THE JOHN MARSHALL JOURNAL OF COMPUTER & INFORMATION LAW

Volume XXVIII Number 3

An International Law Journal on Information Technology

a publication of

The Center for Information Technology and Privacy Law of The John Marshall Law School

THE BOARD'S RESPONSIBILITY FOR INFORMATION TECHNOLOGY GOVERNANCE

LAWRENCE J. TRAUTMAN & KARA ALTENBAUMER-PRICE

Reprinted from
The John Marshall Journal of Computer & Info. Law
Volume XXVIII Number 3 Spring 2011
© 2011 The John Marshall Law School

SPRING 2011

ARTICLES

THE BOARD'S RESPONSIBILITY FOR INFORMATION TECHNOLOGY GOVERNANCE

LAWRENCE J. TRAUTMAN*
KARA ALTENBAUMER-PRICE**

I. OVERVIEW

First comes the fall; then comes the fallout. With accusations that boards of directors of financial institutions were asleep at the wheel while their companies engaged in risky behavior that erased millions of dollars of shareholder value and plunged the country into recession, increasing pressure is now being placed on public company boards to shoulder the burden of risk oversight for the companies they serve. One needs look no further than the passage of the Dodd-Frank Wall Street Reform and Consumer Protection Act and its corporate governance reform efforts for evidence of this sea change.

Few operational areas of every corporation present as much inherent risk or prove as difficult to govern as Information Technology ("IT"). A reasonable question voiced from many boardrooms is: "How can I be expected to govern something I know so little about?"[1] However, recent

* JD, Oklahoma City Univ. School of Law; MBA, The George Washington University; post-graduate studies (Management Information Systems) University of Texas at Dallas; BA, The American University. Mr. Trautman is a past president of the Dallas Internet Society and the New York and Metropolitan Washington/Baltimore Chapters of the National Association of Corporate Directors. He may be reached at www.LJTrautman.com.

** JD, summa cum laude, Texas Tech University School of Law; Bachelor of Journalism, cum laude, The University of Texas at Austin. Ms. Altenbaumer-Price is Director of Complex Claims & Consulting for USI, the largest privately held broker of commercial insurance in the United States. Kara works in USI's Management & Professional Services group, where she consults with USI's director & officer insurance and other management liability clients on issues related to corporate governance, private securities litigation, and regulatory securities enforcement. She may be reached at kara.altenbaumer-price@usi.biz.

1. Peter Weill and Jeanne W. Ross depict Information Technology as one of the "six key assets for any enterprise" (the others being human, physical, financial, intellectual

years have brought a growing realization that not knowing is not an excuse. As more responsibility is placed on boards to oversee all areas of risk that their companies face, there is a critical need to provide effective governance over information technology, along with the necessary leadership from the top, organizational structures, and processes that ensure that IT efficiently sustains and extends the corporate strategies and objectives.

All too often the reality of IT performance and enterprise risk exposure are attributable to IT conflicts with boardroom expectations. Common examples of undesired IT results include:

> business losses, reputational damage and a weakened competitive position; inability to obtain or measure a return from IT investments; failure of IT initiatives to bring the innovation and benefits they promised; technology that is inadequate or even obsolete; inability to leverage available new technologies; and deadlines that are not met and budgets that are overrun.[2]

Here, the body of knowledge encompassing the effective governance of IT is too vast to allow for comprehensive coverage. However, this article provides an overview of some of the main considerations relative to every director's duty to govern IT risk. In particular, this comment will address directors' roles in the risk oversight of the corporations they serve, their role in governance of IT, their role in mitigating IT risks, and ways in which that risk can be transferred to or shared with others. A discussion of these topics will hopefully foster a deeper and productive discussion within boardrooms.

II. IT GOVERNANCE DEFINED

The IT Governance Institute in its Executive Summary and Framework for *Control Objectives for Information and Related Technology 4.1* (COBIT®) provides the following definition: "IT governance is the responsibility of executives and the board of directors, and consists of the leadership, organizational structures and processes that ensure that the enterprise's IT sustains and extends the organization's strategies and

---

property and relationships). *See generally* PETER WEILL & JEANNE W. ROSS, IT GOVERNANCE: HOW TOP PERFORMERS MANAGE IT DECISIONS RIGHTS FOR SUPERIOR RESULTS 6 (2004). Peter Weill, Director of the Center for Information Systems Research ("CISR") and Senior Research Scientist at the Massachusetts Institute of Technology's Sloan School of Management led research during 2001-2003, which studied 256 enterprises in Europe, Asia Pacific and the Americas. During the same general time period parallel studies were conducted by Jeanne Ross and Cynthia Beath (University of Texas).

2. IT GOVERNANCE INST., BOARD BRIEFING ON IT GOVERNANCE 8 (2d ed. 2003), *available at* http://www.isaca.org/Knowledge-Center/Research/Documents/BoardBriefing/26904_Board_Briefing_final.pdf.

objectives."[3] Moreover, COBIT 4.1 contends that:

> IT governance integrates and institutionalizes good practices to ensure that the enterprise's IT supports the business objectives. IT governance enables the enterprise to take full advantage of its information, thereby maximizing benefits, capitalizing on opportunities and gaining competitive advantage. These outcomes require a framework for control over IT that fits with and supports the Committee of Sponsoring Organizations of the Treadway Commission's (COSO's) Internal Control—Integrated Framework, the widely accepted control framework for enterprise governance and risk management, and similar compliant frameworks.[4]

The Corporate and Key Asset Governance Framework presented below depicts a linking of IT and corporate governance.[5] The top of the diagram describes relationships of the board. As agents of the board, the senior executive team (located in the top center area) conducts strategies and performs desirable behaviors to achieve board mandates. Weill and Ross state: "we see strategy as a set of choices:[6] (1) Who are the targeted customers? (2) What are the product and service offerings? (3) What is the unique and valuable position targeted by the firm? (4) What core processes embody the firm's unique market position?"[7] Desirable behaviors embody the beliefs and culture of the organization as defined and enacted through not only strategy but also corporate value statements, mission statements, business principles, rituals, and structures."[8]

While different in every enterprise, Weill and Ross contend that "it is the desirable behaviors, not strategies that create value."[9] The six key assets through which all enterprises accomplish their strategies and create business value are found in the lower half of the table above. Each of these asset groups requires senior management to develop mechanisms to govern their use and management: (1) human assets; (2) financial assets; (3) physical assets; (4) intellectual property assets; (5) information and IT assets; and (6) relationship assets.[10]

III. BOARD'S RESPONSIBILITY FOR IT RISK

Risk management is no longer the exclusive province of the C-suite. A 2009 KPMG study reported that in a survey of audit executives and board members, fifty-eight percent believed that their corporate employ-

3. IT GOVERNANCE INST., COBIT®4.1, EXECUTIVE SUMMARY FRAMEWORK 5 (2007), *available at* http://www.isaca.org/Knowledge-Center/cobit/Documents/COBIT4.pdf.

4. IT GOVERNANCE INST., COBIT®4.1, *supra* note 3, at 5.

5. *See generally* PETER WEILL & JEANNE W. ROSS, *supra* note 1, at 5.

6. PETER WEILL & JEANNE W. ROSS, *supra* note 1, at 5 (citing Constantinos C. Markides, *In Search of Strategy,* 40 MIT Sloan Mgt. Rev. No. 3 6-7 (Spring 1999)).

