THE REVIEW OF
SECURITIES & COMMODITIES REGULATION
AN ANALYSIS OF CURRENT LAWS AND REGULATIONS AFFECTING THE SECURITIES AND FUTURES INDUSTRIES

Vol. 52 No. 5 March 6, 2019

THE EXPANDING ROLE OF LAWYERS IN ADDRESSING CYBER RISK AT FINANCIAL FIRMS

Cybersecurity regulatory compliance is imposing a myriad of new responsibilities on counsel of financial firms. The authors discuss, in detail, areas in which such counsel should play a key role, including "reasonable" cybersecurity protections, board oversight, public disclosures, and compliance with specific rules. They then turn to incident response, managing vendor risk, and M&A transactions.

By Avi Gesser, Matthew Kelly, and Samantha Pfotenhauer *

Over the last few years, cybersecurity has become everyone's problem. Major data breaches are costly, difficult to prevent, and cause substantial damage to a company's operations and public image. In 2016, a year in which at least 1,935 data breaches were reported, malicious cyber activity was estimated to have cost the U.S. economy between $57 billion and $109 billion.[1] Equifax alone spent $242.7 million in the seven months following its 2017 breach on related expenses.[2] Between 2013 and 2017, nearly $5.7 billion in losses were caused by a single form of cyber scam — the "business e-mail compromise."[3] For U.S. corporations — particularly those in the financial services industry — cybersecurity risks are not only operational challenges, they pose existential threats. As more companies and consumers fall victim to successful cyber attacks, pressure builds on regulators to act, which has resulted in a proliferation of cybersecurity regulations and guidelines. And with this increase in cyber regulation (as well as civil litigation) come important roles for in-house counsel in advising on data protection issues.

Not that long ago, cybersecurity was viewed as primarily a technical issue, to be handled by a company's IT department. But the rise of a robust regulatory framework means that government agencies

[1] THE COUNCIL OF ECONOMIC ADVISERS, THE COST OF MALICIOUS CYBER ACTIVITY TO THE U.S. ECONOMY 1, 20 (2018), https://www.whitehouse.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf.

[2] Equifax Inc., Current Report (Form 8-K) (Apr. 25, 2018).

[3] SEC, REPORT OF INVESTIGATION PURSUANT TO SECTION 21(A) OF THE SECURITIES EXCHANGE ACT OF 1934 REGARDING CERTAIN CYBER-RELATED FRAUDS PERPETRATED AGAINST PUBLIC COMPANIES AND RELATED INTERNAL ACCOUNTING CONTROLS REQUIREMENTS, Sec. Exch. Act Rel. No. 84429 at 1 (Oct. 16, 2018), https://www.sec.gov/litigation/investreport/34-84429.pdf.

* *AVI GESSER is a partner in Davis Polk's Litigation Department, representing clients in a wide range of cybersecurity issues and counseling companies that have experienced cyber events. He is a frequent writer and commentator on cybersecurity issues. MATTHEW A. KELLY is an associate in Davis Polk's Litigation Department. SAMANTHA PFOTENHAUER is a law clerk in Davis Polk's Litigation Department. Their email addresses are avi.gesser@davispolk.com, matthew.kelly@davispolk.com, and samantha.pfotenhauer@davispolk.com.*

RSCR Publications LLC Published 22 times a year by RSCR Publications LLC. Executive and Editorial Offices, 2628 Broadway, Suite 29A, New York, NY 10025-5055. Subscription rates: $1,197 per year in U.S., Canada, and Mexico; $1,262 elsewhere (air mail delivered). A 15% discount is available for qualified academic libraries and full-time teachers. For subscription information and customer service call (937) 387-0473 or visit our website at www.rscrpubs.com. General Editor: Michael O. Finkelstein; tel. 212-876-1715; e-mail mofinkelstein@gmail.com. Associate Editor: Sarah Strauss Himmelfarb; tel. 301-294-6233; e-mail sarah.s.himmelfarb@gmail.com. To submit a manuscript for publication contact Ms. Himmelfarb. ISSN: 0884-2426.

are now conducting examinations and investigations of firms' cybersecurity regulatory compliance, both before and after actual incidents occur. To anticipate and respond to these regulatory inquiries, in-house lawyers are often required to provide both legal and strategic advice on a range of cybersecurity-related issues, and to work cooperatively with departments throughout their companies to manage the legal, financial, operational, and reputational challenges associated with cyber incidents.

This article seeks to provide a practical overview of the evolving role of counsel of financial institutions in managing cyber risk and achieving cybersecurity compliance. We identify and discuss four areas in which counsel can be expected to play a key role: (1) cybersecurity governance and regulatory compliance; (2) incident response; (3) managing vendor risk; and (4) mergers and acquisitions transactions. Of course, circumstances and arrangements will vary depending on the size and type of institution, as well as its internal structure, business units, operations, risk profile, and corporate history. Many of the functions and roles described below may be allocated between more than one internal counsel, between internal and external counsel, or between different departments or groups (including legal, compliance, risk, information security, or information technology). But regardless of how such functions are allocated within a particular institution, advice of counsel now plays an increasingly critical role in managing the enterprise-level risks associated with cybersecurity.

