2012

THREATS ESCALATE: CORPORATE INFORMATION TECHNOLOGY GOVERNANCE UNDER FIRE

Lawrence J. Trautman

THREATS ESCALATE: CORPORATE INFORMATION TECHNOLOGY GOVERNANCE UNDER FIRE

Lawrence J. Trautman*

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

The author wishes to extend particular thanks to the following for their assistance in the research and preparation of this article: the IT Governance Institute; Jeanne W. Ross and Peter Weill at MIT's Center for Information Systems Research; and, in particular, Kara Altenbaumer-Price. All errors and omissions are my own.

ABSTRACT

In a previous publication *The Board's Responsibility for Information Technology Governance,* (with Kara Altenbaumer-Price) we examined: The IT Governance Institute's Executive Summary and Framework for *Control Objectives for Information and Related Technology 4.1* (COBIT®); reviewed the Weill and Ross Corporate and Key Asset Governance Framework; and observed "that in a survey of audit executives and board members, 58 percent believed that their corporate employees had little to no understanding of how to assess risk." We further described the new SEC rules on risk management; Congressional action on cyber security; legal basis for director's duties and responsibilities relative to IT governance; major sources of IT risk; schematic for an IT governance framework; suggested fundamental questions every board should ask; examined board structure, composition and required IT governance skills; litigation risks and a recital of recent cases; mitigating risk through insurance; and the importance of business continuity planning. As the result of the proliferation of cyberattacks during 2010 and 2011, the SEC's Division of Corporation Finance announced new disclosure guidance for cybersecurity issues during October, 2011.

It has become apparent that newly-disclosed attacks on Information Technology infrastructure have reached crisis proportions. Therefore, a focus on IT governance must be a major priority of management and every corporate board. Issues involving Information Technology are uniquely complex and involve engineering skills that quickly become obsolete in this era of rapid technological change. Here, suggestions are offered about the value of a Chief Information Security Officer and recommendations are made for improving cybersecurity. An examination of recent threats will hopefully assist in bringing a greater understanding of their nature and increased focus on IT governance to the agenda in every boardroom.

Keywords: Accounting, Audit Committee, Board Structure, Corporate Governance, Cyberattack, Cyberwar, Data Breach, Directors, Information Technology, Internal Audit, Internal Controls, International law, Litigation, National Security, Organizational Behavior, Risk Management, Sarbanes-Oxley, SEC, Strategy,

CONTENTS

I. OVERVIEW

In a prior article, *The Board's Responsibility for Information Technology Governance*, (with Kara Altenbaumer-Price) we sounded an alarm about the escalating cyber security threats facing management and every corporate board, addressed a director's role in the risk oversight of the corporations they serve, their role in governance of IT, a director's role in mitigating IT risks, and ways in which that risk can

be transferred to or shared with others.[1] The often catastrophic examples of undesired IT results include: "business losses, reputational damage and a weakened competitive position; inability to obtain or measure a return from IT investments; failure of IT initiatives to bring the innovation and benefits they promised; technology that is inadequate or even obsolete; inability to leverage available new technologies; and deadlines that are not met and budgets that are overrun."[2]

It has become apparent that newly-disclosed attacks on Information Technology ("IT") infrastructure have reached crisis proportions. Therefore, a focus on IT governance must be a major priority of management and every corporate board. Issues involving Information Technology are uniquely complex and involve engineering skills that quickly become obsolete in this era of rapid technological change. Accordingly, it is understandable how directors in many boardrooms wonder "How can I be expected to govern something I know so little about?"[3] The complex modern environment in which data resides has also served to complicate the issues surrounding governance of IT. Professor Henry T.C. Hu, who served as the SEC's inaugural Director of the Division of Risk, Strategy, and Financial Innovation (2009-2011), concludes that "modern financial innovation has resulted in objective realities that are far more complex than in the past, often beyond the capacity of the English language, accounting terminology, visual

[1] Lawrence J. Trautman & Kara Altenbaumer-Price, *The Board's Responsibility for Information Technology Governance,* 28 J. MARSHALL J. COMPUTER & INFO. L., 313 (2011).
[2] Board Briefing on IT Governance, 2d ed., IT Governance Institute, 2003 p. 8. *See id. at* 314.
[3] 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).

display, risk measurement, and other tools on which all depictions must primarily rely."[4] Professor Hu further observes that "such characteristics can be so complex that even 'objective reality' is subject to multiple meanings."[5] I argue that these same complexities found in modern financial innovation (resulting primarily from the growth in high-speed technological data processing and exchange) are also responsible for increased difficulty in governing information technology. Data breaches may have a significant negative impact on shareholder value, with "the affected organization fac[ing] fines or other penalties, in addition to notification and security upgrade costs related to the breach. Further, companies may incur costs resulting from litigation stemming from the potential liability exposure."[6] An examination of recent threats will hopefully assist in bringing a greater understanding of their nature and increased focus on IT governance to the agenda in every boardroom.

Previously, an examination was provided of The IT Governance Institute's Executive Summary and Framework for *Control Objectives for Information and Related Technology 4.1* (COBIT®),[7] review of the Weill and Ross Corporate and Key Asset Governance Framework,[8] and observation "that in a survey of audit executives and board members, 58 percent believed that their corporate employees had little to no

[4] Henry T.C. Hu, *Too Complex to Depict? Innovation, 'Pure Information," and the SEC Disclosure Paradigm,* 90 Texas L. Rev. 1601, 1602 (2012) (describing the environment of risk inherent in complex financial instruments associated with and subsequent to the 2008-2009 global financial crisis).
[5] *Id.*
[6] Kevin M. Gatzlaff & Kathleen A. McCullough, *The Effect of Data Breaches on Shareholder Wealth* (October 1, 2008). RISK MANAGEMENT & INSURANCE REVIEW, Forthcoming. Available at SSRN: http://ssrn.com/abstract=1121172.
[7] *See* Trautman & Altenbaumer-Price, *supra* note 1, *citing* IT Governance Inst., CobiT®4.1, Executive Summary Framework 5 (2007), *available at* http://www.isaca.org/Knowledge-Center/cobit/Documents/COBIT4.pdf.
[8] *Id., citing* Weill & Ross, *supra* note 2, at 5.

understanding of how to assess risk."[9] We further described the new SEC rules on risk management;[10] Congressional action on cyber security;[11] legal basis for director's duties and responsibilities relative to IT governance;[12] major sources of IT risk;[13] schematic for an IT governance framework;[14] suggested fundamental questions every board should ask;[15] examined board structure, composition and required IT governance skills;[16] litigation risks and a recital of recent cases;[17] mitigating risk through insurance;[18] and the importance of business continuity planning.[19] In short, we previously presented a brief primer designed to assist a board in thinking about their IT domain challenges, observing

[9] PR Newswire, *Many Enterprise Risk Management Programs Lack Fundamentals, According to KPMG's Survey of Internal Auditors and Boards* (Jan. 20, 2009), *available at* http://insurancenewsnet.com/article.aspx?a=top_lh&neID=200901201680.2_02300059c02b0d35. *See also* Jody Westby, Governance of Enterprise Security CyLab 2010 Report, at 3 (June 15, 2010) (observing, "it is even worse when it comes to IT risk; with 98 percent of respondents in a recent Carnegie Mellon Cylab survey of Fortune 1000 directors and executives indicating their boards are not "actively addressing" IT operations and vendor management").

[10] Trautman & Altenbaumer-Price, *supra* note 1 at 318, *citing* SEC Releases No. 33-9089; 34-61175, Proxy Disclosure Enhancements (Dec. 16, 2009), *available at* http://sec.gov/rules/final/2009/33-9089.pdf [Final Rule Release]. (The text of the new rule reads: (h) Board leadership structure and role in risk oversight. Briefly describe the leadership structure of the registrant's board, such as whether the same person serves as both principal executive officer and chairman of the board, or whether two individuals serve in those positions, and, in the case of a registrant that is an investment company, whether the chairman of the board is an "interested person" of the registrant as defined in section 2(a)(19) of the Investment Company Act (15 U.S.C. 80a-2(a)(19)). If one person serves as both principal executive officer and chairman of the board, or if the chairman of the board of a registrant that is an investment company is an "interested person" of the registrant, disclose whether the registrant has a lead independent director and what specific role the lead independent director plays in the leadership of the board. This disclosure should indicate why the registrant has determined that its leadership structure is appropriate given the specific characteristics or circumstances of the registrant. In addition, disclose the extent of the board's role in the risk oversight of the registrant, such as how the board administers its oversight function, and the effect that this has on the board's leadership structure. New SEC rules went into effect on February 28, 2010 amending Item 407 of Regulation S-K to require disclosure about the board's role in a company's risk oversight process and its leadership structure).

[11] *Id.* at 317, 319.

[12] *Id.* at 321.

[13] *Id.* at 326.

[14] *Id.* at 328, *citing* Board Briefing on IT Governance, 2d ed., IT Governance Institute, 2003 p. 7. (presenting an overview of the role of IT governance in an enterprise, the responsibilities of boards of directors and executive management for IT governance, and tools to begin implementing effective IT governance.

[15] *Id.* at 329.

[16] *Id.* at 330.

[17] *Id.* at 332.

[18] *Id.* at 337.

[19] *Id.* at 338.

- The average loss from a corporate security breach is $234,000.[20]
- When public companies announce a breach, it typically causes a five percent drop in share price.…[21]
- At least half of data breaches or losses are believed to be caused by a lack of internal controls and process—not hackers or viruses.[22]

…. To be successful, IT governance requires enterprise commitment at the very top. Boards and executive management need to extend governance, already exercised over the enterprise, to IT by way of an effective IT governance framework that addresses strategic alignment, performance measurement, risk management, value delivery, and resource management. IT governance is an integral part of enterprise governance and consists of the leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives. Simply put, IT governance and the effective application of an IT governance framework are the responsibilities of the board of directors and executive management. And IT governance framework, such as *Control Objectives for Information and related Technology* (COBIT)[23] can be a critical element in ensuring proper control and governance over information and the systems that create, store, manipulate and retrieve it.[24] But these risks do not have to be shouldered by the company alone. Many can be transferred to or shared with insurance.

Every Governance and Nominating Committee must access its current inventory of director skill sets to require IT expertise. One choice will be to have and include IT expertise within a dedicated Risk Committee. Best practice for many will dictate that an audit committee include IT expertise and be composed of a qualified vice chairman, familiar with the company's particular audit issues by virtue of experience gained from audit committee service. This will help provide an instant replacement for the committee chair should unexpected developments require. Therefore, every board should have at least two qualified financial experts populating the audit committee and seek IT expertise and experience in director recruitment to help avoid and address the costly private and regulatory lawsuits related to cyber issues that increasingly facing companies. Every board's challenge in addressing IT risk is ongoing vigilance and recognition of the mission critical nature of Information Technology to the enterprise.[25]

---

[20] Erich Schwartzel, *Cybersecurity insurance: Many companies continue to ignore the issue*, PITTSBURGH POST-GAZETTE (June 22, 2010).
[21] Accenture Report, *How Global Organizations Approach the Challenge of Protecting Personal Data*, at 5 (2010) (available at http://www.accenture.com/NR/rdonlyres/836A71D2-4E7E-4E42-A778-4D8A40596296/0/Accenture_Data_privacy_reportLD.pdf).
[22] *Id.*
[23] See, *supra* note 3 at 4.
[24] *See Board Briefing on IT Governance, 2nd Edition supra* note 2 at 5.
[25] Trautman & Altenbaumer-Price, *supra* note 1 at 340-41.

Here, because of the alarming increased rate of disclosed cyber threats, an update of the threat assessment is provided. Hopefully, this synopsis of recent major challenges to IT security will prove helpful.

II. THREATS ESCALATE

Reports of data security breaches and cyber threats are growing by alarming proportions. Pinguelo and Muller list the various forms of cybercrime as: economic or foreign espionage, malicious insiders, spamming, phishing, email extraction programs, and hacking.[26] Professor Scott Shackelford reports that "in 2011, fully 80 percent of 200 surveyed IT executives reported that they had detected one or more attacks."[27] Moreover

> Identity theft alone costs consumers more than $5 billion per year, and firms another $48 billion increasing 21 percent in 2008 alone. In all, hundreds of millions of personal records have been exposed in hundreds of incidents. A single incident involving the theft of a laptop owned by the Veterans Administration led to the loss of 26 million social security numbers of retired and active duty military personnel resulting in a class action lawsuit claiming more than $26.5 billion in damages. In another incident, the Commerce Department managed to misplace more than 1,100 laptops, including 250 from the Census Bureau in 2006. Of these, only 107 were fully encrypted.[28]

---

[26] Fernando M. Pinguelo & Bradford W. Muller, *Virtual Crimes, Real Damages:A Primer On Cybercrimes In The United States and Efforts to Combat Cybercriminals,* 16 Va. J. L. & Tech. 116, 123-136 (2011).

[27] Scott J. Shackelford, *Should Your Firm Invest in Cyber Risk Insurance?* (December 14, 2011), Business Horizons, 2012, 6, Available at SSRN: http://ssrn.com/abstract=1972307, *citing* R. Richardson, *CSI Computer Crime & Security Survey*, (2008) Retrieved Nov. 23, 2011, from i.empnet.com/v2.gocsi.com/pfd/CSIsurvey2008.pfd.at 6 *citing* McAfee, In the Dark: Critical Industries Confronting Cyberattacks. Retrieved Nov. 23, 2011, from www.mcafee.com/us/about/news/2011/q2/20110419-01.aspx.

[28] *Id.* at 6 *citing* FTC, *Consumer Sentinel Network Databook.* (2009) Retrieved Nov. 23, 2011, from www.ftc.gov/sentinel/reports/sentinel-annual.../sentinel-cy2010.pfd.(regarding $5 billion and $48 billion numbers), J. Evers, *Veterans Affairs Faulted in Data Theft,* (2006) Retrieved Nov. 28, 2011, from http://www.zdnet.com/news/veterans-affairs-faulted-in-data-theft/148782 (regarding VA), and A. Sipress, *1,100 Laptops Missing from Commerce Dept.,* WASH. POST, A3 (2006), *See also* A. Michael Froomkin, *Government Data Breaches*, 24 Berkley Tech. L.J., 1018 (2012); University of Miami Legal Studies Research Paper No. 2009-20. Available at: http://ssrn.com/abstract=1427964.

With every year that passes, "as technology has advanced, cybercriminals have become more sophisticated, leveraging stolen information from a company to perform phishing attacks against their customers, business partners and even competitors."[29] Fernando M. Pinguelo and Bradford W. Muller report that "identity theft in cyberspace is a major concern, especially for corporations, as a well-crafted e-mail from your bank or business partner may actually have been sent by a hacker. Indeed, hackers have stolen customer e-mail lists from companies to be used in targeted phishing attacks."[30]

Mike McConnell, former U.S. Director of National Intelligence and now Booz Allen Hamilton Vice Chairman says "there isn't a corporation in the nation today that can't be penetrated, not one."[31] PWC reports that during "2003 there were 21 publicly reported incidents of large-scale loss, theft, or exposure of personally identifiable information."[32] In October 2012 alone, the Privacy Rights Clearinghouse reported 40 data breach incidents, some involving few records, others involving potentially hundreds of thousands.[33] While reported numbers differ depending on source, they are all very alarming. The Privacy Rights Clearinghouse reports that during 2011 (thru December 16,

---

[29] Fernando M. Pinguelo & Bradford W. Muller, *Virtual Crimes, Real Damages Part II: What Businesses Can Do Today to Protect Themselves from Cybercrime, and What Public-Private Partnerships are Attempting to Achieve for the Nation of Tomorrow,* 17 Va. J. L. & Tech. 75, 81 (2012).

[30] *Id. citing* Mike Lennon, *Massive Breach at Epsilon Compromises Customer Lists of Major Brands,* Security Week (Apr. 2, 2011), *available at* http://www.securityweek.com/massive-breach-epsilon-compromises-customer-lists-major-brands.

[31] Ben Worthen, *Watching and Waiting: Most Cyberattacks are Random. But some attackers know exactly whom they want, and how to strike,"* WALL ST. J., April 2, 2012, at R7.