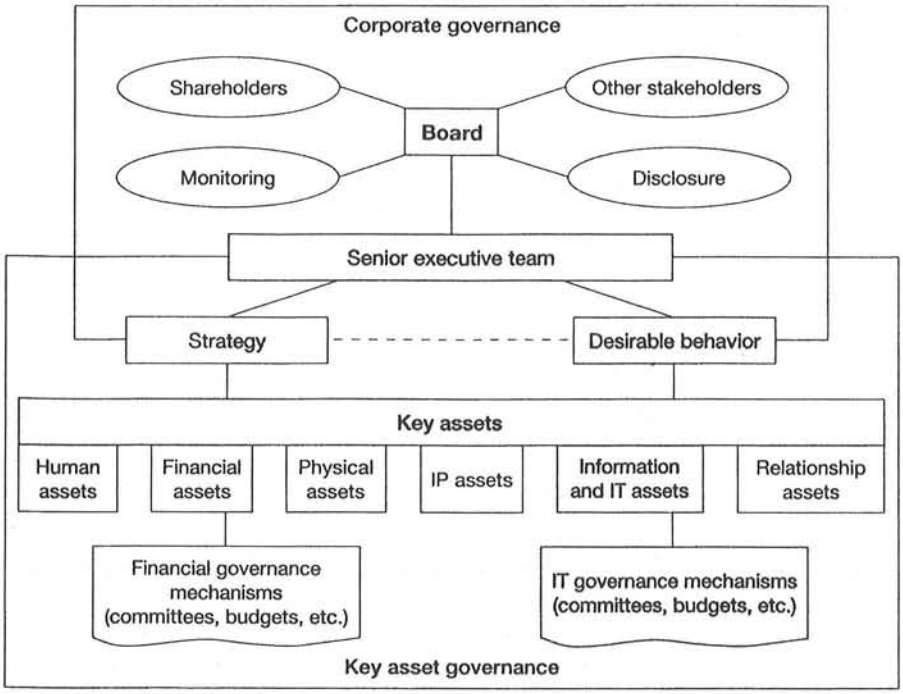
7. *See generally* PETER WEILL & JEANNE W. ROSS, *supra* note 1, at 6.

8. *See generally Id.*

9. *Id.*

10. *Id.*

Corporate and Key Asset Governance



☐ IT governance.

© 2003 MIT Sloan School Center for Information Systems Research (CISR). Used with permission.

ees had little to no understanding of how to assess risk.[11] It is even worse when it comes to IT risk; ninety-eight percent of respondents in a recent Carnegie Mellon Cylab survey of Fortune 1000 directors and executives indicated their boards are not "actively addressing" IT operations and vendor management.[12] These are dangerous statistics for companies operating in a corporate governance landscape where the Securities and Exchange Commission (SEC) believes "risk oversight is a key competence of the board."[13] Additionally, as one U.S. senator put it, "[B]oards will never again be able to say they did not understand the risks that the

11. *Many Enterprise Risk Management Programs Lack Fundamentals, According to KPMG's Survey of Internal Auditors and Boards*, Insurancenewsnet (Jan. 20, 2009), http://insurancenewsnet.com/article.aspx?a=top_lh&neID=200901201680.2_02300059c02b0d35.

12. JODY WESTBY, CYLAB, GOVERNANCE OF ENTERPRISE SECURITY: CYLAB 2010 REPORT 3 (2010), *available at* http://www.govinfosecurity.com/external/boards-report.pdf.

13. SEC Proxy Disclosure Enhancements, 17 C.F.R. §§ 229, 239, 240, 249, 274 (2009), *available at* http://sec.gov/rules/final/2009/33-9089.pdf.

firms they oversee were taking."[14] New regulations that move corporate risk oversight from the exclusive domain of the C-suite and place it in the boardroom have moved (e.g. Dodd-Frank) or are moving forward on multiple fronts, from Congress to the SEC. IT risk is no different from any other business risk under such a regime.

Regulators on Risk Oversight

The SEC on Risk Generally

New SEC rules went into effect on February 28, 2010 amending Item 407 of Regulation S-K to require disclosure about the board's role in a company's risk oversight process and its leadership structure.[15] According to the SEC's final rule release, the new disclosure rules require "companies. . .to describe how the board administers its risk oversight function, such as through the whole board, or through a separate risk committee or the audit committee, for example."[16] Disclosures should address, for example, "whether the individuals who supervise the day-to-day risk management responsibilities report directly to the board as a whole or to a board committee or how the board or committee otherwise receives information from such individuals."[17] Such disclosures should also include an explanation of the board's leadership structure and the "reasons why the company believes that this board leadership structure is the most appropriate structure for the company."[18] In companies in which the CEO and Chairman are the same individual, rule "amendments will require disclosure of whether and why the company has a lead independent director, as well as the specific role the lead indepen-

14. Press Release, Sen. Charles Schumer, Schumer, Cantwell Announce 'Shareholder Bill of Rights' To Impose Greater Accountability on Corporate America (May 19, 2009) ("Schumer"), *available at* http://schumer.senate.gov/new_website/record.cfm?id=313468.

15. The text of the new rule reads: (h) *Board leadership structure and role in risk oversight*. Briefly describe the leadership structure of the registrant's board, such as whether the same person serves as both principal executive officer and chairman of the board, or whether two individuals serve in those positions, and, in the case of a registrant that is an investment company, whether the chairman of the board is an "interested person" of the registrant as defined in section 2(a)(19) of the Investment Company Act (15 U.S.C. 80a-2(a)(19)). If one person serves as both principal executive officer and chairman of the board, or if the chairman of the board of a registrant that is an investment company is an "interested person" of the registrant, disclose whether the registrant has a lead independent director and what specific role the lead independent director plays in the leadership of the board. This disclosure should indicate why the registrant has determined that its leadership structure is appropriate given the specific characteristics or circumstances of the registrant. In addition, disclose the extent of the board's role in the risk oversight of the registrant, such as how the board administers its oversight function, and the effect that this has on the board's leadership structure. 17 C.F.R. §§ 229, 239, 240, 249, 274 (2009).

16. *Id.*

17. *Id*

18. *Id.*

dent director plays in the leadership of the company."[19]

An earlier proposed version of the new rules included a requirement for "information about a director's or nominee's "risk assessment skills."[20] Although the SEC removed this particular requirement based on public comments, the final rule released states, "[I]f particular skills, such as risk assessment or financial reporting expertise, were part of the specific experience, qualifications, attributes or skills that led the board or proponent to conclude that the person should serve as a director, this should be disclosed."[21]

The SEC on Cyber Risk

In light of recent large cyber attacks, the SEC has issued new disclosure guidance requiring public companies to disclose cybersecurity risks that reasonable investors would consider important to investment decisions and how they address them, including whether they have cybersecurity or privacy insurance.[22] The guidance, which goes into effect in 2012, does not create any new SEC disclosure rules and regulations, but provides guidance on how cyber risks should be disclosed within the context of traditional disclosure categories.[23]

The guidance recognizes that companies that suffer cyber attacks may incur "substantial costs and. . .other negative consequences," and lists costs that may need to reported, such as remediating stolen data or repairing system damage, customer incentives designed to retain business after an attack, increased cybersecurity costs, lost revenues, litigation, and reputational damage affecting customer or investor confidence.[24] The agency recognized the risks associated with providing too much detail on attacks or risks, stating, "federal securities laws do not require disclosure that itself would compromise a [company's] cybersecurity."[25] "Instead," the guidance provides, companies "should provide sufficient disclosure to allows investors to appreciate the nature of risks faced by the particular" company.[26]

The guidance provides that cyber risks should be disclosed in the Risk Factors section of public reports if they are among the most significant factors that make an investment speculative or risky.[27] Specifi-

19. *Id.*
20. *Id.*
21. *Id.*
22. SEC CF Disclosure Guidance: Topic Number 2: Cybersecurity (Oct. 13, 2011), *available at* http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.
23. *Id.*
24. *Id.*
25. *Id.*
26. *Id.*
27. *Id.*

cally, the guidance states that prior cyber incidents should be reported and that their frequency and severity needs to be detailed. Appropriate disclosures "may include" discussion of aspects of the company's business that give rise to cybersecurity issues, as well outsourced functions that may give rise to cybersecurity risks and how those risks are managed.[28] A "description of relevant insurance" should also be included.[29]

The SEC guidance states that cybersecurity risks should be addressed in the Management's Discussion and Analysis of Financial Condition portion of reports if known incidents or risks are likely to have a material impact on the company's operations, liquidity, or financial condition.[30] Included in the suggested disclosures is whether a cyber attack causes an increase in cybersecurity costs.[31] Presumably, such costs would include increased cyber insurance costs.

Cyber incidents that materially affect a company's products, services, competitive conditions, or relationships with customers and suppliers should be disclosed in the Description of Business section of public reports.[32] Material litigation involving cyber incidents, such as lawsuits over stolen customer data, should be reported in the Legal Proceedings Section of public filings.[33]

While the risks related to cybersecurity have been increasing for some time, the SEC's guidance only creates more obligations and risks by creating a basis for nondisclosure failures and the related litigation and regulatory risk that comes along with such failures.

