THE DATA SECURITY GOVERNANCE CONUNDRUM: PRACTICAL SOLUTIONS AND BEST PRACTICES FOR THE BOARDROOM AND THE C-SUITE

Thad A. Davis,* Michael Li-Ming Wong,**
and Nicola M. Paterson***

Data breaches and cyber attacks continue to represent increasingly sophisticated threats to corporations of all shapes and sizes. Recent, high-profile data losses and vulnerabilities have prompted heightened regulator, enforcement agency, plaintiff, and public scrutiny of boardroom preparedness.

This Article examines the cybersecurity and cyber attack landscape and identifies core dilemmas that boardrooms face in the current environment. It also explores the various approaches, and examines recent watershed case law on the data breach question. This Article draws guiding principles for compliance from more established regulatory schemes to inform best practices guidance and a flexible, scalable corporate data and cyber-compliance framework.

* Partner & Co-Chair, Securities Litigation Practice Group, Gibson, Dunn & Crutcher LLP. The author is a Certified Information Privacy Professional (CIPP/US).

** Partner & Co-Chair, Securities Enforcement Practice Group, Gibson, Dunn & Crutcher LLP. The author is a Certified Information Privacy Professional (CIPP/US).

*** Associate, Gibson, Dunn & Crutcher LLP. The author is a non-resident fellow with the Georgetown Center on National Security and the Law.

The authors would like to thank Ingrid Davis, Wendy Jan Wong, and Elliot Paterson Sears.

I. INTRODUCTION

Data security breaches have escalated and exploded in recent weeks and months,[1] and boardrooms are under increasing fire for such breaches from regulators, private plaintiffs, and the court of public opinion.[2] A sequence of high-profile data losses have battered Fortune 500 companies in particular;[3] internal and external data security attacks are now seen as a cost of doing business for companies in all industries and of all sizes.[4] In addition, executives are being undermined directly by C-suite-focused

1 *See* PRICEWATERHOUSECOOPERS, *Managing Cyber Risks in an Interconnected World: State of Information Survey*, *2015*, 7 (Sept. 30, 2014), http://www.pwc.com/gx/en/consulting-services/information-security-survey/download.jhtml, *archived at* http://perma.cc/BJ2U-M5YH (reporting that, as of September 2014, there had been a 48% increase in detected security breach incidents since 2013); *see also* Amir Mizroch, *1 Billion Data Records Stolen in 2014, Says Gemalto*, WALL ST. J. DIGITS (Feb. 12, 2015, 5:47 AM), http://blogs.wsj.com/digits/2015/02/12/1-billion-data-records-stolen-in-2014-says-gemalto/, *archived at* http://perma.cc/JE9C-NK8E (finding a 49% increase in known data breaches in 2014, with identity theft accounting for 54% of breaches); *see also* IDENTITY THEFT RESOURCE CENTER, DATA BREACH REPORTS (Dec. 31, 2014), *available at* http://www.idtheftcenter.org/images/breach/DataBreachReports_2014.pdf, *archived at* http://perma.cc/8NXE-GZWA.

2 *See* Nicole Perlroth, *Hacked v. Hackers: Game On*, N.Y. TIMES, Dec. 3, 2014, at F1 (reporting that over the past year "over 552 million people had their identities stolen . . . nearly 25,000 Americans had sensitive health information compromised every day . . . [and] over half of Americans, including President Obama, had to have their credit cards replaced at least once because of a breach").

3 Brand-name victims of external cyber attacks over the past two years abound and include Anthem, Home Depot, JP Morgan Chase, Target, Sony Entertainment, Neiman Marcus, Yahoo!, Snapchat, AT&T, eBay, Google, Apple, multiple news media groups, Adobe, Staples, and Vodafone, to name but a few. *See also id.* (quoting Richard A. Clarke, the United States' first cybersecurity tsar, as saying that "[i]t's almost impossible to think of a company that hasn't been hacked—the Pentagon's secret network, the White House, JPMorgan—it is pretty obvious that prevention and detection technologies are broken").

4 *See* IDENTITY THEFT RESOURCE CENTER, DATA BREACH REPORTS (Dec. 31, 2014), *available at* http://www.idtheftcenter.org/images/breach/DataBreachReports_2014.pdf, *archived at* http://perma.cc/8NXE-GZWA.

data hacks and by their companies' own vulnerabilities, including data access, storage, and procedural weaknesses.[5] The direct and indirect costs of these attacks on the economy, reputations, shareholders, and consumers—whether from the immediate compromise of data or the passed-down costs of mitigating data losses—are also growing at an alarming rate.[6]

Meanwhile, the debate over boundaries in the use of private data by corporations continues to heat up, with so-called "big data"[7] collection and misuse allegations hitting

5 Recent reports allege that hackers are targeting executives directly to secure privileged information. *See* Alan Levin & Michael Riley, *Hackers With Wall Street Savvy Stealing M&A Data*, BLOOMBERG BUS. NEWS (Dec. 1, 2014), http://www.bloomberg.com/news/articles/2014-12-01/hackers-with-wall-street-savvy-stealing-m-a-data-fireeye, *archived at* http://perma.cc/Y4RE-H4CC; *see also* Rachel Feintzeig, Clint Boulton & Joann S. Lublin, *Fears Spread of Sony-Style Hack*, WALL ST. J. (Dec. 17, 2014), http://www.wsj.com/articles/fears-spread-of-sony-style-hack-1418863212, *archived at* http://perma.cc/6LQM-QJPB.

6 These costs are not necessarily reported in financial disclosures, and initial breach losses may not be good predictors of knock-on breach costs. For example, reports suggest that the cost to third-party credit unions of the data security breach at Home Depot was twice as large as that caused by the breach at Target, although direct corporate losses disclosed in Target's regulatory filings are—thus far—significantly larger than those suffered by Home Depot. *See* Press Release, Credit Union National Association, Home Depot Breach Cost Us Nearly Double Those From Target (Oct. 31, 2014), *available at* http://www.cuna.org/Stay-Informed/News-Now/Washington/Home-Depot-breach-cost-CUs-nearly-double-those-from-Target/, *archived at* http://perma.cc/JT4B-N35V; *see also* Press Release, Target Corporation, Target Reports Fourth Quarter and Full Year 2014 Earnings (Feb. 25. 2015), *available at* http://www.sec.gov/Archives/edgar/data/27419/000002741915000008/a2014q4ex-99.htm, *archived at* http://perma.cc/VW7F-959B (disclosing gross expenses of $252 million related to the fourth quarter 2013 data breach, partially offset by a $100 million in insurance receivables).

7 For a discussion of the meaning of "big data," see generally JAMES MANIKA et. al., BIG DATA: THE NEXT FRONTIER FOR INNOVATION, COMPETITION AND PRODUCTIVITY (2011), *available at* http://www.mckinsey.com/insights/business_technology/big_data_the_next_frontier_for_innovation, *archived at* http://perma.cc/G7J6-HMV7; see also INTEL'S BIG DATA BASICS, http://www.intel.com/content/www/us/en/big-data/learn-about-big-data.html, *archived at* http://perma.cc/R7XD-YHW5

the headlines as corporations, consumers, and governments attempt to balance data privacy with leveraging data utility. Fierce competition and the decreasing cost of data storage and complex analysis have incentivized corporate private data accumulation at a galloping pace, but data protection has lagged behind the times.[8] In 2013, President Obama issued Executive Order No. 13636, *Improving Critical Infrastructure Cybersecurity*, calling for the development of a "voluntary risk-based" set of industry standards and best practices for data protection.[9] But what was "voluntary" is now necessary: in January 2015, the President signaled a move away from relying on voluntary action by calling for federal legislation that would force companies to abide by a single set of consumer protection-oriented data security standards.[10] However, data security is not just a consumer industry concern. Whether compelled by lawmakers and regulators or not, security breach sophistication, risks, and impacts are fast evolving, and to avoid devastating losses, C-suite preparedness solutions must follow suit.

(providing big data definitions and examples of methods of harnessing and utilizing such data).

8 *See* Press Release, White House Office of the Press Sec'y, Fact Sheet: Big Data and Privacy Working Group Review (May 1, 2014), http://www.whitehouse.gov/the-press-office/2014/05/01/fact-sheet-big-data-and-privacy-working-group-review, *archived at* http://perma.cc/3LZS-PRY4 ("Driven by the declining cost of data collection, storage, and processing; fueled by new online and real-world sources of data, including sensors, cameras, and geospatial technologies; and analyzed using a suite of creative and powerful new methods, big data is fundamentally reshaping how Americans and people around the world live, work, and communicate.").

9 *See* Exec. Order No. 13,636, 78 C.F.R. § 33 (2013), *available at* http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf, *archived at* http://perma.cc/5YFW-H4PA.

10 *See* Press Release, White House Office of the Press Sec'y, Fact Sheet: Safeguarding American Consumers & Families (January 12, 2015), http://www.whitehouse.gov/the-press-office/2015/01/12/fact-sheet-safeguarding-american-consumers-families, *archived at* http://perma.cc/KD3F-SM9R; *see also* Michael D. Shear & Natasha Singer, *Obama to Call for Laws Covering Data Hacking and Student Privacy*, N.Y. TIMES, Jan. 11, 2015, at A10.