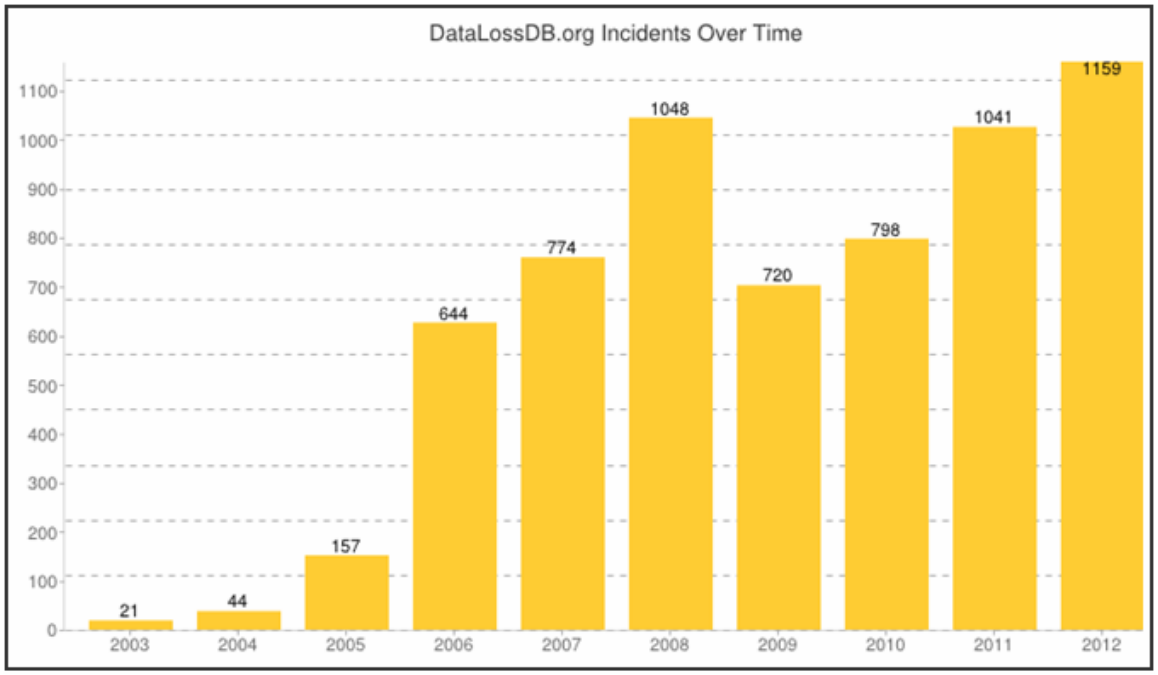
[32] PricewaterhouseCoopers, *Fortifying Your Defenses: The Role of Internal Audit in Assuring Data Security and Privacy,* 1 (July 2012), *available at* *http://cfodirect.pwc.com/CFODirectWeb/Controller.jpf?ContentCode=KOCL-8XCPWA&rss=true.*

[33] Privacy Rights Clearinghouse, *Chronology of Data Breaches 2005-Present*, http://www.privacyrights.org/data-breach (last visited Nov. 4, 2012).

2011), 535 breaches had been tracked, "involving 30.4 million sensitive records."[34]

Table 1, courtesy of Open Source Foundation / DataLossDB.org, "Reported Incidents of Loss, Theft, or Exposure of Personally Identifiable Information (PII)" presents a disturbing picture of the rapid increase in data theft during the last decade.[35]

Table 1
Reported Incidents of Loss, Theft, or Exposure of Personally Identifiable Information (PII)



Source: Open Security Foundation/DataLossDB.org. Figures for 2012 are the latest available at press time, reflecting incidents reported for the first eleven months of the year.

Here Come the Hackers

Hacking may be defined as "gaining unauthorized access to a computer system, programs or data."[36] PwC provides the following example of how easy it is for hackers

[34] Privacy Rights Clearinghouse, *Data Breaches: A Year in Review* (Dec 16, 2011), *available at* https://www.privacyrights.org/data-breach-year-review-2011.
[35] Open Security Foundation/DataLossDB.org, *Data Loss Statistics: Number of Incidents, available at* *http://datalossdb.org/statistics* (last visited Nov. 3, 2012).
[36] *Id.* at 132.

to gain access to information about "corporate databases: using social media to get past IT administrators, the guardians of much company data."[37] Accordingly

> In a number of very recent large breaches, hackers have perused LinkedIn connections to find IT administrators. Then, they locate an administrator's Facebook profile and send him or her an email designed to look as though it came from one of their Facebook friends. Such emails typically provide a link that directs the recipient to log back into Facebook; however, the link is false and instead uploads a file onto the IT administrator's computer, which then provides the hacker a window through which to quickly download sensitive data.[38]

Recent Major Breaches

Here is a partial recital of newly reported major breaches:

- **EMC/RSA.** Encounters a compromise of security tokens during March 2011 and discloses March 17, 2011.[39]
- **EPSILON.** Detects a breach of customer email addresses on March 31, 2011 and discloses the next day.[40]
- **SONY.** Experiences a theft of customer data belonging to 100 million people on April 20, 2011, and makes a public disclosure on April 26, 2011.[41]
- **CITIGROUP.** Detects a breach of credit card numbers affecting 360,069 accounts on May 10, 2011 and discloses on June 9, 2011.[42]
- **LOCKHEED MARTIN.** Encounters a "significant and tenacious attack' against its computer networks on May 21, [2011]."[43]

---

[37] PricewaterhouseCoopers, *supra* note 32.
[38] *Id.* at 5.
[39] Ben Worthen & Anton Troianovksi, *Firms Come Clean on Hacks,* WALL ST. J., June 17, 2011, at B1.
[40] *Id.*
[41] *Id. See also* Ian Sherr, *Hackers Breach Second Sony Services,* WALL ST. J., May 3, 2011, at B1.
[42] *Id.*

- **AUTOMATED DATA PROCESSING.** Announces on June 15, 2011 that it encountered a breach at a recently acquired benefits administration provider.[44]
- **SEGA CORP.** Discloses that "a hacker stole the personal information of nearly 1.3 million users of its online service from a company database… [adding] it doesn't store credit card information…."[45]
- **SK COMMUNICATIONS (South Korea).** Encounters a breach resulting in the compromise of data involving 35 million Nate and CyWorld social network users.[46]
- **STEAM (VALVE, INC.).** Experiences a database breach on November 6, 2011 and reports on November 10, 2011 access of 35 million records containing "user names, hashed and salted passwords, game purchases, email addresses, billing addresses and encrypted credit card information accessed by hacker(s)."[47]
- **TIANYA.** Reports 40 million clear-text passwords and user names of forum members leaked online by hackers discovered on Dec. 25, 2011, reported next day.[48]

---

[43] Ben Worthen, Russell Adams, Nathan Hodge & Evan Ramstad, Hackers Broaden Their Attacks, WALL ST. J., May 31, 2011, at B1.
[44] Press Release, ADP, ADP Statement on Security Breach Investigation (June 15, 2011) (on file with the authors).
[45] Daisuke Wakabayashi, *Data of 1.3 million Users Stolen From Online Service,* WALL ST. J., June 20, 2011, at B4.
[46] Pinguelo & Muller, *supra* note 29 at 77, *citing* Liam Tung, *Anatomy of a Cunning APT: The SK Communications Breach,* CSO ONLINE, (Sept.29, 2011), *available at* http://www.cso.com.au/article/402450/anatomy_cunning_apt_sk_communications_breach.
[47] Open Source Foundation / DataLossDB.org., *Steam (Valve, Inc.)* (Nov. 10, 2011), (showing incident 4942), *available at http://datalossdb.org/statistics.*
[48] Open Source Foundation / DataLossDB.org., *Tianya* (Dec. 25, 2011), (showing incident 5285), *available at http://datalossdb.org/statistics.*

- **ZAPPOS.** The online shoe-and-clothing retailer discloses that a cyberattack breached "at least 24 million customer accounts."[49]
- **NORTEL NETWORKS LTD.** Reports that hackers evidently enjoyed widespread access to this telecommunications firm's computer network (for almost a decade).[50]
- **GLOBAL PAYMENTS, INC.** Credit card processor Global Payments, Inc. reports that "hackers stole account numbers and other key information from up to 1.5 million accounts in North America."[51]
- **SHANGHAI ROADWAY D&B SERVICES CO. LTD.** Reports in March 2012 the largest ever reported incident involving 150 million records (even larger than the Heartland Payments breach).[52]
- **FIDELITY NATIONAL INFORMATION SERVICES.** The Wall Street Journal reports that "security issues at FIS are outlined in a six-page confidential report sent in late February by the Federal Deposit Insurance Corp. [to the company]."[53] Moreover, "the security issues at FIS underscore the potential hazards that banks can face when they outsource some of their basic work." This Jacksonville, Florida-based company, known as FIS, reportedly assists 14,000 financial institutions with transaction processing.[54]

---

[49] John Letzing, *Attack Hits Zappos Accounts,* WALL ST. J., Jan. 17, 2012, at B7.
[50] Siobhan Gorman, *Chinese Hackers Suspected in Long-Term Nortel Breach*, WALL ST. J., Feb. 14, 2012, at A1.
[51] Robin Sidel, *Card Processor: Hackers Stole Account Numbers,* WALL ST. J., April 2, 2012, at C1.
[52] Open Source Foundation / DataLossDB.org., *Shanghai Roadway D&B Marketing Services Co. Ltd.,* (Mar. 3, 2012), (showing incident 5883), *available at* http://datalossdb.org/statistics.
[53] Robin Sidel, *Major Data Firm in Security Pinch,* WALL ST. J., June 6, 2012, at C1.
[54] *Id.*

- **LINKEDIN.** During June 2012 LinkedIn comes "under fire since 6.5 million user passwords were stolen and published on an unauthorized website."[55] A LinkedIn spokesperson "said in a blog post that the Company is working closely with the Federal Bureau of Investigation as it 'aggressively' pursues the perpetrators of this crime."[56]
- **YAHOO.** On July 13, 2012, Yahoo suffers a "data breach that allowed a hacker group to download about 453,000 unencrypted user names and passwords, a revelation that also threatened users' email accounts with other Web companies."[57]
- **ARAMCO.** U.S. Defense Secretary Leon Panetta "noted a July [2012] attack against Saudi Arabia's state oil company, Aramco, in which a virus erased critical files on some 30,000 computers, replacing them with images of burning American flags."[58]
- **KNIGHT CAPITAL.** A computer-trading software glitch on August 1, 2012 results in a $440 million financial loss from a flood of accidental securities trades,[59] resulting during two-days alone in "the company's market value [plunging] to $253.4 million from $1.01 billion."[60] SEC Chairman Mary Shapiro observes "reliance on computers is a fact of life

[55] Shayndi Raice & Ben Worthen, *LinkedIn Defends Reaction In Wake of Password Theft,* WALL ST. J., June 11, 2012, at B3.
[56] *Id.*
[57] Drew FitzGerald, *Yahoo Passwords Stolen In Latest Data Breach,* WALL ST. J., July 13, 2012, at B2.
[58] Julian E. Barnes & Siobhan Gorman, *U.S. Readies Defense Against Cyberthreats,* WALL ST. J., Oct. 12, 2012, at A5.
[59] Julie Steinberg, Jenny Strasburg & Dan Fitzpatrick, J.P. Morgan Rankled by Risk, WALL ST. J., Aug. 31, 2012, at C1.
[60] Jenny Strasburg & Jacob Bunge, *Loss Swamps Trading Firm,* WALL ST. J., Aug. 3, 2012, at A1, *See also* Jacob Bunge, Anupreeta Das & Telis Demos, *Loyalty, Profit Drive Knight Rescue,* WALL ST. J., Aug. 7, 2012, at C1.

not only in markets everywhere, but in virtually every facet of business. That doesn't mean we should not endeavor to reduce the likelihood of technology errors and limit their impact when they occur."[61]

III. THE SONY BREACH

If any director remains unconvinced as to the gravity and magnitude that cyber threats pose to every enterprise, the following assessment from Sony Corp. Chief Executive Howard Stringer should resolve any doubts. Following a 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."[62] With analysts estimating that the breach may result in costs to Sony of as much as $1 billion, Sony Corp. Chief Executive Howard Stringer observes after devoting weeks to resolve the breach that, "he can't guarantee the security of the company's videogame network or any other Web system in the 'bad new world' of cybercrime."[63] Moreover, "maintaining the service's security is a 'never-ending process' and he doesn't know if anyone is 100% secure."[64] Several weeks later, three individuals were arrested in Spain and charged in the Sony web attack.[65]

---

[61] Press Release 2012-151, U.S. Securities and Exchange Commission, *Chairman Shapiro Statement on Knight Capital Group Trading Issue* (Aug. 3, 2012), *available at* htty://www.sec.gov/news/press/2012/2012-151.htm.
[62] Daisuke Wakabayashi, *Sony CEO Warns of "Bad New World,"* WALL ST. J., May 18, 2011, at B1.
[63] *Id.*
[64] *Id.*
[65] Cassell Bryan-Low & David Roman, Spain Arrests 3 in Sony Web Attack, WALL ST. J., June 11-12, 2011, at B1.

IV. NORTEL HACKED

Nortel Networks, a Canadian company, traded publicly in the U.S., "was a pioneering maker of the computer switches and telecom gear that powers much of the world's phone and internet networks."[66] Dating back to at least the year 2000, it appears Chinese-based hackers successfully gained access, by using seven stolen passwords, including a former CEO's, to penetrate and leisurely download materially everything they wanted from Nortel Networks.[67] This breach included the download of "technical papers, research-and-development reports, business plans, employee emails and other documents according to Brian Shields, a former 10-year Nortel veteran who led an internal investigation."[68] The Wall Street Journal observes that "Nortel's breach offers a rare level of detail about a type of international corporate espionage that is of a growing concern to U.S. officials. A U.S. intelligence report released in November [2011] concluded that hackers operating from China… are the world's most 'active and persistent' perpetrators of industrial spying."[69]

Embedded Acquisition Risk?

Nortel has been in the process of selling off its component parts pursuant to their 2009 bankruptcy. However, according to several former employees, "the company didn't fix the hacking problem before starting to sell its assets, and didn't disclose the hacking to prospective buyers."[70] Accordingly, this Nortel example appears to be fair warning to all-- of the Trojan horse potential for highly destructive malware and spyware through acquisitions of data assets. Sean McGurk, credited with previously running the U.S.

[66] Siobhan Gorman, *Chinese Hackers Suspected in Long-Term Nortel Breach*, WALL ST. J., Feb. 14, 2012, at A1.
[67] *Id.*
[68] *Id.*
[69] *Id.*
[70] *Id.* at A16.

government's cybersecurity intelligence center, states "When you are buying those files or that intellectual property, you're also buying that 'rootkit,'… a term that refers to embedded spy software."[71]

> The spyware unearthed in 2009 was a sophisticated mix… researchers found a particularly malicious and hard-to-spot spying tool, namely 'rootkit' software that can give a hacker full control over a computer and enables them to conceal their spying campaign….
>
> On one computer, hackers had set up an encrypted communications channel to an Internet address near Beijing. On the other computer, the investigators found a program that hackers were likely using to sniff out other security weaknesses within Nortel's networks. The hackers had created a 'reliable back door," according to one person familiar with the investigation, allowing them to come and go as they pleased in Nortel's network.[72]

V. WYNDHAM HOTELS: THE FTC TAKES ACTION

During June 2012 The Federal Trade Commission filed suit against international hospitality operator Wyndham Worldwide Corporation and three of its subsidiaries "for alleged data security failures that led to three data breaches at Wyndham hotels in less than two years."[73] The FTC complaint "alleges that these failures led to fraudulent charges on consumers' accounts, millions of dollars in fraud loss, and the export of hundreds of thousands of consumers' payment card account information to an Internet domain address registered in Russia."[74] The April 2008 breach "affected more than 500,000 credit card accounts;" while "two more breaches occurred in 2009, the F.T.C. said, each giving the intruders access to 50,000 or more consumer card accounts."[75] The

---

[71] *Id.*
[72] *Id.*
[73] Press Release, *FTC Files Complaint Against Wyndham Hotels For Failure to Protect Consumers' Personal Information* (June 26, 2012), *available at* http://www.ftc.gov/opa/2012/06/wyndham.shtm.
[74] *Id.*
[75] Edward Wyatt, *Hotel Group Charged Over Data Thefts,* N.Y. Times, June 27, 2012, at B3.

Wyndham case is part of ongoing efforts by the FTC to ensure that companies live up to their privacy and data security promises to consumers.

