Santa Clara High Technology Law Journal

Volume 33 | Issue 2 Article 2

1-2-2017

Managing Cyberthreat

Lawrence J. Trautman

Follow this and additional works at: http://digitalcommons.law.scu.edu/chtlj

Part of the Intellectual Property Law Commons, and the Science and Technology Law Commons

Recommended Citation

Lawrence J. Trautman, *Managing Cyberthreat*, 33 Santa Clara High Tech. L.J. 230 (2017).
Available at: http://digitalcommons.law.scu.edu/chtlj/vol33/iss2/2

This Article is brought to you for free and open access by the Journals at Santa Clara Law Digital Commons. It has been accepted for inclusion in Santa Clara High Technology Law Journal by an authorized editor of Santa Clara Law Digital Commons. For more information, please contact sculawlibrarian@gmail.com.

MANAGING CYBERTHREAT

Lawrence J. Trautman[†]

Cybersecurity is an important strategic and governance issue. However, most corporate CEOs and directors have no formal engineering or information technology training, which leads to a problematic lack of actual cybersecurity knowledge. Particularly in smaller companies with limited resources, knowledge regarding what their enterprise should actually be doing about cybersecurity isn't all that good.

My goal in this article is to explore the unusually complex subject of cybersecurity in a highly readable manner. First, I provide an examination of recent threats. Next, I discuss governmental policy initiatives. Third, I offer some basic tools that can be used by boards and top management to improve the quality of discussions with their information technology executives. It is likely that most top management and corporate directors have never heard of, let alone read: the SANS Critical Security Controls; OWASP Top Ten; CWE/SANS Top 25 Most Dangerous Software Errors; Presidential Executive Order 13636 (& Treasury Dept. Report); Quadrennial Homeland Security Review; or NIST Framework. By offering suggestions about what top managers and boards can do to improve organizational cybersecurity awareness and readiness, this paper makes a worthwhile contribution to the literature of risk management and provides meaningful progress in strengthening the knowledge base and ability of top management and boards to govern enterprise cybersecurity.

[†] B.A., The American University; M.B.A., The George Washington University; post-graduate studies (Management Information Systems) University of Texas at Dallas; and J.D., Oklahoma City University School of Law. Mr. Trautman is Assistant Professor of Business Law and Ethics at Western Carolina University and 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 Lawrence.J.Trautman@gmail.com. The author wishes to extend particular thanks to the following for their assistance in the research and preparation of this article: Admiral Bobby R. Inman, USN (Retired), Former Director of the National Security Agency (NSA) and Deputy Director of U.S. Central Intelligence; Scott Godes, Gary J. Fernandes, Stuart Malawer, Thomas M. Nealon, Arun Sood, James C. Wetherbe, and, in particular, Frederick R. Chang. All errors and omissions are my own.

Keywords: Audit Committee, Board Structure, Corporate Governance, Credit Card Theft, Crime, Cyber, Data Breach, DHS, Directors, Enterprise Risk Management, Hackers, incentives, Information Technology, Internal Controls, Market Failure, National Security, NCCIC, NIST, OWASP; SANS, Sarbanes-Oxley, SEC, Strategy, US-CERT

TABLE OF CONTENTS

INTRODUCTION 232
I. THREATS ESCALATE 236
 A. Top Ten Major Breaches 237
II. HERE COME THE HACKERS 239
 A. Nortel Hacked 240
 B. The Heartland Breach: What Happened 241
 C. Heartland's Lessons Learned 243
 D. FBI Action Against Cybercrime and Credit Card Theft 244
III. BARBARIANS AT THE GATES 246
 A. Post-9/11 Transnational Legal Framework 246
 B. Assault on Federal, State and Local Governments 247
 C. Cyberattack: A National Security Issue 248
 D. Blueprint for a Secure Cyber Future 253
 E. Failure of Cybersecurity Act of 2012 254
 F. Executive Order 13636 and Critical Infrastructure 257
 G. Treasury Report on Cybersecurity Incentives 259
 H. Framework on Improving Critical Infrastructure Cybersecurity 261
  1. Each Enterprise's Need Is Unique 261
  2. The Framework Is Organic 262
 I. Quadrennial Homeland Security Review ("2014 Review") 263
 J. Congressional Cybersecurity Action 266
IV. CORPORATE RESPONSIBILITY FOR RISK GOVERNANCE 266
 A. The SEC on Risk & Dodd-Frank Wall Street Reform 266
 B. SEC Disclosure Guidelines 268
V. BOARD COMPOSITION: THE CASE FOR CYBERSECURITY EXPERTISE 270
 A. Each Board Has Different Levels of IT and Cybersecurity Skills 270
 B. Organizational IT and Cybersecurity Knowledge 270
 C. The Audit Committee: Appropriate Site for IT Expertise and Experience 271
 D. Barriers to IT-Internal Audit Effectiveness 272

VI. YOUR CYBERSECURITY CRISIS MANAGEMENT PLAN 272
VII. A CALL TO ACTION: WHAT YOU CAN DO, NOW! 274
A. Leadership Commitment at the Top...................................275
B. Basic Cyber Hygiene 275
C. SANS Institute Critical Security Controls...........................276
D. OWASP Top Ten 278
E. CWE/SANS Top 25 Most Dangerous Software Errors.......279
F. U..S. Computer Emergency Readiness Team (US-CERT)..280
G. Role and Value of Chief Information Security Officer 281
H. Ten Ways to Improve Cybersecurity..................................281
CONCLUSION 287

INTRODUCTION

Cybersecurity is an important strategic and governance issue.[1] However, most corporate CEOs and directors have no formal engineering or information technology training, which leads to a problematic lack of actual cybersecurity knowledge. Particularly in smaller companies with limited resources, knowledge regarding what their enterprise should actually be doing about cybersecurity isn't all that good.

Speaking at the New York Stock Exchange "Cyber Risks and the Boardroom" Conference, SEC Commissioner Luis A. Aguilar stated that "[o]ver just a relatively short period of time, cybersecurity has become a top concern of American companies, financial institutions, law enforcement, and many regulators."[2] Observing that "[l]aw

[1] *See generally* Susan P. Crawford, *First Do No Harm: The Problem of Spyware*, 20 BERKELEY TECH. L.J. 1433 (2005) (discussing spyware legislation); Urs Gasser & Daniel M. Häusermann, *E-Compliance: Towards a Roadmap for Effective Risk Management*, (Mar. 15, 2007), THE BERKMAN CENTER FOR INTERNET & SOCIETY AT HARVARD LAW SCHOOL § 3, (2007), (discussing internet risk management and maps a comprehensive e-compliance strategy); Lawrence J. Trautman & Kara Altenbaumer-Price, *The Board's Responsibility for Information Technology Governance,* 28 J. MARSHALL J. COMPUTER & INFO. L. 313, 314 (2011) (sounding an alarm about the escalating cybersecurity threats facing management of every enterprise addresses 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"), http://bit.do/BoardResponsibilityforITGovernance; Jonathan Zittrain, *The Generative Internet,* 119 HARV. L. REV. 1974, 1974-80 (2006), (a pioneering work discussing software vulnerabilities).

[2] *Corporate Governance and Cyber Risks: Sharpening the Focus, Address Hearing Before the New York Stock Exchange, Conference on "Cyber Risks and the Boardroom,"* (2014) (Statement of Luis A. Aguilar, Commissioner, U.S. Securities and Exchange Comm'n, Boards of Directors) ("For example, the Director of the Federal Bureau of Investigation (FBI), James Comey, said last November that 'resources devoted to cyber-based threats will equal or even eclipse the resources devoted to non-cyber based terrorist threats.'"), http://bit.do/CorpGovernanceCyberRisks; *Protecting Your Personal Data: How Law*

enforcement and financial regulators have stated publicly that cyber-attacks are becoming both more frequent and more sophisticated,"[3] Commissioner Aguilar warned that "cyber-attacks have become increasingly costly to companies that are attacked. According to one 2013 survey, the average annualized cost of cybercrime to a sample of U.S. companies was $11.6 million per year, representing a 78% increase since 2009."[4] Particularly alarming are survey research results of senior decision-makers among the largest companies in 59 countries indicating that nearly fifty percent of respondents "see cybercrime as a

Enforcement Works With The Private Sector To Prevent Cybercrime: Hearing before the House Comm. on Homeland Sec'y, Subcomm. on Cybersecurity, Infrastructure Prot., and Sec'y Tech., 113th Cong. (2014) (written testimony of Ari Baranoff, Assistant Special Agent in Charge, United States Secret Service Criminal Investigative Division) ("Advances in computer technology and greater access to personally identifiable information (PII) via the Internet have created online marketplaces for transnational cyber criminals to share stolen information and criminal methodologies. As a result, the Secret Service has observed a marked increase in the quality, quantity, and complexity of cybercrimes targeting private industry and critical infrastructure."), http://bit.do/ProtectingPersonalData; *Threats to the Homeland: Hearing before the Senate Comm. on Homeland Sec'y and Gov't Affairs,* 113th Cong. (2013) (statement of James B. Comey, Jr., Director, FBI, U.S. Department of Justice), http://bit.do/ThreatsToHomeland; *see also House Comm. on Homeland Sec'y,* 114 Cong. (2014) (statement of Jeh C. Johnson, Secretary, U.S. Department of Homeland Security) ("DHS must continue efforts to address the growing cyber threat to the private sector and the '.gov' networks, illustrated by the real, pervasive, and ongoing series of attacks on public and private infrastructure."), http://bit.do/JehJohnsonStatement; Remarks by Secretary of Defense Leon E. Panetta to the Business Executives for National Security (Oct. 11, 2012) ("As director of the CIA and now Secretary of Defense, I have understood that cyber attacks are every bit as real as the more well-known threats like terrorism, nuclear weapons proliferation and the turmoil that we see in the Middle East. And the cyber threats facing this country are growing."), http://bit.do/RemarksByLeonPanetta.

[3] *Corporate Governance and Cyber Risks, supra* note 2; for example, on December 9, 2013, the Financial Stability Oversight Council held a meeting to discuss cybersecurity threats to the financial system. *See* U.S. Department of the Treasury Press Release, *Financial Stability Oversight Council to Meet December 9* (2013), http://bit.do/FinancialStabilityOversight. During that meeting, Assistant Treasury Secretary Cyrus-Amir-Mokri said that "[o]ur experience over the last couple of years shows that cyber-threats to financial institutions and markets are growing in both frequency and sophistication." *See* Remarks of Assistant Secretary Cyrus Amir-Mokri on Cybersecurity at a Meeting of the Financial Stability Oversight Council (Dec. 9, 2013), http://bit.do/CyrusAmir-MokriRemarks. In addition, in testimony before the House Financial Services Committee in 2011, the Assistant Director of the FBI's Cyber Division stated that the number and sophistication of malicious incidents involving financial institutions has increased dramatically over the past several years and offered numerous examples of such attacks, which included fraudulent monetary transfers, unauthorized financial transactions from compromised bank and brokerage accounts, denial of service attacks on U.S. stock exchanges, and hacking incidents in which confidential information was misappropriated. *See* U.S. House, House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit, 112 Cong. (statement of Gordon M. Snow, Assistant Director, Cyber Division, FBI, U.S. Department of Justice) (2011), http://bit.do/GordonSnowStatement.

[4] HP Press Release, *HP Reveals Cost of Cybercrime Escalates 70 Percent, Time to Resolve Attacks More Than Doubles* (Oct. 8, 2013), http://bit.do/HPRevealsCostOfCybercrime.

very or fairly low risk to their business."[5] In addition, seventy-four percent of these mostly non-U.S. respondents "whose business had been breached stated that the breach had not been publicly disclosed."[6] One estimate is that "cybercrime costs the United States approximately $100 billion annually."[7]

Top management and corporate directors are busy people. Competing demands for the time and attention of corporate directors include: all the preparation work required by committee assignments (such as audit, compensation, nominating and governance); key top management succession planning; the need to absorb complex information from a company's financial statements; a reading load that includes important internal documents; compliance issues; strategy efforts; mandatory regulatory exposure areas (such as Dodd-Frank, Sarbanes-Oxley, the Foreign Corrupt Practices Act); necessary visits to company facilities; awareness and discussion of major financing issues; and ongoing ad hoc crisis management.[8] In addition, some directors serve as CEO of another organization and may serve as a director of more than one board.[9] Given this environment, developing a sophisticated awareness of cybersecurity issues is a challenge for those having significant competing responsibilities.

