture most leadership teams try to foster…"[38] The same "can do" enthusiasms can lay the seeds to say "that can't happen to us" until it does.

Since courts tend to balance noninterference in corporate management with providing reasonable boundaries for acceptable behavior, the law has developed "tests" over time that provide the basis for decision making[39] without being excessively prescriptive. The author has not found any test courts have applied to date for cyber oversight; however, it is reasonable to expect such tests to emerge. The challenge is that threats evolve constantly, and what is sufficient oversight at one time may quickly become obsolete. The author suggests that the following five factors be considered when evaluating appropriate cyber oversight by the board:

---

[38] Robert S. Kaplan & Annette Mikes, *Managing Risks A New Framework,* Harvard Bus. Rev. 13, Jun. 2012, *available at* http://www.hbr.org.

[39] Cybersecurity issues are commonly broken down into matters concerning loss of confidentiality, loss of data integrity, or the loss of system availability.

1. **Systematic Board Oversight Process:** Does the company employ a state of the art risk management process that is highly responsive, anticipates events, seeks independent views, is appropriately trained in cybersecurity, and has access to appropriate staff and advisors.

2. **Probability of Loss:** How likely is a loss? Consider previous penetrations or events and new or emerging threats and mitigating defenses. An objective and independent opinion is generally preferable.

3. **Value of Loss:** What is the potential consequence of each loss, and the total of all losses combined. What are the cyber assets and which are most valuable? Consider immediate and downstream consequences, including difficult-to-quantify, reputational, goodwill, supplier, shareholder, and customer impacts.

4. **Existence of Ultra-High-Value Consequences ("UHVC"):** Are there some cyber risks that, even with low probability of occurrence, if they occur could threaten life, corporate existence, grave danger to national interests, or portend similar outcomes the impact of which is utterly unacceptable.

5. **Burden:** How difficult is it to become informed of the cyber-risks and relevant facts, and employ processes, procedures, people and technology to

oversee and mitigate risks, even if such mitigation is imperfect?

If the loss probability multiplied by the loss-event value exceeds the burden (mitigation costs), such mitigations should be implemented. The greater the gap, the more important the matter should be to the company. The existence of some ultra-high-value risks warrants special consideration on a case-by-case basis, since some losses cannot be permitted (withstood) under almost any situation. Special care must be afforded to these special cases. Given that the burden of basic director education and oversight is relatively low, it is difficult to assert that such investments are not reasonable if high-value losses are possible.

C. Recommendations

How many cyber red flags are too many? Can a board wait until red flags emerge before liability attaches? At what point is a line crossed that escalates facts from "unpredictable event" to "basic negligence" to "lack of good faith"? The existence of cyber red flags is not, in itself, an indication of director liability or ineffective oversight, but rather paints an emerging picture of the challenges facing the board; how the board discharges that challenge, or its failure to do so, creates the breach to which personal liability may attach. It depends on the circumstances, but these simple factors will provide directors, regulators and

courts a framework in which to consider the trade-space.

In the face of these cyber-security challenges, what factors might mitigate director liability? Is the absence of well-considered efforts to oversee cybersecurity itself a red flag? Recommended cyber-oversight activities and actions include:

i. Have a clear, written board charter for cybersecurity oversight noting responsibilities and scope. The charter is similar to a well-considered Audit Committee charter or in some cases is an element in the Audit Committee charter. Is a specialized committee warranted?
ii. Corporate Policies & Processes covering the many elements of cybersecurity.
iii. The implementation of a director education program on cybersecurity.
iv. The recruitment of directors with cybersecurity skills, knowledge and abilities consistent with the threats the company faces.
v. The use of outside advisors with specialized skills.
vi. Attainment of appropriate security or technical certifications by key staff, overseen by the board and top management.
vii. The existence of employee communication and training programs appropriate for threats the company faces.
viii. Regular, systematic board engagement in cyber oversight, similar to internal audit consideration of policy, practices, reporting,

and resource sufficiency as the result of a systematic risk management process.

ix. Appropriate documentation of the above and a systematic methodology for continuous improvement.

VII. Conclusion

Corporate law will evolve to hold corporate directors more accountable for cybersecurity oversight. Serious cybersecurity threats are a common and growing risk to corporate value, and breaches or failures to protect these computer systems and their data can have grave consequences to a firm's future. Directors have duties of care and loyalty, and the obligation to act on a well-informed basis on important issues impacting corporate affairs. Regulations mandating everything from disclosure of risks to quick disclosure of negative events, to specific technical requirements for system/data security are growing, and this is well known to reasonably well-informed directors.

If a board is found to have systematically ignored such cybersecurity red flags, or utterly failed to design an information system to ensure that the board is well informed with respect to cybersecurity, and if such failure is a contributing cause of corporate loss, the author believes that a reasonable court would find director breach of the duty of care and loyalty, to which director liability would attach. The point is that directors are

expected to be aware and proactive in their oversight, and not idle until cyber disaster strikes.

The good news is that boards can take proactive steps to improve their oversight and thus reduce liabilities without imposing an unreasonable burden on their already demanding role. Discussion at the board level of cyber-security and related risks, the development and use of appropriate metrics, and policies at all levels and the use of appropriate experts in a manner that is similar to what they are familiar with in their oversight of financial controls is a good start. While directors are not expected to be cyber-risk or technology experts, they are fully expected to appropriately oversee important corporate affairs on an informed basis, and in this modern era, it certainly includes cybersecurity for almost all organizations.[40]

[40] This article is not legal advice. Engage appropriate legal council.