The FTC further alleges that "Wyndham's privacy policy misrepresented the security measures that the company and its subsidiaries took to protect consumers' personal information**,** and that its failure to safeguard personal information caused substantial consumer injury. The agency charged that the security practices were unfair and deceptive and violated the FTC Act."[76] According to the FTC, "since 2008 Wyndham has claimed, on its Wyndham Hotels and Resorts subsidiary's website that, 'We recognize the importance of protecting the privacy of individual-specific (personally identifiable) information collected about guests, callers to our central reservation centers, visitors to our Web sites, and members participating in our Loyalty Program ….'"[77] According to the FTC

> The repeated security failures exposed consumers' personal data to unauthorized access. Wyndham and its subsidiaries failed to take security measures such as complex user IDs and passwords, firewalls and network segmentation between the hotels and the corporate network, the agency alleged. In addition, the defendants allowed improper software configurations which resulted in the storage of sensitive payment card information in clear readable text.
>
> Each Wyndham-branded hotel has its own property management computer system that handles payment card transactions and stores information on such things as payment card account numbers, expiration dates, and security codes. According to the FTC, in the first breach in April 2008, intruders gained access to a Phoenix, Arizona Wyndham-branded hotel's local computer network that was connected to the Internet and the corporate network of Wyndham Hotels and Resorts. Because of Wyndham's inadequate security procedures, the breach gave the intruders access to the corporate network of Wyndham's Hotels and Resorts subsidiary, and the property management system servers of 41Wyndham-branded hotels. This access enabled the intruders to:
>
> - install "memory-scraping" malware on numerous Wyndham-branded hotels' property management system servers.

[76] FTC, *supra* note 73.
[77] *Id.*

- access files on Wyndham-branded hotel's property management system servers that contained payment card account information for large numbers of consumers, which was improperly stored in clear readable text.[78]

VI. FBI CYBER CRIME TAKEDOWN

During mid-2012, the Federal Bureau of Investigation (FBI), announced "the largest coordinated international law enforcement action in history directed at 'carding' crimes—offenses in which the Internet is used to traffic in and exploit the stolen credit card, bank account, and other personal identification information of hundreds of thousands of victims globally."[79] The coordinated cybercrime sting—involving 13 countries, including the United States—

> resulted in 24 arrests, including the domestic arrests of 11 individuals by federal and local authorities in the United States, and the arrests of 13 individuals abroad by foreign law enforcement in seven countries. In addition, the federal and local authorities and authorities overseas today conducted more than 30 subject interviews and executed more than 30 search warrants. These FBI coordinated actions result from a two-year undercover operation led by the FBI that was designed to locate cybercriminals, investigate and expose them, and disrupt their activities.
>
> In the course of the undercover operation, the FBI contacted multiple affected institutions and/or individuals to advise them of discovered breaches in order to enable them to take appropriate responsive and protective measures. In doing so, the FBI has prevented estimated potential economic losses of more than $205 million, notified credit card providers of over 411,000 compromised credit and debit cards, and notified 47 companies, government entities, and educational institutions of the breach of their networks.[80]

Those 11 arrests took place "in the United Kingdom (6 arrests), Bosnia (2), Bulgaria (1), Norway (1), and Germany (1). Two additional defendants were arrested in

---

[78] *Id.*
[79] FBI Press Release, *Manhattan U.S. Attorney and FBI Assistant Director in Charge Announce 24 Arrests in Eight Countries as Part of International Cyber Crime Takedown* (June 26, 2012), *available at* http://www.fbi.gov/newyork/press-releases/2012/manhattan-u.s.-attorney-and-fbi-assistant-director-in-charge-announce-24-arrests-in-eight-countries-as-part-of-international-cyber-crime-takedown.
[80] *Id.*

foreign countries based on provisional arrest warrants obtained by the United States in connection with complaints unsealed today in the Southern District of New York."[81] The FBI allegations "chronicle a breathtaking spectrum of cyber schemes and scams… individuals sold credit cards by the thousands and took the private information of untold numbers of people. As alleged, the defendants casually offered every stripe of malware and virus to fellow fraudsters."[82]

Background on the Undercover Operation

According to the FBI press release, "In June 2010, the FBI established an undercover carding forum called "Carder Profit" (the "UC Site"), enabling users to discuss various topics related to carding and to communicate offers to buy, sell, and exchange goods and services related to carding, among other things."[83]

> Since individuals engaged in these unlawful activities on one of many other carding websites on the Internet, the FBI established the UC Site in an effort to identify these cybercriminals, investigate their crimes, and prevent harm to innocent victims. The UC Site was configured to allow the FBI to monitor and to record the discussion threads posted to the site, as well as private messages sent through the site between registered users. The UC Site also allowed the FBI to record the Internet protocol (IP) addresses of users' computers when they accessed the site. The IP address is the unique number that identifies a computer on the Internet and allows information to be routed properly between computers.
>
> Access to the UC Site, which was taken offline in May 2012, was limited to registered members and required a username and password to gain entry. Various membership requirements were imposed from time to time to restrict site membership to individuals with established knowledge of carding techniques or interest in criminal activity. For example, at times, new users were prevented from joining the site unless they were recommended by two existing users who had registered with the site or unless they paid a registration fee.
>
> New users registering with the UC Site were required to provide a valid e-mail address as part of the registration process. The e-mail

[81] *Id.*
[82] *Id.*
[83] *Id.*

addresses entered by registered members of the site were collected by the FBI.[84]

Background on Carding Crimes

The FBI provides a useful explanation of how many of these illegal criminal activities are conducted, as follows

> "Carding" refers to various criminal activities associated with stealing personal identification information and financial information belonging to other individuals—including the account information associated with credit cards, bank cards, debit cards, or other access devices—and using that information to obtain money, goods, or services without the victims' authorization or consent. For example, a criminal might gain unauthorized access to (or "hack") a database maintained on a computer server and steal credit card numbers and other personal information stored in that database. The criminal can then use the stolen information to, among other things, buy goods or services online; manufacture counterfeit credit cards by encoding them with the stolen account information; manufacture false identification documents (which can be used in turn to facilitate fraudulent purchases); or sell the stolen information to others who intend to use it for criminal purposes. Carding refers to the foregoing criminal activity generally and encompasses a variety of federal offenses, including, but not limited to, identification document fraud, aggravated identity theft, access device fraud, computer hacking, and wire fraud.
>
> "Carding forums" are websites used by criminals engaged in carding ("carders") to facilitate their criminal activity. Carders use carding forums to, among other things, exchange information related to carding, such as information concerning hacking methods or computer-security vulnerabilities that could be used to obtain personal identification information; and to buy and sell goods and services related to carding—for example, stolen credit or debit card account numbers, hardware for creating counterfeit credit or debit cards, or goods bought with compromised credit card or debit card accounts. Carding forums often permit users to post public messages—postings that can be viewed by all users of the site—sometimes referred to as threads. For example, a user who has stolen credit card numbers may post a public thread offering to sell the numbers. Carding forums also often permit users to communicate one-to-one through so-called private messages. Because carding forums are, in essence, marketplaces for illegal activities, access is typically restricted to avoid law enforcement surveillance. Typically, a prospective user seeking to join a carding forum can only do so if other, already established users vouch for him or her, or if he or she pays a sum of

[84] *Id.*

money to the operators of the carding forum. User accounts are typically identified by a username and access is restricted by password. Users of carding forums typically identify themselves on such forums using aliases or online nicknames ("nics").

Individuals who use stolen credit card information to purchase goods on the Internet are typically reluctant to ship the goods to their own home addresses, for fear that law enforcement could easily trace the purchases. Accordingly, carders often seek out "drop addresses"—addresses with which they have no association, such as vacant houses or apartments—where carded goods can be shipped and retrieved without leaving evidence of their involvement in the shipment. Some individuals used carding forums to sell "drop services" to other forum members, usually in exchange for some form of compensation. One frequently used form of compensation is a "1-to-1" arrangement in which the carder wishing to ship to the drop must ship two of whatever items he has carded—one for the provider of the drop to forward to the carder and the other for the provider of the drop to keep as payment in kind for the carder's use of the drop. Another frequently used compensation arrangement is for the carder and the drop provider to agree to resell the carded items shipped to the drop and to split the proceeds between them.[85]

VII. BARBARIANS AT THE GATES

Post 9/11 Transnational Legal Framework

The increased reliance on cyber warfare and advances in computer technology as a front line of offensive and defensive national security weapons means that "cybersecurity is the newest and most unique national security issue of the twenty-first century."[86] This defacto new transnational legal environment has evolved following the 9/11 destruction of the World Trade Center in New York City and is "turbocharged by [the] unexpected recent challenges, which include terrorism, financial chaos, and environmental and national security."[87] Stuart S. Malawer observes that "the emergent

[85] *Id.*
[86] Stuart S. Malawer, *Cyber Warfare: Law and Policy Proposals for U.S. and Global Governance,* 58 Virginia Lawyer 28 (2010), *available at* http://ssrn.com/abstract=1437002, *citing* Wesley Clark & Levin, *Securing the Information Highway: How to Enhance the United States Electronic Defenses,* Foreign Affairs 2 (Nov/Dec 2009).
[87] Stuart S. Malawer, *Global Law and Global Challenges* 58 Virginia Lawyer 27 (Feb. 2010), *available at* http://ssrn.com/abstract=1437002.

rules are drawn from disparate legal systems. This newer body of legal rules is termed 'global law,' which can be defined as legal rules drawn from different systems that address a range of cross-border topics."[88] Moreover

> The rules originate from public international law (such as the law of war), specialized international legal systems (such as rules governing the international environment, global trade, and international finance), regional legal systems (governing such areas as human rights), and major national legal systems as they confront transnational problems (such as torture, counterterrorism, and cybersecurity). These rules sometimes establish binding obligations, and other times, something less.
>
> To competently practice law and undertake policy analysis in today's world of failing states, transnational terrorism, global pollution, and growing multilateral institutions, practitioners and policy makers must understand the legal contours of this dramatically changing environment.[89]

Assault on Federal, State and Local Governments

Pinguelo and Bradford W. Muller report that "the weak American economy has caused most states to severely trim their budgets, reducing their ability to devote expenditures to cyberdefense."[90] As a result, most states "remain an appealing target for cybercriminals, as their networks hold some of their citizens' most vital information, including health and driving records, educational and criminal records, professional licenses, and tax information.[91] In particular

> State universities are an especially vulnerable target, as shown in May 2009 when officials at the University of California-Berkeley announced that hackers had stolen the Social Security numbers of approximately 97,000 students, alumni, and others over the course of six months. Meanwhile, in September 2010, cybercriminals stole nearly $1 million from the University of Virginia's College at Wise. The cyber thieves compromised a computer belonging to the university's comptroller, and

---

[88] *Id.*
[89] *Id.*
[90] Pinguelo & Bradford W. Muller, *supra* note 26 at 120, *citing* Deloitte & NASCIO, *State Goverrnments at Risk: A Call to Secure Citizen Data and Inspire Public Trust (2010), available at* http://www.nascio.org/publications/documents/Deloitte-NASCIOCybersecurityStudy2010.pdf.
[91] *Id. citing* Deloitte.com, *Transcript: The Cyber Savvy State Government, available at* http://www.deloitte.com/view/en_US/us/Insights/Browse-by-Content-Type/podcasts/4233ed6b7e109210VgnVCM200000bb42f00aRCRD.htm.

> used a computer virus to gain access to the University's bank account. Luckily, the school was able to recover the money.[92]

While potentially applicable at the state government level, the Government Accounting Office (GAO), in their 2009 report for the federal government, outlined the following six major sources of cyber threats: "foreign nations, criminal groups, hackers, hacktivists [politically motivated attacks], disgruntled insiders and terrorists."[93]

> In a post-9/11 world, the prospect of a rogue cyberterrorist is particularly frightening, especially when considering some of the methods that could be used to cripple the nation: [A] cyberterrorist might hack into computer systems and disrupt domestic banking, the stock exchanges and international financial transactions, leading to a loss of confidence in the economy. Or he might break into an air traffic control system and manipulate it, causing planes to crash or collide. A terrorist could hack into a pharmaceutical company's computers, changing the formula of some essential medication and causing thousands to die. Or a terrorist could break into a utility company's computers, changing pressure in gas lines, tinkering with valves and causing a suburb to detonate and burn.[94]

Cyberattack: A National Security Issue

"The next Pearl Harbor that we confront could very well be a cyberattack that cripples' America's electrical grid and its security and financial systems," observed Central Intelligence Agency Director Leon Panetta in his June 9, 2011 confirmation hearing for the post of secretary of defense before the Senate Armed Services Committee.[95] Pinguelo and Muller report that "espionage is a hot topic in the cyber

---

[92] *Id.* at 120 n18.
[93] *Id.* at 122.
[94] *Id. citing* Mark D. Goodman & Susan W. Brenner, *The Emerging Consensus on Criminal Conduct in Cyberspace,* __ UCLA J.L. & Tech. 3, 18 (2002), *available at* http://www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf.
[95] Anna Mulrine, *CIA Chief Leon Panetta: The Next Pearl Harbor Could Be a Cyberattack,* The Christian Science Monitor, June 9, 2011 available at http://www.csmonitor.com/USA/Military/2011/0609/CIA-chief-Leon-Panetta-The-next-Pearl-Harbor-could-be-a-cyberattack (last viewed June 19, 2011), *see also* Eric Talbot Jensen, *President Obama and the Changing Cyber Paradigm,* 37 WM. MITCHELL L. REV. 5049 (2011), *available at* http://ssrn.com/abstract=1740904, *and* Stuart Malawer, *Cyberwarfare: Law & Policy Proposals for U.S. & Global Governance,* 58 VA. LAWYER 28 (2010) GMU School of Public Policy Research Paper No. 2009-11, *available at* http://ssrn.com/abstract=1437002, *and* Scott Shackelford, *From*

realm. In August 2010, the Department of Defense issued a report discussing China's increased use of 'information warfare units' to develop viruses to attack enemy computer systems and networks."[96] A Wall Street Journal article titled *Cyber Combat: Act of War*, observes "The Pentagon's first formal cyber strategy… represents an early attempt to grapple with a changing world in which a hacker could pose as significant a threat to U.S. nuclear reactors, subways or pipelines as a hostile country's military."[97] Does your organization's management and board have a contingency plan in place in the event that the U.S. power grid is compromised and electricity becomes unavailable for a prolonged period of time?

> Recent attacks on the Pentagon's own systems--- as well as the sabotaging of Iran's nuclear program via the Stuxnet computer worm— have given new urgency to U.S. efforts to develop a more formalized approach to cyber attacks. A key moment occurred in 2008, when at least one U.S. military computer system was penetrated. This weekend Lockheed Martin, a major military contractor, acknowledged that it had been the victim of an infiltration, while playing down its impact….
>
> One idea gaining momentum at the Pentagon is the notion of 'equivalence.' If a cyber attack produces the death, damage, destruction or high-level disruption that a traditional military attack would cause, then it would be a candidate for a "use of force" consideration, which could merit retaliation."[98]

Deputy Secretary of Defense William Lynn says "If we can minimize the impact of attacks on our operations and attribute them quickly and definitively, we may be able to change the decision calculus of an attacker… [noting] a 'foreign intelligence service'

Nuclear War to Net War: Analogizing Cyber Attacks in International Law, 25 BERKELEY J. INT'L L. 191 (2009).

[96] Pinguelo & Bradford W. Muller, *supra* note 26 at 123, *citing* Lolita C. Baldor, *Pentagon Takes Aim at China Cyber Threat,* Associated Press, (Aug. 19, 2010), *available at* http://www.boston.com/news/nation/washington/articles/2010/08/19/pentagon_takes_aim_at_china_cyber_threat/?page=1.

[97] Siobhan Gorman & Julian E. Barnes, *Cyber Combat: Act of War*, WALL ST. J., May 31, 2011, at A1.

