Hastings Business Law Journal

Volume 13
Number 3 *Spring 2017*

Article 1

Spring 2017

The Board's Responsibility for Crisis Governance

Lawrence J. Trautman

The Board's Responsibility for Crisis Governance

*By Lawrence J. Trautman**

> Extracting the energy resources to fuel our cars, heat and light our homes, and power our businesses can be a dangerous enterprise. Our national reliance on fossil fuels is likely to continue for some time and all of us reap benefits from the risks taken by the men and women working in energy exploration. We owe it to them to ensure that their working environment is as safe as possible.
>
> *— Report to the President, National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling (2011)*[1]

I. OVERVIEW

Does management and a board of directors have a clear, communicated plan for disaster scenarios? A clear strategy and implementation plan for reasonably foreseeable industry disasters—before they take place, helps to prevent mistakes made under conditions of severe stress. Survival-threatening disasters such as the:

*J.D., Oklahoma City Univ. School of Law; MBA, The George Washington University; BA, The American University. Mr. Trautman is Assistant Professor of Business Law and Ethics at Western Carolina University and a past president of the New York and Metropolitan Washington/Baltimore Chapters of the National Association of Corporate Directors. He may be contacted at www.ljtrautman.com. The author wishes to extend particular thanks to the following for their assistance in the research and preparation of this article: Alan Beller; Dennis R. Beresford; Rebecca M. Bratspies; John S. Carroll; Michael Froomkin; Cynthia Glassman; Jeffrey N. Gordon; John R. Harrald; Adm. Bobby R. Inman (Ret.); Nancy Leveson; Richard Levick; David Morens; Hitoshi Nasu; Justen R. Noakes; John Olson; David Passmore; James Pursell; Geoffrey Rothwell; Gregory L. Shaw; and Laura Unger. Thanks also to the George Washington University Schools of Business and Law, and in particular, the Denit Trust Challenges in Corporate Governance Series for providing inspiration for this article. All errors and omissions are my own.

1. NAT'L COMM'N ON THE BP DEEPWATER HORIZON OIL SPILL & OFFSHORE DRILLING, REPORT TO THE PRESIDENT, DEEPWATER: THE GULF OIL DISASTER & THE FUTURE OF OFFSHORE DRILLING, vii (2011) [hereinafter *Deepwater*].

Tylenol poisoning case (1982),[2] the Bhopal chemical release (1984),[3] the Exxon Valdez oil spill (1989),[4] the World Trade Center attack on September 11, 2001[5]—and more recently the BP Gulf of Mexico oil spill, Massey Energy West Virginia coal mining disaster, or natural disasters such as hurricanes, fires, or the March 11, 2011 Japanese earthquake and tsunami, constitute every board's worse nightmare. As the commission that investigated the loss of the Columbia space shuttle observed, "complex systems almost always fail in complex ways."[6] This issue of "complexity" seems to be a common characteristic among many of these tragic events. The National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling observes, "Though it is tempting to single out one crucial misstep or point the finger at one bad actor as the cause … any such explanation provides a dangerously incomplete picture of what happened—encouraging the very kind of complacency that led to the accident in the first place."[7]

This paper proceeds in nine parts. First, by offering a few thoughts about contemporary threats. Second, it examines the board of director's responsibility in crisis. Third, it discusses the necessity of commitment at the top of every enterprise if progress is to be made toward crisis preparation, mitigation, and response. Fourth, it looks at several major corporate disasters: the Japanese earthquake and tsunami of 2011; Deepwater Horizon drilling rig debacle; and General Motors ignition switch crisis. Fifth, a framework for analysis is offered, followed by some thoughts about what to do when crisis hits. Sixth, I discuss what to do in those situations where management is implicated, use of special committees of the board, and emergence of the role for special counsel. Workplace and data security issues are then discussed with emphasis on Toyota's 2010 social media recall strategy, and the Target, Sony, and U.S. Office of Personnel Management data breaches. Next, the following

2. *See* Brian Wansink, *Consumer Reactions to Food Safety Crises*, 48 ADVANCES IN FOOD AND NUTRITION RESEARCH 103 (2004), http://ssrn.com/abstract=2474720.

3. *See* David N. Smith, *The Way We Think: Ethics, Health and the Environment in International Business*, 5 ASIAN J. WTO & INT'L HEALTH L. & POL'Y 25 (2010), http://ssrn.com/abstract=1578267; Christopher C. Hood & Henry Rothstein, *Business Risk Management in Government: Pitfalls and Possibilities* (CARR Discussion Paper No. 0, 2000), http://ssrn.com/abstract=471221; Kent Greenfield, *The Disaster at Bhopal: Lessons for Corporate Law?*, 42 NEW ENG. L. REV. 755, (2008), http://ssrn.com/abstract=1312023.

4. *See* Ronen Perry, *Economic Loss, Punitive Damages, and the Exxon Valdez Litigation,* 45 GA. L. REV. 409 (2011), http://ssrn.com/abstract=1611566; Dale B. Thompson, *Valuing the Environment: Courts' Struggles with Natural Resource Damages,* 32 ENVTL. L. 57 (2002), http://ssrn.com/abstract=306319; Catherine M. Sharkey, *The Exxon Valdez Litigation Marathon: A Window on Punitive Damages,* 7 U. ST. THOMAS L.J. 1 (2010), http://ssrn.com/abstract=1588961; Zygmunt J. B. Plater, *The Exxon Valdez Resurfaces in the Gulf of Mexico, and the Hazards of 'Megasystem Centripetal Di-Polarity',* 38 B.C. ENVTL. AFF. L. REV. 1 (2011), http://ssrn.com/abstract=1857492; Sanne H. Knudsen, *A Precautionary Tale: Assessing Ecological Damages after the Exxon Valdez Oil Spill,* 7 U. ST. THOMAS L.J. 95 (2009), http://ssrn.com/abstract=2427832.

5. *See* Douglas Linder, *The Trial of Zacarias Moussaoui: An Account*, FAMOUS TRIALS, http://www.famous-trials.com/moussaoui/1810-home (last visited Mar. 28, 2017).

6. *Deepwater*, *supra* note 1, at viii.

7. *Id.*

enterprise nightmare scenarios are presented: supply chain disruptions; Foreign Corrupt Practices Act (FCPA) violations; internet failure, or data loss from virus or hacker attack; nationalization of assets; natural disasters; adverse political developments; pandemics such as the 2014–15 Ebola scare; prolonged power disruption; strikes and labor actions; and war. Succession planning is the next topic having corporate crisis implications.

My goal here is not to provide a lengthy recital of the details of each of these tragedies. Rather, I attempt to draw upon lessons from each disaster and explore how they may be applied more generally across all industries. Ample footnotes are provided for those desiring more information about any particular aspect. The following pages should not be a comfortable read. Some of the behavior of key decision makers is disturbing. Several crisis situations depict the result of lack of preparation that reaches levels of gross negligence and criminality. In other cases, these highly publicized disasters could have happened to anyone in that industry. In all too many examples, the unfortunate corporate response is primarily "spin" and cover-up until public outcry demands a serious response. While effective risk management is likely the topic highest on every board's agenda, it is imperative that thought be given constantly to crisis management and what a board might expect to confront when a corporate disaster strikes.

Nature of the Threat

> Changes in the nature of security threats and terrorist capabilities have dramatically altered how our government leaders manage national security and defense issues," notes the Business Roundtable in their publication *Committed to Protecting America: CEO Guide to Security Challenges.*[8] Unlike the hostile nation states of the cold war era, today we find a different threat—where "One small, organized group of well-financed terrorists;[9] a lone knowledgeable hacker; or an embittered fanatic each has access to devices that can disrupt business activities and inflict severe economic damage."[10] In the United States, "with the private sector in control of more than 85 percent of the nation's critical infrastructure—the power grid, information and financial services, rails, shipping, and airlines—business leaders recognize the need to partner with government to improve security and manage risks.[11]

8. Business Roundtable, *Committed to Protecting America: CEO Guide to Security Challenges,* (Feb. 2005), http://www.cj.msu.edu/~outreach/wmd/ceo_guide.pdf [hereinafter Business Roundtable].

9. *See* Andrew Higgins & Milan Schreuer, *Attackers in Paris 'Did Not Give Anyone a Chance,'* N.Y. TIMES (Nov. 14, 2015), https://www.nytimes.com/2015/11/15/world/europe/paris-terror-attacks-a-display-of-absolute-barbarity.html.

10. *See* Business Roundtable, *supra* note 8.

11. *Id. See also* Lawrence J. Trautman, *Is Cyberattack the Next Pearl Harbor?,* 18 N.C. J. L. & TECH. 232 (2016) (depicting a fictional account of what a cyber attack on the U.S. might resemble).

Crisis Nexus: Energy is the Lifeblood of our Nation

In their 2011 Report to the President, *The National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling* observed the following inconvenient truth regarding U.S. energy requirements,

> The centrality of oil and gas exploration to the Gulf economy is not widely appreciated by many Americans, who enjoy the benefits of the energy essential to their transportation, but bear none of the direct risks of its production. Within the Gulf region, however, the role of the energy industry is well understood and accepted. The notion of clashing interests—of energy extraction versus a natural-resource economy with bountiful fisheries and tourist amenities—misses the extent to which the energy industry is woven into the fabric of the Gulf culture and economy, providing thousands of jobs and essential public revenues. Any discussion of the future of offshore drilling cannot ignore these economic realities . . .
>
> For the simple fact is that the bulk of our newly discovered petroleum reserves, and the best prospects for future discoveries, lie not on land, but under water . . . The choice of how aggressively to exploit these resources, wherever they may be found, has profound implications for the future of U.S. energy policy, for our need to understand and assure the integrity of fragile environmental resources, and for the way Americans think about our economy and our security. Although much work is being done to improve the fuel efficiency of vehicles and to develop alternative fuels, we cannot realistically walk away from these offshore oil resources in the near future. So we must be much better prepared to exploit such resources with far greater care.[12]

Civilization requires energy to provide heat, lighting and power required for industrial production.[13] Herein lays the tension. Despite the best efforts of

12. *Deepwater*, *supra* note 1, at x–xi.

13. *See* Fred Bosselman et al. *Energy, Economics and the Environment: Cases and Materials, in* ENERGY, ECONOMICS AND THE ENVIRONMENT: CASES AND MATERIALS, (Foundation Press, 2006), http://ssrn.com/abstract=1319022; Edward L. Glaeser, Sari Pekkala Kerr & William R. Kerr, *Entrepreneurship and Urban Growth: An Empirical Assessment with Historical Mines* (Harvard Business School Entrepreneurial Management Working Paper No. 13-015, 2012), http://ssrn.com/abstract =2127249; Jeremy Carl, Varun Rai & David G. Victor, *Energy and India's Foreign Policy, Program on Energy and Sustainable Development*, (Program on Energy and Sustainable Development Working Paper No. 75, 2008), http://ssrn.com/abstract=1400184; David I. Stern, *The Role of Energy in Economic Growth* (USAEE-IAEE Working Paper No. 10-055, 2010) http://ssrn.com/abstract=1715855; David Hodas, *Ecosystem Subsidies of Fossil,* 22 J. LAND USE & ENVTL. L. 599 (2007), http://ssrn.com/abstract=

management to focus on industrial safety, nuclear energy and the extractive industries such as oil and gas or coal mining appear to be inherently dangerous. Over long periods of time, fatal accidents are an unfortunate fact of life.[14] We know from experience that human error or natural disasters will continue to place some of these companies in crisis. Therefore, every board should consider what actions they will take (and have a plan in place) for when the foreseeable crisis happens. I am indebted to industrial safety expert and MIT engineering Professor Nancy Leveson, who states,

> [W]hile some industries have very high accident rates (such as those you mention), others which are equally if not of greater inherent risk (such as commercial aviation and U.S. nuclear submarines) have orders of magnitude fewer accidents. Gas, oil and the extractive industries have high accident rates not because their processes are inherently more dangerous (although they excuse their actions or lack of actions this way) but because they do not do what is necessary to prevent them. Period.[15]

Business Crisis and Continuity Management

In presenting their case advocating use of a comprehensive program for business crisis and continuity management (BCCM), Gregory L. Shaw and John R. Harrald state, "All organizations in all sectors (public, private and not-for-profit) face the possibility of disruptive events that have impacts ranging from mere inconvenience and short-lived disruption of normal operations to the very destruction of the organization."[16] Further, "Organizational functions supporting business disruption, preparedness, response and recovery—such as risk management, contingency planning, crisis management, emergency response, and business resumption and recovery—are established and resourced based on the

1117564; David I. Stern, *The Role of Energy in Economic Growth* (Crawford School Centre for Climate Economics & Policy Paper No. 3.10, 2011), http://ssrn.com/abstract=1878863.

14. *See* Alison D. Morantz, *Coal Mine Safety: Do Unions Make a Difference?*, 66 INDUS. & LAB. REL. REV. 88 (2013), http://ssrn.com/abstract=1846700; Maria Lee, Beyond Safety? The Broadening Scope of Risk Regulation, 62 CURRENT LEGAL PROBS. 242 (2009), http://ssrn.com/abstract=2088170; Anne Marie Lofaso, *What We Owe Our Coal Miners*, 11 HARV. L. REV. 87 (2011), http://ssrn.com/abstract=1792859; Anne Marie Lofaso, *Approaching Coal Mine Safety from a Comparative Law and Interdisciplinary Perspective,* 111 W. VA. L. REV. 1 (2008), http://ssrn.com/ abstract=993830; Roger M. Cooke & George-Neale Kelly, *Climate Change Uncertainty Quantification: Lessons Learned from the Joint EU-USNRC Project on Uncertainty Analysis of Probabilistic Accident Consequence Codes* (Resources for the Future Discussion Paper No. 10-29, 2010), http://ssrn.com/ abstract=1612813.

15. E-mail from Nancy Leveson, Professor of Aeronautics & Astronautics & Eg'r Sys., MIT, to Lawrence J. Trautman, (June 27, 2015, 15:59 CST) (on file with author).

16. Gregory L. Shaw & John R. Harrald, *The Core Competencies Required of Executive Level Business Crisis and Continuity Managers—The Results,* 3 J. HOMELAND SEC. & EMER. MGT. 1 (2006), http://www.bepress.com/jhsem/vol3/iss1/1.

organization's perception of its relevant environments and the risks within those environments."[17] Shaw and Harrald remind us that "The reality of business is that increasing and dynamic threats, business complexity, government regulation, corporate governance requirements, and media and public scrutiny demand an integrated approach to BCCM and its supporting functions."[18] Shaw and Harrald also provide an extensive list of sources designed "to convince businesses to establish readiness programs and take steps to continue, resume and recover their critical business functions and processes to ensure their organizational survival.[19]

II. THE BOARD'S RESPONSIBILITY IN CRISIS

Director's Legal Duties and Responsibilities

Professor Stephen M. Bainbridge has observed that the business judgment rule "pervades every aspect of state corporate law."[20] Corporations are created by state-granted charters with their governance dictated by state law and their corporate directors responsible for managing the affairs of the corporation.[21] Delaware courts

17. *Id*.

18. *Id.*

19. *Id.* at 3, *listing* Business Roundtable, *supra* note 8; *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets (2003),* the Business Continuity Institute's *Business Continuity Management: Good Practices Guidelines (2002)* and the Standards Australia*, Draft Business Continuity Handbook (2003)*, and government publications, directives and legislation such as the *National Response Plan (2004), the National Incident Management System (2004), the 9/11 Commission Report (2004), The Intelligence Reform and Terrorism Prevention Act of 2004,* the Ready.gov—Ready Business Web Site (2004), *the Draft National Infrastructure Protection Plan (2005), See National Response Framework (2008).*

20. *See* Stephen M. Bainbridge, *The Business Judgment Rule as Abstention Doctrine,* (UCLA School of Law, Law and Econ. Research Paper No. 03-18, 2003), http://ssrn.com/abstract=429260, *citing e.g.*, Sinclair Oil Corp. v. Levien, 280 A.2d 717 (Del. 1971) (fiduciary duties of controlling shareholder); Shlensky v. Wrigley, 237 N.E.2d 776 (Ill. App. 1868) (operational decision)*; see also* Douglas M. Branson, *The Rule that Isn't a Rule - the Business Judgment Rule,* 36 VAL. U. L. REV. 631 (2002), http://ssrn.com/abstract=346080; Lynn A. Stout, *In Praise of Procedure: An Economic and Behavioral Defense of Smith v. Van Gorkom and the Business Judgment Rule,* 96 NW U. L. REV. (2002), http://ssrn.com/abstract=290938; Lyman Johnson, *Corporate Officers and the Business Judgment Rule,* 60 BUS. LAW. (2005), http://ssrn.com/abstract=711122; Robert Sprague & Aaron J. Lyttle, *Shareholder Primacy and the Business Judgment Rule: Arguments for Expanded Corporate Democracy,* 16 STAN. J. L. BUS. & FIN. 1 (2011), http://ssrn.com/abstract=1647002.

21. 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."). While more than half of all publicly-owned United States corporations are chartered under the laws of the state of Delaware, corporate counsel and directors will want to closely examine the laws of relevant states when considering any particular matter; *see also* Gilson & Kraakman, *Delaware's Intermediate Standard for Defensive Tactics: Is There Substance to Proportionality Review?,* 44 BUS. LAW 247, 248 (Feb. 1989) ("Delaware corporate law . . . governs the largest proportion of the largest business transactions in history"); Lawrence J. Trautman, *Who Sits on Texas Corporate Boards? Texas Corporate Directors: Who They Are and What They Do,* 16 HOUS. BUS. & TAX L.J. 44 (2016) (describing the experience and demographics of corporate

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."[22] Under Delaware law, directors owe their corporation and shareholders fiduciary duties of care and loyalty.[23] Glassman et al. warn that "Corporate crises come in many varieties. Some have internal causes; some result from external events. There are examples of these crises in newspapers almost daily. However, when a crisis hits, the Board cannot rely on routine processes."[24] Discussing "The Role of Corporate Directors in Dealing with Corporate Crises" a panel including former SEC commissioners and seasoned legal experts note that "External events or pressures can cause a crisis . . . cyber-attacks can seriously disrupt or harm a business. A weather event, such as hurricane Sandy can cause acute unexpected problems. A significant shareholder activist, hostile takeover, or proxy fight could be seen as a crisis as well."[25] In all cases of corporate crisis, "[w]hatever the cause, the Board is expected to act quickly and effectively to mitigate the damage to the

directors in Texas), http://ssrn.com/abstract=2493569; Stephen M. Bainbridge, *Why a Board? Group Decisionmaking in Corporate Governance,* 55 VAND. L. REV. 1 (2002), http://ssrn.com/abstract=266683; Lawrence J. Trautman, *Corporate Boardroom Diversity: Why Are We Still Talking About This?*, 17 THE SCHOLAR: ST. MARY'S LAW REVIEW ON RACE AND SOCIAL JUSTICE 219 (2015), http://www.ssrn.com/abstract=2047750.

22. *See* Lawrence J. Trautman & Kara Altenbaumer-Price, *The Board's Responsibility for Information Technology Governance,* 29 J. MARSHALL J. COMPUTER & INFO. L. 313 (2011), *citing* Unitrin, Inc. v. Am. Gen. Corp., 651 A.2d 1361, 1373 (Del. 1995) (*quoting* Aronson v. Lewis, 473 A.2d 75 (Del. 1992); *see also* Robert J. Rhee, *The Tort Foundation of Duty of Care and Business Judgment*, 88 NOTRE DAME L. REV. 1139 (2013), http://ssrn.com/abstract=2261708; Sean J. Griffith, *Good Faith Business Judgment: A Theory of Rhetoric in Corporate Law Jurisprudence*, 55 DUKE L.J. 1 (2005), http://ssrn.com/abstract=728431.

23. *See* Trautman & Altenbaumer-Price, *supra* note 22, at 313, *citing* Smith v. Van Gorkom, 488 A.2d 858 (Del.Supr. 1985); *see generally* Stephen M. Bainbridge, Star Lopez & Benjamin Oklan, *The Convergence of Good Faith and Oversight* (UCLA School of Law, Law-Econ Research Paper No. 07-09, 2007), http://ssrn.com/abstract=1006097; Julian Velasco, *How Many Fiduciary Duties Are There in Corporate Law?*, 83 S. CAL. L. REV. 1213 (2010), http://ssrn.com/abstract=1457804; Bernard S. Black, *The Core Fiduciary Duties of Outside Directors,* ASIA BUS. L. REV. 3 (2001), http://ssrn.com/abstract=270749; *but see* William T. Allen, *Modern Corporate Governance and the Erosion of the Business Judgment Rule in Delaware Corporate Law* (CLPE Research Paper No. 06/2008, 2008), http://ssrn.com/abstract=1105591; Stuart R. Cohn, *Demise of the Director's Duty of Care: Judicial Avoidance of Standards and Sanctions Through the Business Judgment Rule*, 62 TEX. L. REV. 591 (1983), http://ssrn.com/abstract=2147199; Eric J. Pan, *Rethinking the Board's Duty to Monitor: A Critical Assessment of the Delaware Doctrine*, 38 FLA. ST. U. L. REV. 1 (2011), http://ssrn.com/abstract=1593332; Bernard S. Black, Brian R. Cheffins & Michael Klausner, *Outside Director Liability*, 58 STAN. L. REV. 1055 (2006), http://ssrn.com/abstract=894921.

24. Cynthia Glassman, Alan Beller, John Olson, Lawrence J. Trautman & Laura Unger, *The Role of Corporate Directors In a Crisis, Denit Trust Challenges in Corporate Governance Series*, GEORGE WASHINGTON UNIVERSITY SCHOOL OF BUSINESS, Oct. 21, 2013, http://business.gwu.edu/about-us/research/institute-for-corporate-responsibility/the-series-on-corporate-governance/#Q7 (last viewed June 5, 2017).

25. *Id.*

company."[26] It is the key duties of corporate directors—the duty of care, duty of loyalty, and duty of good faith that represent the foundation of corporate governance.

Duty of Care

Every director's legal duty of care requires a careful, diligent approach to the effective discharge of their individual duties and responsibilities. Professors Lyman P.Q. Johnson and Mark Sides note that,

> [T]he 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 . . .
>
> The duty of due care arises in both the discrete decision-making context *and in the oversight and monitoring areas [our emphasis added]* . . . In the decision-making-setting—whether it involves directors making a routine business decision or responding to a high-stakes unsolicited bid for corporate control—the duty of care inquiry clearly focuses on a board's 'decision-making process.'[27] Directors in that setting are under an obligation to obtain and act with due care on all material information reasonably available.[28]

26. *Id.*

27. *See* Trautman & Altenbaumer-Price, *supra* note 22, at 313, *citing* Lyman P.Q. Johnson and 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.").