In this climate, not integrating data security preparedness into high-level board and C-suite strategy, or assuming that data privacy is just a consumer or tech start-up problem, is an approach that is doomed to fail. Regulatory investigations at home and abroad are on the uptick. In the United States, the Securities and Exchange Commission ("SEC"), the Department of Justice ("DOJ"), the Department of Homeland Security ("DHS"), the Federal Trade Commission ("FTC"), the Federal Communications Commission ("FCC"), the Financial Industry Regulatory Authority ("FINRA"), and the Consumer Financial Protection Bureau, among others, have made clear that they are taking data security seriously and will hold boardrooms accountable.[11] Audit committees, in particular, are under increasing scrutiny, with oversight responsibilities now extending to compliance with a patchwork of new cybersecurity regulations.[12]

In addition, 2014 witnessed a similar escalation in shareholder derivative and class action suits, with proxy advisors taking an active role in recommending action

[11] *See* Comm'r Luis A. Aguilar, *Boards of Directors: Corporate Governance and Cyber-Risks: Sharpening the Focus*, SEC. EXCH. COMM'N (June 10, 2014), http://www.sec.gov/News/Speech/Detail/Speech/1370542057946#.VIUIKYvF_Sg, *archived at* http://perma.cc/RB4L-X73H; *see also* DEPT. OF JUSTICE, http://www.justice.gov/usao/priority-areas/cyber-crime, *archived at* http://perma.cc/2Q4J-CJGY; DEPT. OF HOMELAND SECURITY, http://www.dhs.gov/topic/cybersecurity, *archived at* http://perma.cc/WQ87-J3SS; FED. TRADE COMM'N, http://www.ftc.gov/tips-advice/business-center/privacy-and-security/data-security, *archived at* http://perma.cc/DDU8-LG3J; Press Release, Fed. Commc'ns Comm'n, FCC Plans $10M Fine for Carriers that Breached Consumer Privacy (Oct. 24, 2014), *available at* http://www.fcc.gov/document/fcc-plans-10m-fine-carriers-breached-consumer-privacy, *archived at* http://perma.cc/5ZJ8-M539; FIN. INDUS. REG. AUTH., BUSINESS CONDUCT PRIORITIES (2014), *available at* http://www.finra.org/web/groups/industry/@ip/@reg/@guide/documents/industry/p419710.pdf, *archived at* http://perma.cc/L9AC-KKW4.

[12] *See* Michael Rapoport & Joann S. Lublin, *Meet the Corporate Board's 'Kitchen Junk Drawer'*, WALL ST. J. (Feb. 3, 2015), http://www.wsj.com/articles/meet-the-corporate-boards-kitchen-junk-drawer-1422933078, *archived at* http://perma.cc/39CQ-UTXU.

against boards for serious data breaches.[13] Inter-industry pressures are also growing, with financial institutions—such as credit organizations—exerting pressure on lawmakers to increase corporate accountability for data security breaches.[14]

Added to the risk mix, the vast majority of states now have security breach notification laws that apply to public and private entities alike, and various state regulators, including state attorneys general and financial and insurance regulators have made clear that they—like their federal counterparts—are looking to boards to take proactive steps to secure corporate data.[15] Overseas, European

13 *See, e.g.*, Rick Wilking, *Proxy Adviser ISS Asks Target Shareholders to Vote Against Directors*, REUTERS, May 28, 2014, *available at* http://www.reuters.com/article/2014/05/29/us-target-shareholders-proxy adviser-idUSKBN0E901X20140529, *archived at* http://perma.cc/5YHR-5VY4.

14 *See, e.g.*, Press Release, Credit Union National Ass'n, "Stop the Data Breaches" Is Target of CUNA Campaign for Credit Unions (Oct. 2, 2014), http://www.cuinsight.com/press-release/stop-the-data-breaches-is-target-of-cuna-campaign-for-credit-unions, *archived at* http://perma.cc/CY26-3EN6.

15 As of the time of writing, forty-seven states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have enacted legislation requiring private and government entities to provide notification of data security breaches relating to personally identifiable information. *See* NAT'L CONFERENCE OF STATE LEGISLATURES, *Security Breach Notification Laws* (Jan. 1. 2015), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx, *archived at* http://perma.cc/Y2DA-29LS. California and New York have two of the strictest data-privacy regimes. *See, e.g.,* CALIFORNIA OFFICE OF THE ATT'Y GEN., http://oag.ca.gov/cybersafety, *archived at* http://perma.cc/C67F-ASNS. In January 2015, New York Attorney General Eric T. Schneiderman proposed stricter data security laws in New York that would significantly expand data security breach definitions and corporate reporting requirements. *See* Matthew Goldstein, *New York Attorney General Seeks Expanded Reports on Data Breaches,* N.Y. TIMES, Jan. 15, 2015, at B3. Also in January 2015, a group of 19 state attorneys general collectively wrote to JP Morgan Chase & Co. asking for further information on an alleged 2014 data breach. *See* Chris Dolmetsch, *JPMorgan Asked by States for Detail on 2014 Data Breach*, BLOOMBERG BUS. NEWS (Jan. 14, 2015, 1:38 PM), http://www.bloomberg.com/news/articles/2015-01-14/jpmorgan-asked-by-states-for-more-detail-on-2014-

regulators are seeking to take an even harder line against data misuse with ramped-up data-privacy laws looming on the horizon.[16] The data security conundrum is by no means limited to brand-name entities, and companies of all sizes—both public and private—have suffered from external and internal data breaches and resulting reputation, legal, and related impacts.[17]

data-breach, *archived at* http://perma.cc/3BAP-HRSP. This interest is not new: in 2013, for example, New Jersey Supervising Deputy Attorney General Kenneth Ray Sharpe told corporate representatives that "sooner or later you're going to be a victim of a breach," and that it was his intent to "scream at you to deal with it proactively." Jedidiah Bracy, *Federal and State Regulators Talk Data Security Lessons*, THE PRIVACY ADVISOR (Nov. 7, 2013), http://privacyassociation.org/news/a/federal-and-state-regulators-talk-data-security-lessons/, *archived at* http://perma.cc/P486-4J9L. Attorneys General are not the only state officials taking aim at cybersecurity. New York State's Superintendent of Financial Services considers cybersecurity to be "likely the most important issue [the NY Department of Financial Services ("DFS")] will face in 2015," and recently announced plans to conduct targeted cybersecurity assessments of DFS-regulated banks and insurance companies. *See* Superintendent Benjamin M. Lawsky, *Financial Federalism: The Catalytic Role of State Regulators in a Post-Financial Crisis World*, N.Y. DEP'T OF FIN. SERVS. (Feb. 25, 2015), http://www.dfs.ny.gov/about/speeches_testimony/sp150225.htm, *archived at* http://perma.cc/8EGA-HRS5; *see also* Press Release, N.Y. Dep't of Fin. Servs., NYDFS Announces New, Targeted Cyber Security Assessments for Insurance Companies (Feb. 8, 2015), http://www.dfs.ny.gov/about/press2015/pr1502081.htm, *archived at* http://perma.cc/58DG-PU6D; Press Release, N.Y. Dep't of Fin. Servs., NYDFS Issues Examination Guidance to Banks Outlining New Targeted Cyber Security Preparedness Assessments (Dec. 10. 2014), http://www.dfs.ny.gov/about/press2014/pr1412101.htm, *archived at* http://perma.cc/4QKC-XZQJ.

16 *See infra* Part V. A recent study suggested that a significant number of organizations in Europe lack effective guidance on strategies for complying with Network and Information Security and General Data Protection Regulation legislation. *See generally* Warwick Ashford, *Most EU Businesses Unclear on Latest Cyber Security Laws*, COMPUTER WEEKLY (Jan. 27, 2015, 8:45 AM), http://perma.cc/2T2X-SGBV (finding that most businesses in the UK, France, and Germany feel that guidelines for compliance with EU cybersecurity regulations are unclear, and one-third of organizations polled do not understand the potential impact of future cybersecurity legislation).

17 The Ponemon Institute determined that the total average cost paid by U.S. organizations suffering a known data breach increased from $5.4

In sum, boardroom exposure to data breaches and related fallout has never been greater. Proactive data security risk assessment and preparation should be high on the list of C-suite resolutions for 2015.

C-suite members play a vital role in data security preparedness. Reports suggest that companies with strong data security plans that involve dedicated security specialists, structured breach preparedness, and response systems see dramatically reduced per-record data breach costs.[18] Reports also suggest, however, that a significant number of boards, while concerned about data security, are not taking appropriate action to fulfill their leadership responsibilities.[19] As recent data breaches confirm, even

to $5.9 million from 2013 to 2014. PONEMON INSTITUTE, 2014 COST OF DATA BREACH STUDY: UNITED STATES (2014), May 2014, *available at* http://public.dhe.ibm.com/common/ssi/ecm/se/en/sel03017usen/SEL03017USEN.PDF, *archived at* http://perma.cc/YS9G-YHQR. Add in the cost of undetected data breaches and the indirect costs of dealing with additional insurance, mitigation, and prevention, and the actual costs are almost certainly far higher.

18 *See* PONEMON INSTITUTE, 2014 COST OF DATA BREACH STUDY: UNITED STATES (2014), *available at* http://www-935.ibm.com/services/us/en/it-services/security-services/cost-of-data-breach/, *archived at* http://perma.cc/P68K-GWY5.