[98] *Id.*

had stolen 24,000 files from a U.S. defense contractor in a March [2011] cyberattack."[99] Worthy of note, "Each year, a volume of intellectual property exceeding the size of the Library of Congress is stolen from U.S. Government and private-sector networks, the [mid-2011] Pentagon strategy document says."[100]

Mortimer Zuckerman, chairman and editor in chief of U.S. News & World Report adds, "Cyberterrorism poses a threat equal to that of weapons of mass destruction. A large scale attack could create an unimaginable degree of chaos in America."[101] Zuckerman continues

> We should think of cyberattacks as guided missiles and respond similarly-- intercept them and retaliate. This means we need a federal agency dedicated to defending our various networks. You cannot expect the private sector to know how—or to have the money—to defend against a nation-state attack in a cyberwar… Few nations have used computer networks as extensively as we have to control electric power grids, airlines, railroads, banking and military support. Few nations have more of these essential systems owned and operated by private enterprise. As with 9/11, we do not enjoy the luxury of a dilatory response.[102]

What if major transportation systems are disrupted, such as airlines traffic control systems? Cyber attacks may negatively impact your business operations, even if your enterprise is not the sole focus of attack. What would be the result to your operations if the U.S. payment systems are compromised by a successful cyber attack on financial institutions? The SEC has reported that a study, *Observations on Developments in Risk*

---

[99] Julian E. Barnes & Siobhan Gorman, *Cyberwar Plan Has New Focus On Deterrence*, WALL ST. J., July 15, 2011, at A5.
[100] *Id.*
[101] Mortimer Zuckerman, , *How to Fight and Win the Cyberwar*, WALL ST. J., Dec. 6, 2010, at A19; *See also* Susan W. Brenner & Leo L. Clarke, *Civilians in Cyberwarfare: Conscripts* 43 VAND. J. TRANSNAT'L L. (2010), *available at* http://ssrn.com/abstract=1650743, Susan W. Brenner & Leo L. Clarke, *Civilians in Cyberwarfare: Casualties,* 13 SMU Sci. & Tech. L. Rev. (2010), *available at* http://ssrn.com/abstract=16507438.
[102] *Id.*

Appetite Frameworks and IT Infrastructures, has been conducted by senior financial supervisors from ten countries, concluding

> [T]hat while firms have made progress in developing risk appetite frameworks and have begun multi-year projects to improve IT infrastructure, considerably more work must be done to strengthen these practices. In particular, the aggregation of risk data remains a challenge, despite its criticality to strategic planning, decision making, and risk management.[103]

Richard Clarke, former White House national security advisor to three U.S. presidents, has recently written "If we discovered Chinese explosives laid throughout our national electrical system, we'd consider it an act of war. Digital bombs pose as grave a threat."[104] Just a few days prior to Richard Clarke's published article, Google, Inc. reported that "Chinese hackers targeted the email accounts of senior U.S. officials and hundreds of prominent people in a fresh computer attack certain to intensify growing concern about the security of the Internet."[105] More recently Clarke observes

> Ongoing cyber 'hacktivism' has… demonstrated three things that should cause nations to act. First, the ease with which the hacktivists have been able to steal data and to shut down Web pages suggests that companies (and perhaps governments) in the region [Middle East] have not yet taken cyber security seriously. Governments in other regions (Asia, Europe, North America) have been educating, assisting and regulating companies to improve their cyber security. There has been a notable lack of such government activity in the Middle East, and that inactivity has opened the way for citizen hackers to cause the mischief we see today.
>
> If the hackers turn their attention to disruption and destruction, as some have threatened, they are likely to find the controls for electric power grids, oil pipelines and precious water systems inadequately secured. If a hacker causes real physical damage to critical systems in that

[103] SEC Release No. 2010-256, Senior Supervisors Group Issues Report on Risk Appetite Frameworks and IT Infrastructure (Dec. 23, 2010), *available at* http://sec.gov/news/press/2010/2010-256.htm.
[104] Richard Clarke, *China's Cyberassault on America,* WALL ST. J., June 15, 2011, at A15.
[105] Amir Efrati & Siobhan Gormans, *Google Mail Hack Is Blamed on China*, WALL ST. J., June 2, 2011, at A1. *See also* Siobhan Gorman, *China Tech Giant Under Fire,* WALL ST. J., Oct. 8, 2012, at A1, and Spencer E. Ante, *Huawei's Ally: IBM,* WALL ST. J., Oct. 10, 2012, at B1.

> region, it could quickly involve governments retaliating against each other with both cyber and conventional weapons. Middle Eastern governments need to get their citizen hackers under control and better protect their own critical networks, or they will eventually be dragged into unwanted conflict.
>
> Second, the Arab-Israeli hacker exchanges have demonstrated again the lack of any effective international organization to assist in preventing cyber crime and de-escalating tensions among nations in cyberspace. The Budapest Convention on Cyber Crime, which entered into force in July 2004 and has been ratified by more than 40 countries including the U.S., does require nations to assume responsibilities for any attacks that originate in their cyberspace.[106]

Clarke proposes an "International Cyber Risk Reduction Center," and notes, "If, as happened…., Saudi Arabia's stock market is again knocked off-line by a cyber attack originating in Israel (or vice versa), the Saudi's should be able to call an international center and seek assistance."[107] Furthermore, "Israel as a member of the international center should be able to act promptly to see the attack and shut it down. All of this should happen in a few hours."[108] Scholars are exploring how computer warfare might "limit unnecessary suffering and reduce civilian casualties."[109]

Cybersecurity Act of 2012

Senate Bill S.2105 (Cybersecurity Act of 2012), which failed to clear the Senate during August 2012, required private companies operating critical infrastructure to meet

---

[106] Richard Clarke, *Cyber Attacks Can Spark Real Wars*, WALL ST. J., Feb. 16, 2012, at A13.
[107] *Id.*
[108] *Id., see also* Jay P. Kesan & Carol M. Hayes, *Thinking Through Active Defense in Cyberspace* (October 12, 2010). PROCEEDINGS OF THE WORKSHOP ON DETERRING CYBERATTACKS: INFORMING STRATEGIES AND DEVELOPING OPTIONS, pp. 327-342, National Research Council, Washington, DC: National Academies Press, 2010; Illinois Program in Law, Behavior and Social Science Paper No. LBSS10-02; Illinois Public Law Research Paper No. 10-11. *Available at* SSRN: http://ssrn.com/abstract=1691207, and Jay P. Kesan & Carol M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace* (April 7, 2011). Illinois Public Law Research Paper No. 10-35; Illinois Program in Law, Behavior and Social Science Paper No. LBSS11-18; Harvard Journal of Law and Technology, Forthcoming. Available at SSRN: http://ssrn.com/abstract=1805163.
[109] Brian T.O'Donnell & James C. Kraska, *Humanitarian Law: Developing International Rules for the Digital Battlefield* (May 3, 2003). Journal of Conflict and Security Law, Vol. 8, pp. 133-160, 2003. Available at SSRN: http://ssrn.com/abstract=1830193.

certain security requirements.[110] This proposed legislation required companies operating "power plants, oil pipelines and other vital services to meet certain security standards."[111] Other requirements included establishing a "mechanism for industry to more easily share information on threats with the government."[112] Senator Joseph Lieberman states

> Every day rival nations, terrorist groups, criminal syndicates and individual hackers probe the weaknesses in our most critical computer networks, seeking to steal government and industrial secrets or to plant cyber agents in the cyber systems that control our most critical infrastructure and would enable an enemy to seize control of a city's electric grid or water supply system with the touch of a key from a world away. The current ongoing and growing cyber threat not only threatens our security here at home, but it is right now having a very damaging impact on our economic prosperity. Extremely valuable intellectual property is being stolen regularly by cyber exploitation by people and individuals and groups and countries abroad. It is then being replicated without the initial cost done by American companies. This means jobs are being created abroad that would otherwise be created here. So when we talk about cybersecurity, people naturally focus on the very real danger that an enemy will attack us through cyberspace, but as we think about how to grow our economy and create jobs again, I've come to the conclusion this is one of the more important things we can do to protect the treasures of America's intellectual innovation from being stolen by competitors abroad.
>
> Last year a very distinguished group of security experts, led by former Department of Homeland Security Secretary Mike Chertoff and Defense Secretary Bill Perry issued a stark warning: "The constant assault of cyber assaults has inflicted severe damage to our national and economic security, as well as to the property of individual citizens. The threat is only going to get worse. Inaction is not an acceptable action." I agree.
>
> The Cybersecurity Act of 2012 does several important things to beef up our defenses in the new battleground of cyberspace. First, it ensures that the cyber systems that control our most critical, privately-owned and operated infrastructure are secure. That's the key here—privately owned and operated cyber infrastructure can well be and probably someday will be the target of an enemy attack. Today it is the target of economic exploitation and we've got to work with the private sector to better secure those systems, both for their own defense and for our national defense. In this bill, the systems that will be asked to meet standards are defined as those that if brought down or commandeered

[110] S. 2105, 112th Cong. (2012).
[111] Siobhan Gorman, *Lawmakers Push a Bill on Security*, WALL ST. J., Feb. 15, 2013 at A2.
[112] *Id.*

> would lead to mass casualties, evacuations of major population centers, the collapse of financial markets, or significant degradation of security. So this is a tight and high standard. After identifying the systems that meet those standards, under the legislation, the Secretary of Homeland Security would then work with the private sector operators of the systems to develop security performance requirements. Owners of the privately owned cyber systems covered would have the flexibility to meet the performance requirements with whatever hardware or software they choose, so long as it achieves the required level of security. The Department of Homeland Security will not be picking technological winners or losers and there's nothing in the bill that would stifle innovation.[113]

Cybersecurity Executive Order Draft Circulating

Following defeat of The Lieberman Cybersecurity Act during August 2012, as we go to press, it is reported that The White House is circulating a draft cybersecurity executive order that "would establish a voluntary program where companies operating critical infrastructure would elect to meet cyber security best practices and standards crafted, in part, by the government."[114] John O. Brennan, Assistant to the President for Homeland Security and Counterterrorism gave a speech August 8, 2012, before the Council on Foreign Relations on the topic, "U.S. Policy toward Yemen." Following his prepared remarks, Mr. Brennan remarked that the consequences of the failed legislation is that "we're not going to have enhanced authorities and capabilities of the U.S. government to deal with what is an increasingly serious cyber challenge to our nation and

[113] *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), *available at* http://www.hsgac.senate.gov/hearings/securing-americas-future-the-cybersecurity-act-of-2012; *But see* Susan W. Brenner, *Cyber-Threats and the Limits of Bureaucratic Control* (Oct. 28, 2011), *available at* http://ssrn.com/abstract=1950725.

[114] Jennifer Martinez, *White House Circulating Draft of Executive Order on Cybersecurity,* The Hill.: Hillicon Valley (Sept. 6, 2012), *available at* http://thehill.com/blogs/hillicon-valley/technology/248079-white-house-circulating-draft-of-executive-order-on-cybersecurity. *See also* Siobhan Gorman, *Senator Presses on Cybersecurity,* WALL ST. J., Sept. 19, 2012, at B4.

to our critical infrastructure in particular. We worked very hard to try to push forward and advance the cybersecurity provisions"[115] Mr. Brennan continues

> I still find it incomprehensible that…. the legislation that was calling for minimum performance standards on the cybersecurity front for critical infrastructure that the U.S. government would help develop with private industry, that those minimum performance standards would have to be followed by those elements of the private sector that have responsibility in the critical infrastructure — and …. obviously, there were a lot of people that came out and, I think, misrepresented…. what was in that bill. But believe me, the critical infrastructure of this country is under threat, and the technology that — …. whether it be…. foreign states or cyber hackers and others — they are developing advanced technologies, and we have to improve our defenses on this issue….
>
> [W]hen you do a net assessment, you take a look at what the threat is, and that means what the capabilities are…. it talks about…. what the vulnerabilities are of the target of an attack, and then it talks about intent. Right now I can tell you with great certainty that the vulnerabilities are there, that the capabilities on the threat side are there, and so it's a question of intent, whether or not certain actors are going to operationalize the capability to go against the vulnerabilities that exist in the system….
>
> Every day our…. not just the critical infrastructure…. faces intrusions, but we see that…. intellectual property rights are just…. robbed, you know, people's personal identification. It's a system that.… It's…. privately owned, privately operated space. But that's the environment now where all of our daily lives are conducted…. [C]learly, the market has not developed in a way…. on its own [to satisfy our] cybersecurity requirements. Of course, if it did, then we wouldn't have these intrusions and the billions of dollars of losses that companies are now writing off…. [T]he…. American people are the ones that are going to be at risk, not just because of… personal identification information that is going to be out there, but also the water we drink…. the electricity that we…. depend upon, the hospitals that require that type of support, critical infrastructure — that's increasingly at risk….
>
> [T]here are different types of cyberintrusions that we see. There are cyberintrusions to get to understand your environment. So they go in, and then it's sort of operationally preparing the environments. [They] can go in just to map it so [they] understand it…. to exfiltrate certain type of data, or …. [to] understand it and then…. take actions to disrupt, disable it and destroy [data]….
>
> [W]hat we're seeing now is a lot of intrusions. We're seeing a lot of infiltrations…. and then the next step is, again, the disruptive, disabling,

[115] Ritika Singh, *Transcript of John Brennan's Speech on Yemen and Drones* Lawfare (Aug. 8, 2012), *available at* http://www.lawfareblog.com/2012/08/transcript-of-john-brennans-speech-at-the-council-on-foreign-relations/.

> destructive types of attacks. And so…. electric grids, water treatment facilities…. mass transportation systems…. railways and trains, whatever — if those intruders get into those systems and then can determine how they can in fact interfere in the command and control systems of these systems, they…. could…. put trains onto the same tracks. They can…. bring down electric grids….
>
> [S]ome [foreign countries]…. have tremendous…. cybercapabilities…. some of the most powerful countries in the world… [D]o they want to bring down that critical infrastructure in the United States right now? No, because they rely on the U.S. economy, in fact for a number of reasons. There are some foreign actors out there, though, that if they had the opportunity to bring down elements of the U.S. economy, U.S. infrastructure, I think would do it…. in a instant. So they fortunately don't have the capability at this time. They may have the intent but not the capability. But you also have international criminal groups…. [who] can do things to advance…. criminal intent by bringing down certain types of…. activities or infrastructure. So there could be all types of different reasons or different types of…. groups or people that are doing this….
>
> The president's priority is to protect the safety and security of the American people. That's the physical security of the American people as well as the prosperity of the American people…. And…. we've been pushing. We've worked hard. We delivered our legislative package to the Hill…. April, May of last year, 2011. And unfortunately the Senate bill went down last week…. it may be revived, but we can't wait. So we're doing things. DHS, in conjunction with…. NSA, FBI, others, are working to make sure that we're able to better safeguard our environment but also be able to respond and also to be resilient…. [O]ne of the approaches is if [cyber terrorists] take down some part of our critical infrastructure, you want to be able to…. recover very quickly.[116]

During mid-2012, the New York Times reported that "the United States has mounted repeated attacks with the most sophisticated cyberweapons…. in the case of Olympic Games they invaded the computer controllers that run Iran's nuclear centrifuges, spinning them wildly out of control."[117] Moreover

> The Chinese are Believed to attack America's computer systems daily, but mostly to scoop up corporate and Pentagon secrets…. In March [2012] the White House invited all the members of the Senate to a classified

[116] *Id; See also* Susan W. Brenner, *Organized Cybercrime? How Cyberspace May Affect the Structure of Criminal Relationships,* 4 N.C.J. L. & TECH. (2002), *available at* http://ssrn.com/abstract=436280.
[117] David E. Sanger, *Mutually Assured Cyberdestruction?,* The New York Times, Sunday Review, June 3, 2012, at 4.

> simulation on Capital Hill demonstrating what might happen if a dedicated hacker – or an enemy state – decided to turn off the lights in New York City.[118]

As a result, the Pentagon "has proposed that military cyber-specialists be given permission to take action outside its computer networks to defend critical U.S. computer systems…."[119]

> Advances in technology and mounting concern about the potential for a cyber-attack to damage power stations, water-treatment plants and other critical systems have prompted senior officials to seek a more robust role for the department's Cyber Command.
>
> The proposed rules would open the door for U.S. defense officials to act outside the confines of military-related computer networks to try to combat cyberattacks on private computers, including those in foreign countries.
>
> In establishing the new regulations, officials have sought to overcome concerns that action in another country's networks could violate international law, upset allies or result in unintended consequences, such as the disruption of civilian networks.[120]

Unfortunately, space limitations and the scope of this inquiry prohibit us from exploring this facet further. However, every corporate board should be asking what steps they have taken to deal with a loss of the power grid or internet access.