My goal in this article is to explore the unusually complex subject of cybersecurity in a highly readable manner. First, I provide an examination of recent threats. Next, I discuss governmental policy initiatives. Third, I offer some basic tools that can be used by boards and top management to improve the quality of discussions with their information technology executives. At this point, it is likely that most top management and corporate directors have never heard of, let alone read: the SANS Critical Security Controls; OWASP Top Ten;

[5] EY, *Overcoming Compliance Fatigue: Reinforcing the Commitment to Ethical Growth, 13th Global Fraud Survey*, at 4 (2014) (based on 2,719 interviews of senior decision makers in 59 countries and territories between November 2013 and February 2014), http://bit.do/OvercomingComplianceFatigue.

[6] *Id. See also* Lawrence J. Trautman & Peter C. Ormerod, Corporate Directors' and Officers' Cybersecurity Standard of Care: The Yahoo Data Breach, (Dec. 10, 2016); Lawrence J. Trautman & Peter C. Ormerod, *Industrial Cyber Vulnerabilities: Lessons from Stuxnet and the Internet of Things (IoT)* (unpublished manuscript on file with authors).

[7] Mitchell S. Kominsky, *The Current Landscape of Cybersecurity Policy: Legislative Issues in the 113th Congress,* HARV. NAT'L SEC. J. (Feb. 6, 2014), http://bit.do/LandscapeOfCybersecurityPolicy.

[8] *See generally* Lawrence J. Trautman, *The Matrix: The Board's Responsibility for Director Selection and Recruitment,* 11 FLA. ST. U. BUS. REV. 75 (2012) [hereinafter *Matrix*]; Lawrence J. Trautman, *The Board's Responsibility for Crisis Governance,* 13 HASTINGS BUS. L.J. __ (2016).

[9] *Id.*

CWE/SANS Top 25 Most Dangerous Software Errors; Presidential Executive Order 13636 (& Treasury Dept. Report); Quadrennial Homeland Security Review; or the NIST Framework. Hopefully, these suggestions about what top managers and boards can do to improve cyber awareness and readiness will result in meaningful progress toward strengthening cybersecurity governance.

It is understandable that directors in many boardrooms wonder "How can I be expected to govern something I know so little about?"[10] The complex modern environment in which data resides serves to complicate the issues surrounding governance of cyber risk. Serving as the SEC's inaugural Director of the Division of Risk, Strategy, and Financial Innovation (2009-2011), Professor Henry T.C. Hu, concluded 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 display, risk measurement, and other tools on which all depictions must primarily rely."[11] Professor Hu further observed that "such characteristics can be so complex that even 'objective reality' is subject to multiple meanings."[12] Significant additional costs may result from litigation stemming from potential liability exposure.[13] Professor Frederick Chang observes:

> Cyber infrastructure is tightly woven into the very fabric of our lives and it would be very hard to imagine going back to an earlier time −but we are paying a heavy price for our technological dependence, and the problem is worsening with the passage of time. Our trust in cyberspace has been taken from us by hackers, cybercriminals and sophisticated cyber attackers who intend to do us harm . . . We expect that it should not be impossibly difficult to protect ourselves in cyberspace if/when the need arises. These expectations are simply not being met today. Attacks on both the public

[10] *See* Trautman & Altenbaumer-Price, *supra* note 1, at 313 (citing Peter Weill and Jeanne W. Ross (depicting 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 (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 at the University of Texas).

[11] 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).

[12] *Id.*

[13] *See generally* Kevin M. Gatzlaff & Kathleen A. McCullough, *The Effect of Data Breaches on Shareholder Wealth,* 13 RISK MGMT. & INS. REV. 61 (2010).

> sector and the private sector are rampant. Denial of service, identity theft, and cyber extortion are now all too common . . . financial systems, national critical infrastructure systems, defense systems, and much more are all targets of sophisticated cyber attacks.[14]

I. THREATS ESCALATE

Mike McConnell, Booz Allen Hamilton Vice Chairman and former U.S. Director of National Intelligence observed that "there isn't a corporation in the nation today that can't be penetrated, not one."[15] In his Congressional testimony, Professor Chang stated: "Today our opponents in cyberspace are intelligent, seam-seeking, shape-shifting adversaries, that have an uncanny ability to penetrate and evade cyber defenses and compromise the targeted system."[16]

According to the Privacy Rights Clearinghouse, as of January, 2016, more than 736 million records (from 3,930 data breaches) were reported as breached and exposed during 2015.[17] During 2010, "one company reported a breach of 38 terabytes of information—equivalent to nearly double the amount of text contained in the Library of Congress."[18] Even more troubling "is the fact that the Clearinghouse records are not exhaustive, nor do they reflect breaches occurring outside the United States."[19]

[14] *Cyber R&D Challenges and Solutions: Hearings Before the H. Committee on Science, Space & Technology, Subcommittee on Technology and the Subcommittee on Research*, 113th Cong. (2013) (statement of Frederick R. Chang, President & COO, 21CT, Inc. and former director of research at the U.S. National Security Agency), http://bit.do/CyberRDChallenges.

[15] Ben Worthen, *Watching and Waiting: Most Cyberattacks are Random. But some attackers know exactly whom they want, and how to strike,* WALL ST. J. (Apr. 2, 2012), http://bit.do/CyberattacksAreRandom.

[16] *Is Your Data on the Healthcare.gov Website Secure?: Hearings Before the H. Committee on Science, Space & Technology, Subcommittee on Technology and the Subcommittee on Research*, 113th Cong. (2013) (statement of Frederick R. Chang, Bobby B. Lyle Centennial Distinguished Chair in Cyber Security, Southern Methodist University), http://bit.do/HealthcareWebsiteSecure. *See also* John G. Palfrey, *The Public and the Private at the United States Border with Cyberspace,* 78 MISS. L.J. 241 (2008).

[17] Privacy Rights Clearinghouse, *2015 Data Breach QuickView*, RISKBASED SECURITY, http://bit.do/2015DataBreach.

[18] Sen. Sheldon Whitehouse, *We Need to Act on Cybersecurity*, NAT'L L.J. (May 10, 2010), http://bit.do/ActOnCybersecurity.

[19] *Id.*

Exhibit One:
Reported Incidents of Loss, Theft or Exposure of Personally Identifiable Information (PII)

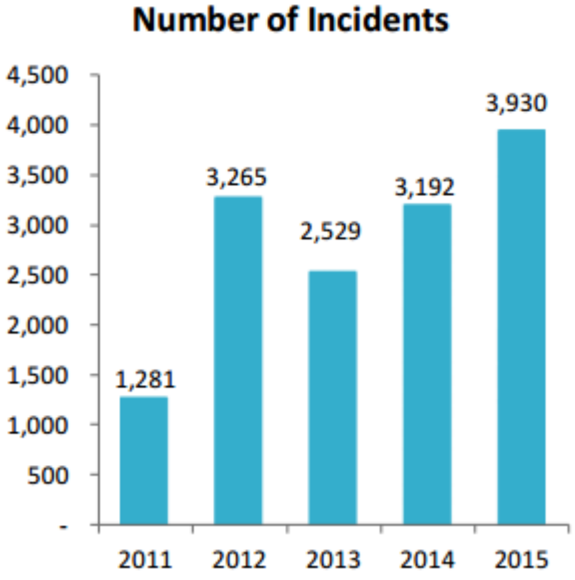

Exhibit One, courtesy of Risk Based Security, Inc., presents a disturbing picture of the rapid increase in data theft over the past five years.[20]

A. Top Ten Major Breaches

Here, courtesy of Risk Based Security, Inc., is a list of the top ten disclosed major breaches to date based on the number of records exposed:[21]

1. **UNKNOWN ORGANIZATION.** Reported breach of 220 million records on August 22, 2014.[22]
2. **UNKNOWN ORGANIZATION.** Reported breach of 191 million exposed records in United States of voter names, addresses, dates of birth, phone numbers, genders, political party affiliations, and

[20] *Data Loss Statistics: Number of Incidents,* RISK BASED SEC., INC. (2015), http://bit.do/DataLossStatistics.

[21] *Id.* at 11-13.

[22] *Id.*

other personal information (12/28/2015).[23]

3. **NYC TAXI & LIMOUSINE COMMISSION.** Breach exposing 173 million records, including customer trip details (6/21/2014).[24]
4. **ADOBE SYSTEMS, INC.** Encounters a hack exposing 152 million records, including customer names, debit and credit card information with expiration dates, IDs on October 3, 2013.[25]
5. **SHANGHAI ROADWAY D&B MARKETING SERVICES CO. LTD.** Replaced the Heartland Payments breach as the largest ever reported incident at the time involving 150 million records in March 2012).[26]
6. **eBAY, INC.** Reports 145 million records compromised on May 21, 2014.[27]
7. **UNKNOWN ORGANIZATION.** A breach involving 140 million records is reported on June 8, 2013.[28]
8. **HEARTLAND PAYMENT SYSTEMS, TOWER FEDERAL CREDIT UNION, BEVERLY NATIONAL BANK, NORTH MIDDLESEX SAVINGS BANK, GOLDEN CHICK.** Heartland involved a theft by cybercriminals using malicious software of 130 million credit and debit card numbers, resulting in a securities fraud class action for "fraudulently misrepresent[ing] the general state of its data security" and concealing an earlier cyberattack during earnings calls and in SEC filings.[29] Heartland knew that the stolen data included names, credit and debit card numbers, and expiration dates.[30]

[23] *Id.*

[24] *Id.*

[25] *Id.*

[26] *Id.*; *Shanghai Roadway D&B Marketing Services Co. Ltd.,* OPEN SOURCE FOUNDATION/DATALOSSDB.ORG. (Mar. 3, 2012), http://bit.do/ShanghaiRoadway.

[27] RISK BASED SEC., *supra* note 20; eBay Inc. Filing with U.S. Securities and Exchange Commission on Form 8-k (May 21, 2014), http://bit.do/eBayFilingSEC.

[28] RISK BASED SEC., *supra* note 20.

[29] *Id.*; *In re Heartland Payment Sys., Inc. Sec. Litig.*, No. 09-01043-AET-TJB, at 5 (D.N.J. Dec. 7, 2009); *see also* Trautman & Altenbaumer-Price, *supra* note 1, at 333 (citing Brian Krebs, *Payment Processor Breach May be Largest Ever*, WASH. POST SECURITY FIX BLOG, http://bit.do/PaymentProcessorBreach (Jan. 20, 2009)).

[30] RISK BASED SEC., *supra* note 20; Trautman & Altenbaumer-Price, *supra* note 1, at 333*;*

9. **TARGET BRANDS INC., FAZIO MECHANICAL SERVICES, INC.** Breach of 110 million records reported on December 18, 2013.[31]
10. **HOME DEPOT.** Breach of 109 million records with details of payment cards and customer email addresses (9/2/2014).[32]

II. HERE COME THE HACKERS

Contemporary examples of cyberattack include the widely discussed breaches at Target,[33] J.P. Morgan Chase,[34] the U.S. Postal Service,[35] Home Depot,[36] and the November 2014 breach of Sony Pictures Entertainment.[37] In many of these more recent cases, the facts

Press Release, Visa, *Heartland Payments Systems Agrees on Settlement to Provide Visa Issuers up to $60M for Data Breach Security Claims* (Jan. 8, 2010), http://bit.do/PaymentProcessorBreach; 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), http://bit.do/HeartlandSettlement3CardBrands; 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), http://bit.do/HeartlandAmExSettlement; Press Release, Heartland Payment Systems, *Heartland Payment Systems Agrees to Settle Cardholder Class Action Claim* (Dec. 21, 2009), PYMNTS.COM, http://bit.do/HeartlandSettleClassAction.

[31] RISK BASED SEC., *supra* note 20.

[32] *Id.*

[33] *See generally* Lawrence J. Trautman, *Is Cyberattack The Next Pearl Harbor?,*18 N.C. J. OF L. & TECH. 232 (2016).

[34] Emily Glazer, Danny Yadron & Daniel Huang, *Hackers May Have Targeted at Least 13 Firms,* WALL ST. J. (Oct. 9, 2014), http://bit.do/HackersTargetedFirms; Sarah Bloom Raskin, Deputy Secretary of the Treasury of the United States, Remarks Before the Meeting of the Texas Bankers' Association Executive Leadership Cybersecurity Conference: *Cybersecurity for Banks: 10 Questions for Executives and Their Boards* (Dec. 3, 2014), http://bit.do/CybersecurityForBanks.