28. *See* Trautman & Altenbaumer-Price, *supra* note 22, at n.231, *citing* Paramount Communications, Inc. v. QVC Network, Inc., 637 A.2d 34, 48 (Del. 1994); *see also* Donald C. Langevoort, *Internal Controls After Sarbanes-Oxley: Revisiting Corporate Law's Duty of Care as Responsibility for Systems*, 31 J. CORP. L. 949 (2006), http://scholarship.law.georgetown.edu/facpub/144/; Christopher M. Bruner, *Is the Corporate Director's Duty of Care a 'Fiduciary' Duty? Does It Matter?,* 48 WAKE FOREST L. REV. 1027 (2013), http://ssrn.com/abstract=2358616; William T. Allen, Jack B. Jacobs & Leo E. Strine, *Realigning the Standard of Review of Director Due Care with Delaware Public Policy: A Critique of Van Gorkom and its Progeny as a Standard of Review Problem,* 96 NW. U. L. REV. 449 (2002), http://ssrn.com/abstract=2529133; Lynn A. Stout & Margaret M. Blair, *Trust, Trustworthiness, and the Behavioral Foundations of Corporate Law,* 149 U. PA. L. REV. 1735 (2001), http://ssrn.com/abstract=241403; Robert J. Rhee, *The Tort Foundation of Duty of Care and Business Judgment,* 88 NOTRE DAME L. REV. 1139 (2013), http://ssrn.com/abstract=2261708; Lucian A. Bebchuk et al., *Director Liability,* 31 DEL. J. CORP. L. 1011 (2006), http://ssrn.com/abstract=946021.

Arising in a takeover context, the Delaware Supreme Court found in the landmark 1985 case of *Smith v. Van Gorkom*,[29] that the experienced and sophisticated directors[30] of Trans Union Corporation were not entitled to the protection of the business judgment rule[31] 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."[32] Before the decision involving the Trans Union board, absent accompanying disloyal acts, it was generally accepted that "courts had rarely found individual directors liable for breaching their duty of care."[33] The Business Roundtable says of the September 11th terrorist attacks that,

> According to Judge Alvin Hellerstein, who administered the lawsuits resulting from the attacks, principles of 'duty of care' and

29. Smith v. Van Gorkom, 488 A.2d 858 (Del. 1985); *see also* Trautman & Altenbaumer-Price, *supra* note 23; *see also* Steven A. Ramirez, *The Chaos of Smith*, 45 WASHBURN L.J. 343 (2006), http://ssrn.com/abstract=1018110; Stephen J. Lubben & Alana J. Darnell, *Delaware's Duty of Care*, 31 DEL. J. CORP. L. 589 (2006), http://ssrn.com/abstract=706481; Cheryl Lyn Wade, *What Independent Directors Should Expect from Inside Directors: Smith v. Van Gorkom as a Guide to Intra-Firm Governance*, 45 WASHBURN L.J. 367 (2006), http://ssrn.com/abstract=888812; Lawrence A. Hamermesh, *Twenty Years after Smith v. Van Gorkom: An Essay on the Limits of Civil Liability of Corporate Directors and the Role of Shareholder Inspection Rights*, 45 WASHBURN L.J. 283 (2006), http://ssrn.com/abstract=1122390; Stephen M. Bainbridge, *Smith v. Van Gorkom* (UCLA School of Law, Law-Econ Research Paper No. 08-13, 2008) http://ssrn.com/abstract=1130972; Bernard S. Sharfman, *The Enduring Legacy of Smith v. Van Gorkom,* 33 DEL. J. CORP. L. 287 (2008), http://ssrn.com/abstract=1059962; Bernard S. Sharfman, *Being Informed Does Matter: Fine Tuning Gross Negligence Twenty Plus Years after Van Gorkom*, 62 BUS. LAW. 135 (2006), http://ssrn.com/abstract=914583.

30. *See* Trautman & Altenbaumer-Price, *supra* note 22, at 313, *citing* Peter V. Letsou, *Cases and Materials on Corporate Mergers and Acquisitions* at 643 n.21 (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.").

31. Van Gorkom, 488 A.2d at 888.

32. Letsou, *supra* note 30, at 644.

33. *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 selfdealing is a search for a very small number of needles in a very large haystack.'"); 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).

> 'foreseeable risk' were forever altered by the tragic attacks. For example, according to Judge Hellerstein: 'Defendants argue that the ground victims lost their lives and suffered injuries from an event that was not reasonably foreseeable, for terrorists had not previously used a hijacked airplane as a suicidal weapon to destroy buildings and murder thousands.' He continued, 'Defendants contend that because the events of September 11 were not within the reasonably foreseeable risks, any duty of care that they would owe to ground victims generally should not extend to the victims of September 11.[34] According to the Court's decision, however, corporate leaders now also must adopt strategies to manage widespread infrastructure disruptions and crises resulting from previously unforeseeable terrorist attacks or nonmalicious infrastructure failures.[35]

Duty of Good Faith

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."[36] Professor Janet E. Kerr, writing during 2005, observes that "because the duty of good faith has not been clearly defined nor fully developed, its definition and application are being driven by numerous forces."[37] Moreover, 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.[38] *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 "due

34. *See* Business Roundtable, *supra* note 8, at 1*, citing* In re September 11 Litigation, United States District Court, S.D.N.Y., Opinion and Order Denying Defendants' Motion to Dismiss, Judge Alvin K. Hellerstein, page 15 (Sept. 9, 2003), reprinted at http://www.nysd.uscourts.gov/sept11/21MC 97_Motions_to_Dismiss_90903.pfd/.

35. *See* Business Roundtable, *supra* note 8, at 81.

36. *See id.* at n.45; *see also* Leo E. Strine, Lawrence A. Hamermesh, R. Franklin Balotti & Jeffrey M. Gorris, *Loyalty's Core Demand: The Defining Role of Good Faith in Corporation Law,* 93 GEO. L.J. 629 (2010), http://ssrn.com/abstract=1349971; Sean J. Griffith, *Good Faith Business Judgment: A Theory of Rhetoric in Corporate Law Jurisprudence,* 55 DUKE L.J. (2005), http://ssrn.com/abstract=728431; Melvin A. Eisenberg, *The Duty of Good Faith in Corporate Law*, 31 DEL. J. CORP. L. 1 (2005), http://ssrn.com/abstract=899212.

37. Janet E. Kerr, *Developments in Corporate Governance: The Duty of Good Faith and Its Impact on Director Conduct,* 13 GEO. MASON L. REV. 1037 (2005-06).

38. *See* Kerr, *supra* note 37, at 1038*; see also* Hillary A. Sale, *Delaware's Good Faith,* 89 CORNELL L. REV. 456 (2004), http://ssrn.com/abstract=456060.

care, good faith, and loyalty."[39] Professor Kerr continues, "recognizing that directors have a fiduciary duty to manage a corporation with good faith in the best interests of all its shareholders and of the long-term health of the corporation, the court opined that whether directors have acted in good faith is a question of fact."[40] Moreover,

> Whether 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.[41]

Delaware Chief Justice E. Norman Veasey observes, "failure to follow the minimum . . . evolving standards of director conduct . . . Sarbanes-Oxley . . . NYSE or NASDAQ Rules (when . . . [SEC] approved) 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."[42] Moreover,

> The 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

39. Kerr, *supra* note 37, at 1045, *citing* Stockbridge v. Gemini Air Cargo, Inc., 611 S.E.2d 600, 606 (2005) (quoting Malone v. Brincat, 722 A.2d 5, 10 (Del. 1998)).

40. *See* Kerr, *supra* note 37, at 1046, *citing Stockbridge*, 611 S.E. 2d at 605.

41. Kerr, *supra* note 37, at 1051.

42. *See* E. Norman Veasey, *Policy and Legal Overview of Best Corporate Governance Principles*, 56 SMU L. REV. 2135, 2141 (2003).

> motivations to be certain that they are honest and not disingenuous or reckless.[43]

Public Policy Considerations

From a public-policy perspective, Professor Gregory Scott Crespi notes that the rationales offered supporting application of the business judgment rule to evaluate director conduct may generally be grouped "into three broad categories: 1) avoiding undue judicial encroachment into business decisions, 2) preserving the central role of the board of directors in corporate governance, and 3) encouraging directors to serve and take appropriate risks."[44] A director's ability to rely on the *business judgment rule* for protection against liability for good faith actions taken will depend on successful demonstration (documentation) of appropriate consideration of risks to the corporation. Hamilton observes that

> [W]hether a judge or jury considering the matter after the fact, believes a decision substantially 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 an objective evaluation of the decision—would expose directors to substantive second quessing by ill-equipped judges or juries, which would, in the long run, be injurious to investor interests. Thus, the business judgment rule is process oriented and informed by a deep respect for all good faith board decisions.[45]

43. *Id.*; *see also* Christine Hurt, *The Duty to Manage Risk*, J. OF CORP. L. 253 (August 3, 2013), http://ssrn.com/abstract=2308007; Robert T. Miller, *Oversight Liability for Risk Management Failures at Financial Firms*, 84 S. CAL. L. REV. 47 (2011), http://ssrn.com/abstract=1739881.

44. Gregory Scott Crespi, *Should the Business Judgment Rule Apply to Corporate Officers, and Does it Matter?*, 31 OKLA. CITY U. L. REV. 237, 244 (2006) (*citing* Lyman P. Q. Johnson, *Corporate Officers and the Business Judgment Rule,* 60 BUS. LAW. 215, 440, 453 (2005)).

45. Robert W. Hamilton, CORPORATIONS INCLUDING PARTNERSHIPS AND LIMITED LIABILITY COMPANIES: CASES AND MATERIALS 787 (7th ed. 2001), noting [By the Court] the vocabulary of negligence while often employed, e.g., *Aronson v. Lewis,* Del. Supr., 473 A.2d 805 (1984), is not well-suited to judicial review of board attentiveness; *see, e.g.,* Joy v. North, 692 F.2d 880, 885–86 (2d Cir. 1982), especially if one attempts to look to the substance of the decision as any evidence of possible 'negligence.' Where review of board functioning is involved, courts leave behind as a relevant point of reference the decisions of the hypothetical 'reasonable person', who typically supplies the test for negligence liability; *see also* Veasey & Seitz, *The Business Judgment Rule in the Revised Model Act,* 63 TEX. L. REV. 1483 (1985).

Duty of Care and Board Responsibility During Crisis

Much as a board will plan for known and/or probable risks, best practice will include a demonstrated and documented pattern of diligent inquiry into foreseeable risks which may result in catastrophic disasters. Contingency plans should be developed for each scenario. The *Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System,* drafted by the Federal Reserve Bank of New York, and published by The Federal Reserve Board, the Office of the Comptroller of the Currency (OCC) and the Securities and Exchange Commission, states that "Boards of Directors should review business continuity strategies to ensure that plans are consistent with the firm's overall business objectives, risk management strategies, and financial resources. Decisions about overall business continuity objectives should not be left to the discretion of individual business units."[46] Specific thoughts about what to do when crisis strikes are provided in the pages to follow.

III. COMMITMENT AT THE TOP

"Developing crisis management, business continuity and disaster recovery programs and then training and testing employees require significant executive time and can emotionally tax a company's workforce. Without direct CEO involvement, crisis planning and recovery programs might not be elevated to a high enough level across the corporation," observes the Business Roundtable.[47] To be effective, organizational crisis planning must have the commitment of all the major players in the corporate drama. Shaw and Harrald observe, "Absent top-level recognition, support, and coordination, these functions may receive minimal or even no attention. Even when recognized and supported, they may be implemented and managed in a non-integrated manner with dispersed authority and responsibility."[48] In discussing the challenges facing every board and CEO, the Business Roundtable observes,

> CEO leadership is essential to improving the resilience of key corporate assets. Physical security is no longer solely a function of securing the perimeter with 'guns, guards and gates.' Companies, at a minimum, already have considered and deployed new layers of physical protection around their most critical facilities, often expanding the corporate perimeter, adding new guard enhancements and building more robust identity checks. But there are limits to such physical security measures … Companies with assets scattered

46. Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System, SEC Release No. 34-47638 (Apr. 7, 2003), http://www.sec.gov/news/studies/34-47638.htm.

47. Business Roundtable, *supra* note 8, at 86.

48. *See* Shaw & Harrald, *supra* note 16, at 2.

> across many countries also must contend with security risks far from corporate headquarters. Working with foreign law enforcement officials, understanding cross-border risks and integrating corporate solutions around the globe may require companies to acquire the negotiating skills of State Department diplomats.[49]

Importance of Enterprise Risk Management

Professor Michelle Harner describes Enterprise Risk Management (ERM) as "a holistic approach to risk management that goes beyond financial risk modeling and seeks to integrate a firm's risk assessment and response practices . . . The goal of risk management should not be the elimination of all risk but rather the pursuit of prudent and informed risk profiling and decision making."[50] Federal Reserve Bank Governor Susan Bies contends that a thoughtfully constructed ERM "process can help . . . provid[e] a framework within which managers can explicitly consider how the organization's risk exposures are changing, determine the amount of risk they are willing to accept, and ensure that they have the appropriate risk mitigants and controls in place to limit risks to targeted levels.[51] Governor Bies observes,

> Of course, ERM is a fairly broad topic, one that can mean different things to different people… I will define ERM as a process that enables management to deal effectively with uncertainty and the associated risk and opportunity, enhancing the capacity to build stakeholder value. Borrowing from ERM literature . . . ERM includes:
>
> - Aligning the entity's risk appetite and strategies;
> - Enhancing the rigor of the entity's risk-response decisions;
> - Reducing the frequency and severity of operational surprises and losses;
> - Identifying and managing multiple and cross-enterprise risks;
> - Proactively seizing on the opportunities presented to the entity; and
> - Improving the effectiveness of the entity's capital deployment.[52]

49. *See* Business Roundtable, *supra* note 8, at 31.

50. *See* Michelle M. Harner, *Barriers to Effective Risk Management*, 40 SETON HALL L. REV. 1323, 1325 (2010), http://ssrn.com/abstract=1621793, *citing* COMM. OF SPONSORING ORGS. OF THE TREADWAY COMM'N (COSO), Enterprise Risk Management–Integrated Framework: Executive Summary (2004) (describing ERM framework).

51. Susan Bies, Governor, U.S. Federal Reserve System, Speech at the National Credit Union Administration 2007 Risk Management Summit: Enterprise Risk Management and Mortgage Lending (Jan. 11, 2007), http://www.federalreserve.gov/newsevents/speech/bies20070111a.htm.

52. Bies, *supra* note 51.

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) is a private sector initiative, jointly sponsored and funded by the American Accounting Association (AAA); American Institute of Certified Public Accountants (AICPA); Financial Executives International (FEI); Institute of Management Accountants (IMA); and The Institute of Internal Auditors (IIA).[53] ERM recognizes that "in the business context, the concept of risk includes not only the probability of loss but also the consequences of that loss or risk event. Managing quantifiable risk is a much easier task than considering unquantifiable risk."[54] Many commentators including COSO "stress the importance of the board's and senior management's role in ERM. Under this framework, the board and senior management are critical in creating a risk culture at the firm–i.e., a culture that values and rewards meaningful assessment and communications regarding risk events."[55] Professor Harner observes that

> The design and implementation of ERM, is firm-specific, but generally involves the board of directors and senior management first mapping the firm's business strategies and risks. Developing an understanding of the linkages between top risk exposures and key strategies and objectives can help both management and risk oversight by identifying where risks are overlapping with an individual strategy and where certain risks may affect multiple strategies.[56]

"Pinpointing a company's most strategic vulnerabilities is a board-level challenge and worthy of a CEO's time and attention."[57] In analyzing global security issues, questions arise such as "Which countries offer the safest and most secure infrastructure for partnering or expanding operations? How should global companies prioritize competing demands for capital protection? And how should companies implement geographic redundancy for key assets and employees?"[58] Increased enforcement focus of the Foreign Corrupt Practices Act ("FCPA") can also result in an expensive and prolonged crisis for the unwary.[59]

53. *See About Us,* COMM. OF SPONSORING ORG.S OF THE TREADWAY COMM'N (COSO), http://www.coso.org/aboutus.htm (last viewed June 5, 2017).

54. *See* Harner, *supra* note 50, at 1329, *citing* Aswath Damodaran, *Risk Management: A Corporate Governance Manual* (2010), http://ssrn.com/abstract=1681017.

55. *Id.* at 1332.

56. *Id.* at 1333.

57. *See* Business Roundtable, *supra* note 8, at 5.

58. *Id.*

59. *See* Lawrence J. Trautman & Kara Altenbaumer-Price, *The Foreign Corrupt Practices Act: Minefield for Directors,* 6 VA. L. & BUS. REV. 145 (2011); Lawrence J. Trautman, *Who Qualifies as an Audit Committee Financial Expert Under SEC Regulations and NYSE Rules?*, 11 DEPAUL BUS. & COM. L.J. 205 (2013).

Success rarely happens out of the blue, it is planned-for and requires enlightened management and a board that is willing to take on the hard work required to achieve success. When the unexpected, enterprise-threatening crisis strikes, it is too late to begin the planning process. Events will quickly spin out of control, further adding to the loss of reputation and avoidable costs necessary to survive and recover with minimal damage. Like succession planning, disaster planning should be viewed as a fundamental responsibility of the board and top management. The Business Roundtable notes, "Government and industry leaders alike are grappling with a host of difficult security questions:

- How can CEOs best create a security philosophy that permeates the corporate culture?
- How should the most important management activities be prioritized?
- How should traditional business functions be restructured and integrated across traditional corporate functions?
- On what specific risks should CEOs focus their attention?
- Where and how should strategic management processes be deployed?
- How should success and failure be measured?
- How should scarce resources be apportioned?
- How should effective leadership be provided as the nature of terrorist threats evolves?[60]

First: Recognize You Are In A Crisis

Harvard professor, former Medtronic CEO and veteran corporate director Bill George says, "Crises often start out in relatively benign ways, and then seemingly minor events escalate into major ones. Unless leaders face reality early, they can easily miss the signals of the deeper crisis that is waiting ahead. Until its leaders acknowledge the crisis, their organizations cannot address the difficulties."[61]

An analysis of leadership behavior during many crisis situations indicate a pattern of simply not acting quickly enough. This could be the result of a human tendency to procrastinate but perhaps there is another explanation. Professor George proposes that, "Many people find reality is just too horrible to face or they are too ashamed, so denial becomes a convenient defense mechanism. If you feel yourself getting defensive, ask yourself, 'What am I defending against? How might denying reality make the situation worse?"[62]

60. *See* Business Roundtable, *supra* note 8, at 5.
61. *See* BILL GEORGE, 7 LESSONS FOR LEADING IN CRISIS 22, Josey-Bass (2009).
62. *Id.*

Role of Audit and/or Risk Committee

The board's role in risk management continues to be among the most important topics in corporate governance.[63] "All directors need to understand those specific risks their company faces and ensure that management has taken ownership of these risk threats."[64] Just as the Audit Committee conducts an inquiry into material weaknesses of financial controls, it seems prudent to assign the monitoring of the existence and the adequacy of a formalized crisis plan to either the board's Audit or Risk Management committee. I am indebted to Rene M. Stulz for a 'typology of risk management," wherein,

> [T]he way we describe the role of risk management suggests important ways in which risk management can go wrong… Let's assume, for now, that the right measure is used given the situation of the firm. Two types of mistakes can be made in measuring risk: known risks can be mismeasured and some risks can be ignored, either because they are unknown or viewed as not material. Once risks are measured, they have to be communicated to the firm's leadership. A failure in communicating risk to management is a risk management failure as well. After management decides what kind of risks to take, risk management has to make sure that the firm takes these risks. In other words, risk managers must manage the firm's risk, a task that may involve identifying appropriate risk mitigating actions, hedging some risks, and rejecting some proposed trades or projects. Lastly, a firm's risk managers may fail to use appropriate risk metrics. With this perspective, there are six types of risk management failures:
>
> 1. Mismeasurement of known risks.
> 2. Failure to take risks into account.
> 3. Failure in communicating the risks to top management.
> 4. Failure in monitoring risks.
> 5. Failure in managing risks.
> 6. Failure to use appropriate risk metrics…
>
> There is little hope for statistical risk models relying on historical data to capture such complicated situations. Rather, a firm has to augment these models with scenario analysis that investigates how crises can unfold and how they will affect it under various assumptions about how it reacts to the crisis. With such scenarios

63. *See* Lawrence J. Trautman, *The Matrix: The Board's Responsibility for Director Selection and Recruitment,* 11 FL. ST. U. BUS. REV. 75 (2012), http://www.ssrn.com/abstract=1998489; Lawrence J. Trautman & Kara Altenbaumer-Price, *D&O Insurance: A Primer*, 1 AM. U. BUS. L. REV. 337 (2012), http://www.ssrn.com/abstract=1998080.

64. D&O Insurance, *supra* note 63, at 116.

> in hand, top management can then understand how crises can endanger [them] and… how to manage risks before they occur so that they can survive them. Such a scenario approach requires economic and financial analysis. It cannot be done by risk management departments populated by physicists and mathematicians. Such an approach also cannot be successful unless top management believes that the scenarios considered represent legitimate threats . . .[65]

Good business practice and common sense seem to dictate that a periodic review be made of your crisis plan along with discussion by the entire board. Following highly publicized disasters of any type, such as the 2011 Japanese tsunami, a review of your exposure and planning for similar crises seems prudent. It is likely your shareholders will want answers to these questions.

Corporate Culture: Value of Openness and Candor

Professor George observes that "[w]ithout a culture of openness and candor, leaders are highly vulnerable to missing the signals of big problems ahead. By the time they acknowledge how deep their problems are—or outsiders like government agencies, consumer watchdog groups, or the media do it for them—it is too late."[66] Professor George continues,

> Why aren't there more truth tellers in organizations? The reason is that they are afraid of getting in trouble with a boss who won't accept bad news. Leaders who are approached by a bearer of bad news may wind up shooting the messenger, because reality is just too painful to face. Look at what happened to Enron's Sharron Watkins when she took her concerns about financial misstatements to chairman Ken Lay. She was not only rebuffed but ostracized within the firm. No wonder many employees hesitate to tell the truth to their bosses . . .
>
> I used to tell people at Medtronic, '[y]ou'll never get fired for having a problem, but you will get fired for covering one up. Integrity is not the absence of lying. Rather, it is telling the whole truth, so that we can gather together the best people in the company to solve the problem.
>
> It is important to publicly express appreciation to the truth tellers so others in your organization will follow suit. Only with a culture of

65. *See* Rene M. Stulz, *Risk Management Failures: What are They and When do They Happen? (Charles A. Dice Center Working Paper No. 2008-18)*, Fisher Coll. of Bus. Working Paper No. 2008-03-017, (2008), http://ssrn.com/abstract=1278073.

66. *See* George, *supra* note 61, at 22.

> candor and openness can organizations cope with crises and act in unison to get on top of them.[67]

IV. JAPANESE EARTHQUAKE AND TSUNAMI OF 2011

Tragedy Strikes

On March 11, 2011, a huge 9.0 magnitude earthquake and subsequent tsunami, estimated at 45 feet, hit the Fukushima nuclear power generating plant in northeast Japan, resulting in the release of radiation into the nearby soil, air and sea. "The twin catastrophes wiped out the normal power and backup generators of nearly all the plant's six reactors and also damaged roads and communications lines through which the plants could seek help."[68] This tragedy resulted in over 11,500 dead, more than 16,400 unaccounted for, and more than 200,000 people were moved to relief shelters soon after the disaster.[69] One year after becoming president of Japanese technology conglomerate Fujitsu Ltd., Masami Yamamoto observed, "I never experienced World War II myself, but I think this is the biggest crisis for Japan since the War."[70]

Global Impact

Almost immediately, global supply chain disruptions became apparent across many industry sectors; including, "quake related shortages of silicon wafers, liquid-crystal display screens, chips, high strength steel and chemicals [which] will affect the auto industry."[71] For example,

> One part emerging as a big problem goes into mass airflow sensors. Made by Hitachi Automotive Systems . . . at a plant north of Tokyo that was damaged by the quake and remains shut down, the electronic part is used by about a dozen auto makers.