19 Press Release, Thomson Reuters, Survey Reveals Increased Cybersecurity Risk to Boardroom Communications, (Nov. 4, 2014), *available at* http://thomsonreuters.com/press-releases/112014/increased-cybersecurity-risk-to-boardroom-communications, *archived at* http://perma.cc/3CM8-YWTF (explaining that among those surveyed, less than half the corporate boards claimed they made decisions on the subject of data security, and only one-third stated that the board frequently requested security information); *see also* UNITED KINGDOM DEPT. FOR BUS. INNOVATION AND SKILLS, 2014 INFORMATION SECURITY BREACHES SURVEY (2014), *available at* http://www.pwc.co.uk/assets/pdf/cyber-security-2014-exec-summary.pdf, *archived at* http://perma.cc/7L8J-EKAT (finding that in the United Kingdom, a quarter of respondent companies had not briefed their board on security risks from 2013 to 2014, and that 13% had *never* briefed their board on such risks). *See generally* Jeremy Hodges, *Cybersecurity Must Be Priority for Corporate Boards, KPMG Says*, BLOOMBERG BUS. NEWS (Jan. 15, 2015, 7:00 PM), http://www.bloomberg.com/news/articles/2015-01-16/cybersecurity-must-be-priority-for-corporate-boards-kpmg-says, *archived at* http://perma.cc/6VUK-NH2P.

sophisticated boards and executives can run afoul of outdated data security plans, and brand-name status may not equate to top-tier data security. Regulators, courts, and public opinion focus on board and manager activity in evaluating whether a corporation is conducting adequate data security risk assessment, preemption, and response. Failure to take necessary protective steps not only results in security weakness and potential liability, but also lowers the chances that third-party security partners—such as law enforcement, insurers, security experts, and other risk responders—will be able to assist a corporation in the event of an attack. As such, it is incumbent on C-suite members to ensure that their data security preparation is up to the complex and fast-evolving task. Finding the necessary guidance in such a fast-paced environment can be daunting, but there are approaches that have proven effective in other compliance regimes that can inform the proactive board. By understanding the value of the data their corporations possess, acknowledging the data security vulnerabilities they face, and taking advantage of best-practices advice in advance of breaches, boards can better defend their companies, shareholders, clients, and their own members against their data security foes.

The following overview examines the dangers faced by boardrooms and their corporations, reviews a selection of data security updates and actions by regulators, courts, overseas investigative bodies, and liability insurance companies, and suggests a consolidated set of starting-point best practices for proactive boards.

II. EXTERNAL AND INTERNAL ATTACKS: THE PERILS OF C-SUITE MANIPULATION

The value and increasing depth and scope of corporate data collections are combining with C-suite vulnerabilities to produce critical data exposures. Hacks, data viruses, scams, skimming, data sharing by disgruntled employees, and other assorted cyber weaponry reside in the consciousness of consumers and regulators. But breaches are about far more than the theft of consumer records and reputational impacts

(serious as they may be). Accumulation hacking[20] is less understood and less easy to detect; moreover, its impact is less immediately ascertainable. And it is being aimed at those with critical business data: C-suite members.

FireEye, a leading security company, recently published two reports revealing that cybercriminals are leveraging security weaknesses and cyber sleight-of-hand to accumulate market edge data from hundreds of organizations.[21] The way the breaches identified in the reports were constructed should give pause to all board members, executives, and their related agents who are in the possession of critical business information. In one, attackers used a targeted breach to steal draft SEC filings. They then used seemingly legitimate email addresses and other sheep's clothing disguises to lure unsuspecting executives into clicking on false login pages and data links and to hand over yet more sensitive information. Attackers also pose as IT support workers, deal advisors, financial experts, and lawyers, and seek out disgruntled employees to act as data sources. These so-called data "phishing" and "pharming" attacks have grown in popularity, especially in the M&A and private equity world where companies and their advisors exchange large amounts of proprietary data outside of controlled data networks and with oftentimes minimally developed business relationships.

---

[20] Accumulation hacking—also known as "pharming"—generally describes the use by hackers of data acquired over time, whether they are internal or external to the organization. The data may include, for example, stolen emails, draft public filings, draft private equity deal documents, and other non-public data. Such data may be released, but hackers may also use it to make market decisions, or to manipulate other employees into providing more valuable data (knowingly or unknowingly).

[21] FIREEYE, *Hacking the Street? FIN4 Likely Playing the Market* (2014), http://www2.fireeye.com/fin4.html, *archived at* http://perma.cc/2L7D-63MU; FIREEYE, *Threat Report: M-Trends 2015: A View From the Front Lines* (2015), http://www2.fireeye.com/WEB-2015RPTM-Trends.html, *archived at* http://perma.cc/M4NM-48AE. *See also* Nicole Perlroth, *Web Thieves Using Lingo of Wall St. Breach Health Care Companies' Email*, N.Y. TIMES, Dec. 2, 2014, at B1.

Recent highly publicized data breaches have underscored the growing reality that attacks on private corporations constitute a national security issue.[22] The attack on Sony Entertainment, allegedly orchestrated and sponsored by North Korea, demonstrates at a high level the potential perils of both the immediate and knock-on consequences of data breaches.[23] In the aftermath of the attacks, Sony was faced with the prospects of being unable to use its computer network and seeing its trade secrets exposed, devalued, and held hostage.[24] Executives, employees, and third parties found themselves dealing with the release of personal communications, health information, and other private data—including social security numbers.[25] The cyber attackers were then able to manipulate those data releases, fear about potential future hacks, and terrorism threats to cause the cancellation of film releases and screenings by several theater chains.[26] It is no stretch to anticipate that hackers will attempt to use similar tactics in the future to extort and disrupt other private industry with potentially

[22] *See Sony Hack: White House Views Attack as Security Issue*, BBC NEWS (Dec. 18, 2014, 7:49 PM), http://www.bbc.com/news/world-us-canada-30538154, *archived at* http://perma.cc/8U22-S4UG.

[23] *See, e.g.*, David Brunnstorm & Jim Finkle, *U.S. Considers 'Proportional' Response to Sony Hacking Attack*, REUTERS (Dec. 18, 2014, 6:57 PM), http://www.reuters.com/article/2014/12/18/us-sony-cybersecurity-northkorea-idUSKBN0JW24Z20141218, *archived at* http://perma.cc/C2X7-2B36; *see also* REUTERS, *Cyber Attack Could Cost Sony Studio As Much As $100 Million*, FORTUNE (Dec. 9, 2014, 7:11PM), http://fortune.com/2014/12/09/cyber-attack-could-cost-sony-studio-as-much-as-100-million/, *archived at* http://perma.cc/VD4R-3ZSA.

[24] *Id.*

[25] Andrea Peterson, *The Cyberattack on Sony Pictures Made Employees Collateral Damage*, THE WASH. POST THE SWITCH (Dec. 3, 2014), http://www.washingtonpost.com/blogs/the-switch/wp/2014/12/03/the-cyberattack-on-sony-pictures-made-employees-collateral-damage/, *archived at* http://perma.cc/VU4X-P9P7.

[26] David Brunnstorm & Jim Finkle, *U.S. Considers 'Proportional' Response to Sony Hacking Attack*, Reuters (Dec. 18, 2014, 6:57 PM), http://www.reuters.com/article/2014/12/18/us-sony-cybersecurity-northkorea-idUSKBN0JW24Z20141218, archived at http://perma.cc/C2X7-2B36.

devastating economic impacts. However, it would also be a mistake to assume that breaches are limited to high-profile targets.

Even more recently, Anthem, the second largest health insurance provider in the United States, reported that hackers accessed and stole sensitive personal data from approximately 80 million accounts, including those of customers and current and former employees.[27] The compromised personal information included account holders' names, dates of birth, email and street addresses, income data, social security numbers, and other sensitive information (although the company states that the breach does not appear to have exposed policyholders' credit card information or medical records).[28] Taken together, however, the information obtained would easily be enough for the criminals—suspected to be a state-sponsored Chinese cyber espionage group[29]—to gain access to the consumers' financial or other accounts.[30] Anthem, for its own part, immediately attempted to close the vulnerability once it was discovered, hired a private cybersecurity firm to review its practices, and is cooperating with the FBI's investigation while offering free credit-monitoring and identity protection services to affected policyholders.[31] But the sheer volume and reach of this hack

27 *See* Drew Harwell & Ellen Nakashima, *China Suspected in Major Hacking of Health Insurer*, WASH. POST (Feb. 5, 2015), http://www.washingtonpost.com/business/economy/investigators-suspect-china-may-be-responsible-for-hack-of-anthem/2015/02/05/25fbb36e-ad56-11e4-9c91-e9d2f9fde644_story.html, *archived at* http://perma.cc/REW4-F4RS.

28 *See* Letter, Joseph R. Swedish, President and CEO, Anthem, Inc., to Members (Feb. 13, 2015), *available at* http://www.anthemfacts.com/ceo, *archived at* http://perma.cc/FX9L-GDQU.

29 *See* Michael A. Riley & Jordan Robertson, *Chinese State-Sponsored Hackers Suspected in Anthem Attack*, BLOOMBERG BUS. NEWS (Feb. 5, 2015), http://www.bloomberg.com/news/articles/2015-02-05/signs-of-china-sponsored-hackers-seen-in-anthem-attack, *archived at* http://perma.cc/HP74-XXWU.

30 *See* Tara Siegel Bernard, *Protecting Yourself From the Consequences of Anthem's Data Breach*, N.Y. TIMES, Feb. 6, 2015, at B4.