ADVISING ON CYBERSECURITY GOVERNANCE AND REGULATORY COMPLIANCE

To understand the full scope of a company's regulatory obligations related to cybersecurity risk management, counsel should first determine which regulators have jurisdiction over the company and/or the data in its possession, and for which kinds of cyber issues, as well as the positions those regulators have taken in the recent past. As part of this exercise, counsel should identify all applicable state, federal, and foreign cybersecurity regulations and should be aware of any potentially relevant proposed laws that may be taking effect within the next two years. These data points should then be synthesized to create a comprehensive picture or map of the company's cybersecurity-related governance and compliance obligations.

The lack of meaningful coordination or agreement between regulators, and the evolving nature of cybersecurity threats, makes this a more challenging exercise than one might imagine. Most U.S. financial institutions are required to have cybersecurity policies and procedures that satisfy — at a minimum — a reasonableness standard like the one enforced by the SEC for broker-dealers and investment advisors, which is described further below. For all U.S. public companies (including financial institutions), the SEC has issued guidance describing expectations on cybersecurity-related disclosures, governance, and insider trading restrictions. Finally, depending on which regulator supervises them and their subsidiaries, firms may be required to comply with other cybersecurity regimes, such as the regime administered by the New York Department of Financial Services ("NYDFS").[4] In each scenario, counsel should be prepared to provide advice regarding the application of the relevant rules and standards in the context of a particular firm's circumstances, and to work cooperatively with other departments and functions to ensure the adequacy of that firm's cybersecurity governance and compliance.

Ensuring "Reasonable" Cybersecurity Protections

Reasonableness remains the most common benchmark for cybersecurity governance and compliance in the United States.[5] As a result, most financial institutions will be — at a minimum — subject to regulation or regulatory oversight that will require "reasonableness" in the design and implementation of

[4] Cybersecurity Requirements for Financial Services Companies, N.Y. COMP. CODES R. & REGS. tit. 23, § 500, *et seq.* (2017) (hereafter "N.Y. Codes").

[5] Avi Gesser et al., *Standards vs. Rules for Cyber Regulation – The Eleventh Circuit Weighs in Against the FTC and in Tacit Support for the NYDFS Approach* (July 9, 2018), https://www.dpwcyberblog.com/2018/07/standards-vs-rules-for-cyber-regulation-the-eleventh-circuit-weighs-in-against-the-ftc-and-in-tacit-support-for-the-nydfs-approach/.

cybersecurity policies and procedures. A common cybersecurity-related role of counsel, therefore, will be to analyze and provide advice regarding the application of this standard in the context of a particular firm's activities.

The Federal Financial Institutions Examination Council ("FFIEC")[6] has issued several statements and resources that direct financial institutions to actively manage cybersecurity risks.[7] For example, the FFIEC 2017 Cybersecurity Assessment tool outlines specific measures firms can take to identify and mitigate cybersecurity risks.[8] The Information Security Booklet of the FFIEC's IT Examination Handbook, updated in 2016, directs firms to conduct risk assessments, designate an information security officer, and establish a written cybersecurity policy, among other obligations.[9] Although FFIEC guidance does not have the force of law, it is used by bank examiners in assessing the level of security risks to a financial institution's information systems and, as such, sets forth supervisory expectations with respect to financial institutions' cybersecurity programs.

Rule 30(a) of Regulation S-P (the "Safeguards Rule"), which implements requirements of the Gramm-Leech-Bliley Act,[10] is the primary U.S. federal securities law provision governing the cybersecurity programs of broker-dealers and investment advisors.[11] It requires regulated entities to have written policies and procedures "*reasonably designed* to: (1) insure the security and confidentiality of customer records and information; (2) protect against any anticipated threats or hazards to the security or integrity of customer records and information; and (3) protect against unauthorized access to, or use of, customer records or information that could result in substantial harm or inconvenience to any customer."[12]

A number of other SEC rules and regulations applicable to certain classes of financial institutions also require reasonableness in the design and enforcement of policies and procedures related to cybersecurity. Rule 201 of Regulation S-ID (the "Identity Theft Red Flags Rule") requires certain classes of financial institutions and creditors to develop and implement written identity theft prevention programs, which must incorporate policies and procedures reasonably designed to respond to red flags of identity theft, including those that arise from cybersecurity incidents.[13] Section 13(b)(2)(B) of the Securities Exchange Act of 1934, which applies to certain classes of public issuers, requires that covered issuers devise and maintain internal accounting controls that reasonably safeguard the company and, ultimately, investor assets, including from cyber-related frauds.[14]

Until recently, it was unclear how the SEC would enforce these requirements when analyzing particular incidents or circumstances. However, the SEC took several steps in 2018 to put industry participants on notice that it intends to conduct highly fact-specific inquiries and hold firms accountable for perceived lapses in the design or implementation of a firm's cybersecurity policies and procedures.

One example of this is the Commission's September 2018 highly publicized enforcement action against Voya Financial Advisors Inc.[15] Voya, a dual-registered broker-dealer and investment advisor, experienced a data

---

[6] The FFIEC is composed of principals from the following: the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Office of the Comptroller of the Currency, the Consumer Financial Protection Bureau, and the FFIEC State Liaison Committee.

[7] *Cybersecurity Awareness*, FFIEC, https://www.ffiec.gov/cybersecurity.htm (last accessed Jan. 11, 2019).