[35] Laura Stevens & Danny Yadron & Devlin Barrett, *U.S. Post Office Says it Was Victim of a Data Breach,* WALL ST. J. (Nov. 10, 2014), http://bit.do/USPostOfficeVictimBreach.

[36] *See* Shelly Banjo, *Home Depot Hackers Exposed 53 Million Email Addresses,* WALL ST. J. (Nov. 6, 2014), http://bit.do/HomeDepotHack; Michael Calia, *Breach Plagues Home Depot,* WALL ST. J. (Nov. 18, 2014), http://bit.do/BreachPlaguesHomeDepot (reporting estimated cost of hacking to be $34 million during 2014).

[37] *See* Center for Strategic & International Studies, Significant Cyber Incidents Since 2006, (reporting that 'Sony Pictures Entertainment is hacked, with the malware deleting data and the hackers posting online employees' personal information and unreleased films. The incident is similar to earlier hacks against South Korean media outlets), http://bit.do/CyberIncidentsSince2006; *see also* Adrienne Debigare, Rebekah Heacock Jones & Jiou Park, *2014 Year In Review,* In Urs Gasser, Jonathan Zittrain, Robert Faris & Rebekah Heacock Jones, *Internet Monitor 2014: Reflections on the Digital World: Platforms, Policy, Privacy, and Public Discourse,* at 12, 22 (Dec. 15, 2014), http://bit.do/ReflectionsOnDigitalWorld; Berkman Center Research Publication No. 2014-17 (Dec. 15, 2014), http://bit.do/Berkman ResearchPublication2014-17.

are still being determined and litigation being brought. However, valuable lessons can be learned from several of the more seasoned breach cases of recent years, including Nortel and Heartland.

A. Nortel Hacked

Of particular importance to corporate boards and executives seeking to acquire other businesses is the example of Nortel, a case study that offers fair warning to all of the Trojan horse potential for highly destructive malware and spyware through acquisitions of data assets. 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."[38] 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.[39] 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."[40] 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."[41]

Nortel has sold 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."[42] Sean McGurk, credited with previously running the U.S. government's cybersecurity intelligence center, stated, "When you are buying those files or that intellectual property, you're also buying that 'rootkit,' . . . a term that refers to embedded spy software."[43]

> The spyware unearthed in 2009 was a sophisticated mix . . . . [R]esearchers

[38] Siobhan Gorman, *Chinese Hackers Suspected in Long-Term Nortel Breach*, WALL ST. J. (Feb. 14, 2012), http://bit.do/ChineseHackersSuspected.

[39] *Id.*

[40] *Id.*

[41] *Id.*

[42] *Id.*

[43] *Id.*

> 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.[44]

B. The Heartland Breach: What Happened

In another useful breach example, Heartland Payment Systems, a major credit card processor, disclosed on January 20, 2009 that cybercriminals had stolen 130 million credit card and debit card numbers, "at the time believed to be the largest security breach ever."[45] As a result, "the company and its officers and directors were forced to pay $60 million in a settlement with Visa,[46] $41.4 million in a settlement with MasterCard,[47] $3.6 million in a settlement with American Express,[48] up to $2.4 million in a consumer cardholder class action[49] over the same breach, as well as the defense costs of the dismissed suit."[50]

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 payments."[51] Learning exactly

[44] Gorman, *supra* note at 38.

[45] Trautman & Altenbaumer-Price, *supra* note 1 at 333 (citing Brian Krebs, *Payment Processor Breach May be Largest Ever*, WASH. POST SEC. FIX BLOG (Jan. 20, 2009), http://bit.do/PaymentProcessorBreach).

[46] *Id.* (citing Press Release, Visa, *Heartland Payments Systems Agrees on Settlement to Provide Visa Issuers up to $60M for Data Breach Security Claims* (Jan. 8, 2010), http://bit.do/HeartlandSettlementToVisaIssuers).

[47] *Id.* (citing 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), http://bit.do/HeartlandSettlement3CardBrands).

[48] *Id.* (citing 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), http://bit.do/HeartlandAmExSettlement).

[49] *Id.* (citing Press Release, Heartland Payment Systems, *Heartland Payment Systems Agrees to Settle Cardholder Class Action Claim* (Dec. 21, 2009), http://bit.do/HeartlandSettleClassAction).

[50] *Id.*

[51] 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, http://bit.do/HeartlandLessonsLearned.

what happened at Heartland and other breaches is helpful in any attempt to stave off future threats. In Heartland, their network compromise "was ultimately determined to be SQL injection":[52]

> 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.[53]
>
> 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.[54]

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."[55] 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,

[52] *Id.* at 3.

[53] *Id.* According to a Heartland press release, "[n]o 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, campus solutions or micropayments operations; Give Something Back Network; or the recently acquired Network Services and Chockstone processing platforms." See Press Release, Heartland Payment Systems, *Heartland Payment Systems Uncovers Malicious Software in its Processing System* (Jan. 20, 2009), http://bit.do/HeartlandUncoversMalicious Software.

[54] Cheney, *supra* note 51 (citing Clarke Canfield & Brian Bergstein, *Hannaford Data Breach Offers Twists from Prior Attacks,* FOSTERS.COM (Mar. 20, 2008), http://bit.do/HannafordDataBreach).

[55] Cheney, *supra* note 51, at 5.

in fact, had received this certification several times during the period in which the vulnerability had been present.[56] 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.[57]

C. 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.[58]

Mr. Carr also 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.[59]

[56] *Id.* at 4.

[57] *Id.* at 4 (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), http://bit.do/FacingUpToChallenges)*; see also* Brendan James Gilbert, *PCI Compliance for Outsources eCommerce Applications* (May 3, 2009), http://bit.do/PCICompliance; and Ulf T. Mattsson, *PCI and Beyond – How to Secure Data in the Most Cost Effective Manner* (Jan. 20, 2009), http://bit.do/SecureDataCostEffective.

[58] Cheney*, supra* note 51, at 8.

[59] *Id.*

D. FBI Action Against Cybercrime and Credit Card Theft

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."[60] As the result of a two-year investigation, the coordinated cybercrime sting, which involved thirteen countries, including the United States,

> resulted in 24 arrests, including the domestic arrests of 11 individuals . . . in the United States, and the arrests of 13 individuals abroad by foreign law enforcement in seven countries . . . [and] 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.[61]

Those eleven arrests took place "in the United Kingdom (six arrests), Bosnia (two), Bulgaria (one), Norway (one), and Germany (one). Two additional defendants were arrested in 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."[62] 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."[63]

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

[60] 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), http://bit.do/24ArrestsCybercrime.

[61] *Id.*

[62] *Id.*

[63] *Id.*

services related to carding, among other things."[64] The UC Site was established by the FBI

> 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 addresses entered by registered members of the site were collected by the FBI.[65]

According to the FBI, the term "carding" involves "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."[66] To illustrate,

> 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 . . . 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 . . . 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.[67]

[64] *Id.*

[65] *Id.*

[66] FBI Press Release, supra note 60.

[67] *Id.*

The term "carding forums" refers to websites used by carders

> to 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.[68]

The FBI provides the following explanation of how many of these illegal criminal activities are conducted:

> 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.[69]

III. BARBARIANS AT THE GATES

A. 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."[70] This de facto new transnational legal environment has evolved following the 9/11 destruction of the World Trade Center in New York City and is

[68] *Id.*

[69] *Id.*

[70] Stuart S. Malawer, *Cyber Warfare: Law and Policy Proposals for U.S. and Global Governance,* 58 VA. LAWYER 28 (2010) (citing Wesley K. Clark & Peter L. Levin, *Securing the Information Highway: How to Enhance the United States Electronic Defenses,* FOREIGN AFFAIRS 2 (Nov/Dec 2009), http://bit.do/SecuringInformationHighway).

"turbocharged by [the] unexpected recent challenges, which include terrorism, financial chaos, and environmental and national security."[71] Stuart S. Malawer observes that "the emergent 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."[72] Moreover,

> [t]he 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.[73]

B. Assault on Federal, State and Local Governments

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, 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."[74] 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."[75] 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."[76] The same group previously claimed responsibility for the PBS and Sony Pictures breaches.[77]

[71] *Id.*

[72] *Id.*

[73] *Id.*

[74] Nick Bilton, *Hacking Group Says It Brought Down C.I.A. Site*, N.Y. TIMES (June 15, 2011), http://bit.do/HackingGroupBroughtDownCIASite.

[75] *Id.*

[76] *Id.*

[77] *Id. See also* Lawrence J. Trautman, The SONY Data Hack: Implications for World Order (unpublished manuscript).

Pinguelo and Muller reported that "the weak American economy [post-2008] has caused most states to severely trim their budgets, reducing their ability to devote expenditures to cyberdefense."[78] 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.[79] 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 used a computer virus to gain access to the University's bank account. Luckily, the school was able to recover the money.[80]

While potentially applicable at the state government level, the Government Accounting Office (GAO), in its 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":[81]

> 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.[82]

C. Cyberattack: A National Security Issue

[78] 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. 120 (2011) (citing Deloitte & NASCIO, *State Goverrnments at Risk: A Call to Secure Citizen Data and Inspire Public Trust* (2010), http://bit.do/CallToSecureData).

[79] *Id.* (citing Deloitte.com, *Transcript: The Cyber Savvy State Government,* (on file with author)).

[80] Pinguelo & Muller, *supra* note 78, at 120, n.18.

[81] *Id.* at 122.

[82] *Id.* (citing Mark D. Goodman & Susan W. Brenner, *The Emerging Consensus on Criminal Conduct in Cyberspace,* 6 UCLA J.L. & TECH. 3, 18 (2002)).

"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.[83] 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."[84] A question every enterprise should ask is whether its top 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. The Wall Street Journal article described the current landscape:

> 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… 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.[85]

Deputy Secretary of Defense William Lynn says that "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."[86] The problem is massive, as "[e]ach year, a volume of intellectual property exceeding the size of the Library of Congress is stolen from U.S. Government and private-sector

[83] Anna Mulrine, *CIA Chief Leon Panetta: The Next Pearl Harbor Could Be a Cyberattack,* THE CHRISTIAN SCIENCE MONITOR (June 9, 2011), http://bit.do/PearlHarborCouldBeCyberattack; *see also* Eric Talbot Jensen, *President Obama and the Changing Cyber Paradigm,* 37 WM. MITCHELL L. REV. 5049 (2011); Stuart Malawer, *supra* note 70; Scott Shackelford, *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law,* 25 BERKELEY J. INT'L L. 191 (2009).

[84] Siobhan Gorman & Julian E. Barnes, *Cyber Combat: Act of War*, WALL ST. J. (May 31, 2011), http://bit.do/CyberCombatActOfWar.

[85] *Id.*

[86] Julian E. Barnes & Siobhan Gorman, *Cyberwar Plan Has New Focus On Deterrence*, WALL ST. J. (July 15, 2011), http://bit.do/CyberwarPlanFocusDeterrence.

networks."[87] 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."[88] During March 2014, the New York Times reports that "Chinese hackers broke into computers that stored the personal information of all United States government employees."[89] During May 2014, the U.S. Department of Justice charged five Chinese hackers, identified as "officers of Unit 61398 of the Third Department of the Chinese People's Liberation Army (PLA)" with cyber espionage directed at six American companies, including: Alcoa; Allegheny Technologies Inc.; U.S. Steel; Westinghouse Electric Co.; U.S. subsidiaries of SolarWorld AG; and others.[90] According to the DOJ,

> The indictment alleges that the defendants conspired to hack into American entities, to maintain unauthorized access to their computers and to steal information from those entities that would be useful to their competitors in China, including state-owned enterprises (SOEs). In some cases, it alleges, the conspirators stole trade secrets that would have been particularly beneficial to Chinese companies at the time they were stolen. In other cases, it alleges, the conspirators also stole sensitive, internal communications that would provide a competitor, or an adversary in litigation, with insight into the strategy and vulnerabilities of the American entity.
>
> "This is a case alleging economic espionage by members of the Chinese military and represents the first ever charges against a state actor for this type of hacking," U.S. Attorney General Eric Holder said. "The range of trade secrets and other sensitive business information stolen in this case is significant and demands an aggressive response. Success in the global market place should be based solely on a company's ability to innovate and compete, not on a sponsor government's ability to spy and steal business secrets. This Administration will not tolerate actions by any nation that seeks to illegally sabotage American companies and undermine the integrity of fair competition in the operation of the free market."
>
> "For too long, the Chinese government has blatantly sought to use cyber espionage to obtain economic advantage for its state-owned industries,"

[87] *Id.*

[88] Julian E. Barnes & Siobhan Gorman, *U.S. Readies Defense Against Cyberthreats,* WALL ST. J. (Oct. 12, 2012), http://bit.do/ReadiesDefense.