VIII. EVEN THE GATEKEEPERS GET HACKED

CIA Encounters Denial of Service Attack

It appears that government agencies are the prime targets of certain groups intent on creating highly-visible cyber disruption problems. On June 15, 2011, "Lulz Security,

---

[118] *Id.*
[119] Ellen Nakashima, *Pentagon Seeks to Expand Rules of Engagement for Cyber-specialists,* Wash. Post, Aug. 10, 2012, at A1.
[120] *Id.*

a group of hackers who have been responsible for a number of recent online data breaches, took aim at some United States government agencies…. The group said via Twitter that it had brought down the Central Intelligence Agency website, presumably with a so-called denial of service attack."[121] Although "a denial of service attack involves using many computers to bombard a Web site with an overload of traffic, knocking it offline--- these types of attacks do not result in data being stolen or servers being breached."[122] During the same week Lulz Security claimed responsibility for several other victims, including an F.B.I. Web site and an internal file from the U.S. Senate Web site."[123] The same group previously claimed responsibility for the PBS and Sony Pictures breaches.[124]

RSA Security

RSA, the security division of EMC Corporation, advertises itself as "a foundation of network and Internet security and a key enabler of e-commerce."[125] RSA provides services based on the RSA algorithm, described as "the most widely used method of implementing public key cryptography and has been deployed in more than one billion applications worldwide."[126] The Wall Street Journal reports, "In a letter to customers…. the EMC Corp. unit openly acknowledged for the first time that intruders had breached its security systems at defense contractor Lockheed Martin Corp. using stolen data from

[121] Nick Bilton, *Hacking Group Says It Brought Down C.I.A. Site*, The New York Times, June 15, 2011, 6:52p.m., *available at* http://bits.blogs.nytimes.com/2011/06/15/hacking-group-says-it-brought-down-c-i-a-site/?...
[122] *Id.*
[123] *Id.*
[124] *Id.*
[125] RSA History, http://www.rsa.com/node.aspx?id=2760 (last visited Sept. 13,2012).
[126] *Id.*

RSA."[127] Moreover, the breach apparently involves "SecurID tokens…. an essential piece of security, acting as an ever-changing password that flashes a series of six digits that should be virtually impossible to duplicate."[128] Company Chairman Art Coviello observed that "The intruders didn't take any Lockheed customer or employee data. But as a precaution, …. RSA will offer to replace nearly all tokens--- millions of them used by government agencies and businesses…."[129] The same Wall Street Journal account attributes Gartner analyst Mark Diodati as saying, "It would have been better if RSA was more forthright from the beginning. They unnecessarily damaged their reputation by holding back."[130]

Fast-forward to mid-2012 and "computer scientists say they have now figured out how to extract [security keys] from a widely used RSA electronic token in as little as 18 minutes."[131] Moreover, "a device made by Siemens took slightly longer; 22 minutes. A third device, made by Gemalto, based in the Netherlands took 92 minutes."[132] Security researcher Dan Kaminsky observes "cryptography breaks very slowly. It's the molasses of computer science… There are many technologies we abstractly know are problematic and we prioritize fixing them less than things that are on fire."[133]

---

[127] Siobhan Gorman & Shara Tibken, *Security 'Tokens' Take Hit*, WALL ST. J., June 7, 2011 at B1.
[128] *Id.*
[129] *Id.*
[130] *Id.* at B1-4.
[131] Somini Sengupta, *Scientists Make Short Work of Breaking Security Keys,* WALL ST. J., June 26, 2012 at B2. (*citing* findings to be published in a research paper to be presented at a cryptography conference in August 2012).
[132] *Id.*
[133] *Id.*

IX. GOVERNANCE OF IT RISK IS THE BOARD'S RESPONSIBILITY

As one U.S. senator put it, "[B]oards will never again be able to say they did not understand the risks that the firms they oversee were taking."[134] By now, every director should understand that IT risk is a major, and particularly challenging, area of governance responsibility. Elsewhere,[135] Kara Altenbaumer-Price and I have presented the legal basis for director liability (business judgment rule, duty of care, duty of loyalty, and duty of good faith) and will not repeat ourselves here except to note that "enterprise risks in an IT setting have the potential to threaten the corporation's very existence. Accordingly, each director's duty of care requires that the board act accordingly to provide effective corporate governance."[136] The following recent regulatory developments deserve attention:

The SEC on Risk & Dodd-Frank Wall Street Reform

The new SEC rules, effective February 28, 2010 amended Item 407 of Regulation S-K to require disclosure about the board's role in a company's risk oversight process and its leadership structure.[137] The SEC recently noted

---

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

[135] Trautman & Altenbaumer-Price, *supra* note 1 at 319-326.

[136] *Id.* at 322.

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

> According to the SEC's final rule release, the new disclosure rules require "companies.… to describe how the board administers its risk oversight function, such as through the whole board, or through a separate risk committee or the audit committee, for example."[138] Disclosures should address, for example, "whether the individuals who supervise the day-to-day risk management responsibilities report directly to the board as a whole or to a board committee or how the board or committee otherwise receives information from such individuals."[139] Such disclosures should also include an explanation of the board's leadership structure and the "reasons why the company believes that this board leadership structure is the most appropriate structure for the company."[140] In companies in which the CEO and Chairman are the same individual, rule "amendments will require disclosure of whether and why the company has a lead independent director, as well as the specific role the lead independent director plays in the leadership of the company."[141]

The Dodd-Frank Act requires large financial institutions to establish independent risk committees on their boards,[142] with at least one member of the committee required to have risk management experience at a large, complex firm.[143]

One approach to the increased emphasis on risk oversight and the possibility of risk committees being mandated for some or all public companies is the pro-active creation of a risk committee.[144] We have previously observed, "While having a stand-alone risk committee can serve to relieve strained audit committees, it is important that

---

such as how the board administers its oversight function, and the effect that this has on the board's leadership structure.

[138] SEC Releases No. 33-9089; 34-61175, Proxy Disclosure Enhancements (Dec. 16, 2009), *available at* http://sec.gov/rules/final/2009/33-9089.pdf. [Final Rule Release].

[139] *Id.*

[140] *Id.*

[141] *Id.*

[142] John Lester & John Bovenzi, *The Dodd-Frank Act: What it does, what is means, and what happens next*, OLIVER WYMAN POINT OF VIEW (2010).

[143] *Id. see also,* Scott Landau, et. al. *Dodd-Frank Act Reforms Executive Compensation and Corporate Governance for All Public Companies*, PILLSBURY CLIENT ALERT (July 15, 2010).

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

qualified, independent directors serve on the risk committee. It is also imperative that creating a risk committee does not abdicate all responsibility for risk away from the rest of the directors."[145]

IT Risk: Why Governance Is Important

Nothing is more fundamental in almost every organization to the support and growth of the business than the effective management of Information Technology. We previously reported that a

> Survey of 5,500 worldwide business leaders, revealed that 58 percent "of executives polled said they have lost sensitive personal information, and for nearly 60 percent of those who have had a breach, it was not an isolated event."[146] Elsewhere, it is disclosed that "65 percent of Fortune 1000 companies were not reviewing their companies' cybersecurity policies.…"[147]
>
> During recent years, IT risk has demonstrated the potential to cause catastrophic losses to the enterprise balance sheet, reputation, and even threaten its very existence. With an *average* loss per breach at $234,000,[148] examples of the effects of an IT failure include: loss of sensitive customer private information; loss of sensitive product or financial data of the corporation; virus attacks by hackers on the company's computer systems and those of its customers or vendors; business interruption losses due to IT downtime; as well as theft and use of client credit card or other sensitive data.[149] At least half of data breaches or losses are believed to be caused by a lack of internal controls and process—not hackers or viruses.[150]

[145] Trautman & Altenbaumer-Price, *supra* note 1 at 320.
[146] Accenture, *supra* note 21.
[147] Schwartzel, *supra* note 20, *see also* Accenture Report, *supra* note 21 ("[O]nly 56 percent of organizations surveyed said it was important or very important to have a policy about their privacy practices.").
[148] *Id.*
[149] USI Insurance Services, *Cyber Liability / Security and Privacy Insurance* (2009) (on file with the authors).
[150] Accenture, *supra* note 21 ("Internal issues—employees (48 percent) and business or system failure (57 percent)—were cited most often as the source of the breaches—a finding that is in stark contrast to common perception that external forces are the biggest threats to privacy and security."

Every board must have contingency plans in place to protect from these cyber threats. Many of the data breaches reported by the Privacy Rights Clearing House involve low technology breaches (i.e. computers being stolen during burglary, former employee's theft of paper records, and dumpster-diving for discarded paper information.[151]

New SEC Disclosure Guidelines

As the result of the proliferation of cyberattacks during 2010 and 2011, the SEC's Division of Corporation Finance announced on October 13, 2011 disclosure guidance for cybersecurity issues.[152] The 2011 Division of Corporation Finance's guidance "is not a new disclosure rule, nor does it give the SEC specific authority to regulate a company's cybersecurity policy. Rather, the guidance is a clarification of existing disclosure obligations…."[153] The Division of Corporation Finance states "For a number of years, registrants have migrated toward increasing dependence on digital technologies to conduct their operations. As this dependence has increased, the risks to registrants associated with cybersecurity have also increased, resulting in more frequent and severe cyber incidents."[154] In addition, "there has been increased focus by registrants and members of the legal and accounting professions on how these risks and their related impact on the operations of a registrant should be described within the framework of the disclosure obligations imposed by the federal securities laws."[155] Accordingly, the Division "determined that it would be beneficial to provide guidance that assists

[151] *See generally,* Trautman & Altenbaumer-Price, *supra* note 1.
[152] SEC Division of Corporation Finance, *CF Disclosure Guidance: Topic No. 2 Cybersecurity* (Oct. 13, 2011), available at http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.
[153] King & Spalding: Public Company Advisor, A Practical Guide to Implementing SEC Guidance on Disclosure of Cybersecurity and Cyber Incidents (Jan. 2012), available at http://www.kslaw.com/imageserver/KSPublic/library/publication/PublicCompanyAdvisor-Jan2012.pdf.
[154] SEC, *supra* note 152.
[155] *Id.*

registrants in assessing what, if any, disclosures should be provided about cybersecurity matters in light of each registrant's specific facts and circumstances."[156] The Division prepared guidance to

> Be consistent with the relevant disclosure considerations that arise in connection with any business risk. We are mindful of potential concerns that detailed disclosures could compromise cybersecurity efforts -- for example, by providing a "roadmap" for those who seek to infiltrate a registrant's network security -- and we emphasize that disclosures of that nature are not required under the federal securities laws.
>
> In general, cyber incidents can result from deliberate attacks or unintentional events. We have observed an increased level of attention focused on cyber attacks that include, but are not limited to, gaining unauthorized access to digital systems for purposes of misappropriating assets or sensitive information, corrupting data, or causing operational disruption. Cyber attacks may also be carried out in a manner that does not require gaining unauthorized access, such as by causing denial-of-service attacks on websites. Cyber attacks may be carried out by third parties or insiders using techniques that range from highly sophisticated efforts to electronically circumvent network security or overwhelm websites to more traditional intelligence gathering and social engineering aimed at obtaining information necessary to gain access.
>
> The objectives of cyber attacks vary widely and may include theft of financial assets, intellectual property, or other sensitive information belonging to registrants, their customers, or other business partners. Cyber attacks may also be directed at disrupting the operations of registrants or their business partners. Registrants that fall victim to successful cyber attacks may incur substantial costs and suffer other negative consequences, which may include, but are not limited to:
>
> - Remediation costs that may include liability for stolen assets or information and repairing system damage that may have been caused. Remediation costs may also include incentives offered to customers or other business partners in an effort to maintain the business relationships after an attack;
> - Increased cybersecurity protection costs that may include organizational changes, deploying additional personnel and protection technologies, training employees, and engaging third party experts and consultants;
> - Lost revenues resulting from unauthorized use of proprietary information or the failure to retain or attract customers following an attack;
> - Litigation; and

[156] *Id.*

- Reputational damage adversely affecting customer or investor confidence.

Disclosure by Public Companies Regarding Cybersecurity Risks and Cyber Incidents

The federal securities laws, in part, are designed to elicit disclosure of timely, comprehensive, and accurate information about risks and events that a reasonable investor would consider important to an investment decision. Although no existing disclosure requirement explicitly refers to cybersecurity risks and cyber incidents, a number of disclosure requirements may impose an obligation on registrants to disclose such risks and incidents. In addition, material information regarding cybersecurity risks and cyber incidents is required to be disclosed when necessary in order to make other required disclosures, in light of the circumstances under which they are made, not misleading. Therefore, as with other operational and financial risks, registrants should review, on an ongoing basis, the adequacy of their disclosure relating to cybersecurity risks and cyber incidents.

The following sections provide an overview of specific disclosure obligations that may require a discussion of cybersecurity risks and cyber incidents.

Risk Factors

Registrants should disclose the risk of cyber incidents if these issues are among the most significant factors that make an investment in the company speculative or risky. In determining whether risk factor disclosure is required, we expect registrants to evaluate their cybersecurity risks and take into account all available relevant information, including prior cyber incidents and the severity and frequency of those incidents. As part of this evaluation, registrants should consider the probability of cyber incidents occurring and the quantitative and qualitative magnitude of those risks, including the potential costs and other consequences resulting from misappropriation of assets or sensitive information, corruption of data or operational disruption. In evaluating whether risk factor disclosure should be provided, registrants should also consider the adequacy of preventative actions taken to reduce cybersecurity risks in the context of the industry in which they operate and risks to that security, including threatened attacks of which they are aware.

Consistent with the Regulation S-K Item 503(c) requirements for risk factor disclosures generally, cybersecurity risk disclosure provided must adequately describe the nature of the material risks and specify how each risk affects the registrant. Registrants should not present risks that could apply to any issuer or any offering and should avoid generic risk factor disclosure. Depending on the registrant's particular facts and circumstances, and to the extent material, appropriate disclosures may include:

- Discussion of aspects of the registrant's business or operations that give rise to material cybersecurity risks and the potential costs and consequences;
- To the extent the registrant outsources functions that have material cybersecurity risks, description of those functions and how the registrant addresses those risks;
- Description of cyber incidents experienced by the registrant that are individually, or in the aggregate, material, including a description of the costs and other consequences;
- Risks related to cyber incidents that may remain undetected for an extended period; and
- Description of relevant insurance coverage.

A registrant may need to disclose known or threatened cyber incidents to place the discussion of cybersecurity risks in context. For example, if a registrant experienced a material cyber attack in which malware was embedded in its systems and customer data was compromised, it likely would not be sufficient for the registrant to disclose that there is a risk that such an attack may occur. Instead, as part of a broader discussion of malware or other similar attacks that pose a particular risk, the registrant may need to discuss the occurrence of the specific attack and its known and potential costs and other consequences.

While registrants should provide disclosure tailored to their particular circumstances and avoid generic "boilerplate" disclosure, we reiterate that the federal securities laws do not require disclosure that itself would compromise a registrant's cybersecurity. Instead, registrants should provide sufficient disclosure to allow investors to appreciate the nature of the risks faced by the particular registrant in a manner that would not have that consequence.

Management's Discussion & Analysis of Financial Condition & Results of Operations (MD&A)

Registrants should address cybersecurity risks and cyber incidents in their MD&A if the costs or other consequences associated with one or more known incidents or the risk of potential incidents represent a material event, trend, or uncertainty that is reasonably likely to have a material effect on the registrant's results of operations, liquidity, or financial condition or would cause reported financial information not to be necessarily indicative of future operating results or financial condition. For example, if material intellectual property is stolen in a cyber attack, and the effects of the theft are reasonably likely to be material, the registrant should describe the property that was stolen and the effect of the attack on its results of operations, liquidity, and financial condition and whether the attack would cause reported financial information not to be indicative of future operating results or financial condition. If it is reasonably likely that the attack will lead to reduced revenues, an increase in cybersecurity protection costs, including related to litigation, the registrant should discuss these possible outcomes, including the amount

and duration of the expected costs, if material. Alternatively, if the attack did not result in the loss of intellectual property, but it prompted the registrant to materially increase its cybersecurity protection expenditures, the registrant should note those increased expenditures.

Description of Business

If one or more cyber incidents materially affect a registrant's products, services, relationships with customers or suppliers, or competitive conditions, the registrant should provide disclosure in the registrant's "Description of Business." In determining whether to include disclosure, registrants should consider the impact on each of their reportable segments. As an example, if a registrant has a new product in development and learns of a cyber incident that could materially impair its future viability, the registrant should discuss the incident and the potential impact to the extent material.