67. *Id.*; *see also* Jeffrey N. Gordon, *Governance Failures of the Enron Board and the New Information Order of Sarbanes-Oxley*, 35 U. CONN. L. REV. 1125 (2003), http://ssrn.com/abstract=391363; Marianne Jennings, *A Primer on Enron: Lessons From A Perfect Storm of Financial Reporting, Corporate Governance and Ethical Cultural Failures*, 39 CAL. W. L. REV. 163 (2003).

68 . Phred Dvorak & Peter Landers, *Japanese Plant Had Barebones Risk Plan*, WALL ST. J., Mar. 31, 2011, at A1.

69. Eric Bellman, *Quake-Induced Misery Extends to Jobs Market*, WALL ST. J., Apr. 1, 2011, at A9.

70. Juro Osawa, *Fujitsu Chief: Biggest Crisis Since War*, WALL ST. J., Apr. 4, 2011, at B1.

71. *See* Mike Ramsey & Sebastian Moffett, *Japan Parts Shortage Hits Auto Makers*, WALL ST. J., Mar. 24, 2011, at B1*; see also* Hiroyuki Kachi & Yoshio Takahashi, *Plant Closures Imperil Global Supplies*, WALL ST. J., Mar. 14, 2011, at A6.

> Hitachi, which has a 60% share of the world's market for airflow sensors, said it hopes to resume operations . . . [but] the area is suffering from water and power shortages.[72]

Almost two weeks after the quake and tsunami, "Japan's chip makers [were] gradually starting to resume operations at their factories in the northeastern part of the country after . . . the subsequent power-supply disruption forced most manufacturers in the region to halt production."[73] Production following such a disaster is often complicated by shortages of materials and power disruptions. Unique to the semiconductor manufacturing process

> Chip plants are usually designed to operate around the clock, and some of the chip manufacturing equipment is composed of so many machines that, once turned off, it can take a week to start up again. Also, every time the entire production line is started, each machine must be inspected to ensure it can operate in a stable way before being switched on again.[74]

Kureha, a relatively obscure provider of a crucial polymer needed to manufacture lithium-ion batteries, reportedly enjoys a dominant 70% global market share for the ingredient. Unfortunately, Kureha's sole manufacturing facility is in Iwaki, near the epicenter of the quake and has been closed since the disaster. Shortages of this obscure polymer reportedly may cause shortage problems for Apple's iPod and many other mobile products that use lithium polymer batteries.[75] In addition to expected higher costs for silicon wafers, the ripple effect of this Japanese disaster on U.S. manufacturers is widespread. For example, just a month following the tsunami it was reported that,

> Railroads will ferry less coal to West Coast ports, and return with fewer Japanese autos destined for car dealers . . . Consumers will feel the impact, too. Higher chip prices should push up manufacturers' costs for cellphones and home electronics. A shortage of certain made-in-Japan autos and parts, is already pushing up the prices of used cars and may delay or preclude some repairs.
>
> Some businesses, including airlines, auto makers, insurance firms, and railroads, will incur the brunt of the impact . . . Delta Airlines Inc. the largest U.S. airline in Japan, estimates its temporary pullback on daily flights to Tokyo's Haneda Airport will slice

72. *See* Ramsey & Moffett, *supra* note 71*; see also* Juro Osawa & YunHee Kim, *Silicon Wafer Supply Disrupted*, WALL ST. J., Apr. 1, 2011, at B4.

73. Juro Osawa, *Japanese Chip Makers Restart*, WALL ST. J., Mar. 24, 2011, at B2.

74. *Id.*

75. Mariko Sanchanta, *Chemical Reaction: iPod Is Short Key Material*, WALL ST. J., Mar. 29, 2011, at B1.

> between $250 million and $400 million from this years earnings . . . The Atlanta-based carrier generates about $2 billion annually, or 8% of its total revenue, from its Japanese operation.[76]

Lessons Learned

The Japanese earthquake and tsunami disaster seems to represent a scenario that illustrates the flaw in maintaining a "just in time" approach to inventory maintenance, particularly when combined with only one source for critical components. While "previous big nuclear accidents, such as those at Three Mile Island in the U.S. and Chernobyl in the former Soviet Union, resulted from poor safety standards and bad management,[77] Kazuo Sato, former head of Japan's Nuclear Safety commission during the late 1990's, observed that "[t]his one was a natural disaster— it's qualitatively different."[78] The Wall Street Journal concluded that Tokyo Electric Power Co.'s disaster plans greatly underestimated the scope of a potential accident at its Fukushima Daiichi nuclear plant,

> The disaster plans, approved by Japanese regulators, offer guidelines for responding to smaller emergencies and outline in detail how to back up key systems in case of failure. Yet the plans fail to envision the kind of worse-case scenario that befell Japan: damage so extensive that the plant couldn't respond on its own or call for help from nearby plants. There are no references to Tokyo firefighters, Japanese military forces or U.S. equipment, all of which the plant operators eventually relied upon to battle their overheating reactors . . .
>
> 'The disaster plan didn't function,' said a former Tepco executive. 'It didn't envision something this big.' . . . Critics allege Japan's regulators and operators tend to avoid talking about or preparing fuller disaster scenarios, partly to avoid scaring the public. Fukushima Daiichi's own report on its accident management protocols says: "The possibility of a severe accident occurring is so small that from an engineering standpoint, it is practically unthinkable.'
>
> Accident management plans are generally written to deal with internal plant problems and don't take into account external shocks such as a quake or terrorist attack, said Hokkaido University Prof.

76. John Shipman & Bob Tita, *Quarterly Net Will Reflect Quake*, WALL ST. J., Apr. 1, 2011, at B1.

77. Phred Dvorak & Peter Landers, *Japanese Plant Had Barebones Risk Plan*, WALL ST. J., Mar. 31, 2011, at A6.

78. *Id.*

> Kenichiro Sugiyama, who served on a government panel on nuclear accident readiness.[79]

In retrospect, the Japanese earthquake and tsunami tragedy shows "There is no such thing as overdoing it in preparing a disaster manual, said Tsuneo Futami, who was superintendent at Fukushima Daiichi from 1997 to 2000. The attitude must be that 'anything can happen tomorrow.'"[80]

Another lesson learned from this crisis is that conditions often deteriorate from the initial assessment of damage. "The Japanese government says that it now thinks that the severity of the month-long crisis at its Fukushima Daiichi nuclear power plant is on par with that of Chernobyl, raising its assessment of the accident's seriousness to the highest level by international standards."[81] Moreover,

> Japan's nuclear regulators said the plant has likely released so much radiation into the environment that it must boost the accident's severity rating on the International Nuclear Event scale to a 7 from 5 currently. That's the highest level by international standards—a level only conferred so far on the Chernobyl accident in the former Soviet Union, which struck almost exactly 25 years ago, on April 26, 1986.[82]

It would not be until 2015, when the Japanese government allowed residents to return to the area near the Fukushima nuclear plant. With the lifting of the evacuation order, it was mostly the elderly who returned. Not until April 2017, a full six years after the crisis that 105 elementary and junior high school students returned to Naraha.[83]

Regulatory Response

A common response to every catastrophe appears to be legislation and increased subsequent oversight and regulation. In the United States, significant examples of regulatory response to crisis include: securities markets reform (Securities Act of 1933)[84] and creation of the U.S. Securities and Exchange Commission (Securities Exchange Act of 1934)[85] following the great depression;

79. Dvorak & Landers, *supra* note 78, at A1-6.

80. *Id.* at A6.

81. Phred Dvorak, Juro Osawa & Yuka Hayashi, *Japanese Crisis Is Ranked Alongside Chernobyl*, WALL ST. J., Apr, 12, 2011, at A11.

82. Dvorak, Osawa & Hayashi, *supra* note 81.

83. Motoko Rich, *Six Years Later, Fukushima Has Its Children Back,* N.Y. TIMES, Apr. 23, 2017, at 12.

84. Securities Act of 1933, 15 U.S.C. § 77(a), http://sec.gov/about/laws/sa33.pdf.

85. Securities Exchange Act of 1934, 15 U.S.C. § 78(a), http://sec.gov/about/laws/sea34.pdf.

Sarbanes-Oxley[86] legislation in response to financial fraud by Enron, WorldCom; Adelphia Communications, etc.; and Dodd-Frank Financial Reform[87] in response to the 2008 financial crisis.[88] Recently, the U.S. Congress has attempted to respond to the contemporary issue of cyberattack.[89] Often, it appears that the well-intentioned legislation response results in excessive cost and undue burdens, vastly increasing the costs of doing business in a highly competitive global economy. However, it also seems that unacceptable systematic risk is only dealt with following crisis and loss of life.

The crisis at the Fukushima nuclear power generating plant has resulted in new worldwide focus on nuclear power and safety.[90] Yukio Edano, the Japanese government's top spokesman, said, "[t]he government is making the utmost efforts to tackle the nuclear issue, but we have to also sincerely respond to criticism that we

86. Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745 (2002).

87. Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, 124 Stat. 1376-2223 (2010).

88. *See* Lawrence J. Trautman, *Personal Ethics & the U.S. Financial Collapse of 2007-08* (unpublished paper), http://ssrn.com/abstract=2502124.

89. *See* Lawrence J. Trautman, *Congressional Cybersecurity Oversight: Who's Who & How It Works*, 5 J. L. & CYBER WARFARE 147 (2016), http://ssrn.com/abstract=2638448.

90. *See* Matthew L. Wald, *Assessing Fukushima Damage Without Eyes on the Inside*, N.Y. TIMES, June 18, 2014 at A4; Matthew L. Wald, *Many Nuclear Reactors Face Costly Safety Reviews Under Revised Quake Estimates*, N.Y. TIMES, Apr. 6, 2014 at Nat'l. 21; Masahiko Aoki & Geoffrey Rothwell, *A Comparative Institutional Analysis of the Fukushima Nuclear Disaster: Lessons and Policy Implications* (2012), http://ssrn.com/abstract=1940207 (identifying three shortcomings of Japanese electric utilities: (1) decision instability that can lead to system failure after a shock; (2) poor incentives to innovate; and (3) the lack of defense-in-depth strategies for accidents); Marius Hofert & Mario V. Wuthrich, *Statistical Review of Nuclear Power Accidents*, (2011), http://ssrn.com/abstract=1923008; Hrabrin Bachev & Fusao Ito, *Fukushima Nuclear Disaster – Implications for Japanese Agriculture and Food Chains* (2013), http://ssrn.com/abstract=2319767; Y.-H. Henry Chen, *Non-Nuclear, Low-Carbon, or Both? The Case of Taiwan* (USAEE Working Paper No. 2110221, 2013), http://ssrn.com/abstract=2110221; Toshio Serita & Peng Xu, *The Fukushima Nuclear Accident, Damage Compensation Resolution and Energy Stock Returns*, Address at 25th Australasian Finance and Banking Conference (Aug. 25, 2012), http://ssrn.com/abstract=2136060; Inder K. Khurana, Richard H. Pettway & K. K. Raman, *The Liability Equivalence of Unfunded Nuclear Decommissioning Costs*, 20 J. ACCT. & PUB. POL'Y 155 (2001); Ioannis Kessides, *The Future of the Nuclear Industry Reconsidered: Risks, Uncertainties, and Continued Potential* (World Bank Policy Research Working Paper No. 6112, 2012), http://ssrn.com/abstract=2096781; André Betzer, Markus Doumet & Ulf Rinne, *How Policy Changes Affect Shareholder Wealth: The Case of the Fukushima Daiichi Nuclear Disaster* (IZA Discussion Paper No. 5896, 2011), http://ssrn.com/abstract=1909376; Nicolas Boccard, *The Cost of Nuclear Electricity: France after Fukushima* (2013), http://ssrn.com/abstract=2353305; Matthew Jude Egan, *The Stewardship Claim at Los Alamos National Laboratory: Managing Hazardous Legal and Regulatory Environments* (May 15, 2008) (unpublished Ph.D. dissertation, UC Berkeley), http://ssrn.com/abstract=1803562; Charles I. Jones, *Life and Growth* (NBER Working Paper No. w17094, 2011), http://ssrn.com/abstract=1854196; Lynne Holt, Paul Sotkiewicz & Sanford V. Berg, *(When) to Build or Not to Build?: The Role of Uncertainty in Nuclear Power Expansion*, 3 TEX. J. OIL, GAS & ENERGY L. 174 (2008), http://ssrn.com/abstract=1331438; Fausto Cavallaro, *The Assessment of Nuclear Energy Costs Using a Fuzzy Approach* (2010), http://ssrn.com/abstract=1595584.

are behind the curve."[91] In the United States, a Nuclear Regulatory Commission task force was formed after the Japanese disaster and "recommended sweeping changes to the agency's regulatory approach to safety issues. It suggested the NRC skip its usual cost-benefit approach, and instead order utilities to conduct reviews of seismic safety using the latest research, and, potentially agree to costly upgrades."[92] Regulators elsewhere are also responding to the Japanese nuclear disaster; "The European Union ordered a round of 'stress tests' for natural and man-made hazards, including earthquakes."[93] Please note the legislative response and increased regulatory scrutiny following each crisis examined.

91 Mitsuru Obe & Takashi Mochizuki, *Tokyo Details Stress-Test Plan for Reactors*, WALL ST. J., July 12, 2011, at A6.

92 Rebecca Smith & Mark Maremont, *Earthquake Risks Probed At U.S. Nuclear Plants,* WALL ST. J., July 19, 2011, at A1; *see also* John S. Carroll, *Incident Reviews in High-Hazard Industries: Sensemaking and Learning under Ambiguity and Accountability*, 9 INDUS. & EVNTL. CRISIS QUARTERLY 175 (1995); John S. Carroll, J. Sterman & Alfred A. Marcus, Playing the Maintenance Game: How Mental Models Drive Organizational Decisions, in DEBATING RATIONALITY: NONRATIONAL ASPECTS OF ORGANIZATIONAL DECISION MAKING, (J. J. Halpem & R. N. Stern, eds., ILR Press, 1998); John S. Carroll, The Organizational Context for Decision Making in High-Hazard Industries, Remarks at the Annual Human Factors and Ergonomics Society (1994), Annual Meeting, in press; John S. Carroll, Organizational Learning Activities in High-Hazard Industries: The Logics Underlying Self-Analysis, 35 J. MGMT. STUDIES 699 (1998); John S. Carroll, *Safety Culture as An Ongoing Process: Culture Surveys as Opportunities for Enquiry and Change*, 12 WORK & STRESS 272 (1998); John S. Carroll et al., Learning in the Context of Incident Investigation Team Diagnoses and Organizational Decisions at Four Nuclear Power Plants, in LINKING EXPERTISE AND NATURALISTIC DECISION MAKING 349 (E. Salas & G. Klein eds., Lawrence Erlbaum, 2001); John S. Carroll & S. Hatakenaka, Driving Organizational Change in the Midst of Crisis, 42 SLOAN MGMT. REV. 70 (2001); John S. Carroll, Jenny W. Rudolph & S. Hatakenaka, S., The Difficult Hand-Over from Incident Investigation to Implementation: A Challenge for Organizational Learning, in SYSTEM SAFETY: CHALLENGES AND PITFALLS OF INTERVENTION 189 (B. Wilpert & B. Fahlbruch, eds., Pergamom, 2002); John S. Carroll, Jenny W. Rudolph & S. Hatakenaka, Learning from Experience in High-Hazard Organizations, 24 RES. ORG. BEHAV. 87 (2002); John S. Carroll, Knowledge Management in High-Hazard Industries: Accident Precursors as Practice, in ACCIDENT PRECURSOR ANALYSIS AND MANAGEMENT: REDUCING TECHNOLOGICAL RISK THROUGH DILIGENCE (J. R. Phimister, V. M. Bier, & H. C. Kunreuther, eds., Nat'l Acad. Press, 2004); Nancy Leveson et al., Systems Approaches to Safety: NASA and the Space Shuttle Disasters, in ORGANIZATION AT THE LIMIT: NASA AND THE COLUMBIA DISASTER 269 (M. Farjoun & W. Starbuck, eds., Blackwell Publishers, 2005); R. Lipshitz, G. Klein & John S. Carroll, *Introduction to the Special Issue of Naturalistic Decision Making in Organizations,* 27 ORG. STUD. 917 (2006); John S. Carroll, S. Hatakenaka & Jenny W. Rudolph, *Naturalistic Decision Making and Organizational Learning in Nuclear Power Plants: Negotiating Meaning between Managers and Problem Investigation Teams,* 27 ORG. STUD. 1037 (2006).

93 Rebecca Smith & Mark Maremont, *Earthquake Risks Probed At U.S. Nuclear Plants*, WALL ST. J., July 19, 2011, at A1.

V. DEEPWATER HORIZON DRILLING RIG DISASTER

With headquarters in London, BP p.l.c. is one of the world's most significant integrated oil and gas companies, having operations in more than 80 countries.[94] By 2008, BP reported that the Deepwater Gulf of Mexico constituted their "largest area of growth in the US."[95] During 2009, BP reported being "involved in a number of discoveries."[96] The most significant of these were in the deep water Gulf of Mexic0. BP stated, "we continue to grow our position and leverage our experience as the largest producer in the Gulf of Mexico."[97] BP's reported production of 387,000 barrels of oil per day from the Gulf of Mexico deep water region represented about 15% of BP's total daily worldwide production.[98]

Law Professor Rebecca M. Bratspies reports that, "Even before the Deepwater Horizon disaster, BP's safety record was abysmal. In a series of high profile incidents, BP's failure to invest in safety left a trail of death and destruction around the world, resulting in multiple criminal and civil sanctions."[99] In just one 2005 example, "BP's largest refinery, a 19.3-million-gallon-a-day facility in Texas City, Texas, exploded, killing fifteen workers and injuring more than 180. Federal investigators discovered more than 300 safety violations at the facility and fined the company $21.3 million."[100] Ultimately, BP paid $50 million in criminal fines, after entering a guilty plea to criminal violations of the Clean Air Act.[101] Significantly, "The Chemical Safety Board attributed the disaster to ill-advised cost-cutting that skimped on maintenance."[102]

The Cost vs. Safety Trade-off

Now, for a brief look at the economics of safety. It is reported that "the cost of leasing the Deepwater Horizon rig from Transocean was approximately $500,000 per day."[103] Unfortunately, drilling ran far behind its scheduled 51-day budget of $96 million. By the time disaster strikes on April 20, 2010, "BP and the Macondo well were almost six weeks behind schedule and more than $58 million over budget. With the Deepwater Horizon rig late for its next drilling location, delay was costing

94. BP p.l.c., Report on Form-20-F for the fiscal year ended Dec. 31, 2009, 6, https://www.sec.gov/Archives/edgar/data/313807/000095012310021364/u08439e20vf.htm#tocpage (last viewed Mar. 5, 2016).

95. *Id.* at 19.

96. *Id*.

97. *Id.* at 18.

98. *Id.* at 22.

99. *See* Bratspies, *supra* note 14, at 7.

100. *Id.* at 13.

101. Bratspies, *supra* note 14, at 13.

102. *Id.*

103. *Id.* at 8.

BP tens of millions of dollars in leasing fees alone."[104] This pattern of cost overruns and time pressure anxiety forms "the backdrop against which BP made a series of fateful decisions in the days and hours before the blowout."[105] Professor Rebecca M. Bratspies reports,

> On April 16, 2010, BP staff and Schlumberrger, an oilfield services provider acting as consultant on the well, recommended that BP triple the number of stabilizers in the well in order to avoid 'a severe gas flow potential. Noting that the design change would take ten hours, BP Team Leader, John Guide, overruled the recommendation. The well was completed without the additional stabilizers. BP finished cementing the well on April 20. Despite having flown a Schlumber crew out to the rig to perform a cement bond log test, BP opted to send them back and forgo the tests, thereby saving $128,000.
>
> Choices by the rig owner, Transocean, further compounded the risk. For at least a year, Transocean had been disabling critical warning and safety systems intended to detect gas leaks and prevent explosions, on the grounds that 'false alarms' would wake up workers. Transocean also elected to bypass a key system on the blowout preventer control panel that might have prevented the explosion by cutting off spark sources once gas got in the drill stack. Five weeks before the disaster a Transocean engineer reported seeing damage to the blowout preventer, a critical piece of safety equipment that was the rig's last line of defense against catastrophic failure. Despite having made extensive representations to regulators about the critical safety role of blowout preventers in preventing major spills, BP apparently either did not know or did not care.
>
> On the day of the explosion, a negative pressure test—a test intended to make sure no gas or oil was seeping into the well—indicated that the well was not properly sealed . . . When the test was run for the fourth time, it [finally] registered the result the team had been looking for. Rather than try to reconcile the contradictory information, the team accepted the last set of results and deemed the test satisfactory—a consequence, perhaps, of the fact that BP has no standard procedures for running the tests or for interpreting the results. Hours later, hydrocarbons entered the well-bore, a gas leak ignited, the blowout preventer failed, and the rig exploded.[106]

104. *Id.*
105. *Id.*
106. *See* Bratspies, *supra* note 14, at 8.

The Regulatory Path to Tragedy

The National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling reports that on the day of the disaster, "regulators, [had] failed to keep pace with the industrial expansion and new technology—often because of industry's resistance to more effective oversight. The result was a serious, and ultimately inexcusable, shortfall in supervision of offshore drilling that played out in the Macondo well blowout.[107]

What Have We Learned From Macondo?

Following their investigation, The National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling issued a recommendations report with conclusions that included the following:

- The explosive loss of the Macondo well could have been prevented.
- The immediate causes of the Macondo well blowout can be traced to a series of identifiable mistakes . . . that reveal such systematic failures in risk management that they place in doubt the safety culture of the entire industry.
- Deepwater energy exploration and production, particularly at the frontiers of experience, involve risks for which neither industry nor government has been adequately prepared, but for which they can and must be prepared in the future . . .
- Fundamental reform will be needed in both the structure of those in charge of regulatory oversight and their internal decision making process to ensure their political autonomy, technical expertise, and their full consideration of environmental protection concerns.
- Because regulatory oversight alone will not be sufficient to ensure adequate safety, the oil and gas industry will need to take its own, unilateral steps to increase dramatically safety throughout the industry, including self-policing mechanisms that supplement governmental enforcement . . .[108] When a failure happens at such depths, regaining control is a formidable engineering challenge—and the costs of failure, we now know, can be catastrophically high . . .[109] There are recurring themes of missed warning signals, failure to share information, and a general lack of appreciation for the risks involved. In the view of the Commission, these findings highlight the importance of organizational

107. *Deepwater*, *supra* note 1, at xii.
108. *Deepwater* Deep Water, *supra* note 1, at xii.
109. *Id.* at ix.

