FINTECH LAW REPORT
E-Banking, Payments & Commerce in the Mobile World

January/February 2018 ▪ Volume 21 ▪ Issue 1

CYBERSECURITY: WHAT EVERY BOARD SHOULD KNOW AND DO

By Paul Gupta and Ariana Y. Goodell

Paul Gupta is a partner in the Data Security and IP Litigation group of Reed Smith LLP, and he is an expert in cybersecurity, patent litigation, and trademark and copyright disputes. Ariana Goodell is an associate in Reed Smith's IP, Tech and Data group, with a focus on cybersecurity, data privacy and information governance issues.

www.reedsmith.com

While cyber attacks have become increasingly common and damaging, there is a growing awareness that corporate boards have not prioritized the prevention and mitigation of those attacks.

Ever since 2005, when some of the first major data breaches were reported, cyber attacks have been exponentially increasing the dangers to companies' operations, profits and stock values, as well as their reputations. By 2015, the total number of detected security incidents climbed to over 50 million. More recently, the May 2017 WannaCry ransomware attack, believed to be the work of cyber actors sponsored by North Korea,[1] caused severe disruption to businesses worldwide. In just a matter of two days after its release, the WannaCry ransomware affected more than 200,000 users in over 150 countries.[2] That one attack is estimated to be responsible for over $4 billion in profit losses,[3] with $1 billion of the losses taking place in the first four days due to prolonged downtime of business operations.[4] It is safe to say that all cyber experts predict that damages resulting from malware attacks will continue to dramatically increase in coming years.

On the one hand, corporate board surveys show that board members are aware of the realities and risks of cyber attacks. On the other hand, those surveys also reveal that boards are putting relatively modest resources into cyber issues. More-

IN THIS ISSUE:

Cybersecurity: What Every Board Should Know And Do 1

Big Data, Big Questions—Insurers and Advanced Data Analytics 13

Regulation and Litigation Update 20

From the Editor 31

THOMSON REUTERS®

42023363

over, our actual experiences suggest that all-too-many companies are unprepared for cyber attacks, which tells us that the highest levels of corporate leadership should be accelerating the efforts to prevent and mitigate cyber attacks.

The need to enhance corporate boards cyber preparedness has begun to receive more attention from the general press. For example, in a notable January 10, 2018 article, the Wall Street Journal reported that "Corporate boards are seeking greater insight into cybersecurity risks in the aftermath of the recent breach at Equifax Inc."[5] The article observed that as cybercriminals damage company reputations and cause tens of millions in remediation and legal costs, some boards are starting to increase cybersecurity oversight and weighing how to delegate responsibilities among directors. The article further reported, however, that despite the concerns of many directors who believe that the companies they serve are not properly protected against cyber attacks, it is uncommon to have board members or committees focused on information technology risks and strategy.

This article will discuss ways to meaningfully increase cyber resiliency by improving board membership and functions. As boards fill vacancies and search for new members, it should be a priority to add people who have working knowledge of cybersecurity vulnerabilities and best practices for mitigation. Boards should also be more assertive in developing and monitoring cyber plans, rather than relying on technical personnel. Just as boards typically have members who are capable of directing the efforts of CFOs and other financial officers, boards should also have members who are capable of directing the efforts of CIOs, CISOs, and other technical people. And, just as boards have members who are familiar with financial concepts and terminology, boards should also have at least some members who understand cyber issues and are familiar with computer terminology. It should also be noted that cyber issues are increasingly having legal aspects, as explained in this article, so it can be especially helpful to have at least one board member who is experienced with both cyber and related legal issues.

I. Six Areas Where Boards Should Provide Leadership

There are at least six areas in which boards should improve their cyber leadership:

FinTech Law Report
West LegalEdcenter
610 Opperman Drive
Eagan, MN 55123

One Year Subscription ● 6 Issues ● $ 1020.00

a. Area #1: Make Security a Team Activity

If properly directed and monitored, employees at all levels of a company can contribute to cybersecurity. Employees' data security efforts, however, need to be carefully coordinated to ensure an effective response. A lack of coordination increases the likelihood of a cybersecurity breach, and can cause a delay in identifying the breach and implementing a response. Coordinating data security efforts is important because legal, regulatory, and contractual requirements typically mandate swift responses and notifications to persons adversely affected by the breach. For instance, the General Data Protection Regulation, effective May 2018, imposes a breach notification requirement of 72 hours.

Boards should build cross-functional teams with senior management buy-in. A security team should have various stakeholders, including at minimum, the staffs of the Chief Information Officer ("CIO"), Chief Information Security Officer ("CISO"), Physical Security Head, Human Resources Head, and General Counsel. Teams' roles should be well-defined and directors should direct managers to establish clear lines of communication, raising awareness through employee training, and establishing proper escalation procedures.

b. Area #2: Monitor Employees' IT Access

Employees routinely have access to the most sensitive company and personally identifiable information ("PII"), and therefore safeguards should be in place to minimize the risk of employee-instigated breaches. Boards should enforce the process for timely termination of access to company property and networks for employees known to be leaving. Additionally, boards should curb potential wrongdoing among IT staff with frequent audits, and monitor "danger zone" employees. Danger zone employees are those who have regular access to PII. Finally, boards should implement a process for reviewing access levels in light of employees' job changes.

c. Area #3: Develop Robust Data-Mapping and Data Retention Plans

Before a company can protect its data assets and networks, the company needs to understand where that data is stored and who has access to it. In the event of a cybersecurity breach, isolating the compromised data and the devices in which it is stored is typically the first action item in an incident response.