DODD-FRANK WALL STREET REFORM

Elsewhere in Washington, Congress passed the Dodd-Frank Act in 2010, which requires large financial institutions to establish independent risk committees on their boards.[34] At least one member of the committee must have had risk management experience at a large, complex firm.[35]

---

28. *Id.*

29. *Id.*

30. *Id.*

31. *Id.*

32. *Id.*

33. *Id.*

34. John Lester & John Bovenzi, *The Dodd-Frank Act: What it does, what is means, and what happens next*, OLIVER WYMAN POINT OF VIEW (2010), http://www.oliverwyman.com/ow/49558.html.

35. SCOTT LANDAU ET AL., DODD-FRANK ACT REFORMS EXECUTIVE COMPENSATION AND CORPORATE GOVERNANCE FOR ALL PUBLIC COMPANIES, PILLSBURY CLIENT ALERT (July 15, 2010), *available at* http://www.pillsburylaw.com/siteFiles/Publications/CorpSec-Tech_ECB_Alert6_07-15-2010.pdf.

An earlier proposed version of the legislation called the Shareholders Bill of Rights Act would have required all public company boards to create a separate risk committee, distinct from the Audit Committee, to be "responsible for the establishment and evaluation of the risk management practices of the" company.[36] While the final version of the Dodd-Frank Act did not require formal risk committees, the message was clear: "By creating separate risk committees, boards will never again be able to say they did not understand the risks that the firms they oversee were taking."[37] In introducing the bill, Senator Charles Schumer stated that, "[d]uring this recession, the leadership at some of the nation's most renowned companies took too many risks. . ."[38] The bill itself contained a recital, stating that, "among the central causes of the financial and economic crises that the United States faces today has been a widespread failure of corporate governance."[39]

With the increased emphasis on risk oversight, and with the possibility of risk committees being mandated for some or all public companies, companies are reevaluating how they handle risk at the board level, with some choosing pro-actively to create a risk committee.[40] While stand-alone risk committees can serve to relieve strained audit committees, it is important that qualified, independent directors serve on risk committees.

It is also imperative that creating a risk committee does not abdicate all responsibility for risk away from the rest of the directors. A risk committee must communicate with the entire board regularly, and the entire board must accept ultimate responsibility for risk oversight at the corporation. In the words of the SEC, "[t]he turmoil in the markets during the past 18 months has reinforced the importance of enhancing transparency, especially with regard to activities that materially contribute to a company's risk profile."[41]

---

36. Shareholder Bill of Rights Act of 2009, S. 1074.IS, 111th Cong. § 5(e)(5) (2009).

37. Schumer, *supra* note 14.

38. Schumer, *supra* note 14.

39. *See* S. 1074.IS.

40. For example, the Bank of New York Mellon Corporation has an independent risk committee whose purpose "is to assist the Board of Directors in fulfilling its oversight responsibilities with regard to (a) the risks inherent in the business of the Corporation and the control processes with respect to such risks, (b) the assessment and review of credit, market, fiduciary, liquidity, reputational, operational, fraud, strategic, technology, data-security and business-continuity risks, (c) the risk management activities of the Corporation and its subsidiaries, and (d) fiduciary activities of the Corporation's subsidiaries." BNY MELLON, RISK COMMITTEE CHARTER *available at* http://www.bnymellon.com/governance/committees/risk.html.

41. SEC Proxy Disclosure and Solicitation Enhancements, 17 C.F.R. §§ 229, 239, 240, 249, 270, 274 (2009), *available at* http://sec.gov/rules/final/2009/33-9089.pdf.

CONGRESSIONAL ACTION ON CYBERSECURITY

A number of cybersecurity bills have been introduced to Congress.[42] The Cybersecurity Act of 2010, sponsored by Senators Jay Rockefeller and Olympia Snowe, would have required, among other things, the National Institute of Standards and Technology to "promote auditable, private-sector developed cybersecurity risk management measures."[43] Some have warned that such requirements would require another Sarbanes-Oxley-like layer of corporate governance.[44] The bill would have created a sort of government seal of approval for cyber security frameworks,[45] and would have provided that federal contractors who "repeatedly fail to comply with best practices and training programs identified by government officials and the private sector [. . .] be required to develop and implement a remediation plan aimed at improving their cybersecurity protections."[46] Senate Majority Leader Harry Reid went on record and stated that he wanted cybersecurity legislation enacted in the last session.[47] Even though a final cybersecurity bill was not passed, it is not hard to imagine another bill being proposed, as well as how a company's requirement that it implement a cyber-remediation plan or its lack of an IT system bearing the government's seal of approval could find its way into the factual allegations in a lawsuit over a security breach.

IV. DIRECTOR DUTIES & INFORMATION TECHNOLOGY GOVERNANCE

The average loss from a corporate security breach is $234,000.[48] When public companies announce a breach, a five percent drop in share price typically occurs.[49] These statistics, coupled with the growing focus

42. *See, e.g.,* Cybersecurity Act of 2010, H.R. 4061, 111th Cong. (2010) (sponsored by Senators Jay Rockefeller and Olympia Snowe) ("Cybersecurity Act") and Protecting Cyberspace as a National Asset Act of 2010 S. 3480, 111th Cong. (2010) (sponsored by Senators Joe Lieberman, Susan Collins, and Thomas Carper) ("Protecting Cyberspace Act").

43. Richard Steinnon, *Rockefeller's Cybersecurity Act of 2010: A Very Bad Bill*, THE FIREWALL (May 4, 2010, 12:43 PM), http://blogs.forbes.com/firewall/2010/05/04/rockefellers-cybersecurity-act-of-2010-a-very-bad-bill/ (May 4, 2010).

44. *Id.*

45. Julia Gruenwald, *Cybersecurity Bill Approved*, Tech Daily Dose (Mar. 24, 2010, 4:05 PM), http://techdailydose.nationaljournal.com/2010/03/cybersecurity-bill-approved.php.

46. *Id.*

47. *Id.*

48. Erich Schwartzel, *Cybersecurity insurance: Many companies continue to ignore the issue*, PITTSBURGH POST-GAZETTE (June 22, 2010), *available at* http://www.post-gazette.com/pg/10173/1067262-96.stm.

49. ACCENTURE, HOW GLOBAL ORGANIZATIONS APPROACH THE CHALLENGE OF PROTECTING PERSONAL DATA 15 (2010), *available at* https://microsite.accenture.com/dataprivacyreport/Documents/Accenture_Data_Privacy_Report.pdf.

by regulators (and litigants) on a director's role with regard to risk oversight, including IT risk, caution directors and beg an examination of the general duties owed by directors to see how IT risk fits into the traditional director duties. Corporations, whose governance is dictated by state law, are created by state-granted charters and run by corporate directors responsible for managing the affairs of the corporation.[50] Because more than half of all publicly owned, United States corporations are chartered under the laws of the state of Delaware,[51] a duty of care discussion will generally focus on the applicable laws of Delaware. However, corporate counsel and directors should closely examine the laws of relevant states when considering any particular matter. The Delaware courts have set out a number of duties required of corporate directors. We address each briefly.

Business Judgment Rule

Delaware courts have stated that the "business judgment rule" is a "presumption that in making a business decision the directors of a corporation acted on an informed basis, in good faith and in the honest belief that the action taken was in the best interests of the company."[52] In Delaware, directors owe their corporation and shareholders fiduciary duties of care and loyalty.[53]

Duty of Care

The duty of care for directors "arises in both the discrete decision-making context and in the oversight and monitoring areas."[54] Prior to

50. *See* Del. Code Ann. tit. 8, § 141(a) (1991) ("The business and affairs of a corporation organized under this chapter shall be managed by or under the direction of a board of directors, except as may be otherwise provided in this chapter or in its certificate of incorporation.").

51. *See* Bradley R. Aronstam, *The Interplay of Blasius and Unocal—A Compelling Problem Justifying the Call for Substantial Change,* 81 Or L. Rev. 429, 429-30 n.4 (2002) (discussing why corporations prefer Delaware as their choice for incorporation); Ronald J. Gilson & Reinier Kraakman, *Delaware's Intermediate Standard for Defensive Tactics: Is There Substance to Proportionality Review?,* 44 Bus. Law. 247, 248 (1989) ("Delaware corporate law. . .governs the largest proportion of the largest business transactions in history").

52. Unitrin, Inc. v. Am. Gen. Corp., 651 A.2d 1361, 1373 (Del. 1995) (*quoting* Aronson v. Lewis, 473 A.2d 75 (Del. 1992)).