[8] *Cybersecurity Assessment Tool*, FED. FIN. INST. EXAMINATION COUNCIL(May 2017), https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_May_2017.pdf.

[9] *FFIEC Information Technology Examination Handbook: Information Security*, FFIEC (Sept. 2016), https://ithandbook.ffiec.gov/media/274793/ffiec_itbooklet_informationsecurity.pdf.

[10] The Gramm-Leech-Bliley Financial Modernization Act of 1999 was the first significant federal law to require financial institutions to meet privacy and data security obligations. Christopher Wolf, *Recent Federal Initiatives on Financial Privacy and Data Security*, 25 REV. BANKING & FIN. SERV. 109, 110.

[11] 17 C.F.R. § 248.30(a).

[12] *Id.* (emphasis added).

[13] 17 C.F.R. § 248.201.

[14] SEC, REPORT OF INVESTIGATION PURSUANT TO SECTION 21(A) OF THE SECURITIES EXCHANGE ACT OF 1934 REGARDING CERTAIN CYBER-RELATED FRAUDS PERPETRATED AGAINST PUBLIC COMPANIES AND RELATED INTERNAL ACCOUNTING CONTROLS REQUIREMENTS, Sec. Exch. Act Rel. No. 84429 at 2 (Oct. 16, 2018), https://www.sec.gov/litigation/investreport/34-84429.pdf.

[15] Voya Fin. Advisers, Inc. Admin. and Cease-and-Desist Proceedings, Sec. Exch. Act Rel. No. 84,288, Investment Advisors Act Rel. No. 5,048 at 2 (Sept. 26, 2018).

breach in which attackers exploited gaps in its technical support procedures to access and steal confidential customer data. The SEC concluded that Voya's cybersecurity policies and procedures were not reasonably designed to detect identity theft risks or respond to cybersecurity attacks. Even though there was no finding of specific economic harm, the SEC imposed on Voya a $1 million penalty for what it deemed to be violations of both the Safeguards Rule and the Identity Theft Red Flags Rule.

A similar message can be gleaned from the SEC's October 2018 Rule 21(a) report regarding payment controls employed by public issuers that had fallen prey to certain fraudulent wire transfer scams.[16] The SEC made clear that it did not presume that the companies covered by the investigation had committed actionable violations of internal accounting controls requirements simply because they had experienced a breach. But the SEC did warn that the obligations imposed under Section 13(b)(2)(B) to devise and maintain internal accounting controls included obligations to reasonably safeguard investor assets from cyber-related fraud, and that companies may be in violation of federal securities laws if they do not adequately assess their own internal controls to manage the evolving risks arising from fraudulent transfer schemes.

In addition to laying the groundwork for future enforcement actions, these efforts illustrate that the SEC is monitoring the reasonableness of firms' cybersecurity policies and procedures, and that it will evaluate firms' programs individually, pursuant to broad existing authority, and using fact-specific standards.

Although it is putting firms on notice that cybersecurity deficiencies can create exposure, the SEC has refused to provide clear rules or checklists that would allow firms to determine what they must do to achieve compliance. Instead, the SEC's expectations will vary based on size, business type, risk profile, and other factors.[17] FINRA has taken a similar approach (while FINRA has referenced firms' use of industry standards and frameworks related to cybersecurity,[18] these materials often themselves provide significant latitude for individual firms or environments). Both the SEC and FINRA have looked at cybersecurity in connection with routine examinations and inspections, and both have published observations regarding what they view as effective programs, while again refusing to promulgate more specific, prescriptive rules. Both have repeatedly underscored, however, that they believe that firms with effective cybersecurity programs are those that conduct meaningful risk assessments and that do not regard cybersecurity compliance as the responsibility of any single department, but instead seek to address it as a matter of corporate governance, with adequate controls and appropriate supervision by firm leadership.[19]

Financial institutions therefore should be prepared to conduct — with input and advice from qualified counsel — individualized assessments of their own risks, responsibilities, and vulnerabilities based on known and emerging cyber threats, and should do so in coordination across departments, and with sufficient resources and oversight. In connection with this process, counsel should understand, and be prepared to provide appropriate and effective challenge to, the design and implementation of the firm's program, based on guidance and statements issued by any relevant regulators and self-regulatory organizations. Counsel must also be prepared to defend — in connection with routine examinations or, potentially, in the wake of a cyber incident — the process that the firm undertakes, as well as its design and implementation of key controls related to cybersecurity.

---

[16] SEC, *supra* note 14.

[17] *Id.* at 6-7; SEC Commission Statement and Guidance on Public Company Cybersecurity Disclosures, Rel. No. 33-10459, 17 C.F.R. 229 and 249, 7-8, 13-14 (Feb. 26, 2018); FIN. INDUS. REG. AUTH. (FINRA), REPORT ON SELECTED CYBERSECURITY PRACTICES (2018), https://www.finra.org/sites/default/files/Cybersecurity_Report_2018.pdf.

[18] FINRA, REPORT ON SELECTED CYBERSECURITY PRACTICES – 2018 (2018), http://www.finra.org/sites/default/files/

footnote continued from previous column…

Cybersecurity_Report_2018.pdf; FINRA, REPORT ON CYBERSECURITY PRACTICES 8-9 (2015), https://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf (discussing possible benefits from consideration of National Institute of Standards and Technology (NIST) Framework, NIST Standards, International Organization for Standardization (ISO), and International Electrotechnical Commission (IEC) Information Technology 27001 and 27002 Frameworks, among others).