> culture and a consistent commitment to safety by industry, from the highest management levels on down.[110]

During 2011, months after the release of the National Commission report, the Republic of the Marshall Islands (where the Transocean rig was registered) issued its report finding that "the rigs blowout resulted from the crew's failure to react to multiple signs of trouble, but it stopped short of saying who was ultimately responsible for the incident."[111] Professor Bratspies contends that "BP knew, long before the Macondo well blew out on April 20, that it had no way to stop the leak. The company knew this when it elected not to conduct a cement bond log test… and when it chose the 'cheap but risky' method to case the well."[112] Significantly, Bratspies contends the company knew it couldn't stop the leak when, on April 9, 2010, BP,

> [C]laimed in written comments that its deep water drilling activities 'would not have an effect, cumulatively or individually, on the environment.' Worst of all, BP knew this when it assured [the U.S. Minerals Management Service (MMS)] that:
>
> > In the event of an unanticipated blowout resulting in an oil spill, it is unlikely to have an impact based on the industry wide standards for using proven equipment and technology for such responses, implementation of BP's regional oil spill response plan which addresses [sic] available equipment and personnel, techniques for containment and recovery and removal of the oil spill.[113]

Response to the Spill

The response to the oil spill was also examined by the National Commission. In its published Recommendations, the Commission stated the following,

> There were remarkable instances of dedication and heroism by individuals involved in the rescue and cleanup. Much was done well—and thanks to a combination of good luck and hard work, the worse-case scenarios did not all come to pass.
>
> But it is impossible to argue that the industry or the country was prepared for a disaster of the magnitude of the *Deepwater Horizon* oil

110. *Id.*

111. Angel Gonzalez, *New Gulf-Spill Report Points to Missed Signs,* WALL ST. J., Aug. 18, 2011, at A3.

112. *See* Bratspies, *supra* note 14, at 12.

113. *Id*.

> spill. Twenty-one years after the *Exxon Valdez* Spill in Alaska, the same blunt response technologies—boom, dispersants, and skimmers—were used, to limited effect . . . Both government and industry failed to anticipate and prevent this catastrophe, and failed again to be prepared to respond to it. If we are to make future deepwater drilling safer and more environmentally responsible, we will need to address all these deficiencies together; a piecemeal approach will surely leave us vulnerable to future crises in the communities and natural environments most exposed to offshore energy exploration and production.[114]

Need for Systematic Risk Assessment and Risk Management Tools

Another observation made by The National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling that seems to be broadly applicable to many industries is that "systematic updating of the risk assessment and risk management tools used as the basis for regulation" appears to have been missing.[115] Here, the regulator, the Minerals Management Service (MMS),

> Attempted under several administrations to promulgate regulations that would have required companies to manage all their activities and facilities, and those of their contractors, under a documented Safety and Environmental Management System (SEMS). But, in the face of industry opposition, MMS did not adopt such a requirement until September 2010, after the BP *Deepwater Horizon* disaster. Industry objections also derailed a past MMS proposal to expand data reporting requirements as a part of an effort to track and analyze offshore incidents and to identify safety trends and lagging and leading indicators. The proposal was abandoned when the Office of Management and Budget agreed with industry complaints about compliance cost (industry also complained about the potential for overlap with Coast Guard reporting requirements). As a result, there has historically been no legal requirement that industry track or report instances of uncontrolled hydrocarbon releases or "near misses"—both indicators that could point to a heightened potential for serious accidents. The United States has the highest reported rate of fatalities in offshore oil and gas drilling among its international peers, but it has the lowest reporting of injuries. This striking contrast suggests a significant under-reporting of injuries in the

114. *See Deepwater*, *supra* note 1, at ix.
115. *Deepwater*, *supra* note 1, at 3.

> United States and highlights the need for better data collection to ensure needed attention to worker safety.[116]

It seems that the lesson here is that construction and systematic updating of the risk assessment and risk management tools should not be just for regulatory purposes, but for ongoing management and board monitoring. This appears fundamental to comport with best practices in enterprise risk assessment and monitoring.

Lessons From Elsewhere Applied to Macondo

The Commission observed that "while industry had devoted billions of dollars to the technologies required for deepwater drilling, it had devoted essentially nothing to creating alternative capabilities to deal with the foreseeable consequences of a disaster."[117] Given that drilling "the Macondo well under 5,000 feet of Gulf water and then over 13,000 feet under the sea floor to the hydrocarbon reservoir"[118] is an inherently risky endeavor, what can be learned elsewhere? The Commission observed,

> Other inherently risky industries and endeavors (e.g. the United States Nuclear Navy, civilian nuclear power plant operators, and chemical manufacturers) have improved their safety culture and performance by creating self-policing organizations involved in standard-setting, auditing, exchanging best practices, training, ensuring accountability, and enforcement. The experience from offshore drilling and production activities, and knowledge of geologic and ocean conditions outside the U.S., can provide insights into potential risks and the best practices for managing them effectively.[119]

Accordingly, the Commission recommends that a new industry-run safety organization be created to work with government regulators, "to define best practices and police them, providing a mechanism for the leading companies to ensure the industry is not compromised by other enterprises with weaker safety standards and records."[120] The Commission's vision is that "[t]he safety institute's board, drawn from the top ranks of the industry, should develop both positive and negative incentives (rewards and sanctions) to help all companies operating offshore

116. *Id.*
117. *Deepwater*, *supra* note 1, at 3.
118. *Id.* at viii.
119. *Id.* at 12.
120. *Id.*

overcome the natural enemies of safety: ignorance, arrogance, and complacency."[121] Professor Joseph Karl Grant contends that

> There are times when corporate law and governance intersect with life, I love and savor these moments . . . [F]rom the 2010 BP oil spill . . . we have many lessons to learn and apply to our own lives… From the BP oil spill I gleaned five (5) basic lessons . . . First, if you lie, or are perceived to be lying, or make an inaccurate statement people will lose trust in you. Second, we are not judged based on how we act in times of comfort, but based on how we react in times of crisis. Third, the Emperor or King may be toppled. Fourth, regulators and the regulated make for strange bedfellows—we must vigilantly guard against regulatory capture. Fifth, and finally, your Big Brother or Big Sister can and will twist your arm when he or she has a chance.[122]

Regulatory Response: Accountability and Governance

Regarding accountability, The Commission recommends that "[a]udit results should be used to hold companies accountable for their performance to each other and to certain business counterparts, including joint-venture partners; suppliers; insurers; and through assurances by the companies' directors, and investors."[123] As to governance, the new industry-run safety organization "should be of, by, and for the private sector. It will need to be created by the CEOs of leading companies and run by a director with unimpeachable integrity and a record of success in process safety that will be respected by its members and accepted by the public."[124]

> But government depends upon the resources and expertise of private companies to contain a blown-out well and to respond to a massive oil spill. Both the industry and government were woefully unprepared to contain or respond to Macondo: all parties lacked adequate contingency planning, and none had invested sufficiently in research and development to improve containment or response technology… it is clear that the oil and gas industry needs to develop large-scale rescue, response, and containment capabilities—including equipment, procedures, and logistics—enabled by extensive training, including full-scale field exercises and

121. *Id.* at 14.

122. *See* Joseph Karl Grant, *What Can We Learn from the 2010 BP Oil Spill?: Five Important Corporate Law and Life Lessons,* 42 MCGEORGE L. REV. 809, 824 (2011), http://ssrn.com/abstract =1701892.

123. *Deepwater*, *supra* note 1, at 15.

124. *Id.*

> international cooperation . . . A future accident will, by definition, be unplanned and unexpected; containing its results will require the coordination of many complex activities going on simultaneously.[125]

VI. GENERAL MOTORS IGNITION SWITCH CRISIS

During 2014, it became apparent that General Motors had known about faulty ignition switches for years and engaged in an elaborate cover-up. More than 100 deaths were attributed to GM's faulty ignition switch problem by the summer of 2015.[126] Manhattan U.S. Attorney's Office head Preet Bharara believes that,

> [T]he auto industry, which had never previously faced federal criminal cases related to product defects, has long needed the threat of criminal liability to spur overdue changes. 'The first line of defense is self-policing within the company. The second is regulators,' Mr. Bharara said in a recent interview with the *Wall Street Journal*. 'When all those things have failed, prosecutors come along with the blunt hammer. That does get some attention in the Board room.[127]

One of America's largest industrial giants, during 2014, GM's worldwide sales reached 9.9 million vehicles, the largest estimated "market share in North America and South America, the number six market share in Europe and the number two market share in the Asia Pacific, Middle East and Africa region."[128] Prompted by the identification of at least 54 frontal-impact crashes, involving more than a dozen fatalities, the GM board of directors hired law firm Jenner & Block on March 10, 2014, to find out the circumstances and why the Cobalt recall took so long to accomplish.[129] The Valukas Report, written by former United States Attorney Anton R. Valukas, states that,

---

125. *Id.* at 16.

126. Christopher M. Matthews & Mike Spector, GM Likely to Face Criminal Charges, WALL ST. J., May 26, 2015 at B1. *See also* Marianne Jennings & Lawrence J. Trautman, Ethical Culture and Legal Liability: The GM Switch Crisis and Lessons in Governance, 22 B.U. J. SCI. & TECH. L. 187 (2016), http://ssrn.com/abstract=2691536 (providing a comprehensive look at GM safety lapses during almost 60 years).

127. *See* Matthews & Spector, *supra* note 126. *See also* Christopher M. Matthews & Mike Spector, *U.S. Mulls Criminal Charges For GM,* WALL ST. J., June 10, 2015 at A1.

128. General Motors Company, Report on Form 10-K for the fiscal year ended Dec. 31, 2014, https://www.sec.gov/Archives/edgar/data/1467858/000146785815000036/gm201410k.htm.

129. Anton R. Valukas, Jenner & Block, Report to Board of Directors of General Motors Company Regarding Ignition Switch Recalls, 5 (May 29, 2014) , http://www.nytimes.com/interactive/2014/06/05/business/06gm-report-doc.html; *see also* Jeff Bennett, *GM Report To Address Missteps,* WALL ST. J., Jun. 2, 2014 at B1; Bill Vlasic, *G.M. Inquiry Cites Years of Neglect Over Fatal Defect,* N.Y. TIMES(June 5, 2014), http://www.nytimes.com/2014/06/06/business/gm-ignition-switch-internal-recall-investigation-report.html?_r=0.

> GM personnel's inability to address the ignition switch problem for over 11 years is a history of failures . . . While GM heard over and over from various quarters—including customers, dealers, the press, and their own employees—that the car's ignition switch led to moving stalls, group after group and committee after committee within GM that reviewed the issue failed to take action or acted too slowly. Although everyone had responsibility to fix the problem, nobody took responsibility.[130]

At Congressional hearings on the GM ignition switch crisis, Fred Upton, Chairman of the House Committee on Energy and Commerce states that "[a] culture that allowed safety problems to fester for years will be hard to change. But if GM is going to recover and regain the public's trust, it must learn from this report and break the patterns that led to this unimaginable systemic breakdown."[131] Unlike a cultural environment that encouraged and rewarded employees for identifying problems and bringing them to the attention of management quickly, the GM work environment apparently offered "resistance or reluctance to raise issues or concerns."[132] Congressman Tim Murphy states,

> Even when a good law . . . is in place it requires people to use common sense, value a moral code, and have a motivation driven by compassion for it to be effective. Here the key people at GM seemed to lack all of these in a way that underscores that we cannot legislate common sense, mandate morality, nor litigate compassion. At some point, it's up to the culture of the company that has to go beyond paperwork and rules.
>
> The failures at GM were ones of accountability and culture. If employees do not have the moral fiber to do the right thing, and do not have the awareness to recognize when mistakes are being made, then the answer must be to change the people or change the culture.[133]

130. Valukas, *supra* note 129, at 2.

131. *The GM Ignition Switch Recall: Investigation Update: Hearing Before the Subcommittee on Oversight and Investigations,* 113th Cong. (2014) (Opening Statement of the Honorable Fred Upton, Chairman, Committee on Energy and Commerce, Subcommittee on Oversight and Investigations), http://energycommerce.house.gov/hearing/the-gm-ignition-switch-recall-investigation-update.

132. Valukas, *supra* note 129, at 252.

133. *The GM Ignition Switch Recall: Investigation Update: Hearing Before the Subcommittee on Oversight and Investigations,* 113th Cong. (2014) (Opening Statement of the Honorable Tim Murphy, Committee on Energy and Commerce, Subcommittee on Oversight and Investigations), http://docs.house.gov/meetings/IF/IF02/20140618/102345/HHRG-113-IF02-20140618-SD004.pdf.

According to Professor Rena I. Steinzor, auto producers such as GM "have grown so complacent that they view billions of dollars in civil penalties and tort damages as unfortunate but routine costs of doing business . . . the legal system fails to instill the wariness in top executives that is essential . . . to make consumer safety their top priority."[134] Another risk you may not have contemplated in business or law school, Professor Steinzor cautions that "Federal prosecutors have started to think about launching criminal probes as soon as they learn about a grave malfeasance that threatens public health, kills consumers or workers, or damages natural resources."[135]

The Department of Justice ("DOJ") announced charges on September 17, 2015 against General Motors of "concealing a potentially deadly safety defect from its U.S. regulator, the National Highway Traffic Safety Administration (NHTSA), from the Spring of 2012 through February 2014, and, in the process, misleading consumers concerning the safety of certain of GM's cars."[136] In their announcement, DOJ states that "[r]ather than move swiftly and efficiently toward recall of at least the population of cars known to be affected by the safety defect . . . GM personnel took affirmative steps to keep the company's internal investigation into airbag non-deployment caused by the defective switch . . . outside of GM's regular recall process."[137] Anthony Foxx, U.S. Department of Transportation Secretary, observed that GM "not only failed to disclose this deadly defect, but as the Department of Justice investigation shows, it actively concealed the truth from NHTSA and the public."[138] U.S. Attorney Preet Bharara of the Southern District of New York states, "[b]y doing so, GM put its customers and the driving public at serious risk. Justice requires the filing of criminal charges, detailed admissions, a significant penalty, and the appointment of a federal monitor. These measures are designed to make sure that this never happens again."[139] Special Inspector General Goldsmith Romero observes, "[t]he worst part about this tragedy is that it was entirely avoidable. GM could have significantly reduced the risk of this deadly defect by improving the key design for less than one dollar per vehicle nut GM chose not to because of the cost."[140] Historically, this type of cost-based decisions was a part of GM's culture. For example, with the Corvair of the 1960s, one of the fixes that was added too late for many were instructions inserted in the owner's manual on the importance of proper rear-end tire inflation was well as guidance on steering in the event the rear

134. *See* Rena I. Steinzor, *(Still) 'Unsafe at Any Speed': Why Not Jail for Auto Executives?*, 9 HARV. L. & POL'Y REV. 901, 904 (2015), http://ssrn.com/abstract=2616755.

135. *Id.* at 927.

136. Press Release, U.S. Department of Justice, U.S. Attorney of the Southern District of New York Announces Criminal Charges Against General Motors and Deferred Prosecution Agreement With $900 Million Forfeiture (Sept. 17, 2015), http://www.justice.gov/opa/pr/us-attorney-southern-district-new-york-announces-criminal-charges-against-general-motors-and (last viewed Mar. 5, 2016).

137. Press Release, *supra* note 136.

138. *Id.*

139. *Id.*

140. *Id.*

wheels of the Corvair happened to turn under due to under-inflation of those tires.[141] U.S. Attorney Preet Bharara announced that General Motors had entered into a deferred prosecution agreement "under which the company admits that it failed to disclose a safety defect to NHTSA and misled consumers . . . The admissions are contained in a detailed statement of facts attached to the agreement."[142] The terms of the agreement require GM to "cooperate with the federal government and establish an independent monitor to review and assess the company's policies and procedures in certain discrete areas relating to safety issues and recalls."[143] GM's announcement also states,

> [T]hat the government's decision to defer prosecution was based on the actions GM has taken to "demonstrate acceptance and acknowledgement of responsibility for its conduct, including:
> - Conducting a swift and robust internal investigation
> - Furnishing investigators with information and a continuous flow of unvarnished facts
> - Providing timely and meaningful cooperation more generally in the government's investigation
> - Terminating wrongdoers
> - Establishing a full and independent victim compensation program that is expected to pay out more than $600 million in awards.[144]

VII. FRAMEWORK FOR ANALYSIS

Conceptual Framework: Business Crisis & Continuity Management

After scouring the crisis management literature, I am indebted to Professors Gregory L. Shaw and John R. Harrald, formerly of the Institute for Crisis, Disaster and Risk Management at the George Washington University for providing "a unique conceptual framework for visualizing, organizing and linking the myriad functional areas and functions inherent in an integrated enterprise-wide business crisis and continuity management program."[145]

141. *See generally* RALPH NADER, UNSAFE AT ANY SPEED, THE DESIGNED-IN DANGERS OF THE AMERICAN AUTOMOBILE 29 (1965).

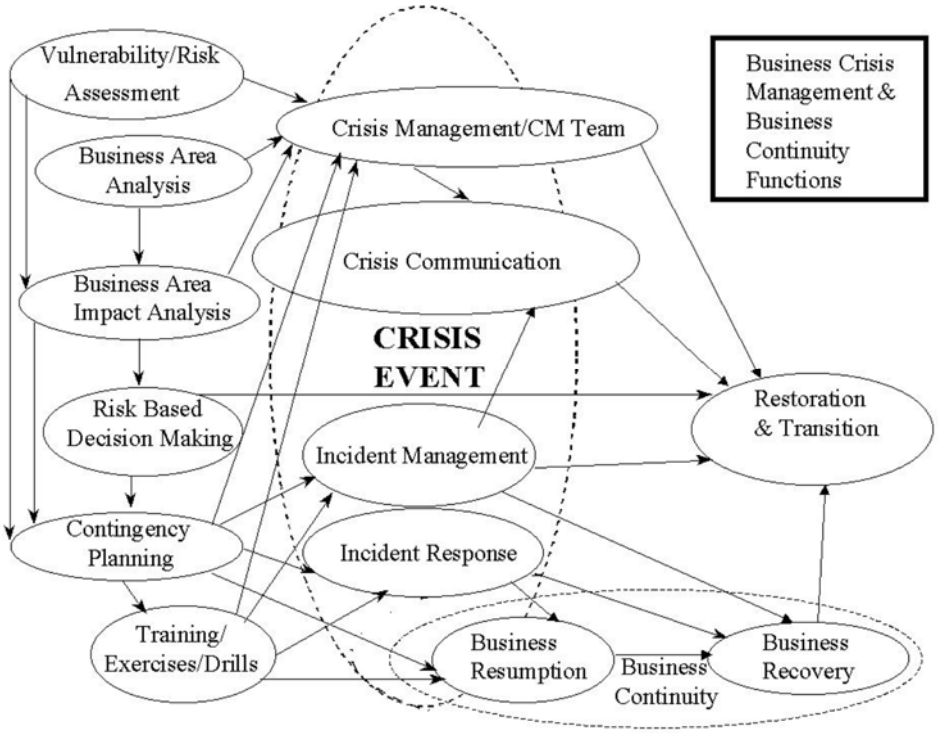
142. *See* Press Release, *supra* note 136.

143. Press Release, General Motors Co., GM Reaches Agreement With U.S. Attorney's Office (Sept. 17, 2015), http://media.gm.com/media/us/en/gm/news.detail.html/content/Pages/news/us/en/2015/sep/0917-doj.html (last viewed June 7, 2017).

144. *Id.*

145. Greg L. Shaw & John R. Harrald, *Identification of the Core Competencies Required of Executive Level Business Crisis and Continuity Managers*, 1 J. HOMELAND SEC. & EMER. MGT. 4 (2004), *citing* John R. Harrald, *A Strategic Framework for Corporate Crisis Management*, Proceeds of the International Emergency Management Society (TIEMS) Conference, 389-397 (May 1998).

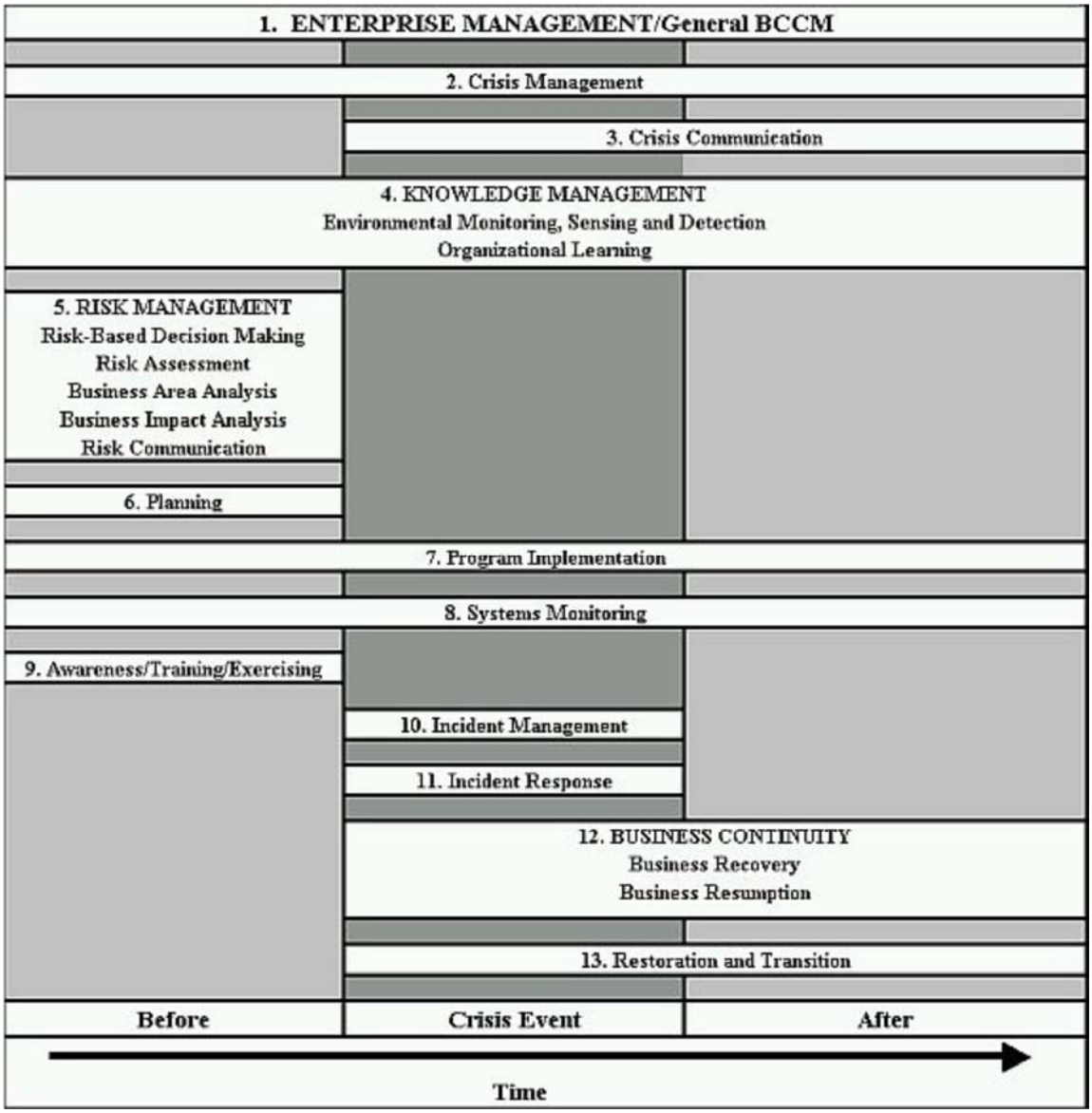
Figure 1
A Strategic Framework for Corporate Crisis Management



Drawing heavily from John R. Harrald's [Figure 1] "Crisis Management and Business Continuity,"[146] Shaw synthesized several frameworks [Figure 2] "into a single framework under which specific functional competencies were identified and analyzed. This framework displays a functional hierarchy (from top to bottom) and the temporal nature of each (from left to right)."[147]

146. *See* Shaw & Harrald, *supra* note 16, at 5.
147. *Id.*

Figure 2
Business Crisis and Continuity Management Framework



I remain indebted to Professors Shaw and Harrald for their identification and grouping of business crisis and continuity management executive level competencies depicted as Figure 3, which provides "a prioritized inventory of competencies (knowledge, skills, abilities and/or attitudes) required for an executive

to effectively manage an enterprise-wide business crisis and continuity management program."[148]

Figure 3
Enterprise Management
General Business Crisis and Continuity Management Competencies

Enterprise Management/General BCCM

1. Establish a consultative process with BCCM stakeholders.
2. Determine local, state and federal laws and regulations with BCCM implications.
3. Determine corporate governance requirements with BCCM implications.
4. Establish and lead a multidisciplinary BCCM Steering Committee.
5. Develop a business case for an overall BCCM program and supporting functions.
6. Communicate top level management's acceptance and support of the BCCM program throughout the organization and to external stakeholders.
7. Define a BCCM program structure that supports overall corporate, business unit, functional and program objectives.
8. Establish policies and procedures that incorporate BCCM considerations into the management of all business operations (existing and developing).
9. Define a measurement process and measures of effectiveness for the overall BCCM program and its component functional areas.
10. Define a BCCM program maintenance process.
11. Determine and specify the roles for internal and external (consultants) personnel in the BCCM program.
12. Incorporate BCCM roles, accountabilities, responsibilities and authority into job/position descriptions.
13. Incorporate BCCM responsibilities into the performance management and appraisal system.
14. Establish a BCCM audit program.