53. Smith v. Van Gorkom, 488 A.2d 858, 872 (Del. Super. Ct. 1985).

54. Lyman P.Q. Johnson & Mark A. Sides, *Corporate Governance and the Sarbanes-Oxley Act: The Sarbanes-Oxley Act and Fiduciary Duties*, 30 Wm. Mitchell L. Rev. 1149, 1197 (2004) (citing Citron v. Fairchild Camera & Instrument Corp., 569 A.2d 53, 66 (Del. 1989)); Brehm v. Eisner, 746 A.2d 244, 264 (Del. 2000) ("Due care in the decision making context is process due care only.").

the landmark case *Smith v. Van Gorkom*,[55] absent accompanying disloyal acts, it was generally accepted that "courts had rarely found individual directors liable for breaching their duty of care."[56] Experts have explained why the experienced and sophisticated directors in that case were not entitled to the protection of the business judgment rule:

> The duty of care specifies the manner in which directors must discharge their legal responsibilities. . .includ[ing] electing, evaluating, and compensating corporate officers; reviewing and approving corporate strategy, budgets, and capital expenditures; monitoring internal financial information systems and financial reporting obligations, and complying with legal requirements; making distributions to shareholders; approving transactions not in the ordinary course of business; appointing members to committees and discharging committee assignments, including the important audit, compensation and nominating committees; and initiating changes to the certificate of incorporation and bylaws.[57]

---

55. Smith, 488 A.2d 858. The Delaware Supreme Court found that the experienced and sophisticated directors of Trans Union Corporation were not entitled to the protection of the business judgment rule and had breached their fiduciary duty to their shareholders "(1) by their failure to inform themselves of all information reasonably available to them and relevant to their decision to recommend the Pritzker merger; and (2) by their failure to disclose all material information such as a. . .reasonable shareholder would consider important in deciding whether to approve the Pritzker offer." *Id.* at 888 (Del.Super. Ct. 1985); *see also* Peter V. Letsou, *Cases and Materials on Corporate Mergers and Acquisitions* n.21 at 643 (2006) (observing "Trans Union's five 'inside' directors had backgrounds in law and accounting, 116 years of collective employment by the company and 68 years of combined experience on its Board. Trans Union's five 'outside' directors included four chief executives of major corporations and an economist who was a former dean of a major school of business and chancellor of a university. The 'outside' directors had 78 years of combined experience as chief executive officers of major corporations and 50 years of cumulative experience of Trans Union. Thus, defendants argue that the Board was eminently qualified to reach an informed judgment on the proposed 'sale' of Trans Union notwithstanding their lack of any advance notice on the proposal, the shortness of their deliberation, and their determination not to consult with their investment banker or to obtain a fairness opinion.").

56. *See* Jacqueline M. Veneziani, *Note & Comment: Causation and Injury in Corporate Control Transactions: Cede & Co. v. Technicolor, Inc.*, 69 WASH. L. REV. 1167, 1194 n.3 (1994). "Before *Van Gorkom* was decided, one commentator had stated that '[t]he search for cases in which directors. . . have been held liable in derivative suits for negligence uncomplicated by self-dealing is a search for a very small number of needles in a very large haystack.'" *Id.* at 1195; Joseph W. Bishop, Jr., *Sitting Ducks and Decoy Ducks: New Trends in the Indemnification of Corporate Directors and Officers*, 77 YALE L.J. 1078, 1099 (1968). *But see* Norwood P. Beveridge, Jr., *The Corporate Director's Duty of Care: Riddles Wisely Expounded*, 24 SUFFOLK U. L. REV. 923, 949 (1990) (disputing Prof. Bishop's statement and noting that there are actually many cases upholding duty of care violations)."

57. Johnson & Sides, *supra* note 54, at 1197 (citing Citron v. Fairchild Camera & Instrument Corp., 569 A.2d 53, 66 (Del. 1989)); Brehm, 746 A.2d at 264 (Del. 2000) ("Due care in the decision-making context is process due care only.").

Duty of Loyalty

The duty of loyalty in Delaware requires "that there shall be no conflict between duty and self-interest."[58] The core concept of the fiduciary "duty of loyalty" has been described as:

> [t]he requirement that a director favor the corporation's interests over her own whenever those interests conflict. As with the duty of care, there is a duty of candor aspect to the duty of loyalty. Thus, whenever a director confronts a situation that involves a conflict between her personal interests and those of the corporation, courts will carefully scrutinize not only whether she has unfairly favored her personal interest in that transaction, but also whether she has been completely candid with the corporation and its shareholders.[59]

Conflicts of interest "do not *per se* result in a breach of the duty of loyalty. Rather, it is the manner in which an interested director handles a conflict and the processes invoked to insure fairness to the corporation and its stockholders that will determine the propriety of the director's conduct. . ."[60] Generally, except in cases where a director has an undisclosed financial interest in the outcome of an IT purchase or contract decision, the duty of loyalty does not seem to require additional focus here.

Duty of Good Faith

We have already seen that in order for a director to have the protection of the business judgment rule against a claim for breach of fiduciary duty, a director must be able to demonstrate that she acted in "good faith."[61] Many factors "define what it means for a corporate director to act in good faith. . .includ[ing] the judicial application of state corporate law, federal and state legislation, shareholder activism. . .corporate governance ratings, and the expectations of the public in response to the media's treatment of current issues in corporate governance.[62] *Stockbridge v. Gemini Air Cargo, Inc.* holds that the board of directors of a Delaware corporation is charged with the legal responsibility to manage its business for the benefit of the corporation and its shareholders with

---

58. Guth v. Loft, 5 A.2d 503, 510 (Del. 1939).

59. Charles R.T. O'Kelley & Robert B. Thompson, Corporations and Other Business Associations: Cases and Materials (5th ed. 2006).

60. Byron Egan, *Director Duties: Process and Proof*, TexasBarCLE Webcast: Corporate Minutes/ Director Duties (Oct. 23, 2008), *available at* http://images.jw.com/com/publications/1044.pdf.

61. *Id.* at n. 45.

62. Janet E. Kerr, *Developments in Corporate Governance: The Duty of Good Faith and Its Impact on Director Conduct*, 13 Geo. Mason L. Rev. 1038 (2005-06).

"due care, good faith, and loyalty."[63] Moreover:

> [w]hether the duty to act in good faith is merely a subset of the duties of care and loyalty, a duty separate and freestanding from the other two duties, or a duty similar to the duty of good faith required in the contractual context, remains to be answered. Importantly, the duty of good faith could be held to encompass compliance with the expectations of the parties involved and conformity to the spirit of the fiduciary relationship. Finally, despite inconsistency and uncertainty, under the emerging definition of the duty of good faith, directors may be held personally liable for corporate misbehavior if their conduct evidences improper motive or ill will, a reckless disregard of known risks, a sustained failure to oversee management, or is so egregious that it is unexplainable on any other grounds other than bad faith.[64]

Considering the duty of good faith in the context of a director's obligations under the federal securities laws, Delaware Chief Justice E. Norman Veasey observes that the "failure to follow the minimum. . . evolving standards of director conduct. . .Sarbanes-Oxley. . .NYSE or NASDAQ Rules. . .might likewise raise a good faith issue. There is no definitive answer to that question, but counsel should advise the directors of that possible exposure and encourage the utmost good faith behavior."[65] Moreover,

> [t]he evolving business and judicial expectations of director conduct over the years are part of the common law grist for the fiduciary duty mill. As Chancellor Allen stressed in Caremark, the kind of sustained inattention of directors exemplified by the failure to institute law compliance programs contemplated by the federal sentencing guidelines and expected of prudent businesses could be held to be a violation of fiduciary duty of good faith. That standard of conduct – good faith – is key to director conduct, and it must be considered when one looks at the directors' processes and motivations to be certain that they are honest and not disingenuous or reckless.[66]

Throughout this article, we examine the evolution of indicia of director "good faith" and standards of review applicable to directorship duties to govern the IT process, investment, and risk exposure.

Duty of Care and Information Technology Risks

Much as a board will plan for the succession of its CEO, best practices for IT Governance will include recognition by the board's nominating and governing committee that IT expertise and experience is

63. *Id.* at 1045 (citing Stockbridge v. Gemini Air Cargo, Inc., 611 S.E. 2d 600, 606 (Va. 2005) (quoting Malone v. Brincat, 722 A. 2d 5, 10 (Del. 1998)).