Legal Proceedings

If a material pending legal proceeding to which a registrant or any of its subsidiaries is a party involves a cyber incident, the registrant may need to disclose information regarding this litigation in its "Legal Proceedings" disclosure. For example, if a significant amount of customer information is stolen, resulting in material litigation, the registrant should disclose the name of the court in which the proceedings are pending, the date instituted, the principal parties thereto, a description of the factual basis alleged to underlie the litigation, and the relief sought.

Financial Statement Disclosures

Cybersecurity risks and cyber incidents may have a broad impact on a registrant's financial statements, depending on the nature and severity of the potential or actual incident.

Prior to a Cyber Incident

Registrants may incur substantial costs to prevent cyber incidents. Accounting for the capitalization of these costs is addressed by Accounting Standards Codification (ASC) 350-40, Internal-Use Software, to the extent that such costs are related to internal use software.

During and After a Cyber Incident

Registrants may seek to mitigate damages from a cyber incident by providing customers with incentives to maintain the business relationship. Registrants should consider ASC 605-50, Customer Payments and Incentives, to ensure appropriate recognition, measurement, and classification of these incentives.

Cyber incidents may result in losses from asserted and unasserted claims, including those related to warranties, breach of contract, product recall and replacement, and indemnification of counterparty losses from their remediation efforts. Registrants should refer to ASC 450-20, Loss Contingencies, to determine when to recognize a liability if those losses are probable and reasonably estimable. In addition, registrants must provide certain disclosures of losses that are at least reasonably possible.

> Cyber incidents may also result in diminished future cash flows, thereby requiring consideration of impairment of certain assets including goodwill, customer-related intangible assets, trademarks, patents, capitalized software or other long-lived assets associated with hardware or software, and inventory. Registrants may not immediately know the impact of a cyber incident and may be required to develop estimates to account for the various financial implications. Registrants should subsequently reassess the assumptions that underlie the estimates made in preparing the financial statements. A registrant must explain any risk or uncertainty of a reasonably possible change in its estimates in the near-term that would be material to the financial statements. Examples of estimates that may be affected by cyber incidents include estimates of warranty liability, allowances for product returns, capitalized software costs, inventory, litigation, and deferred revenue.
>
> To the extent a cyber incident is discovered after the balance sheet date but before the issuance of financial statements, registrants should consider whether disclosure of a recognized or nonrecognized subsequent event is necessary. If the incident constitutes a material nonrecognized subsequent event, the financial statements should disclose the nature of the incident and an estimate of its financial effect, or a statement that such an estimate cannot be made.
>
> Disclosure Controls and Procedures
>
> Registrants are required to disclose conclusions on the effectiveness of disclosure controls and procedures. To the extent cyber incidents pose a risk to a registrant's ability to record, process, summarize, and report information that is required to be disclosed in Commission filings, management should also consider whether there are any deficiencies in its disclosure controls and procedures that would render them ineffective. For example, if it is reasonably possible that information would not be recorded properly due to a cyber incident affecting a registrant's information systems, a registrant may conclude that its disclosure controls and procedures are ineffective.[157]

King & Spalding notes, "the Corp Fin's guidance is designed to aid a public company in the disclosure exercise it undertakes for public filings."[158] Moreover

> Just as with other items, if cybersecurity issues pose a material risk and/or cybersecurity-related costs materially impact operating results (for example, in the case of remediation of a breach), then the risk and/or the impact must be disclosed and described. Companies must consider vulnerability to third-party actors and events like hacker attacks, viruses and malware, as well as the potential for inadvertent disclosure of

[157] *Id.*
[158] King & Spalding, *supra* note 153.

confidential information by the company or others. Corp Fin provided companies with a list of specific risks to consider…

Whether and to what extent disclosure of cybersecurity risks is needed is specific to each company. A number of public companies included a cybersecurity risk factor in their '34 Act filings before Corp Fin issued its guidance, and several others have updated their '34 Act filings to include a cybersecurity risk factor since the October guidance. We believe that given current technology, outsourcing and IT processes, many companies will address cybersecurity in a '34 Act risk factor, regardless of industry, and that a wave of new cybersecurity risk factors will be included in 10-Ks for December 31 year-end companies.

As with all risk factors, specificity counts, particularly when a company has had a prior cybersecurity issue or has undertaken a particular cybersecurity initiative. Of course, Corp Fin acknowledged in its published guidance that specificity does not mean that a company must roadmap its potential weaknesses, which could increase vulnerability to an attack.

However, specificity does mean that each public company should carefully consider the types of cybersecurity risks it faces. Risk factors will be different for the retailer that relies on its website for a significant portion of its sales, the business services company that outsources its customer service function, or the company that could be an attractive target for a Domain Name Server (DNS) attack, because of its important role in global commerce. Accordingly, a company must evaluate the unique threats that it faces, rather than relying on boilerplate disclosure.[159]

Excerpted from recent actual SEC filings (with specific company names omitted), King & Spalding has provided the following examples of risk factor disclosure which illustrates how different industry groups have chosen to describe cyber risk.[160]

Table 2
Cybersecurity Risk Factor Disclosure

Distributor	Information security risks have generally increased in recent years because of the proliferation of new technologies and the increased sophistication and activities of perpetrators of cyber attacks. A failure in or breach of our operational or information security systems, or those of our third party service providers, as a result cyber attacks or information security breaches could disrupt our business, result in the disclosure or misuse of confidential or

[159] *Id.*
[160] *Id.*

	proprietary information, damage our reputation, increase our costs and/or cause losses. As a result, cyber security and the continued development and enhancement of the controls and processes designed to protect our systems, computers, software, data and networks from attack, damage or unauthorized access remain a priority for us. Although we believe that we have robust information security procedures and other safeguards in place, as cyber threats continue to evolve, we may be required to expend additional resources to continue to enhance our information security measures and/or to investigate and remediate any information security vulnerabilities. Third party service providers are responsible for managing a significant portion of our information systems. Our business and results of operations may be adversely affected if the third party service provider does not perform satisfactorily.
Metals Producer	We have put in place a number of systems, processes and practices designed to protect against intentional or unintentional misappropriation or corruption of our systems and information or disruption of our operations. These include, for example, the appropriate encryption of information. Despite such efforts, we are subject to breaches of security systems which may result in unauthorized access, misappropriation, corruption or disruption of the information we are trying to protect, in which case we could suffer material harm. Access to our proprietary information regarding new formulations would allow our competitors to use that information in the development of competing products. In addition, our systems could be subject to sabotage by employees or third parties, which could slow or stop production or otherwise adversely affect our operations. Any misappropriation or corruption of our systems and information or disruption of our operations could have a material adverse effect on our business.
Industrial	We and certain of our third-party vendors receive and store personal information in connection with our human resources operations and other aspects of our business. Despite our implementation of security measures, our IT systems are vulnerable to damages from computer viruses, natural disasters, unauthorized access, cyber attack and other similar disruptions. Any system failure, accident or security breach could result in disruptions to our operations. A material network breach in the security of our IT systems could include the theft of our intellectual property or trade secrets. To the extent that any disruptions or security breach results in a loss or damage to our data, or in inappropriate disclosure of confidential information, it could cause significant damage to our reputation, affect our relationships with our customers, lead to claims against us and ultimately harm our business. In addition, we may be required to incur significant costs to protect against damage caused by these disruptions or security breaches in the future.
Public Utility	We are subject to cyber-security risks primarily related to breaches of security pertaining to sensitive customer, employee, and vendor information maintained by us in the normal course of business, as well as breaches in the technology that manages natural gas distribution operations and other business processes. A loss of confidential or proprietary data or security breaches of other technology business tools could adversely affect our reputation, diminish customer confidence, disrupt operations, and subject us to possible financial liability, any of which could have a material affect on the our financial condition and results of operations. We closely monitor both preventive and detective measures to manage these risks.
Telecom	Attempts by others to gain unauthorized access to our information technology systems are becoming more sophisticated and are sometimes successful. These attempts, which might be related to industrial or other espionage, include

	covertly introducing malware to our computers and networks and impersonating authorized users, among others. We seek to detect and investigate all security incidents and to prevent their recurrence, but in some cases, we might be unaware of an incident or its magnitude and effects. The theft, unauthorized use or publication of our intellectual property and/or confidential business information could harm our competitive position, reduce the value of our investment in research and development and other strategic initiatives or otherwise adversely affect our business. To the extent that any security breach results in inappropriate disclosure of our customers' or licensees' confidential information, we may incur liability as a result. In addition, we expect to devote additional resources to the security of our information technology systems.
Manufacturer	A cyber-attack that bypasses our information technology (IT) security systems causing an IT security breach, may lead to a material disruption of our IT business systems and/or the loss of business information resulting in adverse business impact. Risks may include: □ future results could be adversely affected due to the theft, destruction, loss, misappropriation or release of confidential data or intellectual property □ operational or business delays resulting from the disruption of IT systems and subsequent clean-up and mitigation activities □ negative publicity resulting in reputation or brand damage with our customers, partners or industry peers.
Grocery Store Chain	Our business is increasingly dependent on information technology systems that are complex and vital to continuing operations. If we were to experience difficulties maintaining existing systems or implementing new systems, we could incur significant losses due to disruptions in our operations. Additionally, these systems contain valuable proprietary and financial data, as well as debit and credit card cardholder data, and a breach, including cyber security breaches, could have an adverse effect on us.
Consumer Electronics and Online Marketplace	Our business requires us to use and store customer, employee, and business partner personally identifiable information (PII). This may include names, addresses, phone numbers, email addresses, contact preferences, tax identification numbers, and payment account information. Although malicious attacks to gain access to PII affect many companies across various industries, we may be at a relatively greater risk of being targeted because of our high profile and the amount of PII managed. We require user names and passwords in order to access our information technology systems. We also use encryption and authentication technologies to secure the transmission and storage of data. These security measures may be compromised as a result of third-party security breaches, employee error, malfeasance, faulty password management, or other irregularity, and result in persons obtaining unauthorized access to company data or accounts. Third parties may attempt to fraudulently induce employees or customers into disclosing user names, passwords or other sensitive information, which may in turn be used to access our information technology systems. To help protect customers and the company, we monitor accounts and systems for unusual activity and may freeze accounts under suspicious circumstances, which may result in the delay or loss of customer orders. We devote significant resources to network security, data encryption, and other security measures to protect our systems and data, but these security measures cannot provide absolute security. We may experience a breach of our systems and may be unable to protect sensitive data. Moreover, if a computer security breach affects the company's systems or results in the unauthorized release of PII, our reputation and brand could be materially damaged and use of our products and services could decrease. We would also be exposed to a risk of loss or litigation and possible liability, which could result in a material adverse effect on our business, results of operations and financial condition.
Financial	Our operations rely on the secure processing, storage and transmission of

Services	confidential and other information in our computer systems and networks. Although we take protective measures and endeavor to modify them as circumstances warrant, the security of our computer systems, software and networks may be vulnerable to breaches, unauthorized access, misuse, computer viruses or other malicious code and other events that could have a security impact. Additionally, breaches of security may occur through intentional or unintentional acts by those having authorized or unauthorized access to our or our clients' or counterparties' confidential or other information. If one or more of such events occur, this potentially could jeopardize our or our clients' or counterparties' confidential and other information processed and stored in, and transmitted through, our computer systems and networks, or otherwise cause interruptions or malfunctions in our, our clients', our counterparties' or third parties' operations, which could result in significant losses or reputational damage to us. We may be required to expend significant additional resources to modify our protective measures or to investigate and remediate vulnerabilities or other exposures arising from operational and security risks, and we may be subject to litigation and financial losses that are either not insured against or not fully covered through any insurance maintained by us.

Source: King & Spalding: Public Company Advisor, A Practical Guide to Implementing SEC Guidance on Disclosure of Cybersecurity and Cyber Incidents (Jan. 2012), at Exhibit A.

X. BOARD COMPOSITION: THE CASE FOR IT EXPERTISE

Each Board Has Different Levels of IT Skills

Optimal board composition is different for companies engaged in different industries and at different stages of their lifecycle.[161] The board of a young software or consulting company may be inundated with IT understanding, expertise and talent; while the board of an oil and gas or fast food company may have little understanding of IT issues represented among its board members. IT domain issues must be adequately represented among board members, particularly with significant IT risks related to their business activities, such as internet-based sales.

It's a safe bet that no corporate directors were born with a comprehensive understanding of information technology. Accordingly, "some boards provide directors with IT education sessions outside the boardroom, similar to strategy retreats, which may

[161] *See generally* Lawrence J. Trautman, *The Matrix: The Board's Responsibility for Director Selection and Recruitment,* 11 Fla. St. U. Bus. Rev., 75 (2012), *Available at* http://ssrn.com/abstract=1998489.

be held on the day before or after a full board meeting."[162] Deloitte suggests that "a first session may focus on the organization's overall IT structure and objectives, while subsequent sessions may be scheduled whenever a major IT development occurs."[163]

Organizational IT Knowledge

It appears "relatively few boards draw upon what may be the best source of IT knowledge within the organization – the Chief Information Officer (CIO)." Deloitte suggests that "boards should establish a regular reporting relationship with the CIO, similar to the relationship with the CFO on financial issues, to ensure that IT communications flow smoothly to the board."[164] That is, the language of "business" is required for effectiveness, not the nomenclature of technology. Also, "it may be easier and faster for directors and the CIO to develop an effective rapport when the board members have the opportunity to interact with the CIO outside the boardroom, for example, at a combined board/management dinner prior to a board meeting."[165]

The Audit Committee: Appropriate Site for IT Expertise and Experience

Because the Audit Committee is responsible for quality control, internal accounting controls, and risk assessment, an understanding of the enterprises' IT logically seems to be a foundation issue before audit quality, internal accounting controls,

[162] Deloitte Report, *The Tech-Intelligent Board: Priorities for Tech-Savvy Directors as they oversee IT Risk and Strategy,* 9 (2011), *available at http://www.corpgov.deloitte.com/binary/com.epicentric.contentmanagement.servlet.ContentDeliveryServlet/USEng/Documents/Board%20Governance/Information%20Quality%20and%20Technology/Tech-Intelligent%20Board_Deloitte%20Global%20Center_021111.pdf.*
[163] *Id.*
[164] *Id.*
[165] *Id.*

or risk assessment can be addressed.[166] A key responsibility of the internal audit function is to keep the board's audit committee "apprised of emerging [IT] risks" says PricewaterhouseCoopers, observing that "in the risk assessment report that it presents to the audit committee, internal audit should highlight the organization's significant data security and privacy risks, including any new risks."[167] Moreover, the Audit Committee

> Should identify weaknesses in policies and controls. At one global financial services firm, for example, the internal audit function briefs the audit committee about risks it sees within the company, both present and potential. In turn, the company's audit committee often alerts internal audit and management to emerging security issues that directors hear about at other firms with which they are involved. Such two-way exchanges between internal audit and the audit committee are invaluable in keeping the spotlight on emerging information security risks.
>
> Because the nature of information security risks is evolving continuously, internal audit functions need to stay ahead of the threat curve. Internal audit functions should participate in numerous internal and external forums to stay plugged in to emerging security threats, and practices for protecting against them. Networking internally and externally on information security issues is vital to staying vigilant.
>
> Internal audit's role in ensuring that information security threats are properly considered becomes especially important when a company is ready to roll out a new business process, product, or information system. In such initiatives, the project team does not always believe it has time to fully consider data security, particularly if the initiative has fallen behind schedule…. Internal audit is uniquely positioned to assess whether existing controls are being used, but it must also keep its ear to the ground and move quickly to conduct special audits for new information security threats, which some executives consider as important as regularly scheduled audits.[168]

Barriers to IT-Internal Audit Effectiveness

PwC believes that "for most companies, information security and privacy is [a] critical risk because of its potential to cause financial and reputational damage, and

---

[166] *Id., see also* Lawrence J. Trautman, *Who Qualifies as an Audit Committee Financial Expert Under SEC Regulations and NYSE Rules,* 11 DEPAUL BUS. & COM. L.J. (forthcoming), *available at* http://www.ssrn.com/abstract=2137747.
[167] PricewaterhouseCoopers, *supra* note 32 at 8.
[168] *Id.*

because it is so difficult to mitigate" and that data security attacks may best be combated through the use of three primary lines of defense: 1. *Management,* 2. *Risk Management and Compliance Functions, and* 3. *Internal Audit.*[169] The PwC report "commonly find[s] four barriers in organizations that try to adopt effective data privacy and security measures:

1. A mindset that believes adequate controls are already in place;
2. Cost;
3. Low expectations of internal audit's capabilities in data privacy; and
4. Fragmented responsibilities.[170]

XI. NATURE OF IT LITIGATION RISKS

We have previously reported that "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."[171] Moreover, "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."[172] Very costly regulatory and private lawsuits are resulting from these areas of cyber-related risk.