[19] FINRA, REPORT ON FINRA EXAMINATION FINDINGS 2-3 (2017), http://www.finra.org/sites/default/files/2017-Report-FINRA-Examination-Findings.pdf; SEC, 2018 NATIONAL EXAM PROGRAM EXAMINATION PRIORITIES 9 (2018), https://www.sec.gov/about/offices/ocie/national-examination-program-priorities-2018.pdf.

Counsel need not be a technical expert to perform these functions. But regulators — who themselves are usually not IT professionals — will expect that the nontechnical lawyers who advise the company on cybersecurity regulatory compliance are sufficiently familiar with those issues to discuss them intelligently, and may react negatively if counsel or members of senior leadership seem wholly unfamiliar with the basic details of the firm's cybersecurity controls and defenses. Moreover, the SEC has highlighted — including in the Voya settlement and its Rule 21(a) report — that some of the most critical cybersecurity vulnerabilities and risks at present do not rely on sophisticated technology, but instead use technology to exploit weaknesses in human decision-making, and basic policies and procedures for data security.[20] While a reasonable cybersecurity program therefore will necessarily include certain technical attributes and analysis, effective minimization of risk requires careful application and analysis of nontechnical controls — including with respect to policies, procedures, and training — that do not require particular technical expertise to implement or assess.[21] Examples include requiring voice authorization for changes in wire transfer instructions, implementing regular phishing training and testing for employees, and preventing employees from using personal applications on their phones for sensitive company communications.

To the extent that technical analysis or testing is required to ensure compliance, however, counsel should be prepared to advise as to whether and when external resources should be engaged (e.g., to perform periodic penetration testing or risk assessments).[22] Counsel should carefully consider how to structure any such vendor engagements to preserve any available privileges or protections, where feasible and desirable. Counsel should also be prepared to communicate clear instructions to both vendors and internal team members regarding communication best practices and procedures to ensure clarity in the record regarding the nature and purpose of the work, and to enhance the likelihood that any claims of privilege or protection will be upheld.

[20] SEC, *supra* note 14, at 5; Voya Fin. Advisers, Inc. Admin. and Cease-and-Desist Proceedings, *supra* note 15, at 7-10.

[21] SEC, *supra* note 14, at 5-6.

[22] As FINRA has noted, many firms take a risk-based approach in determining the scope of testing and reviews that may be appropriate, and counsel may be asked to assist in selecting review based on potential legal exposure and regulatory obligations. FINRA, REPORT ON SELECTED CYBERSECURITY PRACTICES – 2018 at 13-14 (2018), http://www.finra.org/sites/default/files/Cybersecurity_Report_2018.pdf.

Oversight and Disclosures

The SEC's oversight of certain companies' cybersecurity practices reaches beyond reasonableness requirements. The SEC's February 2018 Statement and Guidance on Public Companies Cybersecurity Disclosures does not impose any significant new requirements on issuers, but its emphasis on internal reporting mechanisms and board oversight of cybersecurity provides new meaning to existing requirements.[23] The guidance focuses on public companies' obligations to make cybersecurity disclosures, including: (1) prior occurrences of cybersecurity events; (2) the probability and magnitude of potential cybersecurity events; and (3) the company's ability to prevent or mitigate such events. It also reminds companies that the antifraud provisions, which prohibit insider trading on the basis of material nonpublic information, encompass trading on information about cybersecurity risks and incidents. The SEC acknowledges that to maintain accurate disclosures and effectively assess the risks of insider trading, senior management should be informed of cybersecurity incidents as they arise. Companies therefore must facilitate the flow of information concerning such risks and incidents to senior management responsible for disclosure decisions and certifications. Counsel should participate in creating internal reporting mechanisms and procedures that establish reporting lines, and assist in determining what issues require escalation to what levels.

The SEC's guidance also requires the issuer to report on the board's oversight functions, setting the expectation that boards are actively engaged in cybersecurity issues. The SEC directs that disclosures should include "the nature of the board's role in overseeing the management" of cybersecurity risks, to the extent that the risks are material to the issuer's business. The SEC also notes that the board of directors' engagement with senior management on cybersecurity risks is indicative of the board's overall ability to discharge its risk oversight duties. Boards can fulfill their oversight obligations by asking management to report to the board on a number of issues. For instance, management could assess and report on: (1) whether a risk assessment has been conducted on the company's most sensitive electronic and hard-copy information and, if so, the results of that assessment; (2) whether the company's cybersecurity program meets

[23] SEC Commission Statement and Guidance on Public Company Cybersecurity Disclosures, Rel. No. 33-10459, 17 C.F.R. 229 and 249 (Feb. 26, 2018).

industry standards and its regulatory obligations; and (3) what cybersecurity due diligence is conducted on third parties with access to the company's sensitive data. Counsel should participate in these inquiries to ensure that the information conveyed to the board is accurate and complete, and that the board is able to discharge its duties, and to assist in the implementation of any appropriate measures arising out of the report.