64. *Id.* at 1051.

65. *See* E. Norman Veasey, *Policy and Legal Overview of Best Corporate Governance Principles*, 56 Smu L. Rev. 2135, 2141 (2003).

66. *Id.*

required at the board level in order to achieve effective governance. Enterprise risks in an IT setting have the potential to threaten the corporation's very existence. Accordingly, each director's duty of care requires that the board act accordingly to provide effective corporate governance.

V. IT RISK AND WHY GOVERNANCE IS IMPORTANT

In almost all organizations, IT is fundamental to support, sustain, and grow the business. Yet, in a recent survey of 5,500 business leaders worldwide, "58% of executives polled said they have lost sensitive personal information, and for nearly 60% of those who have had a breach, it was not an isolated event."[67] Another recent study showed that sixty-five per cent of Fortune 1000 companies were not reviewing their companies' cybersecurity policies.[68] The board and senior management need to know whether their IT management is: "likely to achieve its objectives; resilient enough to learn and adapt; judiciously manage the risks it faces; and appropriately recognizing opportunities and acting upon them?"[69]

Major Sources of Risk

During recent years, IT risk has demonstrated the potential to cause catastrophic losses to the enterprise balance sheet, reputation, and even threaten its very existence. With an *average* loss per breach at $234,000,[70] examples of the effects of an IT failure include: loss of sensitive customer private information; loss of sensitive product or financial data of the corporation; virus attacks by hackers on the company's computer systems and those of its customers or vendors; business interruption losses due to IT downtime; as well as theft and use of client credit card or other sensitive data.[71] At least half of data breaches or losses are believed to be caused by a lack of internal controls and process—not hackers or viruses.[72] IT is a core asset, necessary to support, sustain, and grow every enterprise of any size. A board should consider and have contingency plans to protect the enterprise from these threats.

---

67. Accenture, *supra* note 49.

68. Schwartzel, *supra* note 48 ("[O]nly fifty-six percent of organizations surveyed said it was important or very important to have a policy about their privacy practices").

69. IT Governance Inst., Board Briefing on IT Governance, *supra* note 2 at 6.

70. Schwartzel, *supra* note 48.

71. USI Insurance Services, Cyber Liability / Security and Privacy Insurance (2009) (on file with the authors).

72. Accenture, *supra* note 49.

COMMITMENT AT THE TOP

To be successful, IT governance requires enterprise commitment at the very top. The challenges associated with achieving understanding and management of the risks involved with implementing new technologies may appear almost insurmountable. Every corporation's IT challenges and concerns will include:

I. Recognizing the importance of IT at the highest (board) level and settling upon goals and necessary resources
II. Aligning IT strategy with the business strategy,
III. Cascading strategy and goals down into the enterprise,
IV. Providing organizational structures that facilitate the implementation of strategy and goals,
V. Insisting that an IT control framework be adopted and implemented, and
VI. Measuring IT's performance[73]

The IT Governance Institute has observed that "usually advice to boards on how to operate is long on board structure, composition, size and independence, but short on risk management and practical IT governance." The *Board Briefing on IT Governance, 2nd Edition* specifically addresses IT governance.[74] Specifically, it posits that boards and management need to assess their capacity to:

- Take advantage of IT's enabling capacity for new business models and changing business practices,
- Balance IT's increasing costs and information's increasing value to obtain an appropriate return from IT investments,
- Manage the risks of doing business in an interconnected digital world and the dependence on entities beyond the direct control of the enterprise,
- Manage IT's impact on business continuity due to increasing reliance on information and IT in all aspects of the enterprise
- Maintain IT's ability to build and maintain knowledge essential to sustain and grow the business, and
- Avoid the failures of IT, increasingly impacting the enterprise's value and reputation.[75]

The overall objective of IT governance, therefore, is to understand the issues and the strategic importance of IT, so that the enterprise can sustain its operations and implement the strategies required to extend its activities into the future. IT governance aims at ensuring that expectations for IT are met and IT risks are mitigated.[76]

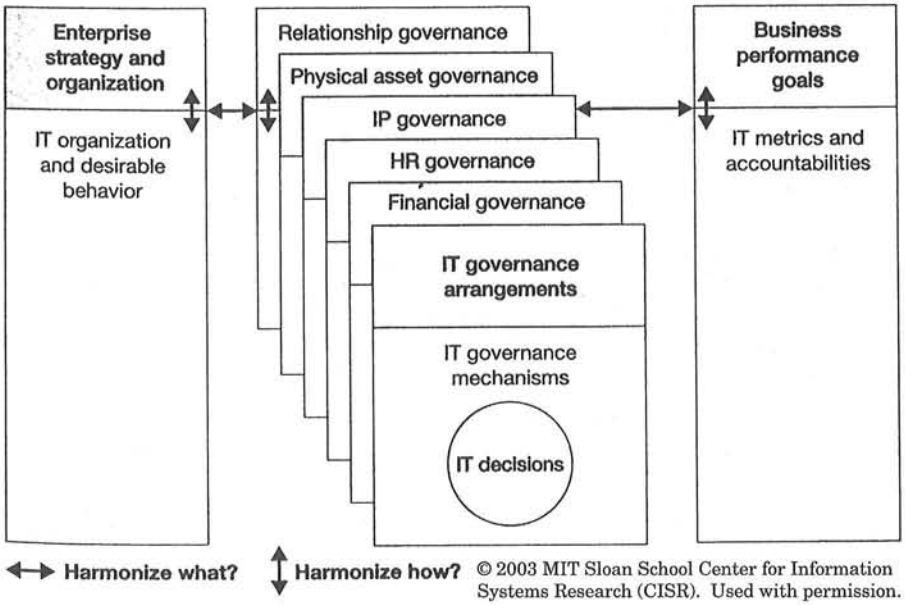
---

73. See USI Insurance, *supra* note 71.
74. IT GOVERNANCE INST., BOARD BRIEFING ON IT GOVERNANCE, *supra* note 2.
75. *Id.* at 7.
76. *Id.* at 7.

NEED FOR IT GOVERNANCE FRAMEWORK

Effective and timely measures aimed at addressing these top management concerns need to be promoted by the governance layer of an enterprise. Hence, boards and executive management need to extend governance, which is already exercised over the enterprise, to IT by way of an effective IT governance framework that addresses strategic alignment, performance measurement, risk management, value delivery and resource management. Simply put, IT governance and the effective application of an IT governance framework are the responsibilities of the board of directors and executive management. IT governance is an integral part of enterprise governance, which consists of the leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives. An IT governance framework, such as *Control Objectives for Information and related Technology* (COBIT),[77] for example, can be a critical element in ensuring proper control and governance over information and the systems that create, store, manipulate and retrieve it.[78]

IT Governance Design Framework



© 2003 MIT Sloan School Center for Information Systems Research (CISR). Used with permission.

77. *Id.* at 7.

78. For a complete overview of the role of IT governance in an enterprise, the responsibilities of boards of directors and executive management for IT governance, and tools to begin implementing effective IT governance, *see id.*

What IT Questions Should the Board Ask?

The IT Governance Institute contends that by simply asking the right questions a board is likely to uncover and address potential problems in advance.[79] Questions may include:

- Does the board understand the risks inherent in the corporate strategy?
- Are the board and executive management on the same page as to the company's risk appetite?
- Is there communication about risks and risk appetite to and from the board, and is it done on a timely basis?
- What kind of agenda time does the board dedicate to discussing risks, including IT risks?
- Does the board have adequate internal or external resources to understand emerging risks from a technical, regulatory or litigation perspective?
- How do you communicate the risk to shareholders?
- Are the board and management setting a proper tone at the top with regard to risk management?
- Do you have the right people in place to manage risk from a technical and tone perspective?
- Do you have a chief risk officer and is he or she the right fit for the job?
- Is there a chief technology officer? What role does he or she play in risk management?
- How critical is IT to sustaining the enterprise and how critical is IT to growing the enterprise?
- How far should the enterprise go in risk mitigation and is the cost justified by the benefit?
- Is IT a regular item on the agenda of the board and is it addressed in a structured manner?
- Is the reporting level of the most senior IT manager commensurate with the importance of IT?
- Does the board of the organization occasionally ask questions about IT?
- Is the board regularly informed of major IT initiatives, their status and issues?
- Does the board approve IT strategy?
- Does the board have a standing IT strategy committee with representation from the business as well as IT?[80]

79. *Id.* at 8.
80. *Id.* at 7.