[89] Matt Apuzzo, *Chinese Businessman is Charged in Plot to Steal U.S. Military Data,* N.Y. TIMES (July 11, 2014), http://bit.do/ChineseChargedStealUSMilitaryData.

[90] Press Release, U.S. Dept. of Justice, *U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage: First Time Criminal Charges Are Filed Against Known State Actors for Hacking* (May 19, 2014), http://bit.do/USCharges5ChineseMilitaryHackers.

> said FBI Director James B. Comey.[91]

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."[92] 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.[93]

What if major transportation systems are disrupted, such as airlines traffic control systems? Cyberattacks 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 cyberattack on financial institutions? The SEC issued a recent study, *Observations on Developments in Risk Appetite Frameworks and IT Infrastructures,* which was conducted by senior financial supervisors from ten countries and concluded

> [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.[94]

Richard Clarke, former White House national security advisor to three U.S. presidents, writes "If we discovered Chinese explosives laid throughout our national electrical system, we'd consider it an act of

[91] *Id.*

[92] Mortimer Zuckerman, *How to Fight and Win the Cyberwar*, WALL ST. J. (Dec. 6, 2010), http://bit.do/FightAndWinCyberwar; *see also* Susan W. Brenner & Leo L. Clarke, *Civilians in Cyberwarfare: Conscripts* 43 VAND. J. TRANSNAT'L L. 1011 (2010); Susan W. Brenner & Leo L. Clarke, *Civilians in Cyberwarfare: Casualties,* 13 SMU SCI. & TECH. L. REV. 249 (2010).

[93] Zuckerman, *supra* note 92.

[94] SEC Release No. 2010-256, Senior Supervisors Group Issues Report on Risk Appetite Frameworks and IT Infrastructure (Dec. 23, 2010), http://bit.do/ReportOnRiskAppetite.

war. Digital bombs pose as grave a threat."[95] Just a few days prior to Richard Clarke's published article, Google 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."[96] Clarke further observes that

> 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 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.[97]

Clarke proposes an "International Cyber Risk Reduction Center," and notes that if "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."[98] 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

[95] Richard Clarke, *China's Cyberassault on America,* WALL ST. J. (June 15, 2011), http://bit.do/ChinasCyberassaultOnAmerica.

[96] Amir Efrati & Siobhan Gorman, *Google Mail Hack Is Blamed on China*, WALL ST. J. (June 2, 2011), http://bit.do/GMailHackBlamedChina; *see also* Siobhan Gorman, *China Tech Giant Under Fire,* WALL ST. J. (Oct. 8, 2012), http://bit.do/ChinaTechUnderFire; Spencer E. Ante, *Huawei's Ally: IBM,* WALL ST. J. (Oct. 10, 2012), http://bit.do/HuaweiAllyIBM.

[97] Richard Clarke*, Cyber Attacks Can Spark Real Wars*, WALL ST. J. (Feb. 16, 2012), http://bit.do/CyberAttacksSparkRealWars.

[98] *Id.*

happen in a few hours."[99] Scholars are exploring how computer warfare might "limit unnecessary suffering and reduce civilian casualties."[100]

D. Blueprint for a Secure Cyber Future

During November 2011, the U.S. Department of Homeland Security published its *Blueprint for a Secure Cyber Future: The Cybersecurity Strategy for the Homeland Security Enterprise*, which was "designed to protect the critical systems and assets that are vital to the United States, and, over time, to foster stronger, more resilient information and communication technologies to enable government, business and individuals to be safer online."[101] The *Blueprint* provides for two areas of action, "Protecting our Critical Information Infrastructure Today and Building a Stronger Cyber Ecosystem for Tomorrow."[102] In addition, four goals for protecting the critical information infrastructure are listed: "reduce exposure to cyberrisk; ensure priority response and recovery; maintain shared situational awareness; and increase resilience."[103] Homeland Security Secretary Janet Napolitano observed:

> Emerging cyber threats require the engagement of the entire society—from government and law enforcement to the private sector and most importantly, members of the public. Today in cyberspace, the Nation faces a myriad of threats from criminals, including individual hackers and organized criminal groups, as well as technologically advanced nation-states. Individuals and well-organized groups exploit technical vulnerabilities to steal American intellectual property, personal information, and financial data. The increasing number and sophistication of these incidents has the potential to impact our economic competitiveness and threaten the public's ability to access and obtain basic services. Government, non-governmental and private sector entities, as well as individuals, families, and communities must collaborate on ways to effectively reduce risk.[104]

[99] *Id.*; *see also* JAY P. KESAN & CAROL M. HAYES, THINKING THROUGH ACTIVE DEFENSE IN CYBERSPACE 327-42 (2010); Illinois Program in Law, Behavior and Social Science Paper No. LBSS10-02; Illinois Public Law Research Paper No. 10-11, http://bit.do/IllinoisPublicLawPaper; Jay P. Kesan & Carol M. Hayes*, Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace,* 25 HARV. J. L. & TECH. 429 (2012).

[100] Brian T.O'Donnell & James C. Kraska, *Humanitarian Law: Developing International Rules for the Digital Battlefield,* 8 J. CONFLICT & SEC. L. 133 (2003).

[101] Blueprint for a Secure Cyber Future: The Cybersecurity Strategy for the Homeland Security Enterprise, U.S. Department of Homeland Security (Nov. 2011), http://bit.do/BlueprintSecureCyberFuture.

[102] *Id.* at iii.

[103] *Id.*

[104] *Id.*

E. Failure of Cybersecurity Act of 2012

Despite consensus that cyberthreats represent a clear and present danger, Congress has not been particularly quick to act during the past decade. Senate Bill S.2105 (Cybersecurity Act of 2012), which failed to clear the Senate in August 2012, required private companies operating critical infrastructure to meet certain security requirements.[105] This proposed legislation required companies operating "power plants, oil pipelines and other vital services to meet certain security standards."[106] Other requirements included establishing a "mechanism for industry to more easily share information on threats with the government."[107] Senator Joseph Lieberman stated:

> 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.[108]

On August 8, 2012, John O. Brennan, at that time Assistant to the President for Homeland Security and Counterterrorism gave his "U.S. Policy toward Yemen" speech before the Council on Foreign

[105] S.2105, 112th Cong. (2012). *See* also Lawrence J. Trautman, Congressional Cybersecurity Oversight: Who's Who & How It Works, 5 J.L. & CYBER WARFARE 147 (2016).

[106] Siobhan Gorman, *Senators Push a Bill on Security*, WALL ST. J. (Feb. 15, 2012); http://bit.do/SenatorsPushSecurityBill; *see generally* Stephen Dycus, *Congress's Role in Cyber Warfare,* 4 J. NAT'L. SEC. L. & POL'Y 153 (2010).

[107] Gorman, *supra* note 106.

[108] *Securing America's Future: The Cybersecurity Act of 2012: Hearing Before the Comm. On Homeland Security and Governmental Affairs*, 112th Cong. (Feb. 16, 2012) (Opening Statement of Chairman Joseph Lieberman), http://bit.do/SecuringAmericasFuture; *but see* Susan W. Brenner, *Cyber-Threats and the Limits of Bureaucratic Control*, 14 MINN. J. L. SCI. & TECH. 137 (2011).

Relations. Following his prepared remarks, Mr. Brennan, now Director of the Central Intelligence Agency, remarked that the consequences of the failed cybersecurity 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 to our critical infrastructure in particular. We worked very hard to try to push forward and advance the cybersecurity provisions"[109] Mr. Brennan continued,

> [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 infiltrate 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, 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 . . . cyber capabilities . . . 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,

[109] Ritika Singh, *Transcript of John Brennan's Speech on Yemen and Drones*, LAWFARE (Aug. 8, 2012), http://bit.do/TrascriptBrennanYemenSpeech.

> 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.[110]

Reports of nation states mounting massive daily attacks against American computers are legion.[111] During mid-2012, the New York Times reported that "In March [2012] the White House invited all the members of the Senate to a classified simulation on Capital Hill demonstrating what might happen if a dedicated hacker—or an enemy

[110] *Id.; see also* Susan W. Brenner, *Organized Cybercrime? How Cyberspace May Affect the Structure of Criminal Relationships,* 4 N.C.J. L. & TECH. 1 (2002).

[111] *See generally* ROBERT AXELROD & RUMEN ILIEV, THE STRATEGIC TIMING OF CYBER EXPLOITS, APSA 2013 Annual Meeting Paper, Am. Pol. Sci. Assn. (2013), http://bit.do/StrategicTimingCyberExploits; Laurie R. Blank, *Cyberwar / Cyber Attack: The Role of Rhetoric in the Application of Law to Activities in Cyberspace*, *in* CYBERWAR: LAW & ETHICS FOR VIRTUAL CONFLICTS (Jens David Ohlin et al. eds., 2015), http://bit.do/RoleOfRhetoric; Paul Ducheine, Joop Voetelink, Jan F. Stinissen & Terry D. Gill, *Towards a Legal Framework for Military Cyber Operations*, *in* CYBER WARFARE: CRITICAL PERSPECTIVES 101-28 (Paul Ducheine et al. eds., 2012), http://bit.do/MilitaryCyberOperations; CYBER WARFARE: CRITICAL PERSPECTIVES 101-28 (Paul Ducheine et al. eds., 2012), Kristen Eichensehr, *The Cyber-Law of Nations,* 103 GEO. L.J. 317 (2015); Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Proctor, Aileen Elizabeth Nowlan, William Perdue & Julia Spiegel, *The Law of Cyber-Attack*, 100 CAL. L. REV. 817 (2012); Eric Talbot Jensen, *Cyber Warfare and Precautions Against the Effects of Attacks,* 88 TEX. L. REV. 1533 (2010); Jay P. Kesan & Carol M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace,* 25 HARV. J.L. & TECH. 429 (2012); AFRODITI PAPANASTASIOU, APPLICATION OF INTERNATIONAL LAW IN CYBER WARFARE OPERATIONS (2010), http://bit.do/CyberWarfareOperations; HAOTIAN QI, CYBER CAPITALISM WITH CHINESE CHARACTERISTICS? DOMESTIC SOURCES OF CHINA'S DIGITAL OFFENSIVE, APSA 2014 Annual Meeting Paper (2014); Nathan Alexander Sales, *Regulating Cyber-Security,* 107 NW. U.L. REV. 1503 (2013); Michael N. Schmitt, *The Law of Cyber Warfare: Quo Vadis?,* 25 STAN. L. & POL'Y REV. 269 (2014); Scott Shackelford & Amanda Craig, *Beyond The New "Digital Divide": Analyzing the Evolving Role of National Governments in Internet Governance and Enhancing Cybersecurity,* 50 STAN. J. INT'L L. 119 (2014); Christina Parajon Skinner, *An International Law Response to Economic Cyber Espionage,* 46 CONN. L. REV. 1165 (2014); T.P., *Chinese Cyber-Attacks, Hello, Unit 61398,* THE ECONOMIST (Feb. 19, 2013), http://bit.do/ChineseCyberAttacksHello; *Communist Chinese Cyber-Attacks, Cyber-Espionage and Theft of American Technology: Hearing Before the H. SubComm. On Oversight and Investigations of the Comm. on Foreign Affairs,* 112th Cong. 112-14 (2011); PETER SOMMER & IAN BROWN, REDUCING SYSTEMIC CYBERSECURITY RISK, Organisation for Economic Cooperation and Development Working Paper No. IFP/WKP/FGS(2011)3, http://bit.do/ReducingSystemicCybersecurityRisk; Paul Stockton & Michele Golabek-Goldman, *Curbing the Market for Cyber Weapons,* 32 YALE L. & POL'Y REV. 239 (2013); Peter Swire, *A Model for When Disclosure Helps Security: What is Different About Computer and Network Security?,* 3 J. TELECOMM. & HIGH TECH. L. 163 (2004); Remus Titiriga, *Cyber Attacks and International Law of Armed Conflicts: A 'Jus Ad Bellum' Perspective,* 8 J. INT'L COMM. L. & TECH. 179 (2013); Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE J. INT'L L. 421 (2011).

state—decided to turn off the lights in New York City.[112] 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":[113]

> 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.[114]

F. Executive Order 13636 and Critical Infrastructure

Following defeat of The Lieberman Cybersecurity Act during August 2012, The White House started circulating a draft cybersecurity Executive Order that "would establish a voluntary program where companies operating critical infrastructure would elect to meet cybersecurity best practices and standards crafted, in part, by the government."[115] On February 12, 2013, President Obama signed Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," which directs the Executive Branch to:

> 1. Develop a technology-neutral voluntary cybersecurity framework;
> 2. Promote and incentivize the adoption of cybersecurity practices;
> 3. Increase the volume, timeliness and quality of cyber threat information sharing;
> 4. Incorporate strong privacy and civil liberties protections into every initiative to secure our critical infrastructure; and

[112] David E. Sanger, *Mutually Assured Cyberdestruction?,* N.Y. TIMES (June 2, 2012), http://bit.do/MutuallyAssuredCyberdestruction.