31 *See* Swedish, *supra* note 28.

is startling. Investigators suspect that the initial intrusion occurred in early December 2014, although Anthem only detected the breach at the end of January 2015.[32] Anthem's CEO and President Obama's chief cybersecurity advisor have revealed that their own personal information was compromised in this breach.[33] Furthermore, revelations that the stolen data was unencrypted have not only trained a harsh spotlight on Anthem's data security practices, but have also raised serious questions about the effectiveness of the main federal health privacy law, HIPAA, which encourages—but does not require—encryption of consumer data contained in servers.[34]

Manipulated breaches underscore the need for boards to identify the location of valuable data and ensure its protection. This assessment includes identifying those both inside and outside the organization with potential access to such data, and identifying individuals who may have reason to use that data improperly. Unfortunately, some reports suggest that many boards are not utilizing even relatively common sense data-protection devices that would thwart opportunistic data attacks. A recent Thompson Reuters survey, for example, found that half the boards it surveyed did not use a secure form of data portal or secure file transfer system.[35] Meanwhile, more than half relied on printed rather than encrypted data and had no system to determine how those documents were secured, tracked, archived, and disposed of. And the majority of board members surveyed used personal mobile and computing devices and commercial email accounts to access company data, making it all the

[32] *See* Brandon Bailey, *Anthem Hackers Tried to Breach System As Early As December*, HUFFINGTON POST (Feb. 6, 2015), http://www.huffingtonpost.com/2015/02/06/anthem-hackers-december_n_6634440.html, *archived at* http://perma.cc/A5X3-73RL.

[33] *See* Swedish, *supra* note 28; *see also* Riley & Robertson, *supra* note 29.

[34] *See* Melinda Beck & Danny Yadron, *Health Insurer Anthem Didn't Encrypt Data in Theft*, WALL ST. J., Feb. 6, 2015, at B1.

[35] Thomson Reuters, *supra* note 19.

more difficult to secure and monitor access to such information adequately.

Boards must also grapple with how to best balance data privacy with leveraging data utility. Companies that deal in data are especially vulnerable to crossing data privacy lines. Data start-ups have seen meteoric success, with big data manipulation and prediction treated as significant competitive advantages. But fast-growing companies can lack the privacy structure safeguards and C-suite savvy to fully appreciate that big data carries with it big risk and responsibility.[36] Even those companies that do not take client data and use it for predictive or advertising purposes must still be aware of and prepare for the sobering reality that if data carries value, others can and will seek to steal and profit from it.

III. SOLUTION SOURCES: FIGHTING IN THE SHADE

While the data security problem is apparent, best boardroom practices and risk solutions are still playing catch-up. The U.S. government, for example, has yet to release a cross-agency data security best-practices manual that gives adequate assurance and instruction to board members. But awareness of government regulator preferences more generally should—in combination with recently released investigation information focused on data security—prove useful in establishing proactive and evolving risk-assessment solution strategies.

[36] Manufacturers of lifestyle applications and related technology, for example, are accumulating health care data in a way that is thus far unregulated. It remains to be seen whether health care privacy laws will be changed to cover health data entered by consumers into such systems, but the possibility exists and corporations need to be aware that regulators and their clients can and will make use of existing and new legal structures. *See* Lisa Kimmel and Janis Kestenbaun, *What's Up with WhatsApp? A Transatlantic View on Privacy and Merger Enforcement in Digital Markets*, ANTITRUST MAGAZINE, Fall 2014.

A. Lessons From Other Regulatory Best Practices: Finding a Plan in an Anti-Corruption Concept?

U.S. enforcement agencies jointly published the *Foreign Corrupt Practices Act Enforcement Manual* in 2012.[37] The Manual resulted from corporate pressure on the U.S. government to provide cross-agency anti-corruption guidance that companies large and small could use to formulate adequate compliance procedures.[38] Anti-corruption may not initially appear relevant to the issue of data security, but anti-corruption, like data security, applies to and impacts companies of all shapes, sizes, locations, and industries. Data security certainly has additional complexities, not the least of which are the myriad ways external cyber attackers can attempt to steal and misuse data, the difficulties in detection, the knock-on impact implicated by such misuse, and C-suite unfamiliarity with technical concepts at issue. But the enforcement principles articulated in the FCPA Manual, particularly those concerning cooperation evaluation and the hallmarks of effective corporate compliance programs, are useful predictors of how regulators may generally approach future data security investigations.[39] The Manual identifies core concepts for such a program. They are framed for FCPA use in terms of compliance, but appear well suited to structuring a data security guidance scheme:

1. Commitment from senior management and clearly articulated policies

---

[37] *See* CRIMINAL DIVISION OF THE U.S. DEP'T OF JUSTICE & THE ENFORCEMENT DIV. OF THE U.S. SEC. AND EXCH. COMM'N, A RESOURCE GUIDE TO THE U.S. FOREIGN CORRUPT PRACTICES ACT (2012), *available at* http://www.justice.gov/criminal/fraud/fcpa/guidance, *archived at* http://perma.cc/MGG4-2Y3Z.

[38] *See id.*; *see also* Gibson, Dunn & Crutcher LLP, *Decoding FCPA Enforcement: The U.S. Government Issues Comprehensive Guidance on the Foreign Corrupt Practices Act* (Nov. 19, 2012), http://www.gibsondunn.com/publications/Documents/DecodingFCPAEnforcement-USGovernment-ComprehensiveGuidance.pdf, *archived at* http://perma.cc/K9WD-9SDF.

[39] Gibson, Dunn & Crutcher LLP, *supra* note 38.

2. Written codes of conduct and related policies and procedures
3. Board oversight and effective resources provided to experts in risk assessment and preparedness
4. Effective risk assessment and response
5. Training and continuing advice
6. Incentives and disciplinary measures
7. Third-party due diligence
8. Confidential reporting and internal investigation
9. Continuous improvement: periodic testing and review
10. Effective due diligence and integration in merger and acquisition environments.

In addition, the Manual underscores the importance of adopting policies that are attuned to shifting overseas, regulator, and state-to-state requirements.[40]

B. Government Responses to Data Security Breaches: Regulators Mount Up

The lack of a united regulatory front on the data security issue means that boards must pay close attention to all those regulators that could conceivably investigate their data security preparedness. The following case studies examine the approaches of the SEC, FTC, FCC, DHS, and DOJ, though this is just the tip of the regulatory iceberg. State attorneys general are taking an active role in investigating data security matters,[41] and unless and until the federal government issues data security regulations that clearly preempt state efforts, executives should plan to comply proactively with the current patchwork of federal and state law and account for regulatory guidance in any board preparedness planning.

40 *See* Criminal Division, *supra* note 37, at 63.

41 *See supra* text accompanying note 16.

1. The Securities and Exchange Commission: Sharpening the Data Security Enforcement Knives

The SEC has made it clear that it is "sharpening" its focus on boardroom data security preparedness.[42] In February, 2015, SEC Chair Mary Jo White confirmed that the Commission is targeting the cybersecurity readiness of market participants.[43] In June 2014, Commissioner Luis A. Aguilar gave a speech dedicated to boardroom oversight of cyber-risks, specifically stating that "there can be little doubt that cyber-risk . . . must be considered as part of [a] board's overall risk oversight."[44] Significant portions of Commissioner Aguilar's speech referenced risk assessment and planning advice that arguably overlaps significantly with the framework used in the FCPA enforcement manual.[45] The Commissioner also referred to the *Framework for Improving Critical Infrastructure Cybersecurity*, which was released by the National Institute of Standards and Technology ("NIST") in February 2014, and asserted that it should serve as a reference point for boardrooms.[46] But Commissioner Aguilar did not mention that in April 2014 the SEC's own Office of Compliance Inspections and Examinations ("OCIE") announced a sample list of requests[47] it intends to use in cybersecurity investigations.[48] These 28

42 Aguilar, *supra* note 11.

43 Press Release, U.S. Sec. & Exch. Comm'n, SEC Alerts Investors, Industry on Cybersecurity (Feb. 3, 2015), *available at* http://www.sec.gov/news/pressrelease/2015-20.html#.VQn59Y7F9yI, *archived at* http://perma.cc/ACN4-XZ23.

44 Aguilar, *supra* note 11.

45 *Id.*

46 *Id.*

47 OFFICE OF COMPLIANCE INSPECTIONS AND EXAMINATIONS, *OCIE Cybersecurity Initiative*, NAT'L EXAM PROGRAM RISK ALERT (Apr. 15, 2014), *available at* http://www.sec.gov/ocie/announcement/Cybersecurity+Risk+Alert++%2526+Appendix+-+4.15.14.pdf, *archived at* http://perma.cc/2XHN-VCPL.

48 The twenty-eight requests for information are partially based on a report and guidance released by the National Institute of Standards and

detailed requests loosely incorporate the NIST framework, but they contain additional pointers for proactive boards. The use of multiple guidance reference points underscores the need for boards to ensure that they receive expert-informed data security advice that is sourced from multiple avenues. The OCIE requests are not rules or regulations, though they clearly suggest that:

1. Boards will be held responsible for ensuring that corporate data is effectively stored and managed and that protocols are established for the use and protection of that data—both before and after a data breach.
2. Boards will be held accountable for ensuring that a corporate culture of data security exists, is fostered, and is effective across all company structures.
3. Boards will be held responsible for ensuring written policies are in place, that cybersecurity responsibilities are effectively assigned and overseen, and that corporate data security policies, procedures, and tools are subject to continuous assessment and improvement.
4. Boards will be expected to have procedures in place to deal with breaches. This may include specific insurance that covers cybersecurity incidents.
5. Boards will be held responsible for ensuring that third parties they entrust with corporate data are subject to data security risk assessment and monitoring of an equivalent level to the corporation itself.