VI. BOARD COMPOSITION: THE CASE FOR INFORMATION TECHNOLOGY EXPERTISE

Each Board Has the Same Fundamental Needs for Director Talent

Every board is responsible for approving nominees for election of directors. Usually, the board will designate a standing committee, commonly known as the Nominating and Governance Committee, which is comprised solely of independent directors—as defined by the relevant stock exchange and the board's corporate governance guidelines—to be responsible for recommending director nominees. Most modern boards have, at a minimum, the following basic standing committees: Audit, Compensation, Executive, and Nominating and Governance. In addition, some boards have chosen to include standing committees such as Compliance, Risk, Conflicts, Finance, and Public Issues and Contributions.

Each Board Has Different Levels of IT Skill Sets

It is easy to see that the optimal board composition is vastly different for companies engaged in different industries and at different stages of their lifecycle. For example, the board of a young software or consulting company may be inundated with IT understanding, expertise and talent, while the board of an oil and gas or fast food company may have little understanding of IT issues represented among its board members. The essential realization must be that an understanding of IT domain issues must be adequately represented among board members, particularly with significant IT risks related to their business activities, such as internet-based sales.

The Audit Committee: Appropriate Site for IT Expertise and Experience

The board's Audit Committee is a standing committee established to comply with the requirements of Section 3(a)(58)(A) of the Securities Exchange Act of 1934. All members of the audit committee must be independent under the rules of the NYSE and the board's corporate governance guidelines. The board must make a determination of the financial literacy and expertise of all members of the Audit Committee, as the board has interpreted such qualifications in its business judgment. In addition, the board must designate an individual as the "financial expert" for the Audit Committee as defined in the Securities Exchange Act of 1934.[81] The Audit Committee of any public corporation will generally

81. *See* SEC Disclosure Required by Sections 406 and 407 of the Sarbanes-Oxley Act of 2002, 17 C.F.R. §§ 228, 229, 249 (2003), *available at* http://www.sec.gov/rules/final/33-8177.

be responsible for (in no particular order of importance):

1. Hiring, firing, compensating, and overseeing the company's independent certified public accounting firm (CPAs).
2. Reviewing the company's annual reports to the SEC, including the financial statements and the "Management's Discussion and Analysis" portion of those reports, and recommending appropriate action to the board.
3. Reviewing the company's audit plans.
4. Reviewing before issuance the company's news releases regarding annual and interim financial results and discussing with management any related earnings guidance that may be provided to analysts and rating agencies.
5. Discussing the company's audited financial statements with management and the independent public accounting firm, including a discussion with the firm regarding matters required to be reviewed under applicable legal or regulatory requirements.
6. Reviewing the company's relationships with the independent public accounting firm.
7. Reviewing the company's compliance and ethics program.
8. Reviewing a report of compliance of management and operating personnel with the company's code of business conduct, including the company's conflict of interest policy.
9. Reviewing the company's non-employee-related insurance programs.
10. Reviewing changes, if any, in major accounting policies of the company.
11. Reviewing trends in accounting policy changes that are relevant to the company.
12. Reviewing the company's policy regarding investments and financial derivative products.
13. Reviewing the annual report of the company's independent public accounting firm related to quality control.
14. Reviewing and discussing the adequacy of the company's internal accounting controls and other factors affecting the integrity of its financial reports with management and with the independent certified public accounting firm.
15. Reviewing the company's risk assessment and risk management policies.

The last three of these Audit Committee responsibilities (quality control, internal accounting controls, and risk assessment) all seem to require confidence and an understanding of the enterprise's IT as a "foundation" before quality or internal accounting controls or risk assess-

---

htm; *see also* SEC Form 20-F, Item 16A, *available at* http://www.sec.gov/about/forms/form20-f.pdf.

ment can be addressed. It is clear that insurance underwriters will weigh the strength and experience of top IT management and IT governance in determining premiums and coverage terms for professional liability coverages, such as cyber security and privacy insurance.

VII. LITIGATION RISKS ASSOCIATED WITH IT ISSUES

IT risks are inherent in a company's operations. Examples of such risks include risks to third parties in operations, such as the inadvertent disclosure of sensitive customer data either by the company itself or third-parties; theft of data by cybercriminals; or exposure of customers to viruses from hackers. IT risks also include direct risks to a company such as the infiltration of viruses in internal systems, business interruption due to security breaches or viruses, the costs of restoring damaged or lost data, or the costs of notifying customers when their data has been compromised.

These risks are being realized in costly private and regulatory lawsuits related to cyber issues.[82] For example, a payment systems processor was sued in a securities fraud class action after cybercriminals stole credit and debit card information.[83] In another instance, a company was sued after a hacker infiltrated its online job application system and sent phishing e-mails to job applicants asking for additional personal information.[84] A retailer found itself embroiled in multiple lawsuits and a multi-state regulatory probe after hackers stole millions of credit and debit card numbers over a two-year period. Recently, an educational institution was sued by its alumni after hackers stole social security numbers.[85]

According to the Privacy Rights Clearinghouse, more than 494,556,046 records have been breached since 2005.[86] In June 2010 alone, the Clearinghouse reported fifty-three data breach incidents, some involving few records, others involving tens of thousands.[87] One company reported a breach of thirty-eight terabytes of information, which is

82. ACCENTURE, *supra* note 49; USI Insurance Services, *supra* note 71.

83. In re Heartland Payment Sys., Inc. Sec. Litig., Case 3:09-cv-01043-AET-TJB, 2009 WL 4798148, at *5 (D.N.J. Dec. 7, 2009).

84. *Aetna Boots Data Breach Class Action Suit*, INFOSECURITY (Mar. 12, 2010), http://www.infosecurity-us.com/view/8024/aetna-boots-data-breach-class-action-suit/.

85. CHUBB GROUP OF INSURANCE COMPANIES, CYBERSECURITY BY CHUBB: INSURING CYBER EXPOSURE FOR BUSINESSES OF ALL KINDS 1 ("INSURING CYBER EXPOSURE"), *available at* http://www.sgdins.com/downloads/CyberSecurity%20by%20Chubb.pdf (last visited Apr. 4, 2011).

86. *Chronology of Data Breaches 2005-Present*, PRIVACY RIGHTS CLEARINGHOUSE, http://www.privacyrights.org/data-breach (last updated Apr. 4, 2011). This number does not reflect the number of incidents of data breach, but rather the number of records involved in those breaches.

87. *Id.*

said to be the "equivalent [of] nearly double the amount of text contained in the Library of Congress."[88] Even more troubling is the fact that the Clearinghouse records are not exhaustive, nor do they reflect breaches occurring outside the United States.[89]

Heartland Payment Systems Case

After a theft by cybercriminals of 130 million credit and debit card numbers, a securities fraud class action was filed against Heartland Payment Systems for "fraudulently misrepresent[ing] the general state of its data security" and concealing an earlier cyber attack during earnings calls and in SEC filings.[90] At the time, it was believed to be the largest security breach ever.[91] Although the breach occurred over the course of 2008, the company did not discover it until January 2009.[92] When Heartland disclosed the breach, the stock price dropped almost eighty percent;[93] it was virtually inevitable that shareholders would sue. It was ultimately revealed that the breach was caused by a piece of "malicious software planted on the company's payment processing network that recorded payment card data as it was being sent for processing to Heartland by thousands of the company's retail clients."[94] Heartland did not know "how long the malicious software was in place, how it got there or how many accounts may have been compromised."[95] However, what Heartland did know is that the stolen data included names, credit and debit card numbers, and expiration dates.[96] While the shareholder class action against Heartland was later dismissed for failure under the PSLRA to plead fraud with particularity,[97] the company and its officers and directors were forced to pay sixty million dollars in a settlement with Visa,[98] $41.4 million in a settlement with MasterCard,[99] $3.6 million in

88. Sen. Sheldon Whitehouse, *We need to act on Cybersecurity*, Nat'l L. J. (2010), *available at* http://www.law.com/jsp/nlj/PubArticlePrinterFriendlyNLJ.jsp?id=1202457824249&slreturn=1&hbxlogin=1.

89. Chronology of Data Breaches 2005-Present, *supra* note 86.

90. In re Heartland, 2009 WL 4798148 at *5.

91. Brian Krebs, *Three Charged with Hacking Dave & Buster's Chain*, Wash. Post Security Fix (May 14, 2008), http://voices.washingtonpost.com/securityfix/2008/05/three_charged_with_hacking_dav.html.