[113] Ellen Nakashima, *Pentagon proposes more robust role for its cyber-specialists,* WASH. POST (Aug. 9, 2012), http://bit.do/PentagonRobustRoleCyberSpecialists.

[114] *Id.*

[115] Jennifer Martinez, *White House Circulating Draft of Executive Order on Cybersecurity*, THE HILL (Sept. 6, 2012), http://bit.do/WhiteHouseDraftCybersecurity. *See also* Siobhan Gorman, *Senator Presses on Cybersecurity,* WALL ST. J. (Sept. 19, 2012), http://bit.do/SenatorPressesCybersecurity.

> 5. Explore the use of existing regulation to promote cybersecurity.[116]

In addition, Presidential Policy Directive-21: Critical Infrastructure Security and Resilience replaces Homeland Security Presidential Directive-7, and directs the Executive Branch to:

> 1. Develop a situational awareness capability that addresses both physical and cyber aspects of how infrastructure is functioning in near-real time;
>
> 2. Understand the cascading consequences of infrastructure failures;
>
> 3. Evaluate and mature the public-private partnership;
>
> 4. Update the National Infrastructure Protection Plan; and
>
> 5. Develop comprehensive research and development plan.[117]

What exactly constitutes "critical infrastructure"? The 2013 Executive Order defines the term "critical infrastructure" as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[118] By way of historical prespective, by the mid-1990s, "the growing threat of international terrorism led policy makers to reconsider the definition of "infrastructure" in the context of homeland security."[119] As early as 1996, President Clinton recognized that:

> These critical infrastructures include telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire and rescue), and continuity of government. Threats to these critical infrastructures fall into two categories: physical threats to tangible property ("physical threats"), and threats of electronic, radio-frequency, or computer-based attacks on the information or communications components that control critical infrastructures ("cyber threats").[120]

[116] *Fact Sheet on Executive Order (EO) 13636: Improving Critical Infrastructure Cybersecurity and Presidential Policy Directive (PPD)-21 Critical Infrastructure Security and Resilience*, U.S. DEP'T OF HOMELAND SEC. (Mar. 2013), http://bit.do/ImprovingCriticalInfrastructure. *See generally* Exec. Order No. 13636, 78 Fed. Reg. 11737 (Feb. 19, 2013), http://bit.do/ImprovingCriticalInfrastructureCybersecurity.

[117] *Id.*

[118] Exec. Order No. 13636, *supra* note 116, at § 2.

[119] JOHN MOTEFF & PAUL PARFOMAK, CONG. RESEARCH SERV., RL32631, CRITICAL INFRASTRUCTURE AND KEY ASSETS: DEFINITION AND IDENTIFICATION (2004).

[120] Exec. Order No. 13010, 61 Fed. Reg. 37345 (July 15, 1996).

In 2001, Executive Order 13228[121] created the Office of Homeland Security and required the protection of:

- Energy production, transmission, and distribution services and critical facilities
- Other utilities
- Telecommunications
- Facilities that produce, use, store, or dispose of nuclear material
- Public and privately owned information systems
- Special events of national significance
- Transportation, including railways, highways, shipping ports and waterways
- Airports and civilian aircraft
- Livestock, agriculture, and systems for the provision of water and food for human use and consumption.[122]

President Bush's Critical Infrastructure Protection Board was created by Executive Order 13231.[123] A definition of "critical infrastructure was contained in The USA PATRIOT Act of 2001 (P.L. 107-56),[124] and the Bush administration's strategy for homeland security is articulated in *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets.*[125]

G. Treasury Report on Cybersecurity Incentives

The 2013 Executive Order also directs "the Secretary of the Treasury, along with the Secretary of Commerce and the Secretary of Homeland Security to each make recommendations on a set of incentives that would promote private sector participation in the voluntary program."[126] This Treasury Report provides policymakers

[121] Exec. Order No. 13228, 66 Fed. Reg. 51812 (Oct. 10, 2001).

[122] *See id.* Section 3(e)(i)-(vi).

[123] *See* Exec. Order No. 13231, 86 Fed. Reg. 53061 (Oct. 18, 2001).

[124] *See* MOTEFF & PARFOMAK, *supra* note 119 at CRS-7.

[125] *See* Office of the President, *The National Strategy for Physical Protection of Critical Infrastructure and Key Assets* (Feb. 2003).

[126] U.S. DEP'T OF THE TREASURY, TREASURY DEPARTMENT REPORT TO THE PRESIDENT ON CYBERSECURITY INCENTIVES PURSUANT TO EXECUTIVE ORDER 13636, at 2-3, n.4 (2013) (citing Exec. Order 13636, *supra* note 116, at Sec. 8(d)) ("The Secretary of [Homeland Security] shall coordinate establishment of a set of incentives designed to promote participation in the [voluntary cybersecurity] Program. Within 120 days of the date of this order, the Secretary and

with outlines to assess and "evaluate the benefits and relative effectiveness of government incentives in promoting the adoption of the eventual Framework. It seeks to identify types of situations in which private incentives may be insufficient to provide an appropriate level of cybersecurity."[127] In discussing a general approach to principles for government incentives, the Treasury Report observed:

> Generally, government policy tools to provide incentives to private sector participants should be considered when private incentives are insufficient to provide a desirable level of additional investment in an area, such as increasing cybersecurity. Economists refer to this condition as market failure . . . .
>
> When a market failure exists and private market solutions are inadequate, government support in the form of incentives may be appropriate. If a government role is warranted, the potential incentive should ideally: (i) be appropriately tailored and scaled to the magnitude of the under-investment in cybersecurity; (ii) protect taxpayers by being cost-effective while still achieving the policy objectives; (iii) adjust to changing circumstances and the availability of new information; (iv) be coordinated, so as not to duplicate, other incentives; and (v) motivate private sector entities to expend their own resources to further protect their critical infrastructure assets. These principles should be crucial factors in ant decision about whether the government should provide incentives; however, they should not be viewed as requirements.[128]

The Treasury Report further identifies and discusses the following cybersecurity market failures: underinvestment in knowledge; barriers to information sharing; coordination failures; network externalities; and adverse selection of insurance risks.[129] Next, the Treasury Report turns to a discussion and evaluation of potential government incentives, including: enhancing information usage capabilities to support information sharing; leveraging framework adoption to clarify liability risk; government funding to encourage basic cybersecurity research; providing technical assistance; further accelerating the security clearance process; potential tax incentives; and cyber insurance.[130]

Secretaries of the Treasury and Commerce each shall make recommendations separately to the President, through the Assistant to the President for Homeland Security and Counterterrorism and the Assistant to the President for Economic Affairs, that shall include analysis of the benefits and relative effectiveness of such incentives, and whether the incentives would require legislation or can be provided under existing law or authorities to participants in the Program.").

[127] *Id.* at 3.

[128] *Id.* at 3-4.

[129] *Id.* at 5-6.

[130] *Id.* at 8-25. *See generally* Eric Talbot Jensen, *Cyber Warfare and Precautions Against the Effects of Attacks,* 88 TEX. L. REV. 1533 (2010).

H. Framework on Improving Critical Infrastructure Cybersecurity

Executive Order 13636 mandates "development of a voluntary risk-based Cybersecurity Framework—a set of industry standards and best practices to help organizations manage cybersecurity risks. The resulting Framework, created through collaboration between government and the private sector, uses a common language to address and manage cybersecurity risk."[131] Sensitive to imposing additional regulatory requirements on business, the Framework attempts to focus on business needs in a cost-effective way.[132] As a threshold observation, "The Framework complements, and does not replace, an organization's risk management process and cybersecurity program. An organization can use its current processes and leverage the Framework to identify opportunities to strengthen and communicate its management of cybersecurity risk while aligning with industry practices."[133] Important to many, "an organization without an existing cybersecurity program can use the Framework as a reference to establish one."[134]

1. Each Enterprise's Need Is Unique

The Framework recognizes that risk management of cybersecurity requires "a clear understanding of the organization's business drivers and security considerations specific to its use of [information technology] and [industrial control systems] is required. Because each organization's risk is unique . . . the tools and methods used to achieve the outcomes described by the Framework will vary."[135] Accordingly:

> The Framework focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risk as part of the organization's risk management process. The Framework consists of three parts: the Framework Core, the Framework Profile, and the Framework Implementation Tiers. The Framework Core is a set of cybersecurity activities, outcomes, and informative references that are common across

[131] U.S. NAT'L INST. OF STANDARDS AND TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY, Ver. 1.0, at 5 (Feb. 12, 2014), http://bit.do/FrameworkCriticalInfrastructure. *See also* Scott Shackelford, Andrew A. Proia, Brenton Martell & Amanda Craig, *Toward a Global Cybersecurity Standard of Care?: Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices,* 50 TEX. INT'L L.J. 305 (2015).

[132] *Id.*

[133] *Id.* at 4.

[134] *Id.*

[135] *Id.* at 3.

> critical infrastructure sectors, providing the detailed guidance for developing individual organizational Profiles. Through use of the Profiles, the Framework will help the organization align its cybersecurity activities with its business requirements, risk tolerances, and resources. The Tiers provide a mechanism for organizations to view and understand the characteristics of their approach to managing cybersecurity risk . . . .
>
> The Framework enables organizations—regardless of size, degree of cybersecurity risk, or cybersecurity sophistication—to apply the principles and best practices of risk management to improving the security and resilience of critical infrastructure. The Framework provides organization and structure to today's multiple approaches to cybersecurity by assembling standards, guidelines, and practices that are working effectively in industry today . . . .[136]

2. The Framework Is Organic

Designed as "a model for international cooperation on strengthening critical infrastructure cybersecurity," the Framework "references globally recognized standards for cybersecurity."[137] Accordingly, the Framework is intended to be:

> [A] living document and will continue to be updated and improved as industry provides feedback on implementation. As the Framework is put into practice, lessons learned will be integrated into future versions. This will ensure it is meeting the needs of critical infrastructure owners and operators in a dynamic and challenging environment of new threats, risks, and solutions.
>
> Use of this voluntary framework is the next step to improve the cybersecurity of our Nation's critical infrastructure ̶providing guidance for individual organizations, while increasing the cybersecurity posture of the Nation's critical infrastructure as a whole.[138]

The Framework is designed to "be used with a broad array of cybersecurity risk management processes. Examples of cybersecurity risk management processes include International Organization for Standardization (ISO) 31000:2009,[139] ISO/IEC 27005:2011,[140] National Institute of Standards and Technology (NIST) Special

[136] *Id.* at 1.

[137] U.S. NAT'L INST. OF STANDARDS AND TECH., *supra* note 131, at 1-2.

[138] *Id.* at 2.

[139] *Id.* at 6 (citing International Organization for Standardization, *Risk management – Principles and guidelines* n.3-5*,* ISO 31000:2009 (2009), http://bit.do/ISO31000 Riskmanagement.

[140] International Organization for Standardization/International Electrotechnical Commission, *Information technology—Security techniques—Information security risk management,* ISO/IEC 27005:2011 (2011), http://bit.do/InformationTechnologySecurity Techniques.

Publication (SP) 800-39,[141] and the *Electricity Subsector Cybersecurity Risk Management Process* (RMP) guideline.[142] All charged with the responsibility for cybersecurity governance should obtain and become familiar with The Framework. This is a roadmap for having a dialogue about cybersecurity in any organization.