Ensuring Compliance with Rules-Based Cybersecurity Requirements

Finally, in addition to being mindful of the reasonableness requirements and special circumstances of public companies, counsel must consider the potential relevance of various regulators who have promulgated specific, rules-based requirements. These approaches favor concrete measures that companies must take to be deemed compliant, largely without regard to the particular characteristics of the registrant.[24] Rather than requiring companies to meet current industry standards or best practices, rules-based cyber regulation creates them.

The most prominent recent rules-based cybersecurity regime for financial institutions is the NYDFS cybersecurity rules, which went into effect in August 2017.[25] The NYDFS rules require covered entities to adopt and maintain a cybersecurity program that must contain certain specific elements, such as a written cybersecurity policy, a written incident response plan, a chief information security office, annual penetration tests, quarterly vulnerability assessments, encryption of nonpublic information, annual certifications of compliance signed by the board of directors or a senior officer, multifactor authentication, and notifications to the NYDFS within 72 hours of certain cybersecurity events.[26] The rules also require that the company train personnel regularly, and update training to address new risks.

Because rules-based approaches like the one adopted by the NYDFS are prescriptive, they require meaningful preparation to ensure compliance. Counsel must therefore be aware of which regulatory regimes apply to the firm's various operations and activities, keeping in mind possible differences in jurisdictional criteria (including possible claims of jurisdiction based on, for example, registration, customer identities, business activities, or domicile). Counsel should also be prepared to offer advice on conflicts that may arise between efforts to satisfy fixed and aging prescriptive rules regimes versus evolving standards of "reasonableness."

ADVISING ON INCIDENT RESPONSE

Board members often cringe when hearing about the latest cybersecurity incident, and for good reason. In addition to regulatory scrutiny and loss of customer and employee goodwill, cyber breaches are now regularly resulting in significant litigation. Following Target's 2013 data breach, which exposed the credit card information of 40 million credit accounts,[27] Target was named in 50 class action lawsuits,[28] one of which alone settled for $10 million.[29] It also agreed to a $39.4

[24] Avi Gesser et al., *Standards vs. Rules for Cyber Regulation – The Eleventh Circuit Weighs in Against the FTC and in Tacit Support for the NYDFS Approach* (July 9, 2018), https://www.dpwcyberblog.com/2018/07/standards-vs-rules-for-cyber-regulation-the-eleventh-circuit-weighs-in-against-the-ftc-and-in-tacit-support-for-the-nydfs-approach/.

[25] Cybersecurity Requirements for Financial Services Companies, N.Y. CODES § 500, *et seq*. Massachusetts has also long mandated specific elements for information security programs, including secure user authentication protocols, encryption, and firewall protection. Standards for the Protection of Personal Information of Residents of the Commonwealth, 200 MASS. CODE REGS. 17.00, *et seq.* (2010). Additionally, the National Association of Insurance Commissioners has issued an Insurance Data Security Model Law that includes specific measures akin to the NYDFS rules. NAT'L ASSOC. INS. COMM'N, INSURANCE DATA SECURITY MODEL LAW (2017), https://www.naic.org/store/free/MDL-668.pdf. That law has already been adopted by South Carolina, with other states considering similar measures. Don Jergler, *The State of NAIC's Data Security Model Law*, INSURANCE MODEL (Sept. 21, 2018), https://www.insurancejournal.com/news/national/2018/09/21/500119.htm.

[26] For an event to trigger the 72-hour notice requirement, it must either create a reasonable likelihood of materially harming any part of the normal operation of the company, or require notice to be provided to any other government body, self-regulatory agency, or supervisory body.

[27] *Target Confirms Unauthorized Access to Payment Card Data in U.S. Stores*, TARGET (Dec. 19, 2013), https://corporate.target.com/press/releases/2013/12/target-confirms-unauthorized-access-to-payment-car.

[28] Amy Terry Sheehan, *Preserving Privilege Before and After a Cybersecurity Incident (Part Two of Two)*, 1 CYBERSECURITY L. REPORT 7 (2015), https://www.cslawreport.com/article/48.

[29] *Target Agrees to Pay $10 Million to Settle Lawsuit from Data Breach*, REUTERS (Mar. 18, 2015), https://www.reuters.com/article/us-target-settlement-idUSKBN0MF04K20150319.

million settlement with banks and credit unions.[30] Anthem settled consumer claims following its 2015 data breach for $115 million.[31] And the risks are only increasing. 2018 saw an uptick in cyber-related class actions,[32] in part because courts have become more and more receptive to them.[33] In addition, some of the proposed and upcoming privacy legislation in the U.S. create limited private rights of action for violations,[34] which will further contribute to the PR nightmare that companies face in the wake of a cyber incident.

Minimizing the risks that stem from a cyber event begins with careful preparation and planning prior to the occurrence of any incident, followed by levelheaded, efficient, and accountable execution of response plans. As explained further below, counsel plays a critical role in both the preparation and execution stages of incident response, and must work cooperatively with various stakeholders, including security personnel, IT, business units, public relations, human resources, compliance, the board, and management.

Planning and Preparation

The planning before a cyber incident occurs is as important to effective crisis management as the immediate response. Waiting until a cybersecurity incident occurs to decide what steps must be taken can precipitate chaos. Instead, careful consideration of issues likely to arise in the event of a cyber incident can eliminate or mitigate many of the potentially adverse consequences of the event.