Technology. *See* NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY *Framework for Improving Critical Infrastructure Cybersecurity*, (Feb. 12, 2014), *available at* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf, *archived at* http://perma.cc/N4F4-X7J6. Various regulators and agencies reference the NIST standards in their cybersecurity compliance, underscoring the need for corporations to ensure they are aware of and understand these and other reference frameworks.

Not only is OCIE using these requests as the basis for investigations, but myriad other groups, including class-action plaintiffs and insurance underwriters, are likely to frame their own information discovery on this, and similar, risk-assessment guidance. That the SEC is concerned only with a relatively small portion of corporations is no excuse for unlisted companies to ignore that advice. Courts and plaintiffs take their cues from industry guidance, and in the fast-developing world of data security, guidance ignored is potential liability gained.

2. The Federal Trade Commission: Congress' Go-To Watchdog for Consumer Data Security Compliance Sinks Its Teeth into Enforcement

The FTC has taken on a central role in data security enforcement. In 2006 the agency created the Division of Privacy and Identity Protection ("DPIP") with the goal of protecting consumer data.[49] The DPIP has taken aim at big-data collectors and has issued orders requiring companies to establish and maintain privacy programs and procedures.[50] 2014 saw the FTC announce its 50th data security-based enforcement settlement,[51] and the agency has been aggressively pursuing enforcement actions both administratively and in the courts against companies in a variety of industries, including Wyndham, Fandango, Inc., and Credit Karma, Inc.[52] In the fall of 2014, the agency

49 *See* Peder Magee, *Privacy and Identity Protection from the Fair Credit Reporting Act to Big Data*, 29 ANTITRUST MAGAZINE 56, 56–61, Fall 2014.

50 *See id.*

51 Press Release, Fed. Trade Comm'n, FTC Testifies on Data Security before Senate Banking Subcommittee (Feb. 3, 2014), http://www.ftc.gov/news-events/press-releases/2014/02/ftc-testifies-data-security-senate-banking-subcommittee, *archived at available at* http://perma.cc/X7QY-YVJ6.

52 FED. TRADE COMM'N, *Cases and Proceedings: Wyndham Worldwide Corporation* (Nov. 5, 2014), http://www.ftc.gov/enforcement/cases-proceedings/1023142/wyndham-worldwide-corporation, *archived at* http://perma.cc/3JJ6-9E6S (outlining FTC proceedings against Wyndham

announced it was investigating the 2013 Target data breach, and lawmakers have emphasized the agency's role in security enforcement by calling on the FTC to investigate other publicized breaches.[53] Indeed, in January 2015, President Obama chose a speech at the FTC to unveil a package of proposed laws that would require companies to notify consumers within thirty days after theft of personal information is discovered, and that would for the first time create a federal standard in what has, until now, been a state-dominated field.[54]

Like the SEC, FCC, and other regulators, the FTC has issued its own data security compliance guidance.[55] In its November 2014 briefing on the *Wyndham* enforcement case, the FTC referenced its 2007 *Protecting Personal Information: A Guide for Business*.[56] The *Wyndham* case, described more

Worldwide Corporation); *see also* Press Release, Fed. Trade Comm'n, FTC Approves Final Orders Settling Charges Against Fandango and Credit Karma (Aug. 19, 2014), *available at* http://www.ftc.gov/news-events/press-releases/2014/08/ftc-approves-final-orders-settling-charges-against-fandango, *archived at* http://perma.cc/4WSQ-CBUY.

53 Tom Risen, *FTC Investigates Target Data Breach*, U.S. NEWS & WORLD REPORT (Mar. 26, 2014), http://www.usnews.com/news/articles/2014/03/26/ftc-investigates-target-data-breach, *archived at* http://perma.cc/EGM5-RSV8.

54 Shear & Singer, *supra* note 10; *see also* Ellen Nakashima & Katie Zezima, *Obama to Propose Legislation to Protect Firms that Share Cyberthreat Data*, WASH. POST (Jan. 12, 2015), http://www.washingtonpost.com/politics/obama-proposes-legislation-to-protect-consumer-data-student-privacy/2015/01/12/539c4a06-9a8f-11e4-bcfb-059ec7a93ddc_story.html, *archived at* http://perma.cc/V6ZT-KSWR.

55 *See, e.g.*, FED. TRADE COMM'N, FED. TRADE COMM'N PRIVACY REPORT: BALANCING PRIVACY AND INNOVATION (2012), *available at* http://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/ftc-privacy-report, *archived at* http://perma.cc/DL3X-Q44V (recommending best practices for businesses to protect the data of U.S. consumers); *see also* FED. TRADE COMM'N, THE INTERNET OF THINGS: PRIVACY AND SECURITY IN A CONNECTED WORLD (2015), *available at* http://www.ftc.gov/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things, *archived at* http://perma.cc/T9Y5-JPBE.

56 Brief of Plaintiff-Appellee at 5, *FTC v. Wyndham*, No. 14-3514 (3d Cir. Nov. 5, 2014).

fully in Part IV *infra*, involved alleged data security breaches that first occurred in 2008. The FTC's reference to years-old guidance in evaluating corporate compliance with data security measures underscores the importance of paying attention to regulator guidance, whether or not it forms part of a regulation or law. Regulators will seek to use such guidance to provide frameworks for judicial analysis and exemplars of corporate and board missteps. Boards should therefore ensure that their legal advisors and risk management teams are aware of evolving regulator guidance.

The FTC has also strongly indicated that it supports industry-wide efforts to address cybersecurity preparedness. 2014 saw the FTC and DOJ jointly announce that sharing of cyber-threat information would not subject companies to antitrust concerns.[57] This should encourage companies seeking to warn and work with others to identify and address cyber-threats. As discussed *infra* in Part III (B)(6), it also mirrors support given in international jurisdictions to encourage broad solutions to the data security problem. Additionally, FTC representatives have noted that not one of its 50 cases involved one-off security lapses, but rather multiple, system-wide security failures.[58]

3. The Federal Communications Commission: Monitoring the Cloud for Enforcement Opportunities

Following in the footsteps of the SEC, FTC, and related state regulators, on October 24, 2014, the FCC entered the data security fray by announcing the assessment of a $10-million fine against two telecommunications companies for

[57] Press Release, Fed. Trade Comm'n, FTC, DOJ Issue Antitrust Policy Statement on Sharing Cybersecurity Information (Apr. 10, 2014), *available at* http://www.ftc.gov/news-events/press-releases/2014/04/ftc-doj-issue-antitrust-policy-statement-sharing-cybersecurity, *archived at* http://perma.cc/M2L4-CXHW.

[58] *See* OFFICE OF COMPLIANCE INSPECTIONS AND EXAMINATIONS, *supra* note 47.

their alleged failure to secure the private data of hundreds of thousands of private individuals.[59] The agency found that by using unsecured internet-based data storage, the companies had breached sections 201(b) and 222(a) of the Communications Act of 1934.[60] The forfeiture should prove motivating for any company storing data on cloud servers. It remains to be seen how heavily the FCC will used these code sections in the future as part of their enforcement arsenal, but regulator fines and findings all but guarantee the filing of private civil litigation. As such, this potential double barrel of liability should again prompt board action to address data security vulnerabilities.

4. The Department of Justice: Juggling Enforcement and Private-Sector Partnership

The DOJ's position in data security enforcement is complicated by its role in defending against cyber attacks. From a boardroom perspective, the DOJ treads a fine line between being a data security partner and data security enforcer. On December 4, 2014, in response to rampant data security breaches and predictions that "for the foreseeable future, cybercrime will increase in both volume and sophistication," the DOJ announced the establishment of a Cybersecurity Unit.[61] Describing the "intricate rubric of laws and investigatory tools needed to thwart" data security attacks, Assistant Attorney General Leslie R. Caldwell confirmed that the DOJ is focused on addressing "cyber threats on multiple fronts, with both a robust enforcement

---

59 *In re* Application of American International College For Renewal of License, DA 14-1477 (Fed. Comm. Comm'n Oct. 24, 2014) (Notice of Apparent Liability for Forfeiture), *available at* http://apps.fcc.gov/edocs_public/attachmatch/DA-14-1477A1.pdf, *archived at* http://perma.cc/WJ8N-C2Y7.

60 *Id*.

61 Press Release, Dep't of Justice, Assistant Attorney General Leslie R. Caldwell Speaks at Cybercrime 2020 Symposium (Dec. 4, 2014), *available at* http://www.justice.gov/opa/speech/assistant-attorney-general-leslie-r-caldwell-speaks-cybercrime-2020-symposium, *archived at* http://perma.cc/YNL6-JGDF.

strategy as well as a broad prevention strategy."[62] Caldwell further noted that "the private sector has proved to be an increasingly important partner in [the DOJ's] fight against all types of online crime, but particularly cybersecurity-related matters."[63] Acknowledging that cybersecurity is "a fight that the government cannot and will not wage alone," the DOJ has tasked the Cybersecurity Unit with using "extensive outreach" to "facilitate cooperative relationships" with the private sector.[64]

The FBI has also made its preference for data-sharing clear, with FBI Director James B. Comey recently explaining that "without effective sharing [the FBI is] a bit like a police officer patrolling a street with 50-foot high wall."[65] But understandable concerns abound related to data and threat sharing. Not least questions over the extent of information that should be shared, how the government may then use that information, how the data will be stored, whether competitors will have access to such data, and how information sharing with government entities and other private sector peers impacts corporate disclosure requirements.