I. Quadrennial Homeland Security Review ("2014 Review")

The Review of the Department of Homeland Security's mission areas and risk-informed priorities stated that "the terrorist threat in increasingly decentralized and may be harder to detect. Cyber threats are growing and pose ever-greater concern to our critical infrastructure systems as they become increasingly interdependent."[143] In addition, the 2014 Review observed:

> We must, over the next four years, continue efforts to address the growing cyber threat, illustrated by the real, pervasive, and ongoing series of attacks on our public and private infrastructure. This infrastructure provides essential services such as energy, telecommunications, water, transportation, and financial services and is increasingly subject to sophisticated cyber intrusions which pose new risks. As the Federal Government's coordinator of efforts to counter cyber threats and other hazards to critical infrastructure, DHS must work with both public and private sector partners to share information, help make sure new infrastructure is designed and built to be more secure and resilient, and continue advocating internationally for openness and security of the internet and harmony across international laws to combat cybercrime. Further, DHS must secure the Federal Government's information technology systems by approaching federal systems and networks as an integrated whole and by researching, developing, and rapidly deploying cybersecurity solutions and services at the pace that cyber threats evolve. And finally, we must continue to develop cyber law enforcement, incident response, and reporting capabilities by increasing the number and inpact of cybercrime investigations, sharing information about tactics and methods of cyber criminals gleaned through investigations, and ensuring that incidents reported to any federal department or agency are shared across the U.S. government. In addition, the Federal Government must continue to develop good working relationships with the private sector, lower barriers to partnership, develop cybersecurity best practices, promote advanced technology that can exchange information at machine speed, and build the

[141] Joint Task Force Transformation Initiative, *Managing Information Security Risk: Organization, Mission, and Information System View,* NIST Special Publication 800-39 (March 2011), http://bit.do/ManagingInfoSecurityRisk.

[142] U.S. DEP'T OF ENERGY, *Electricity Subsector Cybersecurity Risk Management Process,* DOE/OE-0003 (May 2012), http://bit.do/ElectricitySubsectorCybersecurityRisk.

[143] U.S. DEP'T OF HOMELAND SECURITY, 2014 Quadrennial Homeland Security Review, at 5 (2014), http://bit.do/QuadrennialHomelandSecurityReview.

> cyber workforce of tomorrow for DHS and the Nation.[144]

The 2014 Review provides a description of the strategic environment, guiding principles, strategic priorities such as securing against the evolving threat of terrorism, biological hazards and threats, potential nuclear terrorism, immigration challenges, and associated issues.[145] The 2014 Review also noted that:

> Transnational criminal organizations rely on revenues generated through the sale of illegal drugs and counterfeit goods, human trafficking and smuggling, and other criminal activities. These organizations continue to expand in size, scope, and influence and are capitalizing on technological innovation, including new platforms to sell illicit goods, innovative ways of moving money, tools for coordinating operations, and a variety of other criminal and cyber activities…
>
> As transnational criminal organizations grow stronger and challenge or corrupt governments in many regions, they are moving more freely, expanding their networks, and acquiring and distributing military-grade equipment. Violent extremist networks can also conduct these profitable criminal activities on their own, exploiting the same vulnerabilities in finance, trade and travel, and immigration.[146]

The 2014 Review notes that "Cyberspace and its underlying infrastructure are vulnerable to a wide range of risk stemming from both physical and cyber threats and hazards. Sophisticated cyber actors and nation states exploit vulnerabilities to steal information and money and are developing capabilities to disrupt, destroy, or threaten the delivery of essential services."[147] Cyberspace has brought technological advantage to traditional crimes, including "the production and distribution of child pornography and child exploitation conspiracies, banking and financial fraud, intellectual property violations, and other crimes, all of which have substantial human and economic consequences."[148] The DHS has articulated its mission as "Mission 4: Safeguard and Secure Cyberspace" and is included here as Exhibit Two.

[144] *Id.* at 7-8.

[145] *See generally id.*

[146] *Id.* at 26. *See generally* Lawrence J. Trautman, *Virtual Currencies: Bitcoin & What Now After Liberty Reserve, Silk Road, and Mt. Gox?*, 20 RICH. J.L. & TECH. 13 (2014); Lawrence J. Trautman & George P. Michaely, *The SEC & The Internet: Regulating the Web of Deceit,* 68 CONSUMER FIN. L.Q. REP. 262 (2014); Lawrence J. Trautman & Alvin Harrell, *Bitcoin vs. Regulated Payment Systems: What Gives?*, 38 CARDOZO L. REV. (forthcoming 2017); Lawrence J. Trautman, *Following the Money: Lessons from the Panama Papers, Part 1: Tip of the Iceberg,* __ PENN ST. L. REV. __ (forthcoming), http://bit.do/FollowingTheMoney.

[147] *See* U.S. DEP'T OF HOMELAND SECURITY, *supra* note 143, at 39.

[148] *Id.*

Exhibit Two:
DHS Mission 4: Safeguard & Secure Cyberspace

Goal 4.1: Strengthen the Security and Resilience of Critical Infrastructure

Enhance the exchange of information and intelligence on risks to critical infrastructure and develop real-time situational awareness capabilities that ensure machine and human interpretation and visualization;

Partner with critical infrastructure owners and operators to ensure the delivery of essential services and functions;

Identify and understand interdependencies and cascading impacts among critical infrastructure systems;

Collaborate with agencies and the private sector to identify and develop effective cybersecurity policies and best practices; and

Reduce vulnerabilities and promote resilient critical infrastructure design.

Goal 4.2: Secure the Federal Civilian Government Information Technology Enterprise

Coordinate government purchasing of cyber technology to enhance cost-effectiveness

Equip civilian government networks with innovative cybersecurity tools and protections; and

Ensure government-wide policies and standards are consistently and effectively implemented and measured.

Goal 4.3: Advance Law Enforcement, Incident Response, and Reporting Capabilities

Respond to and assist in the recovery from cyber incidents; and

Deter, disrupt, and investigate cybercrime.

Goal 4.4: Strengthen the Ecosystem

Drive innovative and cost effective security products, services, and solutions throughout the cyber ecosystem;

Conduct and transition research and development, enabling trustworthy cyber infrastructure;

Develop skilled cybersecurity professionals; enhance public awareness and promote cybersecurity best practices; and

Advance international engagement to promote capacity building, international standards, and cooperation.[149]

J. Congressional Cybersecurity Action

During December 2014, just hours before the holiday recess, the U.S. Congress passed several major legislative proposals designed to enhance U.S. cybersecurity: The National Cybersecurity Protection Act of 2014;[150] The Federal Information Security Modernization Act of 2014;[151] The Cybersecurity Workforce Assessment Act;[152] The Homeland Security Workforce Assessment Act;[153] and the Cybersecurity Enhancement Act of 2014.[154] Following signature by the President, these became the first cybersecurity laws to be enacted in over a decade, since passage of the Federal Information Security Management Act of 2002.[155]

IV. CORPORATE RESPONSIBILITY FOR RISK GOVERNANCE

The following regulatory developments deserve the attention of top management and those responsible for cybersecurity governance of any enterprise. Accordingly, attention is given to a discussion of recent comments by the SEC on risk, Dodd-Frank legislation, and SEC disclosure guidelines.

A. The SEC on Risk & Dodd-Frank Wall Street Reform

Effective February 28, 2010, SEC rules amended Regulation S-K (Item 407) to require disclosure about the board's role in a company's risk oversight process and its leadership structure.[156] The SEC noted:

[149] *Id.* at 78.

[150] National Cybersecurity Protection Act of 2014, Pub. L. No. 113-282, 128 Stat. 3066 (2014).

[151] Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 128 Stat. 3073 (2014).

[152] Cybersecurity Workforce Assessment Act, Pub. L. No. 113-246, 128 Stat. 2880 (2014).

[153] Border Patrol Agent Pay Reform Act of 2014, Pub. L. No. 113-277, 128 Stat. 2995 (2014).

[154] Cybersecurity Enhancement Act of 2014, Pub. L. No. 113-274, 128 Stat. 2971 (2014).

[155] *See generally* Mitchell S. Kominsky, *supra* note 7 (citing ERIC A. FISCHER, CONG. RESEARCH SERV., RL42114, FEDERAL LAWS RELATING TO CYBERSECURITY: OVERVIEW AND DISCUSSION OF PROPOSED REVISIONS (2014)). *See also* Lawrence J. Trautman, *Cybersecurity: What About U.S. Policy?*, 2015 J.L. TECH. & PUB. POLY 341 (2015).

[156] 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

> 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."[157] 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."[158] 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."[159] 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."[160]

Large financial institutions are required by the Dodd-Frank Act to establish independent risk committees on their boards,[161] with at least one member of the committee required to have risk management experience at a large, complex firm.[162] Highly disruptive developments such as Bitcoin's blockchain technology continue to confront financial service providers with substantial risk management issues.[163] This comes at a time when many of the world's largest financial institutions are still engaged in recovering and rebuilding capital after the global financial collapse of 2007-2008.[164]

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."

[157] Proxy Disclosure Enhancements, Securities Act Release No. 9089, Exchange Act Release No. 61,175, Investment Company Act Release No. 29,092, at 44 (Dec. 16, 2009).

[158] *Id.*

[159] *Id.* at 43.

[160] *Id.*

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

[162] *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).

[163] *See generally* Lawrence J. Trautman, *Is Disruptive Blockchain Technology the Future of Financial Services?*, 69 THE CONSUMER FIN. L.Q. REP. 232 (2016) ; Lawrence J. Trautman & Kara Altenbaumer-Price, The Importance of Insurance in Managing Corporate Cyberthreat Risk, (unpublished paper).

[164] *See generally* Lawrence J. Trautman, *Personal Ethics & the U.S. Financial Collapse of 2007-08*, (forthcoming), http://bit.do/PersonalEthics.

Creation of a risk committee is one pro-active approach to the increased emphasis on risk oversight and the possibility of risk committees being mandated for some or all public companies.[165] As observed elsewhere, "While having a stand-alone risk committee can serve to relieve strained audit committees, it is important that 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."[166]

B. SEC Disclosure Guidelines

The proliferation of cyberattacks during 2010 and 2011 resulted in the SEC's Division of Corporation Finance announcing disclosure guidance for cybersecurity issues on October 13, 2011.[167] The Division of Corporation Finance stated: "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."[168] 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."[169] Accordingly, the Division "determined that it would be beneficial to provide guidance that assists registrants in assessing what, if any, disclosures should be provided about cybersecurity matters in light of each registrant's specific facts and circumstances."[170] 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

[165] 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 (Apr. 12, 2016), http://bit.do/RiskCommitteeCharter.

[166] Trautman & Altenbaumer-Price, *supra* note 1, at 320.

[167] *CF Disclosure Guidance: Topic No. 2 Cybersecurity*, SEC DIV. OF CORP. FIN. (Oct. 13, 2011), http://bit.do/SECCFDisclosure.

[168] *Id.*

[169] *Id.*

[170] *Id.*

> 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
> - Reputational damage adversely affecting customer or investor confidence

The Division further stated that

> 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 . . . .[171]

V. BOARD COMPOSITION: THE CASE FOR CYBERSECURITY EXPERTISE

A. *Each Board Has Different Levels of IT and Cybersecurity Skills*

Optimal corporate board composition is different for companies engaged in different industries and at different stages of their lifecycle.[172] The board of a young software or consulting company may be inundated with information technology (IT) understanding, expertise and talent; while the board of an oil and gas or fast food company may have little understanding of IT issues. IT domain issues must be adequately represented among corporate board members, particularly for companies having significant cybersecurity 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 cybersecurity and information technology. Accordingly, "some boards provide directors with IT education sessions outside the boardroom, similar to strategy retreats, which may be held on the day before or after a full board meeting."[173] 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."[174]

B. *Organizational IT and Cybersecurity 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

[171] *Id.*

[172] *See generally* Trautman, *supra* note 8, at 88.

[173] Deloitte Report, *The Tech-Intelligent Board: Priorities for Tech-Savvy Directors as they oversee IT Risk and Strategy,* at 9 (2011), http://bit.do/Tech-IntelligentBoard.

[174] *Id.*

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."[175] 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."[176]

C. 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, or risk assessment can be addressed.[177] 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."[178] 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.

[175] *Id.*

[176] *Id.*

[177] *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. 205 (2013).

[178] PricewaterhouseCoopers, *Fortifying Your Defenses: The Role of Internal Audit in Assuring Data Security and Privacy,* 8 (2012), http://bit.do/InternalAuditDataSecurity.

> 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.[179]

D. 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 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: Management; Risk Management and Compliance Functions; and Internal Audit.[180] 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.[181]

VI. YOUR CYBERSECURITY CRISIS MANAGEMENT PLAN

Every enterprise should have a cybersecurity 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."[182] In addition,

> 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

[179] *Id.*

[180] *Id.* at 6.

[181] *Id.* at 9.

[182] Pinguelo & Muller, *supra* note 80, at 82.