> For example, a payment systems processor was sued in a securities fraud class action after cybercriminals stole credit and debit card information. Another company was sued after a hacker infiltrated its online job application system and sent phishing e-mails to job applicants asking for additional personal information.[173] A retailer found itself embroiled in

[169] *Id.* at 6.
[170] *Id.* at 9.
[171] Trautman & Altenbaumer-Price, *supra* note 1 at 332.
[172] *Id.*
[173] *Aetna boots data breach class action suit*, INFOSECURITY.COM (March 12, 2010).

> multiple lawsuits and a multi-state regulatory probe after hackers stole millions of credit and debit card numbers over a two-year period[174] and an educational institution was sued by its alumni after hackers stole social security numbers.[175]

William Roberds and Stacey L. Schreft report that "Identity theft can take many forms in practice and need not involve data breaches."[176] Moreover

> The Federal Trade Commission divides identity theft into two broad categories: *existing-account fraud* and *new-account fraud*. Existing account fraud occurs when a thief steals an existing payment card or similar account information (e.g., a checking account number) and uses these to purchase goods and services. Traditionally, new account fraud occurs when a thief uses someone else's PID to open a new account. An increasingly prevalent type of identity fraud is *fictitious* or *synthetic identity fraud,* in which a thief combines information taken from a variety of sources with invented information to create a new, fictitious identity.[177]

Analysis of Data Breach Litigation

According to the Privacy Rights Clearinghouse, more than 567,788,137 records (from 3,470 data breaches) have been reported as breached since 2005.[178] "One company reported a breach of 38 terabytes of information—equivalent nearly double the amount of text contained in the Library of Congress."[179] Even more troubling "is the fact that the

---

[174] Chubb Group of Insurance Companies, *CyberSecurity by Chubb: Insuring Cyber Exposures for Businesses of All Kinds, http://www.sgdins.com/downloads/CyberSecurity%20by%20Chubb.pdf* (last visited July 20, 2010).
[175] Chubb Group of Insurance Companies, *CyberSecurity by Chubb: Insuring Cyber Exposures for Businesses of All Kinds, http://www.sgdins.com/downloads/CyberSecurity%20by%20Chubb.pdf* (last visited July 20, 2010), *See also* George H. Pike, *Lost Data: The Legal Challenges,* Information Today, Vol. 23, No. 10, p. 1, 2006; U. of Pittsburgh Legal Studies Research Paper Series. *Available at* http://ssrn.com/abstract=1431586.
[176] William Roberds & Stacey L. Schreft, *Data Breaches and Identity Theft,* (Sept. 1, 2008), Federal Reserve Bank of Atlanta Working Paper No. 2008-22, *available at* http://ssrn.com/abstract=1296131.
[177] *Id.*
[178] Privacy Rights Clearinghouse, *supra* note 33.
[179] Sen. Sheldon Whitehouse, *We need to act on cybersecurity*, NAT'L L. J. (May 10, 2010).

Clearinghouse records are not exhaustive, nor do they reflect breaches occurring outside the United States."[180]

A review of the literature reveals that relatively little information is available about litigation over data breach issues—the ultimate outcomes and choices over which breaches are litigated and which are not. Romanosky, Hoffman and Acquisti observe that "It is difficult (and perhaps impossible) to assess the aggregate costs and benefits for both consumers and firms of different privacy regimes in purely monetary terms."[181] However, "while there exists some legal scholarship regarding data breach litigation, it typically examines a narrow subset of lawsuits, usually focusing on high-profile cases or those with published opinions."[182] Because "as few as 15% of all lawsuits produce reported opinions, any conclusions reached from examining particular, high-profile, cases are likely unrepresentative of the full population of data breach lawsuits. Consequently, it is still unknown what characteristics these lawsuits actually possess, and how 'successful' they have been."[183] Looking at 230 federal breach lawsuits covering the period 2000 to 2010, analysis reveals

> [T]hat federal data breach lawsuits typically exhibit the following characteristics. First, plaintiffs seek relief for one or more of: actual loss from identity theft (e.g. financial or medical fraud), emotional distress, cost of preventing future losses (e.g. credit monitoring and identity theft insurance), and the increased risk of future harm. Second, the lawsuits are usually private class actions, though some are brought by public entities

---

[180] *Id.*

[181] Sasha Romanosky, David A. Hoffman, & Alessandro Acquisti, *Empirical Analysis of Data Breach Litigation* 2 (February 19, 2012). Temple University Legal Studies Research Paper No. 2012-30. Available at SSRN: http://ssrn.com/abstract=1986461.

[182] *Id. citing* D. Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age,* 80 S. Cal. L. Rev. 241-248 (2007), D. Citron, *Mainstreaming Privacy Torts,* 99 Cal. L. Rev. 101-189 (2011), D. Rice, *Civil Actions for Privacy Violations: Where Are We?* Howard Rice Nemerovski Canady Falk & Rabkin (2007), and A. Serwin, *Poised on the Precipice: A Critical Examination of Privacy Litigation,* 25 Santa Clara Computer & High Tech. L. J. 4 (2009).

[183] *Id.citing* D. Hoffman, A. Izenman & J.R. Lidicker, *Docketology, District Courts, and Doctrine,* 85 Wash. U.L. Rev. 681 (2007).

> such as the Federal Trade Commission or state attorneys general. Third, defendants are typically large firms such as banks, medical/insurance entities, retailers, or other private businesses. Fourth, complaints allege a staggering range of both common law (tort, breach of contract) and statutory causes of action. And fifth, cases generally either settle, or are dismissed (either as a matter of law, or because the plaintiff was unable to demonstrate actual harm).[184]

Romanosky, Hoffman and Acquisti "find that the odds of a firm being sued are 3.5 times *greater* when individuals suffered financial harm, but over 6 times *lower* when the firm provides free credit monitoring to those affected by the breach."[185] In addition, "the odds of a firm being sued from improperly disposing data are 3 times greater relative to breaches caused by lost/stolen data, and 6 times greater when the data breach involved the loss of financial information."[186] As to settlement, Romanosky, Hoffman and Acquisti's

> Results suggest that defendants settle 30% more often when plaintiffs allege financial loss from a data breach, or when faced with a certified class action suit. The odds of a settlement are found to be 10 times greater when the breach is caused by a cyber-attack, relative to lost or stolen hardware, and the compromise of medical data increases the probability of settlement by 31%.[187]

Heartland Payment Systems Case

We previously reported on the Heartland Payment Systems case, believed then to be the largest security breach ever.[188] Heartland involved a theft by cybercriminals of 130 million credit and debit card numbers, resulting in a securities fraud class action for

---

[184] *Id.* at 3.
[185] *Id.*
[186] *Id.*
[187] *Id.*
[188] *See* Trautman & Altenbaumer-Price, *supra* note 1 at 333 *citing* Brian Krebs, *Payment Processor Breach May be Largest Ever*, WASH. POST SECURITY FIX BLOG, http://voices.washingtonpost.com/securityfix/2009/01/payment_processor_breach_may_b.html (Jan. 20, 2009).

"fraudulently misrepresent[ing] the general state of its data security" and concealing an earlier cyber attack during earnings calls and in SEC filings.[189] Heartland's stock price dropped almost 80% when the breach was disclosed.[190] Eventually it was revealed that the breach was caused by malicious software.[191] Heartland knew that the stolen data included names, credit and debit card numbers, and expiration dates.[192]

> Ultimately, the company and its officers and directors were forced to pay $60 million in a settlement with Visa,[193] $41.4 million in a settlement with MasterCard,[194] $3.6 million in a settlement with American Express,[195] up to $2.4 million in a consumer cardholder class action[196] over the same breach, as well as the defense costs of the dismissed suit and internal investigation costs incurred by the company.[197]

On August 13, 2009 the Federal Reserve Bank of Philadelphia Payment Card Center hosted a workshop to "discuss lessons learned as a result of [the Heartland] event [and to examine] the changing nature of data security in consumer electronic

[189] *In re Heartland Payment Sys., Inc. Sec. Litig.*, Case 3:09-cv-01043-AET-TJB, at 5 (D. N.J. Dec. 7, 2009).
[190] *Id.*
[191] Krebs, *supra* note 187.
[192] *Id.*
[193] Press Release, Visa, Heartland Payments Systems Agrees on Settlement to Provide Visa Issuers up to $60M for Data Breach Security Claims (Jan. 8, 2010) (*available at* http://corporate.visa.com/media-center/press-releases/press974.jsp).
[194] Press Release, *Heartland Payment Systems, Heartland Payment Systems® and Mastercard Agree to $41.4 Million Intrusion Settlement: Company has now reached breach-related settlements with three major card brands (May 19, 2010) (*available at *http://www.heartlandpaymentsystems.com/article/Heartland-Payment-Systems-and-Mastercard-Ag-6349.aspx).*
[195] Press Release*, Heartland Payment Systems, Heartland Payment Systems and American Express Agree to $3.6 Million Intrusion Settlement:* Settlement marks first agreement with a card brand related to 2008 intrusion (Dec. 17, 2009) (available at *http://www.heartlandpaymentsystems.com/article/Heartland-Payment-Systems-and-American-Expr-3047.aspx).*
[196] Press Release, Heartland Payment Systems, Heartland Payment Systems Agrees to Settle Cardholder Class Action Claim (Dec. 21, 2009) (*available at* http://www.heartlandpaymentsystems.com/article/Heartland-Payment-Systems-Agrees-to-Settle-3051.aspx).
[197] Trautman & Altenbaumer-Price, *supra* note 1 at 333.

payments."[198] Accordingly, costs resulting from this data breach were reported as follows:

> Immediately following the breach, [Heartland] lost 50 percent of its market capitalization and, as of August 2009, had spent more than $32 million on legal fees, forensic costs, reserves for potential card brand fines, and other related settlement costs… [and] others in the payments chain also face losses when data breaches occur. Most important, if the breach is significant enough or if there are a number of breaches over a short period of time, consumer confidence in card-based electronic payments may suffer, causing consumers to switch to less efficient forms of payments.[199]

The Heartland Breach: What Happened

An understanding of exactly what happened at Heartland and other breaches is important to stave off future threats. Accordingly, "the method used to compromise Heartland's network was ultimately determined to be SQL injection."[200]

> Code written eight years ago for a web form allowed access to Heartland's corporate network. This code had a vulnerability that (1) was not identified through annual internal and external audits of heartland's systems or through continuous internal system-monitoring procedures, and (2) provided a means to extend the compromise from the corporate network to the separate payment processing network. Although the vulnerability existed for several years, SQL injection didn't occur until late 2007.
>
> After compromising Heartland's corporate network, the intruders spent almost six months and many hours hiding their activities while attempting to access the processing network, bypassing different anti-virus packages used by Heartland. After accessing the corporate network, the fraudsters installed sniffer software that was able to capture payment card data, including card numbers, card expiration dates, and, in some cases, cardholder names as the data moved within Heartland's processing system.[201]

---

[198] Julia S. Cheney, *Heartland Payment Systems: Lessons Learned from a Data Breach* (Jan. 1, 2010), FRB of Philadelphia – Payment Cards Center Discussion Paper No. 10-1, *Available at* http://www.ssrn.com/abstract=1540143.
[199] *Id.* at 18.
[200] *Id.* at 3.
[201] *Id.* (*observing* According to a Heartland press release, 'No merchant data or cardholder Social Security numbers, unencrypted personal identification numbers (PIN), addresses or telephone numbers were involved in the breach. Nor were any of Heartland's check management systems; Canadian, payroll,

> The fraudsters' focus on compromising data as they moved within Heartland's network – data in transit – rather than when they were stored in consumer databases – or, in other words, when data were at rest – was a relatively new phenomenon… One example, if not the first, of this expansion in focus toward data-in-transit compromises was the data breach at Hannaford Brothers announced in early 2008.[202]

Heartland's Response

Heartland Chairman and CEO Robert Carr outlines Heartland's response to the breach as "rest[ing] on two pillars aimed at the merchant acquiring and processing side of the payment system: improve data sharing and better secure data, particularly data in transit."[203] The Heartland breach was particularly unexpected since the company "was certified by network-approved quality security assessors (QSAs) as being PCI compliant at the time of the breach and, in fact, had received this certification several times during the period in which the vulnerability had been present.[204] In addition,

> [Mr. Carr] used this point not to diminish PCI but rather to emphasize that PCI compliance is a minimum standard and that most companies regularly do much more than required by PCI. Heartland Payment Systems was one of those companies that had met its PCI requirements and had made data security one of its top, if not its top, business priorities. Carr said that Heartland manages data security 24/7 and has about 7 percent of its information technology staff focused on security efforts, including a recently hired senior executive who focuses solely on data security and strategy. That data breach occurred despite Heartland's strong focus on data security and its status as being PCI compliant has led Carr to the opinion that more must be done to increase the security of data transfers (data in transit) among participants in the payments system, including merchants.[205]

---

campus solutions or micropayments operations; Give Something Back Network; or the recently acquired Network Services and Chockstone processing platforms.' For more information see the press release, 'Heartland Payment Systems Uncovers Malicious Software in its Processing System,' Heartland Payment Systems, Jan. 20, 2009. (www.2008breach.com/Information20090120.asp).

[202] *Id. citing* Clarke Canfield & Brian Bergstein, *Hannaford Data Breach Offers Twists from Prior Attacks,* Associated Press, March 20, 2008.

[203] *Id.* at 5.

[204] *Id.* at 4.

[205] *Id.citing,* James C. McGrath & Ann Kjos, *Information Security, Data Breaches, and Protecting Cardholder Information: Facing Up to the Challenges,* Payment Cards Center, 6 (Sept. 13-14, 2006),

Heartland's Lessons Learned

Heartland Chairman and CEO Robert Carr offered the following additional comments about the Heartland data breach incident

> 1. Do not underestimate the insider threat,
> 2. Ensure the appropriate audit scope, and
> 3. Maintain in-house security expertise at the senior executive level.
>
> [Mr.] Carr emphasized that insider threats may not stem from intentional fraud but rather from misplaced employee goodwill. For example, an employee may retain cached files, including account information, on their computer in order to more quickly process customer service requests. In addition, security protocols must be universally applied and enforced among all employees, at all levels of hierarchy and across all departments. Ensuring that auditors have a wide scope to review systems for security vulnerabilities is also important to identify situations, such as happened at Heartland, in which fraudsters were able to penetrate the processing system by first compromising another, separate network, in this case the corporate network. Finally, security expertise and strategic planning are critical skills that should be emphasized at the highest levels of the corporate structure.[206]

Other Data Breach Cases

We have previously reported that "Aetna was sued by a data breach victim after its job application web site was hacked and job applicants began receiving phishing e-mails asking for additional personal information."[207] Moreover,

> The case was dismissed for failure of a lack of standing because the particular plaintiff had not received one of the e-mails and could not prove his actual data had been breached.[208] Still, the headache of

---

available at www.philadelphiafed.org/payment-cards-center/events/conferences/2007/C2006SeptInfoSecuritySummary.pfd), *see also* Brendan James Gilbert, *PCI Compliance for Outsources eCommerce Applications* (May 3, 2009), *available at* http://www.ssrn.com/abstract=1409136, and Ulf T. Mattsson, *PCI and Beyond – How to Secure Data in the Most Cost Effective Manner* (Jan. 20, 2009), *available at* http://www.ssrn.com/abstract=1330466.

[206] *Id.* at 8.

[207] Trautman & Altenbaumer-Price, *supra* note 1, *citing Aetna boots data breach class action suit*, INFOSECURITY.COM (March 12, 2010).