The DOJ's partner posture is extra food for thought for board members seeking to establish stronger data security policies and procedures. It remains to be seen what role the Cybersecurity Unit will play in enforcement, particularly in combination with other regulatory agencies. The strongest board position at this juncture appears to be a robust data security plan commensurate with the best practices espoused by the regulators and courts. Boards should also ensure that their cybersecurity plan includes contacts within relevant federal and state enforcement agencies in the event there is an incident. Such robust policies will then theoretically allow

62 *Id.*

63 *Id.*

64 *Id.*

65 *See* James B. Comey, *Addressing the Cyber Security Threat*, FED. BUREAU OF INVESTIGATION (Jan. 7, 2015), *available at* http://www.fbi.gov/news/speeches/addressing-the-cyber-security-threat, *archived at* http://perma.cc/HJ7A-F38T.

boards and executives to involve the DOJ and related state entities both in preparing for and in rapidly addressing data security events as they come to light with less fear of unintended enforcement consequences.

5. The Department of Homeland Security: Lead Cook in the Kitchen?

The biggest brand name victim of data security breaches is the United States itself. Like the private sector, the federal government has found itself reeling in the wake of massive breaches, large-scale theft of data, and the structural reality that cyber attackers are not hindered by accountability. In December 2014, President Obama signed reforms to the Federal Information Security Management Act.[66] The most visible impact of these changes is that DHS is now the lead enforcement agency in the federal government's internal fight against data breaches.[67] It remains to be seen how effective this assignment will be in practice—the Office of Management and Budget is still the lead overall agency with cyber-security authority in the federal government. But DHS has the upper hand in terms of its sheer number of data security experts, and this means that DHS will now lead the forthcoming federal information security incident center.

Underscoring again the interplay with private sector data security efforts, in December 2014, DHS' Deputy Undersecretary for Cybersecurity testified that because "the private sector owns and operates over 85% of the Nation's critical infrastructure, information sharing and capability development partnership becomes especially critical between the public and private sectors."[68] The Deputy

66 *See* Eric Chabrow, *DHS Big Winner in Congressional CyberSec Vote*, BANK INFO SECURITY (Dec. 12, 2014), http://www.bankinfosecurity.com/dhs-big-winner-in-congressional-cybersec-vote-a-7672/p-2, *archived at* http://perma.cc/6L22-VLZ2.

67 *See id*.

68 *Cybersecurity: Enhancing Coordination to Protect the Financial Sector: Hearing Before the S. Comm. on Banking, Hous. & Urban Affairs*,

Undersecretary's listing of the various interrelationships between government agencies (including the preparedness programs used by DHS and its agency) and private-sector partners again underscores the best practices roadmap described herein:

1. Corporations need to be aware of the value of their data, and the vulnerabilities of the systems they use to protect that data.
2. Mitigation efforts need to be sophisticated, individually tailored, and constantly evolving.
3. Corporations should be aware of the agencies that could be involved in prevention, identification, and possible after-the-fact investigation of data-related incidents.
4. The role of the federal government as a partner and enforcer is picking up steam, and boards should inform themselves of the options available to their corporations for taking advantage of preparation tools provided by the government.

As with the DOJ, it remains to be seen how DHS' private-sector partnership role will develop, but for now it provides both opportunities and enforcement questions for private actors. The danger of too many cooks in the preparedness kitchen is a very real one, but parsing out the acronyms and identifying potential government partners and enforcers is something that boards should add to their data security to-do lists.

6. Overseas Regulator Lessons: Great Britain Tells Boards to Develop Bespoke Data Security Policies and Procedures

The best practices listed above find support in advice offered by overseas regulators. In 2012, the British

113th Cong. (2014) (statement of Dr. Phyllis Schneck, Deputy Undersec'y for Cybersecurity, U.S. Dep't of Homeland Sec.), http://www.banking.senate.gov/public/index.cfm?FuseAction=Files.View&FileStore_id=990f3741-335b-49be-ad3a-a43475ac41b5, *archived at available at* http://perma.cc/ZND5-3DVL.

government released a list of *Key Questions for CEOs and Boards* and cybersecurity guidance for business.[69] The posture of the guidance and questions reinforces the critical role of board members in data security compliance. For example, the guidance states in part that:

1. Board members are likely to be key targets of data attacks and should actively plan to preempt and prevent them;
2. Proactive management of cyber risk at the board level is critical;
3. The board is responsible for identifying key information assets, assessing attack vulnerabilities, allocating cyber-risk responsibilities, and requesting regular data intelligence from those responsible for data security; and
4. The board is responsible for developing a written information policy that is championed by the board, supported through regular training, and understood and followed by the entire workforce.

Of particular note, the advice encourages "technical staff to enter into information sharing exchanges with other companies in [their industry] sector and/or across the economy in order to benchmark, learn from others, and help identify emerging threats." This sentiment is reflected in the FTC and DOJ's recent press release assuring companies that data security threat sharing will likely not result in antitrust liability.[70]

---

69 UNITED KINGDOM DEP'T FOR BUS. INNOVATION & SKILLS, CYBER RISK MANAGEMENT – A BOARD LEVEL RESPONSIBILITY (2012), *available at* http://stewartroom.co.uk/wp-content/uploads/2014/07/UK-Cyber-Security-Cyber-Risk-Management-Board-Level-Responsibility.pdf, *archived at* http://perma.cc/5U6L-7MH8.

70 *See* Fed. Trade Comm'n, *supra* note 57.

IV. COMPARING COURTROOM AND REGULATOR LIABILITY: LESSONS FROM RECENT SHAREHOLDER ACTION AND REGULATORY ENFORCEMENT

The relative novelty of cyber attacks and large-scale data privacy breaches means there is a dearth of case law to guide the proactive boardroom. This is likely to change, and quickly, as judicial decision-making catches up with recent data security breaches. In November 2014, for example, Target and Home Depot disclosed that they were facing, respectively, "more than 100" and "more than 44" civil lawsuits as a result of recent data breaches.[71] Critically, as regulators focus more of their attention on data security-related actions, this civil docket activity is likely to increase.

2014 was a watershed year for data security actions in the courts. Decisions involving the Wyndham and Target data breaches are particularly informative and may prove helpful for boards seeking judicial guidance.

A. Wyndham

An October 2014 decision from the District Court for the District of New Jersey marks one of the first instances of a court tackling the data-privacy issue in the shareholder derivative suit context.[72] Meanwhile, earlier in the year, the

71 Target, Annual Report (Form 10-Q) (Nov. 26, 2014), *available at* http://www.sec.gov/Archives/edgar/data/27419/000002741914000036/tgt-20141101x10xq.htm#s85963B857DE7901F0418C85BA8F7AFBE, *archived at* http://perma.cc/A3GZ-VMJ5; Home Depot, Annual Report (Form 10-Q) (Nov. 25, 2014), *available at* http://www.sec.gov/Archives/edgar/data/354950/000035495014000047/hd_10qx11022014.htm, *archived at* http://perma.cc/AG4T-HSCX. Target also announced ongoing investigations by state and federal agencies, including state attorneys general, the FTC, and the SEC. *See also* Target, Annual Report (Form 10-K) (Jan. 31, 2015), *available at* http://www.sec.gov/Archives/edgar/data/27419/000002741915000012/tgt-20150131x10k.htm#s9489D92FD3BEDE1DCA05A5EBAF3AC4D6, *archived at* http://perma.cc/Z664-DH58.

72 Palkon, et al. v. Holmes, et al., No. 2:14-cv-01234, 2014 WL 5341880 (D. N.J. Oct. 20, 2014).

FTC's own enforcement action relating to the same alleged data security breach was allowed to proceed past the motion-to-dismiss stage by the District Court for the District of Arizona. As such, *Palkon v. Holmes* and *FTC v. Wyndham* provide valuable insight into potential future judicial treatment of data security claims brought against board members and corporations, respectively.[73]

From 2008 to 2010, Wyndham Worldwide Corporation fell victim to three externally orchestrated data breaches that resulted in the exposure of private financial data belonging to hundreds of thousands of its customers.[74] In the aftermath of the breaches, the FTC began investigating Wyndham's data security practices and brought legal action against the company.[75] Shareholders submitted two demand letters to the board, each insisting that the board bring a suit on behalf of Wyndham against named directors and officers, among others. The board instructed the corporation's audit committee to evaluate the demands. After the committee and board declined to pursue them, a shareholder filed a derivative suit alleging that the corporation and various directors and officers failed to implement adequate data security mechanisms. This failure, the shareholder alleged, resulted in reputational damage and the incurrence of substantial legal fees defending the FTC suit.

Applying Delaware law, the district court dismissed the shareholder's allegations with prejudice. It explained that, as with any derivative suit, the shareholder would have to show that the board's demand refusal was made in bad faith or based on an unreasonable investigation.[76] The court found that the shareholder had failed to overcome this "high burden."[77] The court took particular note of the fact that the board and the audit committee discussed the cyber attacks at

[73] *Id.*

[74] *Id.* at *1.

[75] *Id.*

[76] *Id.* at *3.

[77] *Id.*

multiple meetings over a four-year period.[78] The court further emphasized that Wyndham's general counsel gave a presentation on the breaches and/or data security generally at every quarterly board meeting. The shareholder also failed to identify any red flags or facts showing that directors and officers knew that data controls were inadequate and failed to act to remedy those inadequacies.