Incident Response Plan. An incident response plan ("IRP") will guide the company's response to an incident and can prevent counsel or senior management from overlooking important decisions under the stress of the event. Development and maintenance of an effective IRP is not only best practice, it is often a hallmark of a reasonable cybersecurity program and may be required by certain regulatory regimes.[35] Counsel should generally ensure that there is a written IRP that: (1) includes procedures that address whom to notify in certain circumstances (which may include employees, senior management, the board, auditors, customers, vendors, insurers, regulators, investors, and the market in the event of a significant incident), and how to prioritize the timing of that notification; (2) provides for the roles of various functions (business, security, legal, information technology, human resources, etc.); (3) anticipates several different types of cybersecurity incidents; and (4) is periodically updated and tested.

Tabletop Exercises and Mock Drills. Counsel should coordinate tabletop exercises and mock incident scenarios to test the incident response plan, including notification and communication plans. The exercise will reveal the company's ability to navigate an incident before it happens, and allow executives to hone their emergency policies, procedures, and decision-making. After conducting exercises, counsel should update the incident response plan to reflect lessons learned.

Breach Notification Obligations. In addition to breach notification obligations under the Gramm-Leach-Bliley Act ("GLBA"),[36] financial firms are subject to different breach notification requirements in every U.S. state, which dictate when and how companies must disclose a cyber incident to customers, regulators, and credit reporting agencies.[37] Many, but not all, state data breach notification laws provide that compliance with the notice provisions promulgated pursuant to GLBA suffices to meet the notice requirements under the state

[30] Jonathan Stempel & Nandita Bose, *Target in $39.4 million settlement with banks over data breach*, REUTERS (Dec. 2, 2015), https://www.reuters.com/article/us-target-breach-settlement-idUSKBN0TL20Y20151203.

[31] Plaintiff's Memorandum in Support of Preliminary Approval of Class Action Settlement, *In re Anthem, Inc. Data Breach Litigation*, No. 15-MD-02617-LHK, 2017 WL 3699869 (N.D. Cali. June 23, 2017).

[32] Cara M. Peterman, *The Rise of Cyber-Related Securities Fraud Class Actions*, LAW360 (Mar. 12, 2018), https://www.law360.com/articles/1019321/the-rise-of-cyber-related-securities-fraud-class-actions; Sheehan, *supra* note 28.

[33] Some federal circuit courts have adopted a more lenient standard for standing when personally identifiable information has been exposed but there is no proof of actual harm. Stephen Forte, *Standing Considerations in Federal Data Breach Litigation*, SHIPMAN & GOODWIN (Nov. 27, 2018), https://www.dataprivacywatch.com/2018/11/2161/; Travis LeBlanc & Jon R. Knight, *A Wake-Up Call: Data Breach Standing Is Getting Easier*, 4 Cybersecurity L. Report 1 (2018), https://www.cslawreport.com/article/600.

[34] *See, e.g.*, California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.150 (effective Jan. 1, 2020).

[35] Cybersecurity Requirements for Financial Services Companies, N.Y. CODES § 500.16.

[36] Interagency Guidelines Establishing Information Security Standards, 70 Fed. Reg. 59, 15736-54 (Mar. 29, 2005) (codified as 12 C.F.R. pt. 30).

[37] ALISSA M. DOLAN, CONG. RESEARCH SERV., DATA SECURITY AND BREACH NOTIFICATION LEGISLATION: SELECTED LEGAL ISSUES 3 (2015), https://fas.org/sgp/crs/misc/R44326.pdf.

statute.[38] Counsel must determine the company's cybersecurity disclosure and breach notification obligations, and evaluate what the company will do to ensure it will meet them. Many of these obligations are not clear-cut, but require judgment to determine if the firm has taken appropriate steps to comply. For example, many obligations turn on whether the breach is likely to result in "harm" to the person whose data was compromised.[39]

Establish Regulatory Contact. Counsel should consider developing a primary contact at each relevant regulatory agency that they could contact in the event of an incident. It may be beneficial to open lines of communication early, so the company can better seek and receive guidance in the event of an incident, and be more familiar with the expectations of regulators, prior to and during an incident.

Consider Cyber Insurance. Counsel should review insurance policies to understand what kind of cyber risks are covered (e.g., legal fees, business interruption, ransom payments, equipment replacement, etc.) and whether additional risks should be considered.[40]

Ransom Payments. Companies should consider having at least an informal policy regarding cyber ransom payments, which might include a decision tree as to when, if ever, the company would consider making a payment. That way, counsel can assess the legal and other risks associated with making such payments in advance, rather than in the heat of an actual attack. If the company would consider making a ransom payment in certain circumstances, as many companies do, it should consider retaining a consultant capable of making Bitcoin or other crypto payments on short notice. In any event, counsel should develop a contact in law enforcement, such as the FBI, Department of Justice, or Homeland Security, that could assist during and after a cyber-attack.

Contractual Obligations. A company may have contractual obligations related to cybersecurity, such as an obligation to notify customers of a cybersecurity event or to maintain certain cybersecurity measures. Counsel should review contracts and determine the company's obligations, and make sure that future contracts contain obligations that are reasonable. Counsel should also explore the company's obligations to third parties and evaluate the steps it is taking to ensure that these obligations will be met.