> 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.[183]

Every enterprise can implement the following elements of a crisis management plan *before* a crisis takes place. Of particular importance, identifying and having a relationship with the professionals needed to assist in stressful times is always best handled when sufficient time is available to make reasoned decisions. A cyber disaster requires making decisions about:

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.[184]

Hyundai Capital Services Inc., South Korea's largest consumer-finance company, sustained a computer system hack and blackmail attempt from two groups of hackers.[185] Mr. Chung, Hundai Capital's chief executive, believed:

> 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

[183] *Id.*

[184] *See* Lawrence J. Trautman, Jason Triche & James C. Wetherbe, *Corporate Information Technology Governance Under Fire,* 8 J. STRAT. & INT'L STUD. 110 (2013).

[185] Evan Ramstad, *Executive Learns from Hack: CEO Now Treats IT Department as Critical to Hyundai Capital's Operations,* WALL ST. J. (June 21, 2011), http://bit.do/ExecLearnsFromHack.

> 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.[186]

VII. A CALL TO ACTION: WHAT YOU CAN DO, NOW!

We now turn our attention to specific recommendations about what every organization can do to increase their cybersecurity defenses. Professor Frederick Chang paraphrases 19th century engineer and mathematical physicist Lord Kelvin to say that "you can't manage what you don't measure."[187] While important cybersecurity defense work

> [i]s taking place, we need improvements in hard, objective metrics and measures of security. Metrics are needed at many very practical levels. At a very tactical level, how do you know if computer system A is more or less secure than computer system B? Is computer system A more or less secure than it was last month? Last year? At a corporate level, how do you measure the security of your corporate information technology infrastructure? Is it more secure now than it was last year? Do the measures allow a pinpoint assessment of where corporate improvements are necessary? At a much more macro level, what metrics are best used to determine if the industry as a whole is making progress toward improving its cybersecurity posture? How would you measure the effect of an important government policy change in cybersecurity? Is it making the difference that was intended? It is relatively straightforward to determine the effects of changing the speed limit on [traffic] accidents. It won't be so clear for cybersecurity. Developing a disciplined, agreed-upon, and readily implementable set of metrics for cybersecurity remains a hard problem. Perhaps we can look for some assistance from other fields − medical research has successfully employed metrics to improve the science of human health. Measures of human health and cyber health share an important common ingredient: in both cases we are attempting to measure the absence of something bad (human disease or system compromise).[188]

Lessons to be learned from those on the front lines of cybersecurity defense include: leadership commitment at the top; focus on basic cyber hygiene; the SANS Institute Critical Security Controls; the OWASP Top Ten list; CWE/SANS Top 25 most dangerous software errors list; the DHS National Cybersecurity and Communications Integration Center (NCCIC) and U.S. Computer Emergency Readiness Team (US-CERT); thoughts about the role and

[186] *Id.*

[187] *See* Chang testimony, *supra* note 14.

[188] *Id.*

value of a chief Information Officer; and the U.S. Department of the Treasury's list of ten ways to improve cybersecurity.

A. Leadership Commitment at the Top

Like any other challenge requiring enterprise resources of significant time and money, to be successful, governance of IT and cybersecurity issues require commitment at the very top. Deloitte states 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 comfortable in addressing issues related to IT."[189] In many 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."[190] 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[191]

B. Basic Cyber Hygiene

Perhaps the most significant step that can be taken to prevent cyber intrusion in your organization is to require frequent changes to passwords. It is the weakest link in technology systems that often define security issues:

> Hackers need just one way in. As technical security measures improve (e.g.

[189] Deloitte, *supra* note 173, at 9.

[190] *Id.*

[191] Trautman & Altenbaumer-Price, *supra* note 1, at 326 (citing USI Insurance Services, *Cyber Liability / Security and Privacy Insurance* (2009) (on file with the author)).

> greater use of encryption), then people increasingly become the weakest link. Hackers often employ a tactic known as 'social engineering' to trick computer operators to divulge sensitive information that can be used to compromise a system (e.g. a password). These tactics can be extremely effective and much easier to accomplish than a technical compromise. Indeed the well-known hacker Kevin Mitnick reported in testimony to Congress that he was so successful in social engineering that he rarely had to resort to a technical attack. More generally, there are a well-known set of cognitive biases that people use to assess risk and make decisions. These biases often cloud our reasoning and cause us to improperly assess risk, in many domains, including in cyberspace. We must take steps to strengthen the weakest link. Gaining a much richer understanding of the cognitive biases at work in the context of decision-making in cyberspace would be just one of many important issues that need research at the intersection of psychology and cybersecurity.[192]

C. SANS Institute Critical Security Controls

Over the years the National Security Agency (NSA) became increasingly concerned that, in everyday practice, efforts to govern data systems and prevent breaches, had all too often become "exercises in reporting on compliance and have actually diverted security program resources from the constantly evolving attacks that must be addressed."[193] Accordingly, during 2008 NSA started "prioritizing a list of the controls that would have the greatest impact in improving risk posture against real-world threats. A consortium of U.S. and international agencies quickly grew, and was joined by experts from private industry and around the globe."[194] This list ultimately became known as the Critical Security Controls and was coordinated through the SANS Institute. The Council on CyberSecurity, a global, independent, non-profit entity committed to a secure and open Internet assumed responsibility during 2013. SANS noted that:

> The Critical Security Controls focuses first on prioritizing security functions that are effective against the latest Advanced Targeted Threats, with a strong emphasis on "What Works" - security controls where products, processes, architectures and services are in use that have demonstrated real world effectiveness. Standardization and automation is another top priority, to gain operational efficiencies while also improving effectiveness. The actions defined by the Controls are demonstrably a subset of the comprehensive catalog defined by the National Institute of Standards and Technology (NIST) SP 800-53. The Controls do not attempt to replace the work of NIST, including the Cybersecurity Framework developed in response to Executive Order 13636. The Controls instead

[192] Chang testimony, *supra* note 14.

[193] *The CIS Critical Security Controls for Effective Cyber Defense*, SANS INSTITUTE, http://bit.do/CriticalSecurityControls.

[194] *Id.*

> prioritize and focus on a smaller number of actionable controls with high-payoff, aiming for a "must do first" philosophy. Since the Controls were derived from the most common attack patterns and were vetted across a very broad community of government and industry, with very strong consensus on the resulting set of controls, they serve as the basis for immediate high-value action.[195]

Exhibit Three is "Critical Security Controls: Version 5." More information and a description regarding each of these component part items may be found at the SANS Institute website.[196]

Exhibit Three:
SANS Critical Security Controls: Version 5

1: Inventory of Authorized and Unauthorized Devices

2: Inventory of Authorized and Unauthorized Software

3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

4: Continuous Vulnerability Assessment and Remediation

5: Malware Defenses

6: Application Software Security

7: Wireless Access Control

8: Data Recovery Capability

9: Security Skills Assessment and Appropriate Training to Fill Gaps

10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches

11: Limitation and Control of Network Ports, Protocols, and Services

12: Controlled Use of Administrative Privileges

13: Boundary Defense

14: Maintenance, Monitoring, and Analysis of Audit Logs

15: Controlled Access Based on the Need to Know

16: Account Monitoring and Control

17: Data Protection

18: Incident Response and Management

[195] *Id.*

[196] *Id.*

19: Secure Network Engineering

20: Penetration Tests and Red Team Exercises

D. OWASP Top Ten

The Open Web Application Project (OWASP) is a world-wide not-for-profit organization having a stated mission of making "software security visible so that individuals and organizations worldwide can make informed decisions about true software security risks."[197] The OWASP website reports: eighty-seven chapters in the United States; twelve in Canada; thirty-nine in Latin America; sixty in Europe; sixty-one in Asia/Pacific/Middle East; sixteen in Africa; and eight student chapters.[198] The OWASP top ten has been translated into many different languages and represents a broad consensus of OWASP members about location of the most critical web application security flaws and is depicted in Exhibit Four below.[199]

Exhibit Four:
Open Web Application Project (OWASP) Top 10 List, 2013

A1 Injection

A2 Broken Authentication and Session Management

A3 Cross-Site Scripting (XSS)

A4 Insecure Direct Object References

A5 Security Misconfiguration

A6 Sensitive Data Exposure

A7 Missing Function Level Access Control

A8 Cross-Site Request Forgery (CSRF)

A9 Using Components with Known Vulnerabilities

A10 Unvalidated Redirects and Forwards

Source: OWASP Top 10 – 2013

OWASP urges all organizations to "adopt this awareness document within their organization and start the process of ensuring that their web applications do not contain these flaws. Adopting the

[197] *See generally* The Open Web Application Project, *Welcome to OWASP*, http://bit.do/OpenWebAppProject.

[198] The Open Web Application Project, *OWASP Chapter*, http://bit.do/OWASPChapter.

[199] The Open Web Application Project, *Category: OWASP Top Ten Project*, http://bit.do/OWASPTopTen.

OWASP Top Ten is perhaps the most effective first step towards changing the software development culture within your organization into one that produces secure code."[200] Also available at the OWASP website are a number of other valuable tools, including: OWASP Mobile Top 10 Risks; OWASO Top 10 Cheat Sheet; Top 10 Proactive Controls; and OWASP Top 10 Mapped to the Web Hacking Incident Database.[201]

E. CWE/SANS Top 25 Most Dangerous Software Errors

Another source of useful threat assessment tools is The Common Weakness Scoring System (CWSS).[202] The CWSS "provides a mechanism for prioritizing software weaknesses in a consistent, flexible, open manner. It is a collaborative, community-based effort that is addressing the needs of its stakeholders across government, academia, and industry."[203] Often software developers "face hundreds or thousands of individual bug reports for weaknesses that are discovered in their code. In certain circumstances, a software weakness can even lead to an exploitable vulnerability."[204] The CWSS reports that:

> Due to this high volume of reported weakness, stakeholders are often forced to prioritize which issues they should investigate and fix first, often using incomplete information. In short, people need to be able to reason and communicate about the relative importance of different weaknesses. While various scoring methods are used today, they are either ad hoc or inappropriate for application to the still-imprecise evaluation of software security.
>
> Software developers, managers, testers, security vendors and service suppliers, buyers, application vendors, and researchers must identify and assess weaknesses in software that could manifest as vulnerabilities when the software is used. They then need to be able to prioritize these weaknesses and determine which to remediate based on which of them pose the greatest risk. When there are so many weaknesses to fix, with each being scored using different scales, and often operating with incomplete information, the various community members, managers, testers, buyers, and developers are left to their own methodologies to find some way of comparing disparate weaknesses and translating them into actionable

[200] *Id.*

[201] *Id.*

[202] *Common Weakness Scoring System,* MITRE CORP., http://bit.do/CommonWeaknessScoring.

[203] *Id.*

[204] *Id.*

information.[205]

The CWSS offers quantitative measurements, a common framework for prioritizing software application security weaknesses, and the ability to customize priorities.[206] Further, the CWSS "is organized into three metric groups, with each group offering multiple metrics: the base finding; attack surface; and environmental metric groups.[207] An attempt was made in the 2010 SANS/CWE Top 25 Most Dangerous Errors list "to perform quantitative prioritization of CWE entries using a combination of Prevalence and Importance, which became the basis of CWSS 0.1 later in the year."[208] Forty-one candidate weaknesses were rated by survey and used to generate a "Top 25" list. In addition:

> The 2010 Top 25 was structured in a way to support multiple points of view that could reflect different prioritizations of the weaknesses. The creation of separate focus profiles stemmed from some critiques of the original 2009 Top 25, in which a generalized Top 25 list would not necessarily be useful to all audiences, and that a customized prioritization would be ideal. Eight focus profiles were provided with the 2010 Top 25. For example, the Educational Emphasis focus profile evaluated weaknesses that are regarded as important from an educational perspective within a school or university context. It emphasized the CWE entries that graduating students should know, including weaknesses that were historically important or increased the breadth of coverage. A separate focus profile ranked weaknesses based solely on their evaluated Importance, which would be useful to software customers who want the most serious issues removed, without consideration for how frequently they occur or how resource-intensive it is to fix. These ranking-oriented focus profiles made the Top 25 more useful to certain audiences, and their construction and management have served as a useful predecessor to CWSS and vignettes.[209]

F. U.S. Computer Emergency Readiness Team (US-CERT)

The U.S. Computer Emergency Readiness Team (US-CERT) is the 24-hour operational arm of the DHS National Cybersecurity and Communications Integration Center (NCCIC). CERT is designed to lead "efforts to improve the nation's cybersecurity posture, coordinate cyber information sharing, and proactively manage cyber risks to the Nation while protecting the constitutional rights of Americans. US-CERT strives to be a trusted global leader in cybersecurity—

[205] *Id.*

[206] *Id.* at 2.