While instructive in how to handle shareholder derivative suits, boards should not rely solely on the *Palkon* court's investigative focus points in developing effective data security policies. The pleading requirements imposed on shareholders in such suits are burdensome and rarely overcome. Similar obstacles do not stand in the way of the government or the court of public opinion—a fact proven by the FTC's successful passing of the motion to dismiss hurdle in its own case against Wyndham. It remains to be seen how the FTC will fare on appeal—indeed during oral argument on March 3, 2015 the Third Circuit panel expressed skepticism about the FTC's data security enforcement powers under the FTC Act—[79] but the case proves the interest of regulators in prosecuting data security claims, and the use of such prosecutions by shareholders and others looking for a litigation springboard. Informed plaintiffs are also likely to find *Palkon* instructive in how to more effectively plead such complaints. Moreover, the legal costs in securing a dismissal even of a shaky derivative suit can be significant and may not—as discussed *infra*—be covered by

78 *Id.* at *5–*6.

79 The FTC filed its Third Circuit briefing on November 5, 2014. Oral argument was heard on March 3, 2015, with the Third Circuit panel questioning whether the FTC's anti-fraud powers as delineated in Section 5 of the FTC Act extend to policing data security practices. *See* Oral Argument, Fed. Trade Comm'n, v. Wyndham Worldwide Corp., No. 14-3514 (3d Cir. argued Mar. 3, 2015), *available at* http://epic.org/amicus/ftc/wyndham/, *archived at* http://perma.cc/LP5Y-CB5R. The panel also asked the parties for supplemental briefing on the question of whether the FTC can bring an unfairness claim relating to data security without first formally issuing regulations on that topic. FTC v. Wyndham, ELEC. PRIVACY INFO. CTR., http://epic.org/amicus/ftc/wyndham/, *archived at* http://perma.cc/LP5Y-CB5R.

general insurance policies. Additionally, it is notable that the *Wyndham* case involved external rather than internal data breaches. The attention of legislators, regulators, and the public is also focused on internal misuse of private data. While it remains to be seen whether courts will take a different approach to such cases, it would be prudent to expect more exacting scrutiny for internal, versus external, data security breaches.

B. Target

In contrast to the derivative shareholders in the *Wyndham* case, the putative class members in two sets of the consolidated cases arising out of the 2013 Target data breach managed to clear the motion-to-dismiss hurdle.

On December 2, 2014, the District Court for the District of Minnesota denied in large part Target's motion to dismiss the claims of a plaintiff group of banks and other card-issuing institutions.[80] The putative class alleged that Target had been negligent, and had also breached Minnesota state consumer protection laws when it failed to prevent the leak of consumer data. In a roadmap for other plaintiff cases, the court found that plaintiffs had adequately pled their negligence, negligence per se, and state law claims, including their claim that Target had failed to install effective data security measures, and may even have disabled or not made full use of security measures that it had installed.[81] The case also underscores the clash between the financial sector and retailers over data privacy, and raises the specter of corporation-versus-corporation data-privacy actions blazing trails for follow-on consumer suits.

---

[80] *In re* Target Corp., No. 14-md-02522, 2014 U.S. Dist. LEXIS 167802, at *22 (D. Minn. Dec. 2, 2014) (order granting in part and denying in part motion to dismiss).

[81] The court dismissed without prejudice plaintiffs' negligent-misrepresentation-by-omission claim that Target had failed to disclose weaknesses in its security system that it had an obligation to disclose. Plaintiffs were granted the opportunity to file an amended complaint to address the lack of properly pled reliance facts in their initial pleading. *See id.* at *16–17.

On December 18, 2014, the district court similarly allowed the consumer class action—based on data breach and consumer protection statutes of multiple jurisdictions—to proceed.[82] The court's opinion foreshadows multiple future data security litigation issues, including the question of whether private actors can enforce state data-breach notice statutes.[83] Finding three separate sets of enforcement provisions (attorney general enforcement only, non-exclusive or ambiguous remedies, and no enforcement language) the court dismissed the attorney general and no-private-right-of-action data-breach claims.[84] It remains to be seen whether state legislatures will amend these laws to permit such action in the future.

Of course, surviving a motion to dismiss is far from a guarantee of success on the merits, but the fact remains that defending a case past the motion to dismiss stage can be incredibly costly, and plaintiffs will make full use of successful complaints and motion briefing in wording their own data security claims in the future.

More generally, as data security cases hit the dockets, the reality is that judges are likely to become jaded to any form of "ostrich" or reaction-after-the fact defenses and more informed about regulator-preferred best practices. Data

[82] *In re* Target Corp. Customer Data Security Breach Litig., No. 14-2522 (PAM/JJK), 2014 WL 7192478 (D. Minn. Dec. 18, 2014).

[83] Relatedly, in March 2015, the district court granted preliminary approval to a $10 million settlement for Target customers impacted by the data breach. Hiroko Tabuchi, *$10 Million Settlement in Target Data Breach Gets Preliminary Approval*, N.Y. TIMES, Mar. 20, 2015, at B3. Final approval is dependent on a hearing in November 2015. Similarly, in April 2015, Target announced it had reached a $19 million settlement with financial institutions that issued MasterCard-branded credit and debit cards that were compromised by the breach. Shailaja Sharma & Nathan Layne, Target Announces $19 Million Data Breach Settlement with MasterCard, Reuters (Apr. 15, 2015, 7:53 PM), available at http://www.reuters.com/article/2015/04/15/us-target-settlement-idUSKBN0N62PA20150415, archived at http://perma.cc/R4PH-PAGN. It remains to be seen whether these settlement formulations will act as precedent for other breach settlements.

[84] *In re* Target Corp. Customer Data Security Breach Litig., No. 14-2522 (PAM/JJK), 2014 WL 7192478 (D. Minn. Dec. 18, 2014).

security breaches are here to stay, and in a similar vein to anti-corruption cases, courts will expect corporations to step up to the data privacy-protection plate.

V. INTERNATIONAL REGULATORY PRESSURES: DATA PRIVACY VERSUS DATA UTILITY

At the same time that companies are wrestling with data security best practices, protection of personal data is stoking a values clash between U.S.-based companies and international governments that goes beyond the issue of data breaches. The question of the proper use of private data and consumer-versus-corporate control over data access and use is coming to a head in a way that could force boards to institute even stricter data-privacy rules.[85] In March 2014, European lawmakers voted in favor of reforming data-protection rules, with proposals including fines of up to 5% of global turnover for companies that abuse customer data.[86] Of course, these proposals require the approval of EU member governments, but recent pressure from heavy European governmental hitters—including Germany and France—combined with apparent multi-front antipathy towards U.S. big-data companies[87] means that boards of companies with

85 Sam Schechner, *Europe Targets U.S. Web Firms,* WALL ST. J., Nov. 28, 2014, at A1. Whereas U.S. regulators appear focused on risk assessment for external cyber attacks, European regulators are focused on regulating the internal use—or misuse—of private data. The EU's March 2014 press release on "data protection reform" does not mention cyber attacks, and instead focuses on corporate misuse of private data. *See* Press Release, European Comm'n, Progress on EU Data Protection Reform Now Irreversible Following European Parliament Vote (Mar. 12, 2014), *available at* http://europa.eu/rapid/press-release_MEMO-14-186_en.htm, *archived at* http://perma.cc/93E8-M7UC.

86 *See* Frances Robinson, *EU to Reform Data Protection Rules*, WALL ST. J. (Mar. 12. 2014), http://online.wsj.com/articles/SB10001424052702303546204579434852620803652, *archived at* http://perma.cc/MHU9-ZHBN; *see also* European Comm'n, Press Release, *supra* note 85.

87 Schechner, *supra* note 85; *see also* Juliette Garside, *From Google to Amazon: EU Goes to War Against Power of US Digital Giants*, THE GUARDIAN (July 5, 2014), http://www.theguardian.com/technology/

international data exposure need to prepare for what is the near-certainty of large-scale data-privacy regulation.

VI. INSURING AGAINST THE INEVITABLE: REEVALUATING DIRECTOR LIABILITY IN THE BREACH-CERTAINTY ERA

Rethinking corporate and boardroom liability insurance has become a vital part of any data security assessment plan. The breaches of the past year have underscored that liability for single-breach incidents can be enormous: Target revealed in January 2015 that the data breach it suffered in late 2013 had cost some $252 million in mitigation, response, and defense expenses, and that it expected to recover only some $100 million from its insurers.[88] Home Depot similarly disclosed $43 million in pre-tax expenses related to the data breach it suffered in 2014, and that it expected to recover only $15 million from its insurers.[89] And it is not just brand-name retailers and banks that are facing significant data breach costs: a Massachusetts hospital recently disclosed that it was facing hundreds of thousands of dollars in data-breach costs—including a $750,000 state privacy law-based settlement—that were not covered under its insurance policies.[90] But even faced with such eye-opening examples, national and international reports suggest that a significant number of corporations of all sizes may lack insurance that would sufficiently cover them in the event of a breach.[91]

Regulators are also pressuring boards to reevaluate their insurance provision. The SEC's recent OCIE information requests expressly ask whether registered entities "maintain

2014/jul/06/google-amazon-europe-goes-to-war-power-digital-giants, *archived at* http://perma.cc/ZTJ5-6R3Z.