148. *See* Shaw & Harrald, *supra* note 16 (observing that "The resulting framework and prioritized competency inventory can assist organizations in structuring an enterprise wide business crisis and continuity management program to meet their specific requirements and provide guidelines for selection and professional development of organizational leaders with business crisis and continuity management responsibilities."). *See also* David J. Smith, Ed. *Business Continuity Management: Good Practices Guidelines,* Business Continuity Institute. London, England (2002), http://www.thebci.org.

VIII. WHEN CRISIS HITS

Needed: Credible Threat Information

A lesson learned by many who have managed their way through crisis is that initial situation information is almost always wrong. For example, Texas-based petroleum refiner Valero has sustained crisis situations brought about by several major hurricanes. James Pursell, Valero's Director of Health, Safety and Emergency Preparedness states that "one of the few things you can almost always count on as being true is that initial situation reports are almost always wrong.[149] Also subject to severe hurricane disruption is Texas-based grocer HEB. Justen R. Noakes, HEB's director of Emergency Preparedness reports encountering the same lack of initial trustworthy situation information as the crisis unfolds.[150] Multiple information channels and sources will be necessary to develop useful information. The Business Roundtable states that,

> The CEO is not typically in the business of gathering threat data. However, because of government classification rules and the structure of the U.S. intelligence community, security professionals will need to develop multiple relationships across federal and state governments to obtain such information. Moreover, security directors may be forced to make assumptions based on available threat information, which is typically incomplete. This process, although not an optimal system of information gathering, is dependent on support from senior principals. Support may take many forms, from encouraging relationships with new federal entities to recognizing the limitations of intelligence gathering as part of security decision making.[151]

The Challenge of Crisis Leadership

Professors Erika Hayes James and Lynn Perry Wooten report that "[m]any organizational leaders have a laissez faire attitude toward the possibility of a crisis happening in their firm, despite the high probability that every business leader and

149. *See* James Pursell, Dir. Health, Safety & Emergency Prep., Valero Corporation, *Crisis Management and Adversity: Opportunities for Organizational Development and Learning*, Remarks before Annual Academy of Management Meeting (Aug. 14, 2011).

150. *See* Justen R. Nokes, Dir. Of Emergency Preparedness, HEB, *Crisis Management and Adversity: Opportunities for Organizational Development and Learning*, Remarks before Annual Academy of Management Meeting (Aug. 14, 2011).

151. *See* Business Roundtable, *supra* note 8, at 35.

every organization will experience a crisis of some significance."[152] As a result, "leaders are underprepared not only for 'managing' crisis situations when they occur, but also—and more important—for leading organizations in turbulent times with a vision or expectation that they and their organizations can be positively transformed by the experience."[153] James and Wooten stress that "it is often the (mis)handling of crisis, not the crisis itself, that can have the most severe consequences, positive and negative for a firm."[154] A recent survey conducted by crisis communication experts Levick Communications and lawyers Pillsbury Winthrop discovered that "though 60 percent of survey respondents said their companies have a crisis plan in place, just 29 percent felt very confident their organization would respond effectively if a crisis occurred. Another 56 percent said they felt somewhat confident."[155] Tom Campbell, head of Pillsbury's Crisis management team, observes that "even among those companies which have developed a crisis plan, 63% report that their company does NOT conduct annual training drills or exercises to test the effectiveness of their plan and ensure that all company employees know what to do if a crisis does occur."[156] Moreover,

> Even more strikingly, fully one-third of those companies which do have a crisis plan could not recall the last time they actually reviewed or revised it, which clearly indicates an out-of-sight/out-of-mind approach to crisis management that may prove a company's undoing . . . Among the survey's key findings:
>
> - In the past three years, 42% of respondents said their company was the subject of a government inquiry or investigation, which can set up off alarm bells for shareholders, investors, customers and employees alike. 24% of respondents claim that their company had faced a natural disaster and an equal number of respondents said their company had experienced a data loss or security breach. 21% of all companies had experienced at least one worker accident or death, while nine percent reported being the target of protesters or a consumer boycott. Significantly, many survey participants experienced multiple crises over the past three years…

152. Erika Hayes James & Lynn Perry Wooten, *Leadership in Turbulent Times: Competencies for Thriving Amidst Crisis*, 2 (Darden Business School, Working Paper No. 04-04, 2004), http://ssrn.com/abstract=555966.

153. *Id*.

154. *Id*. at 3.

155. Press Release, PillsburyWinthrop Shaw Pittman LLP, Just 29% of Corporate Executives Confident of Weathering A Crisis Says Survey (Aug. 11, 2011), http://www.pillsburylaw.com/index.cfm?pageid=19&itemid=5700.

156. *Id.*

> - Following a crisis, 79% of survey respond[ents] said their companies made minor or major changes to their crisis protocol to make it more effective. Among the most popular improvements were additional training (21%) and conducting a crisis audit (18%) followed by strengthened General Counsel oversight, purchased or upgraded business interruption/liability insurance, moved crucial systems off-site, or upgraded technology security systems, all of which scored 14%. Several companies implemented more than one of these improvements.[157]

"What differentiates those firms that thrive following a crisis from those that do not is the leadership displayed throughout the process."[158] Advance preparation is essential, since

> During a crisis, CEO leadership may be needed on several levels. Employees may require one kind of support and guidance, while shareholders and investors may look to the CEO for other types of leadership. Failure to consider human resources needs in advance can impede a corporation's recovery in the event of a disaster.[159]

James and Wooten contend there is "a difference between crisis management and crisis leadership, and that what differentiates firms that thrive following a crisis from those that do not is the leadership displayed throughout the crisis management process."[160] Based upon years of previous research, James and Wooten introduce a framework of six crisis competencies extending,

> [B]eyond managing corporate communication to highlighting the notion that the best crisis leaders are those who build a foundation of trust not only within their organization, but also throughout the supply chain. These leaders then use that foundation to prepare their organizations for difficult times, to contain crises when they occur, and to leverage crisis situations as a means for creating change and, ultimately, a better organization.[161]

157. Press Release, *supra* note 155.
158. *See* James & Wooten, *supra* note 152, at 3.
159. *See* Business Roundtable, *supra* note 8, at 68.
160. *See* James & Wooten, *supra* note 152, at 2.
161. *Id*.

The Disaster Constituencies

The corporate crisis will inevitably create several groups of diverse constituencies: customers, affected communities, employees, governmental regulatory authorities, investors, media, and public opinion. Each of these discrete constituencies will demand immediate attention and likely become increasingly hostile as time passes. Customers will reconsider their loyalty to your products and services and may require reasonable assurances that you can perform to meet your contractual obligations or usual production levels. The community affected by your crisis will want assurances that you will be able to meet your obligations in a timely manner and with least negative impact (the Union Carbide Bopahl chemical disaster and BP oil spill damage to the Gulf of Mexico coastal beaches and estuaries comes to mind). During a corporate crisis, all employees will be concerned about how this will impact their personal future. Government regulatory authorities will be demanding answers and triggering investigations of their own in many cases (this may include separate or multiple municipal, state and federal regulatory agencies). Investors will demand prompt answers upon penalty of selling their positions and timely regulatory disclosures will be necessary. The care and feeding of media requires special skills and experience to minimize damage to corporate reputation. Public opinion for years to come may depend upon how well you have planned.

The Crisis Plan and Team

Crisis expert Laurence Barton observes that "some managers shine in a crisis, while others stumble. The difference between the two is often defined by preparedness, candor, rehearsal, and anticipation of the needs of stakeholders . . . having a crisis plan is likely to increase both the quality of your responsiveness and your stakeholders' perception of you."[162] The Business Roundtable notes that "security incidents nearly always involve complicated transportation challenges. Corporations should consider strategies for identifying, locating and transporting key employees to critical locations under circumstances when the usual modes of transportation may be unavailable.[163]

According to crisis communications experts Levick Communications, the seamless crisis management team should "draw on all the knowledge of the CFO, the marketing experts, investor relations, and lawyers. Their expertise must be provided to the corporate crisis communicators in publicly digestible and credible formats for public consumption. The public is always the end-user in business crisis management."[164] In addition,

162. Laurence Barton, CRISIS LEADERSHIP NOW: A REAL-WORLD GUIDE TO PREPARING FOR THREATS, DISASTER, SABOTAGE, AND SCANDAL 8 (2008).

163. *See* Business Roundtable, *supra* note 8, at 71.

164. PillsburyWinthrop Shaw Pittman LLP, Communication Tools: Crisis Management, http://www.pillsburylaw.com/crisis-management-resource-center (last viewed June 7, 2017).

> Crisis management presents an almost impossible task for many businesses, which is to respond fast enough to a sudden situation before it spins out of control while simultaneously anticipating future situations. The solution is to maintain constant dialogue among the diverse team members, drawing on their diverse skills and backgrounds. Crisis management moves forward in the same way that technology moves forward, with new tools discovered and applied every day. Business crisis management initiatives shouldn't stop moving simply because there's no immediate crisis at hand.[165]

Time is "of the Essence"

Crisis situations do not provide adequate time to pull together a committee to begin discussions about what needs to be done. The Business Roundtable recognizes that "[l]eadership on the part of corporate executives is key to making employees feel safe in the event of a disaster. Coming out early with appropriate information can prevent panic among both company employees and the public in the affected community."[166] In addition, "[h]uman resources officials should make certain that their crisis management, business continuity and disaster recovery plans will enable the company to weather the immediate emergency and recover smoothly afterward."[167] Moreover,

> Given how rapidly workforce issues can escalate during a crisis, human resource managers need to be fully integrated into strategic planning to enable the company to respond immediately. As terrorist threats increase in severity, new, more robust plans may be needed to shepherd a company's workforce through a potential disaster. Corporate officers in charge of human resources and security should consider strategies to attend to the health, welfare and safety of employees before, during and after a crisis.[168]

Role of Effective Communications

Internal communications will be critical in times of crisis to provide situational awareness as to what has happened and the extent of actual and potential damage to employees and enterprise constituencies. Understanding the facts as quickly as possible is imperative to making intelligent decisions. Effective communications will be necessary to determine "[w]hat is the situation in the various

165. *Id.*
166. *See* Business Roundtable, *supra* note 8, at 65.
167. *Id.*
168. *Id.* at 70.

locations affected by the emergency? How are employees reacting? What kinds of information and resources are needed to deal with the immediate emergency? Corporate officials should formulate emergency plans, train employees and carry out drills."[169] In particular, "[h]uman resources officials should empower employees so they will know where to go, what to do, and whom to contact during and after a disaster. It is important to give employees permission to do what they want to do, including contacting their family members and helping one another."[170]

Professional Communications Resources

Communicating with outside constituencies, the press, shareholders, government agencies (federal, state and local—for every location impacted), vendors, families of your employees, and so on, is also important. Thus, having professional public relations communications resources in place before a crisis is paramount. Levick notes, "[p]ublic relations crisis communications are as varied as the stakes themselves. It may mean a reputation is on the line. It may mean there's a lawsuit that must be won, and public perception is a key factor in the outcome. Stock values may be at risk."[171] Moreover,

> The art of public relations crisis communication (Crisis PR) demands that you know who your audiences are and how they can be most effectively reached. Is there a Congressman whose support is crucial during a crisis? If so, the local newspaper in his or her district, in Iowa or Kentucky or Arizona, may be more important than the *Washington Post* or *New York Times.* PR crisis communication at its best demands veteran practitioners with the instincts and the training to finesse such myriad media venues… Public relations crisis communication begins with personal relationships – with reporters, editors, broadcasters – but is leveraged through technology planning and grassroots campaigning.[172]

The questions to be asked include, "[a]re there independent outside parties who can credibly advance your cause? What is the role of online forums? Are there "events" that can be staged—public demonstrations, perhaps, or town meetings that will rally support for your cause or demonstrate momentum in your favor?"[173]

169. *See* Business Roundtable, *supra* note 8, at 66.
170. *Id.*
171. PillsburyWinthrop Shaw Pittman LLP, *supra* note 164.
172. *Id.*
173. PillsburyWinthrop Shaw Pittman LLP, *supra* note 164.

Disaster Scenario Practice Pays Dividends

Crisis scenario testing and training is credited with providing insightful data about program strengths and weaknesses. After the trauma of September 11, 2001, the financial services industry "initiated a significant review of lessons learned with a view towards strengthening their business continuity plans. The agencies believe that it is important for financial firms to improve recovery capabilities to address the continuing, serious risks to the U.S. financial system posed by the post-September 11 environment."[174] Many industry participants "agree that routine use or testing of back-up facilities is necessary and beneficial to ensure financial system viability. They also suggest that testing should be 'end-to-end' involving telecommunication firms, third-party service providers, and securities exchanges."[175] The Business Roundtable believes,

> The CEO must be willing to participate directly in crisis tests and training scenarios. Some companies, for example, take one day out of the year to challenge the CEO on responses to potential "corporate killer" issues. Direct CEO involvement in business continuity and disaster recovery programs is needed to heighten the level of awareness among employees. Having senior corporate officers participate in mock disaster scenarios and evacuation drills, for example, communicates the importance of these drills to the workforce, outside contractors, and others at the facility. The experience also may highlight how the CEO should alter or create governance and management teams.[176]

IX. WHAT IF MANAGEMENT IS IMPLICATED?

Every board will be well-advised to establish a special committee of the board and perhaps hire special counsel whenever it is confronted with a factual situation where management may eventually be found culpable of wrongdoing or even failure to anticipate and provide planning for contingencies in the event of a foreseeable natural disaster. During my research and writing of this article, I circulated early drafts to experts for comment. One of the most helpful responses I received was from MIT engineering professor Nancy Leveson, when she observes,

> Management is ALWAYS implicated in major accidents. I have been doing safety engineering for 35 years and have investigated and read about hundreds of accidents. In every one, management has some responsibility for the events. In some they managed to not be

174. Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System, SEC Release No. 34-47638 (Apr. 7, 2003), http://www.sec.gov/news/studies/34-47638.htm.

175. *Id.*

176. *See* Business Roundtable, *supra* note 8, at 87.

> "implicated" but that is usually due to very poor investigation efforts or efforts by management to hide their guilt.[177]

The Institute for Crisis Management reports that "Executives and Managers are responsible for at least half of all crises, on average, while employees are credited with causing 32% and outside forces triggered the remaining 18% on average, during the past ten years."[178]

Accounting irregularities will almost always result in a situation where a board will be well-advised to form a special committee, independent of management, to investigate. Recent examples of a corporate crisis where management must sustain scrutiny include the 2011 revelations of alleged illegal payments to government officials and telephone hacking by Newscorp International.[179]

Special Committee of the Board

Professors Geoffrey C. Hazard, Jr. and Edward B. Rock observe that "[o]ver the last thirty years, the independent directors have occasionally been represented by independent counsel. Instances include: special litigation committees reviewing derivative suits; independent committees in parent subsidiary mergers and MBOs; and internal investigations of misconduct."[180] Professor James D. Cox states, "[c]onflicts of interest transactions are ubiquitous within today's corporate environment. Executives need to be paid, directors receive compensation for their board service and there frequently are transactions within the corporation's dominant stockholder, to name just a few of the events that regularly pose conflicts of interest issues."[181] In addition, the board's special litigation committee "is a subcommittee . . . that has the power to intercede in shareholder derivative claims brought against other members of the board. It has the authority to decide whether

177. E-mail from Professor Nancy Leveson, Aeronautics and Astronautics and Engineering Systems, Massachusetts Institute of Technology, to Lawrence J. Trautman (June 27, 2015, 15:59 CST) (on file with author).

178. Annual ICM Crisis Report 2010, Institute for Crisis Management (May 2011), http://www.crisisexperts.com/.

179. Alistar MacDonald, Cassell Bryan-Low & Paul Sonne, *Ex-Cameron Aide Arrested in Hacking Case,* WALL ST. J., Jul. 9, 2011, at A9; John Bussey, *The Missteps in Managing News Corp.'s Hacking Crisis,* WALL ST. J., Jul. 21, 2011, at B1; Cassell Bryan-Low, Paul Sonne & Steve Stecklow, *Hacking Testimony Is Disputed,* WALL ST. J., July 22, 2011, at A1. *See also* Lawrence J. Trautman & Peter C. Ormerod, *Corporate Directors' and Officers' Cybersecurity Standard of Care: The Yahoo Data Breach,* 66 AM. U. L. REV. (2017), http://ssrn.com/abstract=2883607.

180. Geoffrey C. Hazard & Edward B. Rock, *A New Player in the Boardroom: The Emergence of the Independent Directors' Counsel* (U. Penn. Inst. For Law & Econ., Research Paper 04-07, 2004), http://ssrn.com/abstract=519242.

181. James D. Cox, *Managing and Monitoring Conflicts of Interest: Empowering the Outside Directors With Independent Counsel*, 48 VILL. L. REV. 1077 (2003).

the derivative claims should be pursued, settled, or dismissed, but its decision is never believed to be in doubt."[182]

On July 21, 2002, a Special Investigative Committee of the Board of Directors of WorldCom, Inc. was created. The members of the Special Committee were new to the Board of WorldCom, and neither the committee members nor their "counsel had any relationship with WorldCom or its personnel during the period when the events under investigation occurred."[183] Worldcom Special Committee member Dennis R. Beresford recalls,

> In the WorldCom situation, the Board selected the same law firm that had done the Enron special investigation. While I was not on the board at that time, I understand the decision was made based on the belief that the law firm would be experienced in dealing with a massive fraud and would "hit the ground running." Also, the WorldCom investigation by the law firm was led by former SEC head of enforcement Bill McLucas and it was felt that his experience would be helpful in both doing the investigation and in gaining SEC acceptance of the findings. Based on his work at Enron, Bill urged the WorldCom board to bring in new directors to oversee the investigation as he felt the Enron investigation was "tainted" a bit by having it overseen by current directors. In other words, as directors of WorldCom would be one of the presumed targets of the investigation, it was believed that having new directors oversee it would give much more credibility.[184]

The Special Committee was directed by the WorldCom board to "conduct a full and independent investigation of the accounting irregularities that gave rise to the announced intention to restate, and such other matters as [the Special Committee] concluded should be considered without any limitations."[185] By way of summary, the Special Committee concluded,

> From 1999 until 2002, WorldCom suffered one of the largest public company accounting frauds in history. As enormous as the fraud

182. Minor Myers, *The Decisions of Corporate Special Litigation Committees: An Empirical Investigation* (Brooklyn Law School, Legal Studies Paper No. 112, 2008), http://ssrn.com/abstract=1162858, *citing* WILLIAM A. KLEIN & JOHN C. COFFEE, JR., BUSINESS ORGANIZATION AND FINANCE: LEGAL AND ECONOMIC PRINCIPLES 209 (9th ed. 2004). *See also* Karen Brenner, Corporate Investigations - Challenges in Corporate Governance (2009), http://ssrn.com/abstract=1684238.

183. WorldCom, Inc. REPORT OF INVESTIGATION BY THE SPECIAL INVESTIGATIVE COMMITTEE OF THE BOARD OF DIRECTORS OF WORLDCOM, INC. (Mar. 31, 2003), http://www.sec.gov/Archives/edgar/data/723527/000093176303001862/dex991.htm.

184. *See* E-mail from Dennis R. Beresford, former Worldcom Special Committee member, to Lawrence J. Trautman (July 1, 2015, 10:43 CST) (on file with author).

185. *See* WorldCom, Inc. REPORT, *supra* note 183 at 2.

> was, it was accomplished in a relatively mundane way: more than $9 billion in false or unsupported accounting entries were made in WorldCom's financial systems in order to achieve desired reported financial results. The fraud did not involve WorldCom's network, its technology, or its engineering. Most of WorldCom's people did not know it was occurring. Rather, the fraud occurred as a result of knowing misconduct directed by a few senior executives centered in its Clinton, Mississippi headquarters, and implemented by personnel in its financial and accounting departments in several locations. The fraud was the consequence of the way WorldCom's Chief Executive Officer, Bernard J. Ebbers, ran the Company. Though much of this Report details the implementation of the fraud by others, he was the source of the culture, as well as much of the pressure, that gave birth to this fraud. That the fraud continued as long as it did was due to a lack of courage to blow the whistle on the part of others in WorldCom's financial and accounting departments; inadequate audits by Arthur Andersen; and a financial system whose controls were sorely deficient. The setting in which it occurred was marked by a serious corporate governance failure.
>
> On June 25, 2002, WorldCom announced that it intended to restate its financial statements for 2001 and the first quarter of 2002. It stated that it had determined that certain transfers totaling $3.852 billion during that period from "line cost" expenses (costs of transmitting calls) to asset accounts were not made in accordance with generally accepted accounting principles ("GAAP"). Less than one month later, WorldCom and substantially all of its active U.S. subsidiaries filed voluntary petitions for reorganization under Chapter 11 of the Bankruptcy Code. WorldCom subsequently announced that it had discovered an additional $3.831 billion in improperly reported earnings before taxes for 1999, 2000, 2001 and first quarter 2002. It has also written off approximately $80 billion of the stated book value of the assets on the Company's balance sheet at the time the fraud was announced.[186]

Another example of a special board committee created to investigate a corporate crisis is illustrated by the Enron board's Special Investigative Committee, chaired by then University of Texas Law School Dean William C. Powers, Jr.[187] The Enron Special Committee was,

186. *Id.* at 1.

187. *See generally* William C. Powers, Jr., Chair Raymond S. Troubh Herbert S. Winokur, Jr., REPORT OF INVESTIGATION BY THE SPECIAL INVESTIGATIVE COMMITTEE OF THE BOARD OF DIRECTORS OF ENRON CORP. (Feb. 1, 2002), http://news.findlaw.com/wsj/docs/enron/sicreport/.