Counsel's Role during Incident Response

Helping a company navigate the response to a significant or potentially material cyber event may be the most important and challenging responsibility of counsel related to cybersecurity compliance. At its core, counsel's role in this setting is to protect the company from the multitude of risks that may arise in the course of an incident response. As soon as possible, counsel should seek to understand the nature of the incident — including whether the event involves an on-premise breach, past or ongoing compromise of systems, or exposure of data — to make informed decisions about the likely exposure and any internal escalation that may be necessary. Although every incident will be different, and much will depend on the incident response planning performed in advance of an actual event, we have outlined below a number of key responsibilities of counsel to reduce the risk of economic harm, lawsuits, and regulatory non-compliance.

Coordinate Execution of Incident Response Plan. Counsel's role in a live incident response scenario will likely include ensuring prompt and careful execution of the firm's incident response plan. Counsel may be responsible for leading or otherwise supporting the firm's incident response team, and must try to ensure efficient, effective, and controlled coordination among its members. This will not only help reduce potential liability based on any preexisting compromise, but will also avoid creating new liability from ineffective or ill-conceived response efforts. To the extent that deviations from the written plan are necessary, rationales for those changes should be well-supported and documented to avoid ex-post claims of policy and procedure violations.

Ensure Satisfaction of Notification Obligations. Counsel will be responsible for providing advice on the company's data breach notification obligations (including contractual notice requirements), and for ensuring that such obligations are satisfied. This is a critical component of effective management of the firm's legal risks in the wake of a breach, as perceptions of late notification can have a significant impact on the public and regulatory assessments of a firm's overall incident response efforts. Counsel should be prepared to

[38] *See, e.g.*, IN ST 24-4.9-3-4(e) (Indiana) ("A financial institution that complies with the disclosure requirements prescribed by the [GLB guidance] as applicable, is not required to make a disclosure under this chapter."); OH ST § 1349.19(F)(1) (Ohio) (materially same).

[39] *See, e.g.*, ALA. CODE § 8-38-5(b); ARK. CODE § 45.48.010; WASH. CODE § 19.255.010(1).

[40] *See, e.g.*, Leslie C. Thorne, *Cyber- Security Insurance Issues in Mortgage Lending*, 34 Rev Bank. & Fin. Serv. No. 12 (Dec 2018).

provide guidance to IT and business personnel about the information needed to decide whether and when notifications are required, and the timing on which such information will need to be compiled. Counsel will likely then be responsible for generating and coordinating the delivery of the notifications to any relevant entities and individuals, as well as ensuring that senior leadership is aware of any significant notification determinations before they occur.

Manage Engagements of Outside Professionals. As soon as possible after a potential incident is identified (or otherwise as described by the firm's incident response plan), counsel should take steps to engage any necessary external resources, including outside counsel, a security or forensics consultant, or a communications or crisis management firm, if needed. As with assessments or testing performed in connection with ongoing cybersecurity risk management, counsel should take care in deciding how to structure engagements of outside professionals — particularly forensics and public relations consultants — so as to maximize the likelihood that any work performed or any communications with the third parties may be subject to attorney-client privilege or any other available protection from disclosure or discovery. Counsel should then oversee and coordinate communications between external and internal teams to ensure such privileges and protections are preserved, as discussed below.

Maintain Privilege. Depending on the nature of the incident, the role of counsel may include maintaining privilege over the investigation. Immediately after identifying a cybersecurity event, counsel should select the components of work that will be completed at their direction, including any work by third parties, and provide guidance as to the steps every employee must take to maintain privilege. Ideally, communications should reflect counsel's involvement and its purpose. Counsel should also coordinate communications with third parties, especially regulators. To maintain privilege, communications between the internal team and outside consultants and vendors should be made through counsel. This is very difficult and a frequent area of friction, as it can slow down communications when employees are working to address incident-related issues as quickly as possible. Nonetheless, counsel is responsible for ensuring that everyone — the internal team and outside consultants — understands the importance of privilege, and for rigorously maintaining it.

Manage Internal Flow of Information. In connection with overseeing the efforts of the firm's incident response team, counsel should be involved in escalation and upward reporting, particularly when required by any thresholds set out in the firm's incident response plan. Counsel should encourage and ensure team members' use of care and discretion in all written communications.

Overseeing External Communications. Counsel should also be involved in external communication flow, including with insurers, auditors, and law enforcement, to ensure consistent messaging and to avoid privilege waiver. Counsel should assess whether voluntary outreach to law enforcement and regulators is appropriate and beneficial in connection with any particular response. In addition, counsel should be involved in communications with industry threat-sharing groups. In all instances, counsel should be careful that external communications maintain business secrets, respect antitrust restrictions, and avoid possible issues related to selective disclosure.

Managing Insider Trading Risk. Company personnel who become aware of undisclosed cyber events may be in possession of material nonpublic information that will create a heightened risk of insider trading. As highlighted by the SEC's February 2018 Statement and Guidance on Public Company Cybersecurity Disclosures, counsel should ensure that steps are taken to limit such risks in the course of executing the firm's incident response process. This can be accomplished not only by limiting dissemination of nonpublic information regarding the incident, but also potentially by the implementation of trading blackout restrictions or preclearance procedures for key stakeholders that are likely to become aware of material nonpublic cyber events. It may also be helpful — depending on the nature of the incident and the analysis needed to assess potential risks — to keep a record of parties who are brought "in the tent" in the course of the response efforts.