88 Target, Annual Report (10-K), *supra* note 71.

89 Home Depot, Annual Report (10-Q), *supra* note 71.

90 Deidre Fernandes, *More Firms Buying Insurance for Data Breaches*, BOSTON GLOBE, Feb. 17, 2014, at B5.

91 *Id.*; *see also* UNITED KINGDOM DEPT. FOR BUS. INNOVATION & SKILLS, *supra* note 19 (finding that just 52% of surveyed large organizations and 35% of small organizations had insurance that would cover them in the event of a breach).

insurance that specifically covers losses and expenses attributable to cybersecurity incidents."[92] So, too, the DHS has opined that a "robust cybersecurity insurance market could help reduce the number of successful cyber attacks by: (1) promoting the adoption of preventative measures in return for more coverage and (2) encouraging the implementation of best practices by basing premiums on an insured's level of self-protection."[93] It is too soon to tell what forms of insurance the SEC and others will deem sufficient, but companies would do well to reassess their insurance provisions with the knowledge that regulators are including them as part of their own data security assessment programs.

Given the relative novelty of data security based claims, boards should ensure that insurance—particularly traditional lines of insurance—will provide coverage in a variety of data-breach scenarios. Boards signing off on new or reissued policies should also be aware that the insurance industry has responded to increasing data security risks by carving out cyber- and data-based coverage. In the absence of overarching government and regulator guidance, insurance companies are providing their own best practice suggestions. For example, ACE Group recently announced that it had assembled "privacy loss mitigation services" to enable business to "tackle privacy and cyber risks."[94] Given insurer control over the underwriting process, these suggestions are in effect de facto best practice requirements. Boards would

92 OFFICE OF COMPLIANCE INSPECTIONS AND EXAMINATIONS, *supra* note 47.

93 DEP'T. OF HOMELAND SEC., *Cybersecurity Insurance*, http://www.dhs.gov/publication/cybersecurity-insurance, *archived at* http://perma.cc/62SU-AC75.

94 ACE GROUP, *When Anti-Virus Software Is Not Enough: ACE Assembles Loss Mitigation Services, Gives Businesses Easy Access to Tools that Tackle Privacy and Cyber Risks* (Oct. 14, 2014, 3:58 PM), http://www.acegroup.com/us-en/newsletters/privacy-loss-mitigation-services-.aspx?j=51696804&e=jennifer.walker@acegroup.com&l=2102745_HTML&u=442983858&mid=10001491&jb=0, *archived at* http://perma.cc/T435-HETZ.

be wise to use them as insight into review factors insurers will use during underwriter investigations.

Data-breach insurance policies, like data-breach complaints, are relatively untested in the courts, so boards should plan on securing expert review both of their insurance provision, together with any insurance determinations made in the event of a breach. Boards should also be aware that securing newer forms of data insurance will likely require underwriter investigations. These investigations—like those conducted by regulators—require significant preparation and self-knowledge regarding corporate data security policies and procedures. Boards seeking to protect their corporations and themselves from internal data breaches should also ensure that their own data use and private actions brought in response to the corporation's general use of private data are covered. This coverage analysis should evolve along with the corporation's and board's data usage.

Directors and Officers ("D&O") and Errors and Omissions ("E&O") policies that lag behind the times could easily result in personal board liability for coverage gaps. A reevaluation of corporate D&O and E&O insurance with developing cyber and data risks in mind should be part of the data-privacy game plan for any proactive board. Board members should take steps to ensure that insurance tailored to the risks faced by their business is part of the protection arsenal for the corporation and for themselves, and that their risk assessment and legal teams are up to the challenge of dealing with data security issues as they develop.

VII.THE HALLMARKS OF AN EFFECTIVE DATA SECURITY PROGRAM: SUGGESTED BEST PRACTICES AND PRINCIPLES

The best of the best practices available to boards is to ensure they understand the guidance put forward by all regulators and investigatory bodies that could conceivably become involved in any data security breach to befall the corporation. That said, in reviewing the complex web of regulatory guidance schemes touching on data security,

there are some themes that are raised again and again. Using the framework at work in FCPA Enforcement, the following section seeks to combine multiple guidance streams into a set of guidance lessons:

1. Data security must start at the top. Within a business organization, data security begins with the board of directors and senior executives setting the proper tone for the rest of the company. Setting the tone means living by it, and boards must take pains to establish their own compliance with data security measures. Boards should assume that they will be held accountable by regulators and private parties with a value interest in the data they are responsible for securing and must take action to secure that data before breaches occur. Board vulnerabilities are moving to the forefront of data-privacy analysis and board members should expect that their own data practices will be examined under the microscope.
2. Data security policies should be clear, current, effective, and subject to periodic review. Such polices should also outline responsibilities for data security and detail proper internal controls, auditing practices, and documentation policies. These policies should emanate from the boardroom to all levels of the company and detail disciplinary procedures to be taken against those who violate such policies. Companies dealing in sensitive data should be particularly aware of who in the corporation has access to such data, and should ensure that adequate monitoring is in place to ensure that data manipulation and retention is both warranted and not contrary to established privacy policies. To be deemed effective, data-privacy policies should also be subject to continuous review and improvement.
3. Boards must be consistently and constantly data-privacy vigilant, and must act with the awareness

that boards are both the source and target of data security breaches. Boards should act to inform themselves of their own and their company's data-breach vulnerabilities. Where expert knowledge gaps exist, boards should take steps to equip their companies with effective and informed advisors. These experts should be granted the resources and board access necessary to effectively conduct their work. Board members should expect to play an active role in monitoring advisor effectiveness. Effective data security policies require an in-depth understanding of a company's business model. Data-privacy laws differ across jurisdictions, and boards must secure the necessary expert advice to ensure that privacy practices comport with every jurisdiction in which it does business. Boards should also ensure that their advisors possess broad knowledge of regulatory requirements and guidance—whether formal or otherwise—so that the corporation is well equipped to deal with enforcement actions.

4. When it comes to effective data security, there is no one-size-fits-all strategy. Data security programs that employ a 'check-the-box' approach will likely be viewed as ineffective. By understanding the data risks that are unique to their corporation, board members and their advisors can tailor-make security programs that will avoid the check-the-box trap. Effective risk assessment and response means being equipped to deal with data security before, during, and after data breaches. Board members should ensure that their companies have contacts with third-party investigative bodies that can assist in the event of a breach, and that the corporation's data security procedures are robust enough to allow those third parties to provide effective assistance. So, too, board members should ensure that insurance for data security breaches is current and effective, and

that their own liability insurance allows them the freedom to actively seek out potential data security policy violations and address them. Regulators will likely take into account the differences in data security programs between small- and medium-sized companies on the one hand, and large multinational corporations on the other hand. But regulators will also expect thoughtful compliance practices from companies that demonstrate awareness of inherent data vulnerabilities and the taking of data security steps commensurate with the resources available to do so.

5. Encouraging a culture of data security compliance requires training and continuing advice, both of which should form an integral part of any data security policy. Regulators will likely look to training that applies throughout an organization's structure, including board members, third-party agents, and business partners, and that is tailored to its audience.
6. To have an effective data security culture, board members should ensure that there are mechanisms in place that foster such a culture. Employees should feel able to report data security issues, and mechanisms should be in place that allow employees to raise concerns and receive guidance on best practices. In the FCPA world, corporations use anonymous reporting hotlines to permit employees to report incidents without fear of reprisals. Similar forms of reporting may be viewed as effective in the data security realm. So too, effective disciplinary measures should be in place to dissuade internal data security breaches. Ensuring that data is effectively secured, that employees understand that procedures are in place to monitor and ensure data safety, and that violating data security warrants disciplinary action are some steps a board can take to buttress

their data security preparedness program. These disciplinary procedures must apply uniformly, and board members must themselves be subject to their reach.

7. As part of risk-based data security due diligence, companies should understand the qualifications and associations of their third-party partners. Board members should request that detailed records be kept on those parties with access to the corporation's data stores, and should ensure that third parties entrusted with access to this data have data security policies of comparable robustness to the corporation's. Board members should be on the lookout for any laws and regulatory guidance that place responsibility on them for the actions of such third parties, and should make sure they adequately document diligence taken in the selection and monitoring of such entities.
8. Effective data security programs should include mechanisms for self-reporting of misconduct and breaches, and monitoring for potential misconduct. And once reported, companies should have a system for investigating such allegations and recording actions taken in response. It is likely that regulators will expect companies to have methods by which employees and others can report potential data misuses—particularly those taking place within the company—without fear of retaliation. With an understanding of the corporation's prime-value data, boards should ensure that those with access to such data are adequately monitored and that those who do not share the company's data security goals are not granted broad access to such data.
9. Once in place, data security preparedness policies should be reevaluated and continuously improved. Boards need to take action to ensure that procedures evolve to take account of the fast-

changing pace of cyber attacks and regulator activity.

10. Boards, especially those in companies that could have any form of international exposure, should ensure that their data security risk assessment and preparedness systems are up to the challenge of dealing with differing regulatory regimes that may be motivated by clashing data-privacy goals. Boards should proactively review guidance and voluntary frameworks referenced by and used by regulators, enforcement agencies, and courts. Seeking data security guidance before—rather than after—data breaches should be a priority for the board.

VIII. CONCLUSION

In sum, data security should form the immediate focus of board action and oversight. Board members should act proactively to understand their corporation's use and storage of sensitive data, identify the vulnerabilities inherent in the possession of any such data, and establish effective policies for protecting that data and responding to data breaches of all kinds. Boards need to also look inward to their own data security compliance actions, and ensure that compliance starts in the C-suite. By taking such steps, board members will go a long way to ensuring compliance with regulatory guidance, to protecting their corporations and themselves from liability, and to positioning their companies to take advantage of the benefits afforded by the governmental resources that are now being aimed at fending off cyber attacks.