92. In re Heartland, 2009 WL 4798148 at *5.

93. *Id.*

94. Krebs, *supra* note 91.

95. *Id.*

96. *Id.*

97. In re Heartland, 2009 WL 4798148 at *8.

98. Press Release, Visa, Heartland Payments Systems Agrees on Settlement to Provide Visa Issuers up to $60M for Data Breach Security Claims (Jan. 8, 2010), *available at* http://corporate.visa.com/media-center/press-releases/press974.jsp.

99. Press Release, Heartland Payment Systems, Heartland Payment Systems® and Mastercard Agree to $41.4 Million Intrusion Settlement: Company has now reached

a settlement with American Express,[100] up to $2.4 in a consumer cardholder class action[101] over the same breach, as well as the defense costs of the dismissed suit and internal investigation costs incurred by the company.

Other Data Breach Cases

A data breach victim sued Aetna after its job application web site was hacked and job applicants began receiving phishing e-mails asking for additional personal information.[102] The case was dismissed for lack of standing because the particular plaintiff had not received one of the e-mails and could not prove his actual data had been breached.[103] Still, the headache of defending and paying for defense of the case was present. Other incidents include:

- TJX, the parent company of TJ Maxx, Marshall's, and HomeGoods, reported the theft of forty million credit card numbers, costing it more than $200.[104] TJX was sued in a class action lawsuit and spent more than $12 million in one quarter "for costs incurred to investigate and contain the intrusion, improve computer security and systems, and communicate with customers, as well as technical, legal, and other fees."[105]
- Dave & Busters was hit by three men who hacked into its registers and stole data from thousands of credit and debit cards. That data was later sold and caused $600,000 in losses to customers.[106]
- A breach at the grocer Hannaford, which also does business as Food Lion, resulted in the theft of more than four million customer credit and debit card numbers.[107]

---

breach-related settlements with three major card brands (May 19, 2010), *available at* http://www.heartlandpaymentsystems.com/article/Heartland-Payment-Systems-and-Mastercard-Ag-6349.aspx.

100. Press Release, Heartland Payment Systems, Heartland Payment Systems and American Express Agree to $3.6 Million Intrusion Settlement: Settlement marks first agreement with a card brand related to 2008 intrusion (Dec. 17, 2009), *available at* http://www.heartlandpaymentsystems.com/article/Heartland-Payment-Systems-and-American-Expr-3047.aspx.

101. Press Release, Heartland Payment Systems, Heartland Payment Systems Agrees to Settle Cardholder Class Action Claim (Dec. 21, 2009), *available at* http://www.heartlandpaymentsystems.com/article/Heartland-Payment-Systems-Agrees-to-Settle-3051.aspx.

102. *Aetna Boots Data Breach Class Action Suit*, *supra* note 84.

103. *Id.*

104. Accenture, *supra* note 49, at 3.

105. Sharon Gaudin, T.J. Maxx Breach Costs Hit $17 Million, INFO. WK. (May 17, 2007, 1:28 PM), http://www.informationweek.com/news/security/showArticle.jhtml?articleID=199601551.

106. Krebs, *supra* note 91.

107. Brian Krebs, *Grocer Says Data Were Compromised*, Wash. Post (Mar. 19, 2008), http://www.washingtonpost.com/wpdyn/content/article/2008/03/18/AR2008031802878.html.

- "A retailer reported that computer hackers stole millions of credit and debit card numbers from the company over a two-year period. News reports indicated that some of the stolen information was used to commit fraud. The retailer faces a multi-state probe, and lawsuits are mounting over the data breach."[108]
- "A media conglomerate lost unencrypted computer backup tapes containing sensitive information, including Social Security numbers, from thousands of people."[109]
- "An educational institution faces a class action lawsuit filed by two alumni whose personal data were among thousands accessed when hackers broke into the school's computer system."[110]
- "A wholesaler announced that thieves had accessed more than one million credit and debit card numbers and transaction information involving thousands of customer checks."[111]
- "An information broker announced that a fraud ring had gained access to thousands of records containing personal and financial information about consumers from the company's database."[112]

Other Relatively New Technology Risks

Beyond just web portals and computer networks, technology is also creating risks in less traditional technology areas. According to a recent study, the increasingly popular Voice over Internet Protocol, or VoIP, method of telephone is creating new corporate risk. "[D]iscount . . .VoIP telephone service, which is rapidly being adopted in the U.S. and throughout the world, is causing a shift from the reliable, secure traditional network now in use, to an Internet environment of extreme risk."[113] VoIP is vulnerable to, among other risks, hacking, identity theft, intellectual property theft, and interruption of service.[114] The report predicts that these risks will cause insurance rates to rise, as well as foster the creation of new cyber insurance products aimed at VoIP-based risks.[115]

---

108. Insuring Cyber Exposure, *supra* note 85 at 1.

109. *Id.*

110. *Id*

111. *Id.*

112. *Id.*

113. Harry Emerson et al., *VoIP Cyber-Security Risks Predicted to Raise Insurance Rates: Flaws Enabling Hacker Attacks on Internet Phone Service are Extensive Per Report by Emerson Development*, ENHANCED ONLINE NEWS (May 26, 2010), http://eon.businesswire.com/news/eon/20100526005868/en/Cyber-Security/cyber-security/espionage.

114. *Id.*

115. HARRY E. EMERSON III, EMERSON DEVELOPMENT LLC, VOIP SECURITY REVIEW INSURANCE: INTERNET BASED TELEPHONY: AN ANTICIPATED PRODUCER OF MAJOR LOSSES IN CYBERSPACE, A NEW FRONTIER FOR INSURANCE CARRIERS (2010), *available at* http://www.ironpipe.net/Assets/VoIPInsuranceReportByEmersonDevelopment.pdf.

REGULATORY MINEFIELD

In addition to lawsuits, there are new regulatory requirements for companies associated with IT risks, in particular identity theft. Forty states now have laws regarding data breach notification.[116] Maine, Maryland, New York, New Hampshire, North Carolina, Vermont, and Virginia require breaches to be reported to a centralized database.[117] Other states, including California, Colorado, Florida, Illinois, Massachusetts, Michigan, Nebraska, Hawaii, and Wisconsin, require some level of publicly available notification, primarily through Freedom of Information requests.[118] Companies that operate internationally may have to contend with the European Union's Data Directive regarding the transfer of personal data between countries.[119]

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.[120] 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.[121] 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.[122]

The reach of the rule is broad. It extends not only to banks and other financial institutions subject to FTC regulation, but to any company which functions as a creditor to its customers, such as retailers that offer charge accounts or store credit cards or auto dealers that offer customer financing.[123] It reaches to any company which bills for services already rendered, such as doctors, lawyers, accountants, or even lawn services.[124] Utility companies and telecommunications providers that bill for the prior month's – rather than the next month's – services would be covered by the Red Flags Rule.[125]

---

116. *Chronology of Data Breaches 2005-Present*, *supra* note 74.

117. *Id.*

118. *Id.*

119. *U.S.-E.U. Safe Harbor Overview*, EXPORT.GOV, http://www.export.gov/safeharbor/eu/eg_main_018476.asp, (last visited July 27, 2010).

120. FTC Press Release, FTC Extends Enforcement Deadline for Identity Theft Red Flags Rule (May 28, 2010), *available at* http://www.ftc.gov/opa/2010/05/redflags.shtm.