> [E]stablished on October 28, 2001, to conduct an investigation of the related-party transactions . . . [which included] examin[ing] the specific transactions that led to the third-quarter 2001 earnings charge and the restatement . . . [and] attempt[ing] to examine . . . two dozen other transactions between Enron and these related-party entities: what these transactions were, why they took place, what went wrong, and who was responsible.[188]

Emergence of Special Counsel

Hazard and Rock predict that a new permanent role has emerged in the board room: that of Counsel to the Independent Directors.[189] Accordingly, "with the additional legal requirement imposed on independent directors by the Sarbanes-Oxley Act and related changes to SEC rules and Stock Exchange listing requirements, the independent directors, especially those on the Audit Committee, will begin to be represented on a *continuing* basis by independent legal counsel."[190]

> When a company launches an internal investigation in the wake of a scandal, the credibility of the investigation depends in no small measure on the perception that the law firm conducting the investigation is independent of the potential wrong doers. To take but one example, when Enron launched an investigation of accounting irregularities, it appointed a special committee of directors, who in turn retained special outside legal counsel, which was largely (although not totally) independent of Enron.[191]

A good example of notable uses of special counsel during a corporate crisis, is found in my previous discussion of General Motors retaining noted attorney Anton R. Valukas to conduct a special independent investigation and issue a report about the circumstances surrounding GM's faulty ignition switch crisis.[192]

188. *Id.*

189. *See* Hazard & Rock, *supra* note 180.

190. *Id.*

191. *Id.*, *citing* William Powers Report to the Board of Directors of the Enron Corporation, February 1, 2002, http://news.findlaw.com/wp/docs/enron/specinv020102rpt1.pdf).

192. *See* Anton R. Valukas, REPORT TO BOARD OF DIRECTORS OF GENERAL MOTORS COMPANY REGARDING IGNITION SWITCH RECALLS, (May 29, 2014), https://s3.amazonaws.com/s3.documentcloud.org/documents/1183508/g-m-internal-investigation-report.pdf (last viewed June 7, 2017).

X. THREAT TO EVERY BOARD: WORKPLACE & DATA SECURITY

Employee Safety

Workplace safety has developed new meaning following the September 11th 2001 World Trade Center attack. The Business Roundtable states, "A corporation needs to have plans in place for what to do if yellow police tape is draped around a key building, if mass evacuations are ordered following a disaster, or if key employees have been harmed or cannot reach a critical worksite."[193]

> Previously, when security primarily called for controlling perimeter access, risk issues did not rise high enough to require the CEO or board of directors to analyze them fully. But in the current risk climate, threats can materialize so quickly and cause so much potential damage to a corporation's operating capability that CEOs need to consider alternative governance and management strategies.[194]

Data Security

Few operational areas of every corporation present as much inherent risk or prove as difficult to govern as Information Technology ("IT") and novel technological advances in the way business is conducted.[195] A reasonable question voiced from many boardrooms is "[h]ow can I be expected to govern something I

193. *See* Business Roundtable, *supra* note 8, at 4.

194. *Id.* at 66.

195. *See generally* Deven R. Desai, *Beyond Location: Data Security in the 21st Century, 56 Communications of the ACM,* (2013), http://ssrn.com/abstract=2237712; Orin S. Kerr, *Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes,* 78 N.Y.U. L. REV. 1596 (2003), http://ssrn.com/abstract=399740; Juliet M. Moringiello, *Warranting Data Security,* 5 BROOK. J. CORP. FIN. & COMM. L. (2010), http://ssrn.com/abstract=1710761; Peter Swire, *A Theory of Disclosure for Security and Competitive Reasons: Open Source, Proprietary Software, and Government Agencies,* 42 HOUS. L. REV. (2006), http://ssrn.com/abstract=842228; Sasha Romanosky & Alessandro Acquisti, *Privacy Costs and Personal Data Protection: Economic and Legal Perspectives,* 24 BERKELEY TECH. L.J. (2009), http://ssrn.com/abstract=1522605; Lawrence J. Trautman, James C. Wetherbe & Jason Triche, *Corporate Information Governance Under Fire,* 8 J. STRATEGIC & INT'L STUD. 105 (2013), http://ssrn.com/abstract=2314119; Lawrence J. Trautman & Alvin Harrell, *Bitcoin Versus Regulated Payment Systems: What Gives?,* 38 CARDOZO L. REV. 1041 (2017), *available at* http://ssrn.com/abstract=2730983; Lawrence J. Trautman, *Is Disruptive Blockchain Technology the Future of Financial Services?,* 69 CONSUMER FIN. L.Q. REP. 232 (2016), *available at* http://ssrn.com/abstract=2786186; Lawrence J. Trautman, *Virtual Currencies: Bitcoin & What Now After Liberty Reserve, Silk Road, and Mt. Gox?,* 20 RICH. J. L. & TECH. 13 (2014), *available at* http://www.ssrn.com/abstract=2393537; Rachel Wellhausen, Multinational Corporations, Nationality, and Government Breach of Contract, APSA 2011 Annual Meeting Paper; MIT Political Science Department Research Paper No. 2011-15 (2011), http://ssrn.com/abstract=1900202.

know so little about?"[196] However, recent years have brought a growing realization that not knowing is not an excuse. As more and more responsibility is placed on boards to oversee all areas of risk 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 Information Technology efficiently sustains and extends the corporate strategies and objectives.

All too often the reality of IT performance and enterprise risk exposure 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."[197]

IT risks are inherent in a company's operations, including, for example, 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 your 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.[198]

In their 2011 journal article, *The Board's Responsibility for Information Technology Governance,* Trautman and Altenbaumer-Price report,

> 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. It was believed at the time

196. 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 property and relationships). *See* PETER WEILL & JEANNE W. ROSS, IT GOVERNANCE: HOW TOP PERFORMERS MANAGE IT DECISIONS RIGHTS FOR SUPERIOR RESULTS 6 (Harv. Bus. Sch. Press) (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), *cited in* Lawrence J. Trautman & Kara Altenbaumer-Price, *The Board's responsibility for Information Technology Governance,* 29 J. MARSHALL J. COMPUTER & INFO. L. 313 (2011).

197. *See* Trautman & Altenbaumer-Price, *supra* note 22 at 314, *citing* Board Briefing on IT Governance, 2d ed., IT Governance Institute, 8 (2003).

198. *See* Urs Gasser, Jonathan Zittrain, Robert Faris, Rebekah Heacock Jones, Internet Monitor 2014: Reflections on the Digital World: Platforms, Policy, Privacy, and Public Discourse Berkman Center Research Publication No. 2014-17 (2014), http://ssrn.com/abstract=2538813.

> to be the largest security breach ever. Although the breach occurred over the course of 2008, the company did not discover it until January 2009. When Heartland disclosed the breach, the stock price dropped almost 80%; 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." Heartland did not know "how long the malicious software was in place, how it got there or how many accounts may have been compromised." What Heartland did know is that the stolen data included names, credit and debit card numbers, and expiration dates. While the shareholder class action against Heartland was later dismissed for failure under the PSLRA to plead fraud with particularity, the company and its officers and directors were forced to pay $60 million in a settlement with Visa, $41.4 million in a settlement with MasterCard, $3.6 million in a settlement with American Express, up to $2.4 million in a consumer cardholder class action over the same breach, as well as the defense costs of the dismissed suit and internal investigation costs incurred by the company.[199]

Cyber risk has proven costly for many years now. In his July 28, 2010 Statement before the House Judiciary Subcommittee on Crime, Terrorism, and Homeland Security, FBI Assistant Director Gordon M. Snow observed, "[c]yber thieves use data mining on social networking sites as a way to extract sensitive information. This can be done by criminal actors on either a large or small scale . . . The impact . . . can be substantial . . . with the consequences ranging from a mere inconvenience to financial ruin."[200] Moreover,

> These criminals are increasingly professionalized, organized, and have unique or specialized skills. In addition, cyber crime is increasingly transnational in nature, with individuals living in different countries around the world working together on the same schemes. In late 2008, an international hacking ring carried out one of the most complicated and organized computer fraud attacks ever conducted. The crime group used sophisticated hacking techniques to compromise the encryption used to protect data on 44 payroll debit cards, and then provided a network of "cashers" to withdraw

199. *See* Trautman & Altenbaumer-Price, *supra* note 22 at 333.

200. *The FBI's Efforts to Combat Cyber Crime as it Relates to Social Networking Sites, Before the H. Judiciary Subcomm. On Crime, Terrorism, and Homeland Security*, (July 28, 2010) (statement of Gordon M. Snow, Asst. Dir., Cyber Div, Federal Bureau of Investigation.

> more than $9 million from over 2,100 ATMs in at least 280 cities worldwide, including cities in the United States, Russia, Ukraine, Estonia, Italy, Hong Kong, Japan and Canada. The $9 million loss occurred within a span of less than 12 hours. The cyber underground facilitates the exchange of cyber crime services, tools, expertise, and resources, which enables this sort of transnational criminal operation to take place across multiple countries.[201]

Trautman also reports that "costs attributable to cybersecurity losses vary dramatically, according to one 2013 survey the "average annualized cost of cyber-crime to a sample of U.S. companies was $11.6 million per year, representing a 78% increase since 2009."[202] IBM Cybersecurity Counsel Andrew H. Tannenbaum warns about the continued loss of U.S. industry's most valuable intellectual property having "been stolen in milliseconds."[203] Senator Joseph Lieberman states that "Extremely valuable intellectual property is being stolen regularly by cyber exploitation, by people and individuals and groups and countries abroad . . . This means jobs are being created abroad that would otherwise be created here."[204] Sarah Bloom Raskin, Deputy Treasury Secretary, reports that "what we can be sure of is that the financial costs are real and increasing; they stem from the disruption of business, erosion of customers, and the associated loss of revenue, from expenses incurred to secure systems, and appropriately notify customers."[205]

201. *The FBI's Efforts to Combat Cyber Crime as it Relates to Social Networking Sites, Before the H. Judiciary Subcomm. On Crime, Terrorism, and Homeland Security*, (July 28, 2010) (statement of Gordon M. Snow, Asst. Dir., Cyber Div, Federal Bureau of Investigation.

202. *See* Lawrence J. Trautman, *Cybersecurity: What About U.S. Policy*, 2015 J. L. TECH. & POL'Y 341, 356 (2015), *citing* Luis A. Aguilar, Commissioner, U.S. Securities and Exchange Comm'n, Boards of Directors, Corporate Governance and Cyber Risks: Sharpening the Focus, Address Before the New York Stock Exchange, Conference on "Cyber Risks and the Boardroom" (June 10, 2014), http://www.sec.gov/News/Speech/Detail/Speech/1370542057946#.U6t-wvldWHg., *citing* HP Press Release, HP Reveals Cost of Cybercrime Escalates 70 Percent, Time to Resolve Attacks More Than Doubles (Oct. 8, 2013), http://www8.hp.com/us/en/hp-news/press-release.html?id=1501128.

203. *See* Lawrence J. Trautman, *Cybersecurity: What About U.S. Policy*, 2015 J. L. TECH. & POL'Y 341, 356 (2015), *citing* The Growing Cyber Threat and its Impact on American Business: Hearings Before the H. Perm. Select Comm. Intelligence, 114th Cong. 1 (2015) (statement of Andrew H. Tannenbaum, Cybersecurity Counsel, IBM), http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/TannenbaumSFR03192015.pdf.

204. *See* Lawrence J. Trautman, *Cybersecurity: What About U.S. Policy*, 2015 J. L. TECH. & POL'Y 341, 356 (2015), *citing* Joseph Lieberman, *Securing America's Future: The Cybersecurity Act of 2012:* Hearing Before the Comm. On Homeland Security and Governmental Affairs, 112th Cong. (Feb. 16, 2012) (Opening Statement of Chairman Joseph Lieberman), http://www.hsgac.senate.gov/hearings/securing-americas-future-the-cybersecurity-act-of-2012.

205. *See* Sarah Bloom Raskin, Deputy Secretary of the Treasury of the United States, Remarks Before the Meeting of the Texas Bankers' Association Executive Leadership Cybersecurity Conference: Cybersecurity for Banks: 10 Questions for Executives and Their Boards (Dec. 3, 2014), http://www.treasury.gov/press-center/press-releases/Pages/jl9711.aspx. (last viewed Mar. 5, 2016).

Target Breach

Major U.S. retailer Target Corporation sells "a wide assortment of general merchandise and food through . . . store and digital channels . . . At January 31, 2015, [Target] employed approximately 347,000 full-time, part-time and seasonal employees . . . During the sales period from Thanksgiving to the end of December [2014] . . . employment levels peaked at approximately 447,000."[206]

Target experienced a data breach during the fourth quarter of 2013, when "an intruder stole certain payment card and other [customer] information from [their] data network (the Data Breach) . . . As of January 31, 2015 [Target has] incurred $252 million of cumulative Data Breach-related expenses, partially offset by $90 million of expected insurance recoveries, for net cumulative expenses of $162 million."[207] As of the same date, Target disclosed that "more than 100 legal "actions have been filed in courts in many states, along with one action in Canada, and other claims have been or may be asserted . . . on behalf of [customers], payment card issuing banks, shareholders or others seeking damages."[208] The Congressional Research Service reports that back-of-the-envelope estimates made by independent sources range "from $240 million to $2.2 billion in fraudulent charges alone. This does not include additional potential costs to consumers concerned about their personal information or credit histories, potential fines or penalties to Target, financial institutions, or others; or any costs to Target related to loss of consumer confidence."[209] According to testimony provided by Target executive vice president and chief financial officer John J. Mulligan, the chronology of the breach is as follows:

- November 12, 2013—intruders breached Target's computer system. The intrusion was detected by Target's security systems, but the company's security professionals took no action until notified by law enforcement of the breach.
- December 12, 2013—the Department of Justice (DOJ) notified Target that there was suspicious activity involving payment cards that had been used at Target.
- December 13, 2013—Target met with DOJ and the U.S. Secret Service.
- December 14, 2013—Target hired outside experts to conduct a thorough forensic investigation.

206. Target Corporation, Report on Form 10-K for the fiscal year ended Jan. 31, 2015, 2, 3 (2015), https://www.sec.gov/Archives/edgar/data/27419/000002741915000012/tgt-20150131x10k.htm#s2AC222A90C0DF88C3C65A5EBB013D478.

207. *Supra* at 17 to financial statements.

208. *Id.*

209. *See* N. Eric Weiss & Rena S. Miller, *The Target and Other Financial Data Breaches: Frequently Asked Questions,* Congressional Research Service Report, 2 (Feb. 4, 2015), https://www.fas.org/sgp/crs/misc/R43496.pdf (last viewed Mar. 5, 2016).

- December 15, 2013—Target confirmed that malware had been installed and that most of the malware had been removed.
- December 16 and 17, 2013—Target notified payment processors and card networks that a breach had occurred.
- December 18, 2013—Target removed the remaining malware.
- December 19, 2013—Target made a public announcement of the breach.
- December 27, 2013—Target announced the theft of the encrypted PIN data.
- January 9, 2014—Target discovered the theft of PII.
- January 10, 2014—Target announced the PII theft.[210]

Just a few months after the cyber breach, Target CEO Gregg Steinhafel, a 35-year company employee resigned.[211] According to Congressional testimony provided by a Target executive, "an intruder used a vendor's access to Target's system to place malware on point-of-sale (POS) registers. The malware captured credit and debit card information."[212] Almost two years after the Target breach, trade groups representing credit unions and community banks report expenses of more than $350 million "to reissue credit and debit cards and deal with other issues related to the Target breach and a subsequent hacking at Home Depot."[213]

Sony Breach

During November 2014, a cyber-attack was successfully waged against Sony Pictures Entertainment (SPE) resulting in a significant disruption of business operations, the destruction of computer systems, rendering inoperable thousands of company computers, and the theft of significant amounts of proprietary commercial information and the personally identifiable data and confidential communications of

210. *Id.* at 3.

211. Eric Basu, *Target CEO Fired- Can You Be Fired If Your Company is Hacked?,* FORBES June 15, 2014, http://www.forbes.com/sites/ericbasu/2014/06/15/target-ceo-fired-can-you-be-fired-if-your-company-is-hacked/.

212. *See* Weiss & Miller, *supra* note 209, *citing* Testimony of John J. Mulligan, executive vice president and chief financial officer, Target, before U.S. Congress, Senate, Committee on Commerce, Science, and Transportation, Protecting Personal Consumer Information from Cyber Attacks and Data Breaches, 113th Cong., 2nd sess., March 26, 2014, at http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=c2103bd3-8c40-42c3-973b-bd08c7de45ef; U.S. Congress, Senate, Committee on the Judiciary, Privacy in the Digital Age: Preventing Data Breaches and Combating Cybercrime, 113th Cong., 2nd sess., February 4, 2014, at http://www.judiciary.senate.gov/pdf/02-04-14MulliganTestimony.pdf, and U.S. Congress, House of Representatives, Committee on Energy and Commerce, Subcommittee on Commerce, Manufacturing, and Trade, Protecting Consumer Information: Can Data Breaches Be Prevented?, 113th Cong., 2nd sess., February 5, 2014, http://docs.house.gov/meetings/IF/IF17/20140205/101714/HMTG-113-IF17-Wstate-MulliganJ-20140205.pdf.

213. *See* Robin Sidel, *Three Banks Put Kibosh On Target Pact,* WALL ST. J., June 3, 2015, at C1. *See also* Robin Sidel, *Small Lenders Cry Foul Over Breach Costs,* WALL ST. J., Apr. 28, 2015, at C1.

employees.[214] Within hours following discovery of the network intrusion Sony reported this incident and requested FBI assistance. State actor North Korea is alleged to have committed a major cyber-attack on the data systems of Sony Corporation in retaliation for a proposed Christmas day-release of the Hollywood motion picture spoofing a fictitious plan to assonate the leader of North Korea.[215] The FBI reports that

> Sony's quick reporting facilitated the investigators' ability to do their jobs, and ultimately to identify the source of these attacks. As a result of our investigation, and in close collaboration with other U.S. government departments and agencies, the FBI now has enough information to conclude that the North Korean government is responsible for these actions. While the need to protect sensitive sources and methods precludes us from sharing all of this information, our conclusion is based, in part, on the following:
>
> - Technical analysis of the data deletion malware used in this attack revealed links to other malware that the FBI knows North Korean actors previously developed. For example, there were similarities in specific lines of code, encryption algorithms, data deletion methods, and compromised networks.
> - The FBI also observed significant overlap between the infrastructure used in this attack and other malicious cyber activity the U.S. government has previously linked directly to North Korea. For example, the FBI discovered that several Internet protocol (IP) addresses associated with known North Korean infrastructure communicated with IP addresses that were hardcoded into the data deletion malware used in this attack.
> - Separately, the tools used in the SPE attack have similarities to a cyber-attack in March of last year against South Korean banks and media outlets, which was carried out by North Korea.
>
> We are deeply concerned about the destructive nature of this attack on a private sector entity and the ordinary citizens who worked there. Further, North Korea's attack on SPE reaffirms that cyber threats

214. Press Release, Federal Bureau of Investigation, Update on Sony Investigation (Dec. 19, 2014), http://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation (last viewed Mar. 5, 2016).

215. *See* Lawrence J. Trautman, Managing Cyberthreat, 33 SANTA CLARA COMPUTER & HIGH TECH. L.J. 230 (2016), http://ssrn.com/abstract=2534119; Lawrence J. Trautman & George P. Michaely, *The SEC & The Internet: Regulating the Web of Deceit,* 68 CONSUMER FIN. L.Q. REP. (2015), http://www.ssrn.com/abstract=1951148; Lawrence J. Trautman, *The SONY Data Hack: Implications for World Order*, (unpublished manuscript).

> pose one of the gravest national security dangers to the United States. Though the FBI has seen a wide variety and increasing number of cyber intrusions, the destructive nature of this attack, coupled with its coercive nature, sets it apart. North Korea's actions were intended to inflict significant harm on a U.S. business and suppress the right of American citizens to express themselves. Such acts of intimidation fall outside the bounds of acceptable state behavior.[216]

The November 2014 breach was not Sony's first major encounter with a massive breach. About forty-three (43) months earlier, as the result of a 2011 cyberattack, Sony shut down its PlayStation Network "on April 20 [2011] when it found evidence of an intrusion, but it didn't reveal the data breach to users until April 26. The company said it didn't know conclusively until April 25 that some personal information had been accessed."[217]

Other Data Breach Cases

By now, reports of data breaches are widespread.[218] To illustrate the enormity of this contemporary problem, in just one day alone while I was drafting this article,

216. *See* Press Release, *supra* note 214.