ADVISING ON VENDOR RISK

To protect its sensitive information, companies must ensure that the vendors that have access to such information are taking reasonable steps to protect it. The FTC has shown interest in the impact of vendor relationships on firms' management of cybersecurity risks, bringing at least one action in the last year.[41] A technology company had failed to prevent its vendor

[41] *Mobile Phone Maker BLU Reaches Settlement with FTC over Deceptive Privacy and Data Security Claims*, FEDERAL TRADE COMMISSION (Apr. 30, 2018), https://www.ftc.gov/news-events/press-releases/2018/04/mobile-phone-maker-blu-reaches-settlement-ftc-over-deceptive.

from collecting and recording its customers' personal information, including communications, without the customers' knowledge. The FTC took issue with the company's failure to monitor its vendor, and the company's misleading policies that promised that customers' information would be protected from misuse. States have also demonstrated a growing interest in vendor management. Effective March 2019, the NYDFS cybersecurity rules require its regulated entities to have a vendor diligence program that includes procedures to identify and assess vendor risks, policies outlining the "minimum cybersecurity practices" and cooperation obligations required of vendors, due diligence procedures to evaluate the vendors' cybersecurity practices, and procedures to complete periodic tests of the risks and cybersecurity practices of vendors.[42] Likewise, the Colorado Division of Securities' recent cybersecurity regulations require broker-dealers and investment advisers to provide oversight of potential risks and vulnerabilities affecting vendors.[43]

Counsel can (and should) provide guidance to prevent companies from running afoul of regulations due to a vendor's actions. Companies should spell out their privacy and security expectations to vendors.[44] To ensure those expectations are met, counsel should make sure that due diligence is performed on vendors to understand how their services work, what they are afforded access to, and what must be done to conform their conduct to the promises the company has made to customers. Counsel should also review vendor contracts to ensure that vendors with access to the company's sensitive information have sufficient cybersecurity practices and insurance, will inform the company promptly of a breach, and will cooperate with the company in any breach investigation.

ADVISING ON M&A TRANSACTIONS

Cybersecurity issues impact M&A transactions, in sometimes imperceptible but significant ways. With any M&A deal, counsel is part of the team that performs due diligence to gather information needed to form a complete assessment of a company's value, including any vulnerabilities. Cybersecurity risks, however, often evade due diligence efforts and go undetected. What may begin as a minor cybersecurity vulnerability could turn into a destructive incident years later and drastically alter the perceived value of the transaction. For instance, Marriott's apparent failure to detect a data breach that began in Starwood's database two years before it acquired the company in 2016 led to the exposure of 500 million customer records.[45] Following announcement of the breach, Marriott's stock dropped 5.6% in one day. Early reports claim that Marriott could face up to $1 billion in regulatory and civil liabilities.[46]

To mitigate the risk of undetected cybersecurity events and incidents, counsel should make sure that comprehensive cybersecurity due diligence is conducted, which may include diligence on a target's critical vendors. For example, counsel should identify the types of sensitive data that the target possesses (such as credit card or healthcare data), why it is collected, where the data is stored, with whom it is shared, which jurisdictions it touches, when it will be deleted, and what steps are being taken to protect it. Counsel should also assess what new regulatory regimes may apply as a result of the merger. Merger agreement representations and warranties may need to go beyond compliance with applicable laws to include compliance with internal and external policies, contractual obligations, and industry standards, and careful consideration must be given to risk allocation in the event that an undetected breach causes significant losses post-closing. In 2019, cybersecurity and privacy risks have the potential to be just as consequential as nearly any other risk evaluated during a transaction, and need to be treated as such.

CONCLUSION

The landscape of cybersecurity compliance is changing rapidly, but what is clear is that more regulation is coming, and with it, an increased role for counsel in areas such as governance and compliance, incident response, breach notification, managing vendor risk, and mergers and acquisitions. ■

---

[42] Cybersecurity Requirements for Financial Services Companies, N.Y. CODES § 500.02.

[43] COLO. CODE REGS. § 3-704-1:51-4.8.

[44] Lesley Fair, *Lesson of BLU: Make the Right Privacy, Security Calls When Working with Service Providers*, FEDERAL TRADE COMMISSION (Apr. 30, 2018), https://www.ftc.gov/news-events/blogs/business-blog/2018/04/lesson-blu-make-right-privacy-security-calls-when-working.

[45] *Marriott Breach: Starwood Hacker Gains Access to 500 Million Customer Records*, FORBES (Nov. 30, 2018), https://www.forbes.com/sites/forrester/2018/11/30/marriot-breach-starwoods-hacker-tier-rewards-millions-of-customer-records/#565e9a9b5703.

[46] Patrick Clark, *Marriott CFO Calls $1 Billion Estimate on Cyber Breach Premature*, BLOOMBERG (Dec. 5, 2018), https://www.bloomberg.com/news/articles/2018-12-05/marriott-cfo-calls-1-billion-estimate-on-cyber-breach-premature.