121. FTC Credit Practices Rule, 16 C.F.R. §681.2 (2009).

122. *Id.*

123. *Id.*

124. *Id.*

125. *Id.*

VIII. MITIGATING IT RISK THROUGH INSURANCE

Important in identifying IT risks and developing processes for mitigating and preventing them is the consideration of how the financial burden of such risks can be shared with others. There are two primary considerations from an insurance perspective with regard to IT risks: (1) cyber liability related to the breach itself, and (2) D&O liability related to a failure to properly manage IT risk. Indeed,

> [t]he need for cyber coverage is growing. More companies are growing their revenue through online sales. As a result, they are becoming more exposed. Further, they are relying on outsourced service providers for web hosting, credit card processing, call centers, document storage, and data warehousing. Subsequently, they are spending more time validating and reviewing the data security standards and risk management practices of these providers. In addition, many customers are now requiring proof of insurance that will address privacy breach events.[126]

A new form of professional insurance called cyber liability or security and privacy insurance has arisen to address the portion of these risks that are not covered by traditional director & officer insurance policies. Many carriers now offer policies that provide coverage for a company's first and third-party costs for responding to a cyber issue, such as: the costs of restoring lost data or business interruption losses when a company's electronic systems are down, the costs of suits from customers and other third parties for disclosure of sensitive information, or suits for damages by hackers who use a company's system to inflict damage on others.[127] Policies may also include the cost of notifying customers of a data breach—which can be tens of thousands of dollars—or crisis management expenses when responding to a major cyber event.[128] Premiums for such policies—once more than $100,000—can now be purchased for as little as $10,000.[129]

From an insurance perspective, cyber liability is broadly defined as liability associated with e-business; the Internet; computer networks; the use of computer technology; privacy issues; computer virus transmission; and other means by which compromised data is passed to a third

126. Toby L. Merrill, *Cyber Liability Market is older, wiser, smarter and still growing*, INSURANCE JOURNAL (Jan. 29, 2007), http://www.insurancejournal.com/magazines/mag_features/2007/01/29/76734.htm.

127. USI Insurance Services, *supra* note 71; CHUBB GROUP OF INSURANCE COMPANIES, CYBERSECURITY BY CHUBB: HOW WILL YOU SURVIVE A DATA SECURITY BREACH? WHY CYBER INSURANCE MIGHT NOT BE OPTIONAL ANYMORE ("CYBER INSURANCE"), *available at* http://www.chubb.com/businesses/csi/chubb10600.pdf; INSURING CYBER EXPOSURE, *supra* note 85.

128. Schwartzel, *supra* note 48. ("Breach notification costs are estimated at between $30 and $100 per customer.").

129. *Id.*

party.[130] Cyber liability encompasses both first party liability, designed to cover a company's direct losses in the event of a breach, and third party liability, designed to cover obligations to third parties resulting from a cyber event. Examples of first party costs and/or coverage include:

- Data Asset / Data Restore: Covers data restoration expenses after a data breach.
- Business Interruption: Covers the costs related to a shutdown after a security breach.
- Cyber Extortion / E-threat: Covers expenses and ransom in cases of credible threat or when an extortion demand is received.
- Crisis Management / Reward expenses: Covers costs of responding to the breach, including the cost of public relations consultants.[131]

Third party coverage, on the other hand, addresses:

- Network Security: When hackers use a company's systems to inflict damage on others.
- Privacy / Disclosure Injury: When private information is disclosed from either a computer network or a paper file.
- Suits by customers arising from the unauthorized dissemination of their personal information.[132]

Finally, a third area, defined in many policies as media, content, or intellectual property coverage, relates to injury from losses related to the display of material online, including infringement of trademark or copyright, business disparagement, libel, or slander.[133] Not only are such policies increasingly viewed by many companies as a business necessity, some believe Congress may ultimately require them.[134]

IX. DISASTER RECOVERY AND BUSINESS CONTINUITY PLANNING

Another important consideration in a time of major security breach that will fall on the shoulders of directors and officers, is communicating with shareholders and the public about the breach as it unfolds. As British Petroleum's public relations missteps showed last year, this crucial part of handling any major business crisis can significantly mitigate or exacerbate a company's liability depending on how it is handled. A major security breach is no different. However, crisis management and communication requires planning beforehand to ensure that policies and

130. Merrill, *supra* note 126; *Cyber Liability Insurance Explained*, INSURE NEW MEDIA http://www.insurenewmedia.com/pages/cyberliability.asp (last visited July 21, 2010).

131. USI Insurance Services, *supra* note 71; CYBER INSURANCE, *supra* note 127; INSURING CYBER EXPOSURE, *supra* note 85.

132. *Id.*

133. *Id.*

134. Schwartzel, *supra* note 48.

procedures are in place to handle communication regarding a crisis as soon as it begins and to prepare for the cost of outside consultants and communication efforts.

> A business continuity plan can mean the difference between survival and failure. Depending on the nature of your business such a plan could be the result of an afternoon's thought and a few pages filed away, just in case. But the time will be well spent. For bigger companies, the plan could be the culmination of an analysis of threats and their effect, a thorough asset management review that identifies available and relocatable resources (including manual work-arounds) and a cost effective disaster recovery solution. Such an extensive plan will also include a testing phase designed to convince your organization that it can work.[135]

A good crisis management plan anticipates and plans for crises possible in a particular industry or business model and fully considers the disclosures that should be made as to potential risks. For example, if a significant source of a business's revenues are through online sales, and a hacker causes the company's web site to go offline, the company should be prepared for a shut down in its online ordering system and the resulting business interruption, as well as prepared to communicate with and reassure customers when the system is restored. The plan should also handle communication both internally and externally at the time of crisis; including what external disclosures should be made in order to satisfy reporting obligations, and to preserve relationships with regulators, investors, and customers without increasing liability. One important element of this planning can be to include crisis communication and management in a company's D&O insurance program. A number of major insurance carriers now recognize the importance of prompt crisis management and offer coverage for such services in their cyber insurance policies, including some on a first-dollar basis.

X. CONCLUSION

Few enterprise operational areas present as much inherent risk or prove as difficult to govern as Information Technology. To recap a few of the facts presented throughout this article:

- IT failures include loss of sensitive and private customer information; loss of sensitive product or financial data of the corporation; virus attacks by hackers on the company's computer systems and those of its customers or vendors; business interruption losses due to IT downtime; as well as theft and use of client credit card data.[136]

135. Kate Lister, *Cyber Crime: Can You Afford to Ignore It?*, AMERICAN EXPRESS OPEN FORUM SMALL BUSINESS OWNER BLOG (Apr. 30, 2010), http://www.openforum.com/idea-hub/topics/money/article/cyber-crime-can-you-afford-to-ignore-it-kate-lister.

136. USI Insurance Services, *supra* note 71.

- The average loss from a corporate security breach is $234,000.[137]
- When public companies announce a breach, it typically causes a five percent drop in share price.[138]
- A number of cybersecurity bills have been introduced in Congress.[139]
- At least half of data breaches or losses are believed to be caused by a lack of internal controls and process—not hackers or viruses.[140]

A reasonable question voiced from many boardrooms is "How can I be expected to govern something I know so little about?"[141] To be successful, however, IT governance requires enterprise commitment at the very top. Boards and executive management need to extend governance, already exercised over the enterprise, to IT by way of an effective IT governance framework. This framework should address strategic alignment, performance measurement, risk management, value delivery, and resource management. IT governance is an integral part of enterprise governance and consists of the leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives. Simply put, IT governance and the effective application of an IT governance framework are the responsibilities of the board of directors and executive management. Having an IT governance framework, such as *Control Objectives for Information and related Technology* (COBIT)[142] can be a critical element in ensuring proper control and governance over information and the systems that create, store, manipulate and retrieve it.[143] But these risks do not have to be shouldered by the company alone. Many can be transferred to or shared with insurance.

Every Governance and Nominating Committee must access its current inventory of director skill sets to produce the required IT expertise. One choice will be to have and include IT expertise within a dedicated Risk Committee. Best practice for many will dictate that an audit committee include IT expertise and be composed of a qualified vice chairman, familiar with the company's particular audit issues by virtue of experience gained from audit committee service. This will help provide an instant replacement for the committee chair should unexpected developments require. Therefore, every board should have at least two quali-

137. Schwartzel, *supra* note 48.

138. ACCENTURE, *supra* note 49 at 5.

139. *See, e.g.,* Cybersecurity Act, *supra* note 42, and Protecting Cyberspace Act, *supra* note 42.

140. ACCENTURE, *supra* note 49 at 5.

141. WEILL & ROSS, *supra* note 1 at 2.

142. *See* IT GOVERNANCE INST., COBIT®4.1 EXECUTIVE SUMMARY FRAMEWORK, *supra* note 3 at 4.

143. *See* IT GOVERNANCE INST., BOARD BRIEFING ON IT GOVERNANCE, *supra* note 2 at 5.

fied financial experts populating the audit committee and seek IT expertise and experience in director recruitment to help avoid and address the costly private and regulatory lawsuits related to cyber issues that increasingly facing companies. Every board's challenge in addressing IT risk is ongoing vigilance and recognition of the mission critical nature of Information Technology to the enterprise.