217. Daisuke Wakabayashi, *Sony CEO Warns of "Bad New World,"* WALL ST. J., May 18, 2011, at B1.

218. *See* Derek E. Bambauer, *Ghost in the Network,* 162 U. PA. L. REV. (2014), http://ssrn.com/abstract=2232471; Shelly Banjo, *Home Depot Hackers Stole Buyer Email Addresses,* WALL ST. J., Nov. 7, 2014, at A1; Ian Brown, Lilian Edwards & Christopher Marsden, Information Security and Cybercrime, LAW AND THE INTERNET (3rd ed., L. Edwards, C. Waelde, eds., Oxford: Hart, 2009), http://ssrn.com/abstract=1427776; Michael Calia, *Breach Plagues Home Depot,* WALL ST. J., Nov. 19, 2014, at B3;Julia S. Cheney, *Heartland Payment Systems: Lessons Learned from a Data Breach*, FRB OF PHILADELPHIA - PAYMENT CARDS CENTER DISCUSSION PAPER NO. 10-1 (2010), http://ssrn.com /abstract=1540143; A. Michael Froomkin, Government Data Breaches, 24 BERKLEY TECH. L.J. 1019 (2009), http://ssrn.com/abstract=1427964; Kevin Gatzlaff & Kathleen A. McCullough, *The Effect of Data Breaches on Shareholder Wealth*, 13 RISK MGMT. & INS. REV. 1 (2008), http://ssrn.com/abstract =1121172; Emily Glazer, Danny Yadron & Daniel Huang, *Hackers May Have Targeted at Least 13 Firms*, WALL ST. J., Oct. 9, 2014, at C1; Lauren Henry, *Information Privacy and Data Security,* CARDOZO LAW REVIEW DE NOVO, 107 (2015), http://ssrn.com/abstract=2600495; Trey Herr & Allan A. Friedman, *Redefining Cybersecurity*, AMERICAN FOREIGN POLICY COUNCIL - DEFENSE TECHNOLOGY PROGRAM BRIEF, No. 8, (Jan. 2015), http://ssrn.com/abstract=2558265; David E. Sanger & Nicole Perlroth, Bank Hackers Steal Millions Via Malware, N.Y. TIMES, Feb. 15, 2015 at A1; Susan Sproule & Francine Vachon, *The Prevention and Mitigation of Breaches of Personal Information Databases: A Theoretical Framework,* 11 J. TECH. & HUMAN USABILITY 1 (2015), http://ssrn.com/abstract=2511603; David Thaw, *The Efficacy of Cybersecurity Regulation*, 30 GA. ST. U. L. REV. 287 (2014), http://ssrn.com/abstract= 2241838; David Thaw, *Data Breach (Regulatory) Effects,* CARDOZO L. REV. DE NOVO 151 (2015), http://ssrn.com/abstract=2595297; Sarah Oh, Estimates for Reasonable Data Breach Prevention (June 12, 2015), http://ssrn.com/abstract=2616968; Lawrence J. Trautman & Peter C. Ormerod, Industrial Cyber Vulnerabilities: Lessons from Stuxnet and the Internet of Things, (unpublished manuscript), *available at* http://ssrn.com/abstract=2982629.

the *Wall Street Journal* reported news articles having the following headlines: "Israel-Linked Spyware Hit Iran Talks"[219]; "Reports: FEC Data Vulnerable to Hacks"[220]; and "France Says Russians Carried Out Cyberattack."[221] These disturbing reports of alleged nation-state cyber-attacks come just days after the cyber theft of personal employment "records of as many as four million people in one of the most far-reaching breaches of government computers."[222] Other deeply troubling headlines of recent data breaches include: "Russian Hackers Read Obama's Unclassified Emails, Officials Say"[223] and "Breach At IRS Exposes Returns."[224]

XI. DIGITAL AGE & CRISIS MANAGEMENT: SOCIAL MEDIA CHALLENGES

Unlike one-way traditional communications mediums such as newspapers, radio and television—the Internet, Facebook and Twitter (immediate and bi-directional) has resulted in new challenges to effective crisis management. Facebook has emerged as the dominant social network in the United States. Facebook reports a daily average of 1.28 billion active users during March 2017, with "approximately 85.8% of daily active users . . . outside the U.S. and Canada."[225]

Toyota 2010 Recall of 2.9 Million Vehicles

Jay Rajasekera of the International University of Japan recalls the unprecedented global media coverage due to "Toyota's brand name, its newly acquired title as the 'No. 1 automaker in the world,' and its rather lethargic response

219. Adam Entous & Danny Yadron, *Israel-Linked Spyware Hit Iran Talks,* WALL ST. J., June 11, 2015, at A1.

220. Brody Mullins & Rebecca Ballhaus, *Reports: FEC Data Vulnerable to Hacks,* WALL ST. J., June 11, 2015, at A4.

221. Sam Schechner, *France Says Russians Carried Out Cyberattack,* WALL ST. J., June 11, 2015, at A6.

222. Devlin Barrett, Danny Yadron & Damian Paletta, *Chinese Suspected in Huge Data Hack,* WALL ST. J., June 5, 2015, at A1. *See also* Devlin Barrett & Carol E. Lee, *U.S. Unsure What Hackers Got,* WALL ST. J., June 6-7, 2015, at A3; David E. Sanger & Julie Hirschfeld Davis, *Data Breach Tied to China Hits Millions,* N.Y. TIMES, June 5, 2015, at A1; Damian Paletta, *Security Clearance Forms Accessed In Federal Hack,* WALL ST. J., June 13-14, 2015, at A1.

223. Michael S. Schmidt & David E. Sanger, *Russian Hackers Read Obama's Unclassified Emails, Officials Say,* N.Y. TIMES, Apr. 26, 2015 at A1. *See also* Laura Saunders, *Tax ID Theft Victims Cite Woes With IRS,* WALL ST. J., May 28, 2015, at A3.

224. John D. McKinnon & Laura Saunders, *Breach at IRS Exposes Returns,* WALL ST. J., May 27, 2015, at A1.

225. Facebook, Newsroom, Company Info, Stats, http://newsroom.fb.com/company-info/ (last viewed June 7, 2017).

time to the incidents, some of which reportedly happened several years ago."[226] Moreover,

> Once the media around the world started flashing the stunning news of the big recall of 2.9 million vehicles, on January 21, 2010, which was on top of the 3.9 million recalled just a few months prior, the reaction from all the corners, including Toyota's own customers, the general public, the politicians, and the financial markets was unprecedented in Toyota's history. The total number of Toyota's recalls related to the serious safety defect connected to sudden acceleration would eventually climb up to 8.6 million globally . . . .
>
> With Internet and social media such as Facebook and Twitter in full form, the negative news spread at unprecedented speed to Europe, China, and around the world, including Toyota's home market of Japan…
>
> In the U.S., where hordes of lawyers could be in the waiting eagerly to help any victim or their families go up against Toyota, financial and punitive damages could be severe. . . As soon as the big recall of 2.3 million vehicles was announced on January, 2010, Toyota ordered the dealers to temporarily suspend the sales of eight models involved in the recall for sticking accelerator pedal . . . .
>
> . . . the biggest challenge for Toyota is to maintain the public trust. Indeed, voluntary recalls, if done in a timely manner, can help boost the trust of a company, as happened in previous Toyota recalls. However, the situation was different this time, because the company was in a way forced by the US government, which had received a significant influx of complaints. This forced-recall definitely did not create a positive image for Toyota's reputation which had been meticulously created over several decades through a carefully planned strategy and public relations campaigns . . . .[227]

Armed with an MBA from Babson College in the United States and with less than a year's experience as Toyoda president, Akio Toyoda faced a public relations crisis "when he was called to testify before the US Congress on February 23, 2010. Already under fire by the US media for not apologizing early and also not sufficiently, his performance, broadcasted live around the world, was a defining moment for Toyota and for corporate Japan."[228] Among the questions at the time: "[d]id he apologize enough? Was his performance sincere? Did it look like he was trying to conceal something? Mr. Rajasekera observes that "A survey conducted by

226. Jay Rajasekera, *Crisis Management in Social Media and Digital Age: Recall Problem and Challenges to Toyota,* Int'l University of Japan Graduate School of International Management Working Paper No. IM-2010-02 at 4 (2010), http://www.ssrn.com/abstract=1603027.

227. *Id.*

228. *Id.* at 7.

TV broadcaster CBS News in the US, following Mr. Toyoda's testimony, the public did not rate Toyoda's explanation very positively—overall only 27% believed that Toyoda was telling the truth; almost 50% said Toyoda was hiding something."[229]

Toyota's Social Network Strategy

Observing that "social media, if properly used, is also a way to keep an eye on the public mood when some significant issue that affects a large number of people occurs, such as the present recall which had raised emotions high in many Toyota customers,"[230] Mr. Rajasekera concludes that "Toyota seemed to have realized the importance of SNS [Social Network Sites] early on."[231] Moreover,

> With manufacturing operations in 27 countries, and a dealer network in 170 countries, Toyota is a giant organization. In any large organization, coordinating all the media releases, let they be for news papers, TV, or SNS, such as You Tube, Twitter, and Facebook, must be done carefully in order to prevent public confusion . . . . As soon as the recall crisis started getting media attention, Toyota quickly put together an 'Online Newsroom' and a 'social media strategy team' to coordinate all the media releases from different organizations of the company, like public relations, customer services, and dealers.
>
> In addition to Toyota's own efforts, anyone interested in knowing or wanting to express an opinion has the option to get on with any SNS media and exchange opinions.

Among the SNS sites Toyota is operating include:

- Twitter feeds; twitter.com/TOYOTA
- Facebook; facebook.com/Toyota
- YouTube; youtube.com/Toyota
- YouTube USA; youtube.com/user/TototaUSA
- Pressroom Toyota; pressroom.toyota.com/

> In reasoning that the company had not had a major backlash from its customers, especially in the US, where media was providing sensational coverage around the clock, Toyota had stated that it had increased number of customers in its Facebook page. That is true, Toyota fans to this SNS site has been growing about 10% monthly. But, the fact of the matter is that all the other major US brands had also been adding fans to their Facebook SNS sites as well.[232]

229. *Id.*
230. *Id.* at 9.
231. *Id.*
232. *Id.*

Social Media Provides Immediate Feedback

Mr. Rajasekera points out that a major benefit of social media "is that a company can gather practically real-time information about customer feelings or complaints. A Toyota fan club, such as in Facebook, may not quite reflect all sides as the people joining it may already have a positive opinion about the brand.[233] Mr. Rajasekera continues,

> In fact the recall process had opened up quite a few SNS groups attacking Toyota. The company may want to tap into such groups as well to follow up on their messages from time to time. In Facebook itself, one can see more than 10 such SNS groups, with revealing names such as '*Anti-Toyota'*, '*Anti-Toyota Prius Group!* and '*anti prius movement*."[234] But the total number of members in such groups is quite small—less than 1% of the number in Toyota's official Facebook SNS. What sends a signal of concern to Toyota may be the growth of the membership of such SNSs and the rate the members keep posting the messages; plus of course the contents within those messages.
>
> One SNS site that had been in operation well before the current round of recalls became a menace to Toyota is a public site called PRIUSchat.[235]

XII. HAVE YOU CONSIDERED THE FOLLOWING NIGHTMARE SCENARIOS?

Reasonably foreseeable disasters are often industry specific: airlines (plane crashes); chemical and refineries (explosions); manufacturing (undiscovered defects or design flaws); oil and gas exploration (petroleum spills or explosions); pharmaceuticals (adverse reactions to or unknown dangers from prescription drugs); transportation (train wrecks, trucking accidents, etc.). It seems difficult, if not impossible, to justify not planning for each of these circumstances.

The "business judgment" rule is procedural; it's critically important that the board and management have a documented history of diligent preparation for a reasonably foreseeable crisis.[236] Here is a non-exhaustive list of a few other disruptive events which could escalate into crisis proportions given the right circumstances:

233. *Id.* at 11.
234. *Id.*
235. *Id.*
236. *See* Barton, *supra* note 162 at 8.

1. CROP FAILURES IMPACTING SUPPLIES OF NECESSARY RAW MATERIALS

Supply chain risk is a foreseeable problem that every business needs to consider. Mitigating risk by insurance, hedging, or some other appropriate strategy— or at least being cognizant of the nature of such risks is required. Supply chain risks come in many varieties. Every enterprise should question the extent to which they are subject to supply chain risk and have contingencies in place when the disruption takes place.

2. FOREIGN CORRUPT PRACTICES ACT ("FCPA") VIOLATIONS

With often devastating consequences, individuals and business entities of any size may run afoul of U.S. and international bribery and corruption laws.[237] Trautman and Altenbaumer-Price have observed that "Increased international commerce between the United States and faster growing economies such as The People's Republic of China (PRC), as well as third world economies rich in natural resources but poor in infrastructure like Nigeria, have created the potential for significant exposure to international corruption.[238] Accordingly, recent enforcement trends

> demand that U.S. directors understand the basic foundation for doing business without running afoul of the FCPA. With an increasing demand for United States citizens to sit on boards dealing with significant exposure to emerging economies and Chinese developments, the FCPA has become an area that directors of both public and private companies alike cannot ignore. With the increase in business operations around the globe by U.S. companies, the risk associated with anti-bribery laws increases. Any attempt to assess corporate risk for an FCPA violation requires an understanding of how the statute operates and is enforced.[239]

237. Lawrence J. Trautman, U.S. Entrepreneurial Risk in International Markets: Focus on Bribery and Corruption, (unpublished manuscript), https://ssrn.com/abstract=2912072. *See also* Mike Koehler, *An Examination of Foreign Corrupt Practices Act Issues,* 12 RICH. J. GLOBAL L. & BUS. (2013), http://ssrn.com/abstract=2298644; Lawrence J. Trautman, Anthony "Tony" Luppino & Malika S. Simmons, *Some Key Things U.S. Entrepreneurs Need to Know About The Law and Lawyers*, 46 TEX. J. BUS. L. 155 (2016), http://ssrn.com/abstract=2606808; Lawrence J. Trautman, *Following the Money: Lessons from the "Panama Papers," Part 1: Tip of the Iceberg*, 121 PENN ST. L. REV. 807 (2017), *available at* http://ssrn.com/abstract=2783503.

238. Lawrence J. Trautman & Kara Altenbaumer-Price, *The Foreign Corrupt Practices Act: Minefield for Directors,* 6 VA. L. & BUS. REV. 145, 146 (2011). *See also* Lawrence J. Trautman, *American Entrepreneur in China: Potholes on the Silk Road to Prosperity,* 12 WAKE FOREST J. BUS. & INT'L PROP. L. 427 (2012), http://www.ssrn.com/abstract=1995076.

239. *Id. See also* Lawrence J. Trautman & Kara Altenbaumer-Price, *Foreign Corrupt Practices Act: An Update on Enforcement and SEC and DOJ Guidance,* 41 SEC. REG. L. J. 241 (2013),

3. INTERNET DISRUPTION, OR DATA LOSS FROM VIRUS OR HACKER ATTACK

Elsewhere, Trautman and Alterbaumer-Price provide common examples of undesired Information Technology risks, including: "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."[240] Many boards now recognize the value of having cyber expertise and are actively recruiting technology experience to their audit or risk committees.[241]

4. NATIONALIZATION OF ASSETS BY SOVEREIGNS

History is chock full of instances of asset nationalization. Recent examples of nationalization include: Bolivia (oil & gas);[242] Cuba (all foreign-owned private);[243] Iceland (banking);[244] Ireland (banking);[245] The Netherlands (insurance and banking);[246] New Zealand (railway and airlines);[247] Portugal (banking);[248]

http://ssrn.com/abstract=2293382; Lawrence J. Trautman & Kara Altenbaumer-Price, Lawyers, Guns and Money – The Bribery Problem and U.K. Bribery Act, 47 THE INT'L LAW. 481(2013), http://www.ssrn.com/abstract=2276738.

240. Trautman & Altenbaumer-Price, supra note 22, citing Board Briefing on IT Governance, 2d ed., IT Governance Institute, 2003 p. 8. *See also* Lawrence J. Trautman, *E-Commerce and Electronic Payment System Risks: Lessons from PayPal,* 17 U.C. DAVIS BUS. L.J. 261 (2016), http://www.ssrn.com/abstract=2314119; Lawrence J. Trautman, Managing, 33 SANTA CLARA HIGH TECH. L.J. 230 (2016), http://ssrn.com/abstract=2534119.

241. *See* Joann S. Lubin, *The Newest Board Member: Digital,* WALL ST. J., June 10, 2015, at A1; Shelly Banjo, Wal-Mart Taps Tech Expert: Retailer Names 30-Year-Old Instagram CEO Kevin Systrom to Its Board, WALL ST. J., Sept. 30, 2014, at B3. *See also* Lawrence J. Trautman, *The Matrix: The Board's Responsibility for Director Selection and Recruitment,* 11 FLA. ST. U. BUS. REV. 75 (2012), http://ssrn. com/abstract=1998489; Lawrence J. Trautman, *Who Qualifies as an Audit Committee Financial Expert Under SEC Regulations and NYSE Rules?,* 11 DEPAUL BUS. & COMM. L.J. 205 (2013), http://www.ssrn. com/abstract=2137747.

242. Carin Zissis, Bolivia's Nationalization of Oil and Gas, Council on Foreign Relations (May 12, 2006), http://www.cfr.org/economics/bolivias-nationalization-oil-gas/p10682.

243. Hugh Thomas, *Cuba; the Pursuit of Freedom*, 224-252 (Harper & Row., 1971).

244. *See Crisis Report: Icelandic Ministers Were Negligent*, Iceland Review Online, Dec. 4, 2010, http://www.icelandreview.com/icelandreview/search/news/Default.asp?ew_0_a_id=360575.

245. *Government Nationalises 'Fragile' Anglo Irish Bank*, Irishtimes.com, Jan. 1, 2009, http://www.irishtimes.com/newspaper/frontpage/2009/0116/1232059654021.html.

246. Dutch Media Split Over Fortis Nationalization, Reuters, Oct. 4, 2008, http://www.reuters.com/article/2008/10/04/us-fortis-media-idUSTRE49314H20081004.

247. The Rail 'Turn-Around Plan, Kewi Rail, May 18, 2010, http://www.kiwirail.co.nz/uploads/Publications%20and%20Reports/Overview%20of%20KiwiRails%20Turn-around%20plan.pdf.

248. *Portugal Announces Nationalization of Troubled BPN Bank*, CHINA ECONOMIC NET, Nov. 3, 2008, http://en.ce.cn/subject/financialcrisis/financialcrisiswr/200811/03/t20081103_17267231.shtml.

Sweden (banking);[249] United Kingdom (banking, Rolls-Royce, British Leyland, British Rail and National Coal Board);[250] United States (mortgage, banking automotive);[251] and Venezuela (oil & gas, cement, steel, rice, glass-manufacturing).[252]

5. NATURAL DISASTERS (EARTHQUAKE, TORNADO OR HURRICANE)

Anyone who has lived in Florida or along the U.S. Gulf of Mexico coastline understands the annual threat of hurricane season. Years later, the aftermath of Hurricane Katrina (2005) continues to plague residents of New Orleans and the Gulf coast. We have examined previously the tragedy caused by the March 11, 2011, earthquake and subsequent tsunami which resulted in the release of radiation into the nearby soil, air and sea. "The twin catastrophes wiped out the normal power and backup generators of nearly all the Fukushima nuclear power plant's six reactors"[253]

6. ADVERSE POLITICAL DEVELOPMENTS (TARIFFS, TRADE WARS, ETC.)

Unexpected political developments in countries responsible for raw materials, manufacturing or significant market demand will be a topic deserving the attention of management and the board. Adverse changes in these situations may not be readily foreseeable and may be the result of retaliatory tariffs or political events (such as government regime change) that cannot be readily anticipated.

249. Carter Dougherty, *Stopping a Financial Crisis, the Swedish Way*, N.Y. TIMES, Sept. 22, 2008, http://www.nytimes.com/2008/09/23/business/worldbusiness/23krona.html.

250. Steve Schifferes, The Lessons of Nationalism, BBC News, Feb. 18, 2008, http://news.bbc.co.uk/2/hi/business/7250252.stm; Northern Rock Confirms Job Cuts, BBC NEWS, Aug. 29, 2008, http://news.bbc.co.uk/2/hi/business/7587718.stm; Graeme Wearden, Government to Spend £50bn to Part-Nationalize UK's Banks, Guardian.co.uk, Oct. 8, 2008.

251. Zachary A. Goldfarb, David Cho and Binyamin Appelbaum, Treasury to Rescue Fannie and Freddie, Washingtonpost.com, Sept. 7, 2008, http://www.washingtonpost.com/wp-dyn/content/article/2008/09/06/AR2008090602540.html?hpid=topnews; Steven D. Levitt, Diamond and Kashyap on the Recent Financial Upheavals, Freakonomics.com, Sept. 18, 2008, http://www.freakonomics.com/2008/09/18/diamond-and-kashyap-on-the-recent-financial-upheavals/; and Micheline Maynard, A Primer on the New General Motors, N.Y. TIMES.COM, July 10, 2009, http://www.nytimes.com/2009/07/11/business/11primer.html.

252. *See* Simon Romero and Clifford Krauss, Venezuelan Plan Shakes Investors, N.Y. TIMES, (Jan. 10, 2007), http://www.nytimes.com/2007/01/10/business/worldbusiness/10venezuela.html?ex=1169182800&en=07f6ff6cdd4c284a&ei=5070; Venezuela Nationalizes Private Steel Plant, CNN, Nov. 1, 2010, http://articles.cnn.com/2010-11-01/world/venezuela.nationalization_1_steel-plant-steel-mill-manufacturing-plant?_s=PM:WORLD; and Frank Jack Daniel, Venezuela to Nationalize U.S. Firm's Oil Rigs, Reuters, June 24, 2010, http://www.reuters.com/article/2010/06/24/us-venezuela-nationalizations-idUSTRE65N0UM20100624.

253. Phred Dvorak & Peter Landers, *Japanese Plant Had Barebones Risk Plan,* WALL ST. J., March 31, 2011, at A1.

7. PANDEMIC INFLUENZA (I.E., AVIAN FLU, SWINE FLU, ETC.)

While the influenza virus may have been with us since the beginning of time, according to many historians the first recognized instance of pandemic influenza seems to be 500 years ago, in year 1510 A.D.[254] Public health doctor David M. Morens notes that "other influenza pandemics probably did occur earlier, and about those we can say that they are NOW recognized as probably being both influenza and being pandemic."[255] Laurence Barton reports that, "there have been 10 pandemics over the past three centuries, the most notorious being the global flu of 1918 that killed tens of millions of people."[256] Barton continues,

> If you fast-forward to 1976, over 400 people died near the banks of the Ebola River in the Democratic Republic of the Congo as a result of a vicious, toxic pathogen. While 400 people may seem pithy compared to the death toll in 1918, it was the *manner* in which the victims of the Ebola virus died that should make you lose sleep; some medical journals reported that the organs of some of the victims poured out of their bodies within days of contracting the virus. Some in the medical community are concerned that if such a virus were to spread again (it had a whopping 95 percent fatality rate), the impact could be unprecedented. If local officials had not immediately burned affected bodies after the initial outbreak, some scientists have concluded that it was theoretically possible that the human race could have been obliterated within three months. This is no exaggeration: It was *that bad.*[257]

254. *See* David M. Morens, Jeffery K. Taubenberger, Gregory K. Folkers, and Anthony S. Fauci, *Pandemic Influenza's 500th Anniversary,* CLIN. INFECT. DIS. (2010) 51 (12): 1442-1444.

255. E-mail from David M. Morens, M.D., CAPT, United States Public Health Service, Senior Advisor to the Director, Office Of the Director, National Institute of Allergy and Infectious Diseases, National Institutes of Health, to Lawrence J. Trautman (July 6, 2015 10:18 CST) (on file with author).

256. *See* Laurence Barton, *supra* note 162 at 109.

257. *Id.*

Recent threats include the 2014-15 ebola scare,[258] the 2015 South Korean outbreak of Middle East Respiratory Syndrome (MERS),[259] and the 2016 spread of Zika virus.[260] From these examples, it seems clear that the threat of pandemic influenza is a scenario that every board should contemplate and discuss. Barton believes,

> Whenever "it" hits—whatever "it" is—its impact on the companies we own or work for will be devastating. The flu is a virus and as such will necessitate the mass development of a specific vaccine, a process that likely will take months to complete. Antibiotics are useful, but they are only effective in treating secondary illnesses caused by the flu. What's more, their availability would likely be limited only to those who can afford them. Crossing national borders and traveling internationally could be indefinitely limited or suspended. A travel or shipping embargo could be enacted (Canada shuts its borders to all international air traffic in 2003 following a bird flu outbreak) once it becomes clear that the virus has infected an alarming number of victims . . . . [M]ost companies have never taken the time to ask: What if 30 percent of all of our employees become sick and incapable of working? What if our products were impounded at port terminals and held for months? What if customers simply stop buying our product merely because *they* are hunkered down at home?[261]
>
> If a pandemic were to force curtailments in global trade, even for thirty days, imagine the impact: Commerce conducted via ports and worldwide rail stations could be suspended, and truck, tanker ship, and airliner traffic could be slowed or stopped. Products won't

258. *See* Betsy McKay & Peter Wonacott, *After Slow Ebola Response, World Seeks to Avoid Repeat,* WALL ST. J., Dec. 30, 2014, at A1; Betsy McKay, *West African Nations Struggle to Rebuild Health-Care After Ebola,* WALL ST. J., June 5, 2015, at A1; Jack Nicas, Ana Campoy & Betsy McKay, *New Push To Check Spread of Ebola,* WALL ST. J., Oct. 16, 2014, at A1; Drew Hinshaw, *For Want of Gloves, Ebola Doctors Die,* WALL ST. J., Aug. 16-17, 2014, at A1; Betsy McKay, Miguel Bustillo & Melinda Beck, *Ebola Case Puts Focus on Safeguards,* WALL ST. J., Oct. 13, 2014, at A1; Scott Gottlieb & Tevi Troy, Opinion, *Stopping Ebola Before It Turns Into a Pandemic,* WALL ST. J., Oct. 4-5, 2014, at A13; Bradley Hope, *Virus Hunter Goes After Epidemics,* WALL ST. J., May 21, 2015, at C2; Betsy McKay, *Ebola Proves Persistent in Guinea, Where Crisis Started,* WALL ST. J., Apr. 2, 2015, at A10; Manny Fernandez, *Ebola Crisis Brings Abundance of Caution Into a Dallas Community,* N.Y. TIMES, Oct. 4, 2014 at A13; Kevin Sack, Jack Healy & Frances Robles, *Life in Quarantine: 21 Days of Fear and Loathing,* N.Y. TIMES, Oct. 19, 2014 at A1; Manny Fernandez, Michael D. Shear & Abby Goodenough, *Texas Narrows Ebola Focus to 10 Considered to Be at Greatest Risk,* N.Y. TIMES, Oct. 4, 2014 at A1; Alan Feuer, News Analysis, *The Ebola Conspiracy Theories,* N.Y. TIMES, Oct. 19, 2014 at 5; Peter Loftus, *Ebola Drug Trial Is Suspended,* WALL ST. J., June 20-21, 2015, at B4.