[208] *Id.*

defending and paying for defense of the case were present. Other incidents include:

- TJX, the parent company of TJ Maxx, Marshall's, and HomeGoods, reported the theft of 40 million credit card numbers, costing it more than $200 million.[209] TJX was sued in a class action lawsuit and spent more than $12 million in one quarter "for costs incurred to investigate and contain the intrusion, improve computer security and systems, and communicate with customers, as well as technical, legal, and other fees."[210]
- Dave & Busters was hit by three men who hacked into its registers and stole data from thousands of credit and debit cards. That data was later sold and caused $600,000 in losses to customers.[211]
- A breach at the grocer Hannaford, which also does business as Food Lion, resulted in the theft of more than 4 million customer credit and debit card numbers.[212]
- A retailer reported that computer hackers stole millions of credit and debit card numbers from the company over a two-year period. News reports indicated that some of the stolen information was used to commit fraud. The retailer faces a multi-state probe, and lawsuits are mounting over the data breach.[213]
- A media conglomerate lost unencrypted computer backup tapes containing sensitive information, including Social Security numbers, from thousands of people.[214]
- An educational institution faces a class-action lawsuit filed by two alumni whose personal data were among thousands accessed when hackers broke into the school's computer system.[215]
- A wholesaler announced that thieves had accessed more than one million credit and debit card numbers and transaction information involving thousands of customer checks.[216]
- An information broker announced that a fraud ring had gained access to thousands of records containing personal and

[209] Accenture, *supra* note 21, *see also* Siobhan Gorman, *Arrest in Epic Cyber Swindle*, WALL ST. J. (Aug. 18, 2009).
[210] Sharon Gaudin, *T.J. Maxx Breach Costs Hit $17 Million*, INFO. WK. (May 17, 2007).
[211] Brian Krebs, *Three Charged with Hacking Dave & Buster's Chain*, WASH. POST SECURITY FIX BLOG (May 14, 2008).
[212] Brian Krebs, *Grocer Says Data Were Compromised*, WASH. POST (Mar. 19, 2008).
[213] Chubb Group of Insurance Companies, *CyberSecurity by Chubb: Insuring Cyber Exposures for Businesses of All Kinds, http://www.sgdins.com/downloads/CyberSecurity%20by%20Chubb.pdf* (last visited July 20, 2010).
[214] *Id.*
[215] *Id.*
[216] *Id.*

financial information about consumers from the company's database.[217]

Regulatory Minefield: Data Breach Notification

Much has been written about the complex patchwork of domestic and international data breach statutes and penalties.[218] Data breach notification laws are now found in forty states.[219] For example, "Maine, Maryland, New York, New Hampshire, North Carolina, Vermont and Virginia require breaches to be reported to a centralized data base."[220] In addition, "other states, including California, Colorado, Florida, Illinois, Massachusetts, Michigan, Nebraska, Hawaii and Wisconsin, require some level of publicly available notification, primarily through Freedom of Information requests."[221] Morever, "companies that operate internationally may have to contend with the European Union's Data Directive regarding the transfer of personal data between countries."[222]

---

[217] *Id.*

[218] *See generally* Sasha Romanosky, Alessandro Acquisti & Richard Sharp, *Data Breaches and Identity Theft: When is Mandatory Disclosure Optimal?* (2010), *available at* http://ssrn.com/abstract=1989594, Paul M. Schwartz, & Edward J. Janger, *Notification of Data Security Breaches*, 105 Mich. L.Rev. 913, 2007; Brooklyn Law School, Legal Studies Paper No. 58. *available at* http://ssrn.com/abstract=908709, Sasha Romanosky, Rahul Telang & Alessandro Acquisti, *Do Data Breach Disclosure Laws Reduce Identity Theft?,* 30 J. of Policy Analysis and Mgmt., 256-286, (2011). *available at* http://ssrn.com/abstract=1268926, Dana Lesemann, *It's Not the Breach, it's the Cover-Up: Using Digital Forensics to Mitigate Losses and Comply with Florida's Data Breach Notification Statute,* 82 Florida Bar Journal, (Feb. 2008), *available at* http://ssrn.com/abstract=1671810, Alana Maurushat, *Data Breach Notification Law Across the World from California to Australia,* Privacy Law and Business International, (Feb. 2009), *available at* http://ssrn.com/abstract=1412063, Mark Burdon, Bill Lane & Paul Von Nesson, *The Mandatory Notification of Data Breaches: Issues Arising for Australian and EU Legal Developments* 26 Computer Law & Security Rev., 115 (2010) *available at* http://ssrn.com/abstract=1697929, Dana Lesemann, *Once More Unto the Breach: An Analysis of Legal, Technological and Policy Issues Involving Data Breach Notification Statutes,* 4 Akron Intel. Prop. J., 203, (2010), available at http://ssrn.com/abstract=1671082, and Jane K. Winn, *Are 'Better' Security Breach Notification Laws Possible?* 24 Berkley Tech. L..J. (2009), *available at* http://ssrn.com/abstract=1416222.

[219] Trautman & Altenbaumer-Price, *supra* note 1, at 336 *citing* Privacy Rights Clearinghouse, *supra* note 33.

[220] *Id.*

[221] *Id.*

[222] *Id. citing* European Union Safe Harbor Overview, U.S. Dept. of Commerce Int'l Trade Admin. export.gov Web site, http://www.export.gov/safeharbor/eu/eg_main_018476.asp, (last visited Sept. 13, 2012).

Another example of IT risk regulation is the Federal Trade Commission's "Red Flags Rule" requiring certain companies to implement an identity theft program, (effective December 31, 2010).[223]

> Under the rule, financial institutions subject to FTC oversight and all companies—both private and public—that extend credit to their customers must have a written plan in place to detect and respond to identity theft.[224] The plan must identify the red flags inherent to a particular company's operations, such as scenarios in which there is risk for exposure of sensitive customer information or in which there are indicators that customer data may have already been breached.[225]
>
> The reach of the rule is broad. It extends not only to banks and other financial institutions subject to FTC regulation, but to any company that functions as a creditor to its customers, such as retailers that offer charge accounts or store credit cards or auto dealers that offer customer financing.[226] It extends to any company that bills for services already rendered, such as doctors, lawyers, accountants, or even lawn services.[227] Utility companies and telecommunications providers that bill for the prior month's—rather than the next month's—services would be covered by the Red Flags Rule.[228]

XII. YOUR IT CRISIS MANAGEMENT PLAN

Best practice mandates that every board have a crisis management plan in place before a disaster occurs, since "advance planning is a key prevention measure for any business. In an emergency incident response situation, a well-written and properly socialized incident response plan will be the best method to inform the relevant stakeholders, identify the incident, and contain the security breach."[229] In addition

---

[223] Trautman & Altenbaumer-Price, *supra* note 1, at 336 *citing* FTC Press Release, FTC Extends Enforcement Deadline for Identity Theft Red Flags Rule (May 28, 2010) (*available at* http://www.ftc.gov/opa/2010/05/redflags.shtm).
[224] 16 C.F.R. §681.2.
[225] *Id.*
[226] *Id.*
[227] *Id.*
[228] *Id.*
[229] Pinguelo & Muller, *supra* note 29 at 82.

> Often times during an emergency situation, well-intentioned administrators make changes that either disrupt the business or jeopardize the integrity of the digital evidence. It is critical that the incident response plan lays out a proper chain of command.
>
> Companies should also perform a mock-incident response training scenario once a year to ensure adoption of the plan and its effectiveness, as a well-oiled machine functions much more efficiently than a rusty one. A mock-incident exercise will also test the viability of the written plan. Finally, companies should work with a team of dedicated IT security experts who are knowledgeable and experienced in dealing with IT security threats and incident response. This can be an internal team or an external partner. It may not always make sense for every organization to have this level of expertise in-house, thus partnering with a reputable company may be the more reasonable solution.[230]

The following elements of a crisis management plan represent steps that every board can take *before* a crisis takes place. Identifying and having a relationship with the professionals needed to assist in stressful times is always best handled when you have sufficient time to make reasoned decisions. A cyber disaster, in particular, requires decisions regarding:

1. **Damage Assessment-** How you intend to ascertain exactly what has happened.
2. **Public Relations-** How you intend to respond (since timeliness is critical).
3. **Need for Outside assistance-** Who is needed to assist you with this highly technical problem.
4. **Resources needed to cure** defects that allowed this breach to happen.
5. **How you intend to monitor** & prevent future reoccurrences.

A perfect example of having a crisis management plan in place is that of Bryan Kennedy, President & CEO Irving, Texas-based of Epsilon Data Management. Epsilon describes itself as "the world's largest permission-based email marketing provider,

[230] *Id.*

sending over 40 billion emails annually."[231] When Epsilon discovered on March 31, 2011 that customer email addresses had been stolen, its crisis management plan enabled the company to assess the situation and react quickly. After determining that the data hacked was not of the type required by law to be disclosed (didn't involve medical data, credit-card or Social-Security numbers), Epsilon decided to fully disclose the incident the next day.[232]

Ted Chung, chief executive of Hyundai Capital Services Inc., South Korea's largest consumer-finance company, sustained a computer system hack and blackmail attempt from two groups of hackers.[233] Mr. Chung now believes

> His biggest mistake was that he used to treat the information-technology department as simply one of many units that helped the company get its main job done. Learning from this hacking experience, he now treats the Information Technology function as "central to everything the company does. Since the attack, Mr. Chung has spent weeks learning the ins and outs of network architecture, security infrastructure and the tradeoffs between data protection and customer satisfaction.
>
> The IT department, which has added a security unit, now reports directly to the CEO. The company has slowed the introduction of several new products to ensure they don't create new holes in security.[234]

XIII. A CALL TO ACTION

Commitment at the Top

To be successful, IT governance requires enterprise commitment at the very top. Deloitte contends that it is difficult to get IT issues on the board agenda because "in some cases, the board lacks members with the appropriate experience and expertise to be

[231] Epsilon About Us, http://www.epsilon.com/About-Us/p36-l1 (last visited June 18, 2011).
[232] Ben Worthen & Anton Troianovksi, *Firms Come Clean on Hacks,* Wall St. J., June 17, 2011, at B1.
[233] Evan Ramstad, *Executive Learns from Hack: CEO Now Treats IT Department as Critical to Hyundai Capital's Operations,* WALL ST. J., June 21, 2011, at B6.
[234] *Id.*

comfortable in addressing issues related to IT."[235] In some organizations, "senior technology officers are poorly equipped to communicate and work with the board. And when management and the board have not previously established clear and consistent communications on IT matters, IT often remains a foreign topic in the boardroom."[236] The challenges associated with achieving understanding and management of the risks involved with implementing new technologies may appear almost insurmountable. Every corporation's IT challenges and concerns will include:

- Recognizing the importance of IT at the highest (board) level and settling upon goals and necessary resources
- Aligning IT strategy with the business strategy
- Cascading strategy and goals down into the enterprise
- Providing organizational structures that facilitate the implementation of strategy and goals
- Insisting that an IT control framework be adopted and implemented
- Measuring IT's performance[237]

Role and Value of Chief Information Security Officer

Information technology governance may benefit from the presence of a skilled Chief Information Security Officer (CISO). Professor Scott Shackelford says that "most would have thought that, as a leading IT company, Sony would have had a senior manager devoted to information security."[238]

> Yet when the company was hacked in April 2011, it did not have a Chief Information Security Officer. Firms with a CISC (or equivalent title) have been reported to experience fewer costs when a breach occurred: $157 per

[235] Deloitte, *supra* note 161, at 9.
[236] *Id.*
[237] USI Insurance Services, *Cyber Liability / Security and Privacy Insurance* (2009) (on file with the authors).
[238] Shackelford, *supra* note 27 at 16.

record, versus $236 per record for firms without strategic security leadership that is part of overall enterprise risk management.[239]

Ten Ways to Improve Cybersecurity

Pinguelo and Muller note that "although companies cannot prevent all hacking incidents, these relatively simple measures—combined with diligent employee training, custom technology tools tailored to a business' needs, and through incident response planning—can help improve a company's cybersecurity and prepare it to respond effectively to those incidents that do occur."[240] Accordingly, Pinguelo and Muller provide the following ten measures to improve cybersecurity and response to attacks:

1. The most effective way to prevent cybercrime at the workplace is through enhancing employee knowledge. Training that generates awareness of the security threats that may come from email, privileged access, weak passwords and the like is vital. Training should also be provided to all employees on the topics of social engineering, tampering, and fraud, using a top-down approach.
2. Employees should be instructed to create robust passwords on their systems. It is advisable to use a complex alphanumeric password with a minimum length of 7 characters. If possible, the password should include the use of ASCII characters. These passwords can be relatively simple and easy to memorize without losing their effectiveness, such as eX@mple.
3. At a minimum, companies should encrypt their sensitive data with AES encryption. It does not impose as significant of a problem if your company's data is stolen, but the cybercriminals are unable to read it.
4. A business should take all of its sensitive or proprietary information and put it in 'the bank.' Network segmentation is an effective method to lock down and secure a part of the network or systems that has the most confidential data. Another benefit of this method is that the cost of securing and locking down a portion of a company's network is far less expensive than doing the same for the entire enterprise.
5. Companies should also perform a quarterly vulnerability scan of the external network and an annual scan of the internal network. This routine maintenance can uncover gaps and holes that may be left on a company's network and systems.

---

[239] *Id. citing* C. Costanzo, *Is Your Company Prepared for Cyber Risk,* (2011), Retrieved Nov. 23, 2011, *available at* http://www.boardmember.com/MagazineArticle_Details.aspx?id=5943&page=1, and D. Drouin, *Cyber Risk Insurance: A Discourse and Preparatory Guide, SANS Institute InfoSec Reading Room.*(2004).

[240] Pinguelo & Muller, *supra* note 29 at 85.

6. Companies would be well-served to practice better management of access at every level: network, system, and user credentials. This includes purging or disabling default accounts, accounts belonging to former employees, and accounts that are no longer used. Further, as the saying goes, *'Quis custodiet ipsos custodies?'* (Who will guard the guards themselves?). Privileged user/system accounts and administrators have rights to all areas of the enterprise. Companies must have in place some type of monitoring or logging system that tracks these administrators and others, especially around areas where sensitive data is stored. This will ultimately provide a detailed record for accountability and may even act as a deterrent.
7. Companies must properly monitor egress network traffic for anomalies or spikes in the netflow data. For example, if a company discovers that its data is being exfiltrated out of the enterprise to an IP address in Eastern Europe, and the company has no customers there, then that should set off a few alarms.
8. Business should monitor log data because it provides a wealth of information before, during, and after the breach. It is important to log relevant systems and devices properly, as the fingerprints of a hacker are normally found there. Log data is the forensic investigator's crime scene in the form of digital evidence.
9. A company's IT team should keep secure code development in mind, as failure to do so may open the enterprise to an attack on its website or software. Typically when programming or developing code or website content, the only goal is to make sure it is functional. There are various vulnerabilities—stemming from poor code reviews and poor application testing—such as SQL injection, cross-site scripting, and exploitation of session variables. Companies should ensure that secure coding practices are combined with practical web/software application scanning.
10. The easiest way for a hacker to get in is through an 'open door.' Specifically, this open door may come in the form of insecure remote-access services that are public-Internet-facing and are not locked down. Such an open door could potentially provide a hacker with direct control of a server with access to the company's network. An 'open door' may also be exposed through vulnerabilities in the company's software or through an inexcusably weak password for a system that has been long forgotten. Two-factor authentication is one way to secure remote access services to keep hackers from gaining entry to the corporate network.[241]

[241] *Id.* at 83, *citing* Wade Baker, et. al, *Verizon RISK Team, 2011 Data Breach Investigations Report (2011), available at* http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf.; John Schwartz, *U.S. Selects a New Encryption Technique,* N.Y. TIMES, (Oct. 3, 2000), *available at* http://www.nytimes.com/2000/10/03/business/technology-us-selects-a-new-encryption-technique.html.; Kenneth N. Rashbaum, 18 Rich. J.L. & TECH. 9, 32-33 (2012); THE OPEN WEB APPLICATION SEC. PROJECT, OWASP TOP 10, A1 (2010), *available at* https://www.owasp.org/index.php/Top_10_2010-Main; and G. Hoglund & G. McGraw, *CAPEC-21: Exploitation of Session Variables, Resource IDs and other Trusted Credentials,* CAPEC (Jan. 1, 2007), *available at* http://capec.mitre.org/data/defititions/21.html.

XIV. CONCLUSION

It has become apparent that newly-disclosed attacks on Information Technology infrastructure have reached crisis proportions. Therefore, a focus on IT governance must be a major priority of management and every corporate board. Issues involving Information Technology are uniquely complex and involve engineering skills that quickly become obsolete in this era of rapid technological change. An examination of recent threats will hopefully assist in bringing a greater understanding of their nature and increased focus on IT governance to the agenda in every boardroom.