[207] *Id.*

[208] *Common Weakness Scoring System, supra* note 202, at 39.

[209] *Id.*at 40.

collaborative, agile, and responsive in a dynamic and complex environment."[210] CERT describes its mission as follows:

> Through its 24x7 operations center, US-CERT accepts, triages, and collaboratively responds to incidents; provides technical assistance to information system operators; and disseminates timely notifications regarding current and potential security threats and vulnerabilities… US-CERT leverages the Protected Critical Infrastructure Information (PCII) Program to prevent inappropriate disclosure of proprietary information or other sensitive data. Established in response to the Critical Infrastructure Information Act of 2002 (CII Act), the PCII Program enables members of the private sector to voluntarily submit confidential information regarding the nation's critical infrastructure to DHS with the assurance that the information will be protected from public disclosure.[211]

Through its National Cyber Awareness System (NCAS), CERT is a valuable source of information about cyber threats and software vulnerability. In addition, it is an appropriate place to report breaches and other related matters. Interested parties can find valuable cyber information at the CERT website and subscribe to data feeds and mailing lists.

G. 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,"[212]

> 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 record, versus $236 per record for firms without strategic security leadership that is part of overall enterprise risk management.[213]

H. Ten Ways to Improve Cybersecurity

Pinguelo and Muller note that "although companies cannot prevent all hacking incidents . . . relatively simple measures—

[210] U.S. Computer Emergency Readiness Team (US-CERT), *About Us*, http://bit.do/ComputerEmergencyReadiness.

[211] *Id.*

[212] Shackelford, *supra* note 83, at 16.

[213] *Id.* (citing Chris Costanzo, Is Your Company Prepared for Cyber Risk, (2011), http://bit.do/CyberRiskInsurance; Denis Drouin, *Cyber Risk Insurance: A Discourse and Preparatory Guide, SANS Institute InfoSec Reading Room* (2004)).

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."[214] Elsewhere, I've cited a useful list of ten measures to improve cybersecurity and response to attacks provided by Pinguelo and Muller.[215]

Exhibit Five, created by the U.S. Department of the Treasury to address the needs of commercial banks, is a list of ten questions any enterprise can use to think about cybersecurity. While drafted to meet the particular needs of banks, these questions may be tailored to fit the needs of any line of business. Deputy Treasury Secretary Sarah Bloom Raskin explains that "at Treasury we have framed our thinking about cybersecurity and financial industry preparedness against cyber-attacks around three categories of activities: (1) baseline protections, (2) information sharing, and (3) response and recovery."[216]

Exhibit Five:
U.S. Department of the Treasury's
Ten Questions in Thinking About Cybersecurity

> … baseline protections are the policies, procedures, and other controls that [are] adopted to prevent penetration of their networks and systems, and to prevent damage assuming that there has been access.
>
> 1. **Is cyber risk part of our current risk management framework?** Banks should have risk management frameworks that are appropriately tailored to the cyber risks presented by their specific businesses and operations. Ideally, your cybersecurity risk management is part and parcel of your enterprise risk management framework, key components of which are technology, process, and people.
>
> CEOs and boards of directors should identify the cyber threats presented by their particular activities and operations and match those threats to appropriate technology solutions. Then CEOs and boards should adopt policies, procedures, and other controls—like training and governance—to not only address identified cyber threats that their technology solutions cannot control, but also to reasonably anticipate possible breakdowns and overrides of that technology.
>
> Finally, CEOs and boards should do their best to employ highly qualified people to monitor and continually reassess the effectiveness of the deployed technology and controls, including those technologies or controls which are not directly operated by the institution. When appropriately designed and executed, technology, process, and people form a risk management

[214] Pinguelo & Muller, *supra* note 80, at 85.

[215] *See* Trautman, Triche & Wetherbe, *supra* note 184.

[216] Raskin, *supra* note 34.

structure and the necessary first lines of defense against cyber-attacks.

2. **Do we follow the NIST Cybersecurity Framework?** The National Institute of Standards and Technology, or NIST… released the Framework for Improving Critical Infrastructure Cybersecurity in February [2014]. The NIST Cyber Framework is a well-considered approach to strengthening the resilience of critical infrastructure. Banks should use the framework to reduce cybersecurity threats both within the bank and with outside vendors.

The framework is a risk-based approach to managing cybersecurity that can help identify your bank's cyber posture and determine its risk profile and tolerance. Importantly, the framework is not a technical document; it focuses on oversight process for management and governance. For example, it provides advice on how to develop organizational communication plans for responding to attacks, and provides a common language and set of practices, standards, and guidelines. And for organizations that have developed enterprise-risk management approaches, the NIST framework need not replace those approaches; instead the framework can be used to better inform and apply those established risk-management approaches when the risks and associated controls are cyber-related. The NIST framework also provides firms with a tool to evaluate vendors and other third-parties that have access to their networks, systems, and data…

3. **Do we know the cyber risks that our vendors and third-party service providers expose us to, and do we know the rigor of their cybersecurity controls?** Third-party vendors—and any other third parties with access to a firm's networks, systems, and data—can present a significant cybersecurity hazard. As you know, given the nature of modern IT services, many banks do not own or operate their systems for payment services or other back-office processes. This means that personnel with access to your networks, systems, and data may not even be employed by your bank.

As such, it is imperative that you understand the security safeguards that your vendors and other relevant third-parties have in place. At a minimum, this means four things: (1) knowing all vendors and third-parties with access to your systems and data, (2) ensuring that those third parties have appropriate protections to safeguard your systems and data, (3) conducting ongoing monitoring to ensure adherence to protections, and (4) documenting protections and related obligations in your contracts.

4. **Do we have cyber risk insurance? And if we do, what does it cover and exclude?** Is our coverage adequate based on our cyber risk exposure? While the cyber insurance market is relatively new, it is growing. More than fifty carriers now offer some type of cyber insurance coverage.

Unlike the past, now some form of cyber coverage exists for organizations of all sizes, from small, family-owned shops to Fortune 500 companies. Policyholders can now find coverage to match a broad array of cyber risks, ranging from liability and costs associated with data breaches to business interruption losses and even tangible property damage caused by cyber events.

Cyber insurance cannot protect your institutions from a cyber incident any more than flood insurance can save your house from a storm surge or D&O insurance can prevent a lawsuit. But what cyber risk insurance can do is provide some measure of financial support in case of a data breach or cyber incident. And, significantly, cyber risk insurance and the associated underwriting processes can also help bolster your other cybersecurity controls. Qualifying for cyber risk insurance can provide useful information for assessing your bank's risk level and identifying cybersecurity tools and best practices that you may be lacking.

I have been asking our insurance and cyber experts at Treasury to think about how to encourage an environment where market forces create insurance products that enhance cybersecurity for businesses. Ideally, we can imagine the growth of the cyber insurance market as a mechanism that bolsters cyber hygiene for banks across the board.

5. **Do we engage in basic cyber hygiene?** Here I am referring to ensuring that your bank engages in fundamental practices to bolster the security and resilience of your networks and systems. What exactly does this mean? Things like: Knowing all the devices connected to your networks. Knowing what is running—or attempting to run—on your networks. Knowing who has administrative permissions to change, bypass, or override system configurations and then reducing that number to only those who need those privileges. And also: patching software on a timely basis, and conducting continuous, automated vulnerability assessments and remediation. The Center for Internet Security, working with others including the Department of Homeland Security, launched the Cyber Hygiene Campaign in April [2014]. By some estimates, engaging in basic cyber hygiene will prevent 80 percent of all known attacks. This is the basic "blocking and tackling" that doesn't take a computer wizard to understand.

Information Sharing

… By information sharing, I'm referring to the sharing of timely, actionable information regarding cyber vulnerabilities, threats, and incidents with a view toward limiting attacks and stopping contagion across systems, networks, and other institutions. We know that the most effective defenses do not happen in isolation. Instead, the banks most sophisticated in cyber defense are those that play an active role in the information-sharing community, which leads us to the sixth question you should be asking…

6. **Do we share incident information with industry groups? If so, when and how does this occur?** When bad actors attack one bank, it is possible—and increasingly likely—that those actors or others will use the same or similar methods to target other institutions. We saw this play out earlier this year during the attack on JP Morgan Chase's systems. That attack was not limited to JP Morgan Chase, but reportedly targeted other institutions as well.

Sharing knowledge of vulnerabilities, threats, and incidents allows banks to benefit from the experience of others. This benefit is more acute today, when banks act as correspondents and comprise an interconnected system; and when an intrusion at one bank may quickly enable an intrusion at another…

Response and Recovery

…Given the sheer number and continual morphing of assaults, we know that a goal of avoiding every attack is currently "pie-in-the-sky," so instead we have to increasingly focus our efforts on making response and recovery more efficient, effective, and predictable.

7. **Do we have a cyber-incident playbook and who is the point person for managing response and recovery?** Whether it is a stand-alone document or part of a larger business continuity and disaster recovery plan, your bank should consider having a detailed, documented plan that designates who is responsible for leading the response-and-recovery efforts; and that individual, as well as the entire organization, should know his or her authority. The person you choose to lead this effort should have exceptional organizational and communication skills because he or she will quarterback internal and external interactions.

8. **What roles do senior leaders and the board play in managing and overseeing the cyber incident response?** The CEO and the board have to understand what their respective roles will be in the event of a significant cyber incident at the bank or in an adjacent sector such as energy or telecommunications that might significantly affect the bank. This means clearly understanding when and which matters get escalated to the CEO. It also means understanding whether the full board or a committee—like risk or audit—is initially tasked to oversee the response from a governance perspective. Attacks can create confusion and fear, but the damage can be vastly minimized if leaders clearly understand their roles in response and attack mitigation.

To practice those roles, it makes sense for banks to participate in cyber exercises that simulate a cyber intrusion. These exercises allow CEOs, directors, and other key players to figure out how they will navigate the pressures and problems that come from the intrusion.

The Treasury is developing an exercise regime designed to test communication and decision-making during cyber incidents, an effort that will involve institutions from across the financial sector as well as departments and agencies throughout government. Likewise many trade associations regularly organize cybersecurity exercises… Think of these exercises as complicated fire drills; proactive engagement with regulators and law enforcement through these exercises helps to better prepare your banks for actual attacks.

9. **When and how do we engage with law enforcement after a breach?** It is important to remember that most cybersecurity breaches are crimes, some of which are crimes in progress. As such, your cyber-incident playbook should contemplate when, based on the data gathered, you should reach out to law enforcement. Because many of you may not have had reason to reach out to federal law enforcement agencies who specialize in cyber-crimes, we recommend that financial institution leaders—at banks of all sizes—cultivate relationships with local U.S. Secret Service and FBI

field offices. These teams are spread out across the country, and have personnel dedicated to cybersecurity. This relationship-building should start now if it hasn't already, before a cyber event is unfolding. If you need help making those connections, our team will facilitate those introductions.

10. **After a cyber incident, when and how do we inform our customers, investors, and the general public?** Transparency is key. To instill trust and confidence, the messages you communicate should avoid technical jargon and legalese and provide clear and consistent information. In addition, for those organizations that are public companies, you will have additional considerations regarding the timing and content of your disclosure if the breach is considered material information. These are some reasons why having draft messages for various scenarios is an important part of your bank's playbook, given the possibility that events may be serious and fast-moving.[217]

[217] *Id.*

CONCLUSION

Now more than ever, governance of cybersecurity risk requires continuous education and vigilance. In cyberspace, barbarians are always at the gate. This article attempts to explore the unusually complex subject of cybersecurity in a readable manner. Many of the most significant cyber breaches to date and have been examined. Next, recent governmental policy initiatives, including President Obama's Executive Order 13636 and related Treasury Department report, the Quadrennial Homeland Security Review, and NIST Framework have been reviewed. Important tools are available to improve the quality of discussion between boards, management, and information technology executives: the SANS Critical Security Controls; OWASP Top Ten; CWE/SANS Top 25 Most Dangerous Software Errors; resources from the DHS National Cybersecurity and Communications Integration Center (NCCIC) and U.S. Computer Emergency Readiness Team (US-CERT); and the U.S. Treasury's list of ten ways to improve cybersecurity. Hopefully, these suggestions about what top managers and boards can do to improve cyber awareness and readiness will result in meaningful progress toward strengthening cybersecurity governance.