259. *See generally* Alastair Gale & Kwanwoo Jun, *South Korea Said to Falter Early in Outbreak,* WALL ST. J., June 10, 2015, at A7.

260. Betsy McKay, *New Studies Tie Zika More Closely to Impairments,* WALL ST. J., Mar. 5-6, 2016 at A3.

261. *See* Laurence Barton, *supra* note 162 at 110.

> be shipped (food rots in storage), services can't be sold (your customers are home tending to the sick, and income will come to a halt (no mail or delivery service; IT servers may be on autopilot—but remember that your data recovery people are also out sick). Yet your employees will still expect to be paid, because somehow—magically!—the banks that oversee our mortgages and car payments will still expect *their* payments.[262]

The U.S. financial regulators have recognized the serious threat of pandemic, observing,

> For almost 100 years, the nation has not had reason to plan for a protracted absentee rate of 30 to 50 percent of a firm's personnel for four to six weeks in waves over a 12 to 18-month period; yet today firms are working to find ways to contain the spread of such an influenza, protect employees, and maintain continuity of critical business operations.[263]

8. PROLONGED POWER DISRUPTION

As might be expected, the financial services industry has been focused on the impact of prolonged power disruption for some time. Others may learn from this industry's experience. During the early 1990s, the SEC

> [E]stablished a number of programs to improve the resiliency of this critical financial sector. For example, in the early 1990s, the Commission established its Automation Review Policy ("ARP") and a cadre of specialized staff to review the capacity and resiliency of the securities markets and clearing organizations. The Commission's ARP staff inspects the information technology systems of these entities and controls over those systems, participates in periodic comprehensive evaluations of these systems, and issues

262. *Id*. *See also* Bradly J. Condon & Tapen Sinha, *Chronicle of a Pandemic Foretold: Lessons from the 2009 Influenza Epidemic,* (2009) http://ssrn.com/abstract=1398445.

263. *See* Joint Report on Efforts of the Private Sector to Implement *the Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System*, U.S. Board of Governors of the Fed. Res. System, Office of the Compt. of the Currency & Sec. and Exchange Commission Report (Apr. 27, 2006), http://www.sec.gov/news/press/studies/2006/soundpractices.pdf.

> recommendations for improvements in these programs as necessary . . . The Commission has worked extensively with the markets and clearing organizations since the tragic events of September 11th to improve their capacity to withstand wide-scale disruptions. These efforts have included fostering the development of backup data centers and trading floors, as well as agreements between markets to serve as backup trading venues for each other's securities if events warrant. The Commission has also worked with other regulators to establish best practices guidelines to strengthen the resilience of core clearance and settlement organizations. The SEC has supplemented these efforts by issuing a Policy Statement that sets forth certain basic principles of business continuity planning, including a next-day resumption goal, that should be applied by the trading markets . . .[264]

The Northeast Power Grid Failure

The northeast power grid failure of August 14–15, 2003 was a crisis "triggered not by terrorists but by a severe, cascading power outage [that] caused a major blackout [and] left 50 million people in eight states and two Canadian provinces without electricity."[265] The scope of this power failure "clearly demonstrated that the financial services sector, transportation services, telecommunications sector, water system and electric power grid are all interconnected."[266] The SEC

> [W]as consult[ing] repeatedly with officials at the securities markets and clearing organizations within the affected areas in the greater New York metropolitan region. In addition, the staff conducted a series of conference calls during the outage that provided opportunities for markets and clearing organizations

264. *See* Written Statements of the U.S. Securities and Exchange Commission Concerning the Performance of the Securities Markets During the Northeast Power Outage and Hurricane Isabel, SEC (Oct. 20, 2003), http://www.sec.gov/news/testimony/ts102003sec.htm.

265. *See* Business Roundtable, *supra* note 8 at 4.

266. *See* Business Roundtable, *supra* note 8 at 66.

> outside of New York to hear directly from the affected organizations concerning how they were coping with the power failure and how they planned to operate under these conditions . . . .[267]

Some of the commentators to the draft *Interagency Paper on Sound Practices to Strengthen the resilience of the U.S. Financial System* stated that

> The description of a wide-scale, regional disruption should include parameters for a range of probable events (*e.g.*, power disruption, natural disaster) and include the expected duration of the outage (*e.g.*, 5, 10, or 30 days) . . . . The commenters agree that a within-the-business-day recovery and resumption objective for core clearing and settlement organizations is appropriate and acknowledge that a two-hour recovery time objective is an achievable goal, although somewhat aggressive for some because of the volume and complexity of transaction data involved. There is general consensus that the end-of-business-day recovery objective is achievable for firms that play significant roles in critical markets, although many state that this is possible only if firms are able to utilize synchronous data storage technologies, which can limit the extent of geographic separation between primary and back-up sites . . . . A number of commenters support the concept of establishing back-up sites for operations and data centers that do not rely on the same infrastructure and other risk elements as primary sites and note that such diversification of risk is a long-standing principle of business continuity planning for financial firms.[268]

267. Written Statements of the U.S. Securities and Exchange Commission Concerning the Performance of the Securities Markets During the Northeast Power Outage and Hurricane Isabel, SEC (Oct. 20, 2003), http://www.sec.gov/news/testimony/ts102003sec.htm.

268. Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System, SEC Release No. 34-47638 (Apr. 7, 2003), http://www.sec.gov/news/studies/34-47638.htm.

Power outages are a concern for those doing business in many major industrial countries. The largest known power blackout in history on July 31, 2012 is estimated to have left a population of 680 million in India without power, wreaking "havoc on businesses and travelers. About 200 trains stopped operating for several hours. Metro rail services in New Delhi and its suburbs were halted. About 270 miners were stuck in two underground coal mines in eastern India as elevators stopped working."[269] The second-worse event is believed to have taken place the prior day in India, impacting "a population of 370 million, followed by a 2005 outage in Indonesia that left almost 100 million in the dark."[270] During late 2015, Ted Koppel publishes a nightmare scenario involving a cyberattack on the U.S. power grid, with devastating results.[271] Given the 2015 terrorist attacks on Paris[272] and elsewhere, Koppel's foreshadowing seems far from science fiction.

9. STRIKES AND LABOR ACTIONS

Labor strikes and work actions seem to be a daily fact of life. For example, the following strikes were reported (not an exhaustive list) while writing this article: a strike at the world's largest copper mine;[273] the U.S. National Football League lockout;[274] a state government workers strike in Wisconsin;[275] the New York police union;[276] and the NBA lockout.[277] If you rely on a sole source for critical materials or parts, an unforeseen strike or labor action may result in a crisis for you.

10. TERRORISM EVENTS

269. Amol Sharma, Saurabh Chaturvedi & Santanu Choudhury, *India's Power Network Breaks Down*, WALL ST. J., August 1, 2012, at A8.

270. *Id.*

271. *See generally* Ted Koppel, LIGHTS OUT: A CYBERATTACK; A NATION UNPREPARED; SURVIVING THE AFTERMATH (Crown Pub. 2015).

272. *See* Higgins & Schreuer, *supra* note 9. *See also* Lawrence J. Trautman, *Is Cyberattack The Next Pearl Harbor?*, 18 N.C. J.L & TECH. 232 (2016), http://ssrn.com/abstract=2711059.

273. Anthony Esposito, *Strike at Chile Escondida Copper Mine in Day 5*, Market Watch (July 25, 2011), http://www.marketwatch.com/Story/story/print?guid=584FFADE-C793-4CCD-87EA-665F437E6E9F.

274. Ralph Vacchiano, *NFL Lockout Will Continue For a Few More Weeks, Judge Urges League & Players to Start Talking Again*, N.Y. DAILY NEWS (Apr. 6, 2011, 10:48 p.m.), http://www.nydailynews.com/sports/football/nfl-lockout-continue-weeks-judge-urges-league-players-start-talking-article-1.109747.

275. *Labor Organizers Consider General Strike in Wisconsin as Gov. Scott Walker Refuses to Negotiate Over Anti-Union Bill*, DEMOCRACY NOW (Mar. 1, 2011), http://www.democracynow.org/2011/3/1/frank_emspak_of_workers_independent_news.

276. Editorial, *Gov. Cuomo's Breakthrough Labor Agreement With Police Union is Fair for Workers, New York Taxpayers*, N.Y. DAILY NEWS (Apr. 14, 2011), http://www.nydailynews.com/opinion/gov-cuomo-breakthrough-labor-agreement-police-union-fair-workers-new-york-taxpayers-article-1.109802.

277. Mitch Lawrence, *Lakers' Derek Fisher Says NBA Players are 'Frustrated' by Labor Negotiations as Lockout Looms*, N.Y. DAILY NEWS (June 9, 2011), http://www.nydailynews.com/sports/basketball/lakers-derek-fisher-nba-players-frustrated-labor-negotiations-lockout-looms-article-1.128382.

Laurence Barton contends that every organization needs to assess four fundamental issues related to terror awareness

1. How exposed is your organization?
2. How would you notify and evacuate your employees in the event of a threat or incident?
3. How will your enterprise achieve its goals and objectives (after all, that is why you are in business)
4. Do you have sufficient insurance to sustain your organization after a calamity?[278]

Best practice would suggest that boards "should always act on the assumption that you could be a direct or secondary target in a major terrorist attack. Even if a weapon of mass destruction (WMD) or another calamity does not directly impact your business, historically the impact of terror on business has been profound."[279] To further develop the point, Barton suggests that boards should consider the wider impact range including

- Immediate loss of life and survivors who must grapple with permanent injuries.
- Traumatized employees, customers, and others who witness an attack and must assist those who suffer from massive injuries.[280]

11. WAR

Since the beginning of time, with the exception of brief interludes, war seems to be a fixture of the human condition. As Palmer and Perkins observe "[w]ar needs no documentation to prove its horrors. It destroys and ruins lives beyond number; it makes anything like normal existence impossible; it imposes immense burdens on national economies and imperils the freedoms of everyone; it endangers man's very existence on this planet."[281]

12. TECHNOLOGY

Technology is inextricably linked with the other issues enumerated in this paper. New solutions and new problems will likely arise as technological advancement marches forward. Over half a century ago, John von Neumann discussed this in Fortune magazine, "[t]echnological evolution is still accelerating.

278. *See* Barton, *supra* note 162, at 175.

279. *Id.*

280. Barton, *supra* note 162, at 175.

281. NORMAN D. PALMER & HOWARD C. PERKINS, INTERNATIONAL RELATIONS: THE WORLD COMMUNITY IN TRANSITION 211 (2nd ed. 1957), https://catalog.hathitrust.org/Record/006693757 (last visited Mar. 12, 2017).

Technologies are always constructive and beneficial, directly or indirectly. Yet their consequences tend to increase instability . . . ."[282] He also warned that "[a]ll experience shows that even smaller technological changes than those now in the cards profoundly transform political and social relationships. Experience also shows that these transformations are not *a priori* predictable and that most contemporary 'first guesses' concerning them are wrong."[283]

XIII. IMPACT OF A CRISIS ON DIRECTOR TENURE AND BOARD COMPOSITION

Succession Planning

Companies must have a plan of succession in place in case top executives are incapacitated or die. Only two things are certain in life: death and taxes, so companies should plan for both. Examples of unplanned corporate successions are numerous.[284] David F. Larcker and Brian Tayan report that succession planning seems to be focused on compliance at many companies, "rather than operational (i.e., the company has a list of potential candidates but could not name a permanent successor . . . immediately)." According to survey data, "39 percent of companies report having zero 'ready now' internal candidates to fill the CEO role."[285] Incredibly, "on average, boards spend only 2 hours per year discussing succession."[286] Every board of directors should think about the unthinkable and create a contingency plan in case a disaster, like an airplane crash, takes the lives of several board members or key managers all at once. Planning for the continuation of governance is a fundamental duty of every board,[287] particularly during a crisis. The Business Roundtable stresses that

282. John von Neumann, *Can We Survive Technology*, FORTUNE (June 1955), *reprinted in* ROBERT L. PFALTZGRAFF, JR., POLITICS AND THE INTERNATIONAL SYSTEM, 247 (1969).

283. Von Neumann, *supra* note 282, at 251.

284. *See* Robin Sidel & Joann S. Lubin, *AmEx President Dies on Plane,* WALL ST. J., (May 29, 2015, 6:27 p.m.), https://www.wsj.com/articles/american-express-ed-president-gilligan-dies-1432925490; Justin Scheck & David Gauthier-Villars, *Total CEO de Margerie Embraced Risky Investments,* WALL ST. J. (Oct. 21, 2014, 3:24 p.m.), https://www.wsj.com/articles/shares-in-total-recover-strongly-after-opening-lower-1413883822; Lalitha *Naveen, Management Turnover And Succession Planning In Firms* (Arizona State University Working Paper, 2000), http://ssrn.com/abstract=219931.

285. DAVID F. LARCKER & BRIAN TAYAN, ROCK CENTER FOR CORPORATE GOVERNANCE AT STANFORD, CLOSER LOOK SER. NO. CGRP-16, SEVEN MYTHS OF CORPORATE GOVERNANCE 2 (June 1, 2011), https://www.gsb.stanford.edu/faculty-research/publications/seven-myths-corporate-governance.

286. *Id.*

287. *See generally* Lawrence J. Trautman, *The Matrix: The Board's Responsibility for Director Selection and Recruitment,* 11 FLA. ST. U. BUS. REV. 75 (2012), http://ssrn.com/abstract=1998489; Anup Agrawal, Charles R. Knoeber & Theofanis Tsoulouhas, CEO Succession: Insiders versus Outsiders, (2000), http://ssrn.com/abstract=213629; Shawn Mobbs & Charu G. Raheja*, Internal Managerial Promotions: Insider Incentives and CEO Succession,* 18 J. CORP. FIN. 1337 (2012), http://ssrn.com/abstract=1102688; Noam Wasserman, Nitin Nohria & Bharat N. Anand, *When Does Leadership Matter? The Contingent Opportunities View of CEO Leadership* (Harvard Business School Working Paper No.

> CEOs must consider the impact that security events have on employees and, in turn, on operations and resilience. Consider a scenario in which a corporation's critical business continuity experts cannot be flown to the problem site. CEO and board involvement are especially pressing, for example, when designing CEO succession strategies. How a company will function if the CEO, other senior managers and large numbers of employees are harmed deserves serious deliberation.[288]

Because executive teams tend to be located in close proximity, best practice suggests that consideration be given to "having someone in another location who could take over in a crisis. To assure business continuity in the event of a disaster, a corporation also should have information about employees available at several different locations, not just at a central headquarters."[289]

XIV. LESSONS LEARNED

Despite the countless mistakes that have been made, we have come to learn better ways to deal with disasters. Here are some tips to consider and apply when crisis strikes:

1. Treat those injured with respect and dignity;
2. Have your team and contingency plans in place;

01-063, Jan. 2001), http://ssrn.com/abstract=278652; John Harry Evans, Nandu J. Nagarajan & Jason D. Schloetzer, *CEO Turnover and Retention Light: Retaining Former CEOs on the Board*, 48 J. ACCT. RES. 1015 (2010), http://ssrn.com/abstract=1600799; MATTEO TONELLO, JOHN C. WILCOX & JUNE EICHBAUM, THE CONFERENCE BOARD, EXECUTIVE ACTION SER. NO. 312, THE ROLE OF THE BOARD IN TURBULENT TIMES: CEO SUCCESSION PLANNING (Aug. 2009), http://ssrn.com/abstract=1448021; Robert C. Giambatista, W. Glenn Rowe & Suhaib Riaz, *Nothing Succeeds Like Succession: A Critical Review of Leader Succession Literature Since 1994,* 16 LEADERSHIP Q. 963 (2005), http://ssrn.com/abstract=1403431; DAVID F. LARCKER & BRIAN TAYAN, ROCK CENTER FOR CORPORATE GOVERNANCE AT STANFORD, CLOSER LOOK SER. NO. CGRP-05, CEO SUCCESSION PLANNING: WHO'S BEHIND DOOR NUMBER ONE? (2010), http://ssrn.com/abstract=1678062; DAVID F. LARCKER & BRIAN TAYAN, ROCK CENTER FOR CORPORATE GOVERNANCE AT STANFORD, CLOSER LOOK SER. NO. CGRP-24, SUDDEN DEATH OF A CEO: ARE COMPANIES PREPARED WHEN LIGHTNING STRIKES? (2012), http://ssrn.com/abstract=2018678; Qianru Qi, The Role of Board of Directors in CEO Succession: Theory and Evidence (2011) (unpublished Ph.D. dissertation, Purdue University), http://ssrn.com/abstract=1786545; JASON D. SCHLOETZER & EDWARD FERRIS, THE CONFERENCE BOARD, DIRECTOR NOTES NO. DN-V5N3, PREPARING FOR A SUCCESSION EMERGENCY: LEARNING FROM UNEXPECTED CEO DEPARTURES (Feb. 2013), http://ssrn.com/abstract=2231236; Scott D. Graffin, Mason A. Carpenter & Steven Boivie, *What's All That (Strategic) Noise? Anticipatory Impression Management in CEO Succession,* 32 STRATEGIC MGMT. J. 748 (2011), http://ssrn.com/abstract=1611903; Volker Laux, *Corporate Governance, Board Oversight, and CEO Turnover,* 8 FOUNDATIONS AND TRENDS IN ACCOUNTING 1 (2014), http://ssrn.com/abstract=2447404.

288. *See* Business Roundtable, *supra* note 8, at 8.

289. *See* Business Roundtable, *supra* note 8, at 71.

3. Follow COSO's guidance[290] on examining enterprise risk management [ERM]:
   a. Discuss the company's risk management philosophy and risk appetite;
   b. Understand ERM practices;
   c. Regularly review your portfolio of risks relative to risk appetite; and
   d. Always be apprised of the most significant enterprise risks and responses.
4. Benefit from having previously conducted crisis drills, so that employees have thought about likely problems and have the essence of a plan in place;
5. Get the facts as soon as possible (very often initial situational awareness reports are inaccurate);
6. Control communications with all stakeholders & address their need to be informed;
7. Have a dedicated crisis manager in place that is responsible for keeping up with potential threats, maintaining crisis contingency plans, and acts as a liaison with appropriate government officials; and
8. Obtain experienced legal, accounting, compliance and crisis guidance.

Ethics and Public Policy

History teaches that some of us will be responsible corporate leaders and discharge our fiduciary duties of care by protecting crucial corporate assets, in particular, human life. Some of us during crises or in preparation for foreseeable disasters will be responsible citizens and recognize the sanctity of life by treating our fellow human beings with dignity and respect. Unfortunately, history also shows that others among us will be motivated to seek profit at the expense of the health and well-being of others. Acknowledging history, some propose that "[w]hen instances of corporate misconduct lead to death or grievous bodily injury, those cases should be a top priority and [the] DOJ should use every available resource and tool to prosecute not only the responsible companies but, more importantly, the individuals responsible for the criminal conduct."[291] For this reason, Professor Jane Barrett contends that "[t]he only way to hold scofflaw businesses accountable is to hold the individuals who make the decisions that lead to the criminal conduct accountable."[292] Professor Barrett further observes that

290. COSO has continued to publish guidance on ERM since releasing its Enterprise Risk Management – Integrated Framework in 2004. *See, e.g.*, PATCHIN CURTIS, PH.D. & MARK CAREY, DELOITTE & TOUCHE LLP, RISK ASSESSMENT IN PRACTICE (Oct. 2012).

291. Jane F. Barrett, *When Business Conduct Turns Violent: Bringing BP, Massey, and Other Scofflaws to Justice,* 48 AM. CRIM. L. REV. 287, 332 (2011), http://ssrn.com/abstract=1864612.

292. *Id.*

> [D]eath as a result of industrial activity is not an aberration nor is it likely to stop without more aggressive enforcement. The litany of the names of those killed during the last decade in 'industrial accidents' is far too long. What is sadder still is that many of these were preventable deaths. . . . Every life that is lost due to a preventable industrial event is one life too many. As a society, we place a very high value on human life and hard work. The enforcement of our laws should reflect these values and protect people, particularly workers from [those] who needlessly gamble worker lives and our environment for financial benefits or career advancement. It is past time to seriously address the trivialization of public safety crimes committed by corporate executives, managers, employees and agents.[293]

Proposed Legislation

According to Professor Barrett, "Congress has a model from which to build a criminal negligence felony for those who gamble with the lives of their employees and the general public while engaging in inherently dangerous business activities. . . . the Seaman's Manslaughter Law."[294] A similar punishment could be considered, "a violation of the Seaman's Manslaughter Law is a felony punishable by ten years in jail."[295]

XV. CONCLUSION

Creating a clear strategy and implementation plan for foreseeable industry disasters—before they occur, helps prevent mistakes made under stressful conditions. Low probability but survival-threatening disasters such as the BP Gulf of Mexico oil spill, or natural disasters such as the March 11, 2011, Japanese earthquake and tsunami, constitute any board's worse nightmare. But companies need to be awake, alert, and think about the unthinkable before, even by a slim chance, it happens. An attempt has been made to draw lessons from each of these disasters and explore how those lessons may be applied more generally across all industries when crises strike. While effective risk management is perhaps the topic highest on every board's agenda, it is imperative that thought be given to what a board might expect to confront when a corporate disaster strikes and how they will manage during crisis itself.

293. *Id.* ar 332–33.

294. *Id.* at 330, *citing* Act of July 7, 1838, § 12, 5 Stat. 304, 306 ("This statute criminalizes 'misconduct, negligence or inattention to duties,' by a captain, engineer, pilot or other person employed on a vessel, that leads to the death of a person. It is also a crime to cause the death of a person by 'fraud, neglect, connivance, misconduct or violation of law.").

295. *Id. citing* 18 U.S.C. §§ 1115, 3559 (2006).

Despite the best efforts of management to focus on industrial safety, nuclear energy and extractive industries such as oil and gas or coal mining appear to be inherently dangerous over long periods of time such that fatal accidents are inevitable. Experience teaches us that human error or natural phenomena will continue to plague these companies and more disasters are forthcoming. Therefore, every board should consider what actions they will take when the foreseeable crisis occurs.