Accordingly, directors should monitor data mapping, data retention, and disposition. This is an area of scrutiny by the U.S. Securities and Exchange Commission ("SEC"). The SEC's 2015 Cybersecurity Examination Initiative indicates that in the process of examining registered entities regarding cybersecurity matters, the SEC's Office of Compliance Inspections and Examinations will review "[f]irm policies and procedures related to enterprise data loss prevention and information related to . . . data mapping, with particular emphasis on understanding information ownership and how the firm documents or evidences PII." [6]

Over and over, reported cybersecurity breaches involve electronically stored information ("ESI") the company had no business or legal reason to retain. Directors need to focus on the issue that information assets become liabilities if they exceed their useful life. Thus, creating an accurate data map for a company is imperative.

Conducting data mapping exercises goes hand-in-hand with data retention exercises because it enables a company to identify the ESI that it no longer needs. By identifying the ESI no longer necessary to retain, the company can effectively mitigate the risk of losses associated with cybersecurity breaches of unnecessarily retained ESI.

d. Area #4: Think About What You Aren't Thinking About

Boards should direct managers to conduct a holistic review of all potential issues that impact cybersecurity preparedness. Even companies that have invested millions of dollars in cybersecurity measures, and have sophisticated IT breach prevention programs in place, can be foiled by a lack of attention to physical security. Massive losses can also be caused by third-party vendors. Third-party vendor cybersecurity is just as important as a company's cybersecurity. Boards should ensure that the company is reviewing contracts of third-party vendors and auditing the access to their network.

e. Area #5: Maintain IT Business Continuity Plans

The recent WannaCry malware attack demonstrated how disruptive a cyber incident can be to critical business operations. For example, the National Health Service in the United Kingdom was forced to cancel thousands of scheduled operations and appointments because the "WannaCry" malware threatened to delete crucial files unless the NHS paid ransoms.[7] Therefore, board members should ensure the company has an effective business continuity plan outlining defensive strategies that minimize operational downtime. Additionally, directors should direct managers to utilize employees or external resources to perform periodic assessments to evaluate the company's cybersecurity readiness.

f. Area #6: From Day One, Prepare for Litigation

Plaintiffs have been aggressively filing cases arising from significant data breaches, often as class actions. After a breach, remediation efforts will generate sensitive information that could be used by an adversary to prove negligence by directors and their companies.

However, other evidentiary privileges may apply to protect such information, notably the attorney-client privilege and the work product doctrine. For example, a recent case[8] involving a retailer and a credit card issuer demonstrates how counsel can protect remedial investigative work conducted after a data breach. The retailer sued the credit card company after it fell victim to a cyber-attack involving credit and debit card purchases at its retail stores. The retailer's general counsel hired a cybersecurity investigation firm to conduct a forensic investigation of the breach. When the credit card company requested the general counsel's records related to the investigation, the court largely denied it's discovery requests on grounds that the investigation firm was retained to aid in providing legal advice to the retailer.

To ensure an uninhibited and free flow of communication amongst the IR team, boards should have procedures to ensure that a lawyer is involved in all stages of incident response ("IR") work, including the preventative efforts (e.g., cybersecurity policy development and internal auditing), and remedial efforts to respond to a cybersecurity breach. The IR team should also have their outside partners on retainer. [9] Addition-

ally, the team should take care to preserve metadata and "chain of custody" information, and should have litigation holds in place.

II. Regulatory and Litigation Background

Federal and state agencies are increasingly taking regulatory enforcement action against companies for their cybersecurity failings. Additionally, a number of derivative lawsuits have been filed against companies related to cybersecurity and privacy breaches. Many claims have been dismissed because the company was found to have made a reasonable business judgment at the board level regarding cybersecurity. With the increase of regulatory enforcement and derivative suits, it is important that boards are involved in their company's cybersecurity plan.

a. SEC Enforcement

The SEC considers cybercrime to be "the greatest threat" to U.S. markets.[10] The new SEC chairman Jay Clayton stated during his Senate confirmation hearing that he was of the opinion that public companies are not adequately disclosing information pertinent to cybersecurity.[11] Additionally, Mr. Clayton said he supported legislation that would require companies to disclose whether any board members have particular cybersecurity experience, and added he believed investors should know how boards are dealing with cyber issues.[12]

> *"I think cybersecurity is an area where . . . I don't think there is enough disclosure in terms of whether there is oversight at the board level that has a comprehension for cybersecurity issues. I believe that is something that investors should know, whether companies have thought about the issues, whether it's a particular expertise at the board or not. I agree it's something companies should know. It's a very important part of operating a significant company, and any significant company has cyber risk issues."*[13]

The SEC recently signaled it would bring cases over public company disclosures of cyber security risks and data breaches, which may include enforcement actions against directors.

The SEC has already brought several actions against registered investment firms for cybersecurity failings. For example, in 2015, a major investment firm R.T. Jones was charged with failing to establish the required cybersecurity policies and procedures in advance of a breach. The breach compromised the personally identifiable information (PII) of approximately 100,000 individuals, including thousands of the firm's clients.[14] Without admitting or denying the findings, the firm settled and agreed to cease and desist from committing or causing any future violations of Rule 30(a) of Regulation S-P. The firm also agreed to be censured and pay a $75,000 penalty.[15]

Because stock price can be significantly impacted by the occurrence of a cyber-incident, directors should assume that both regulators and plaintiffs' counsel will be more likely to challenge both nondisclosure of cybersecurity breaches or vulnerabilities and insufficient implementation of an IR plan. Directors should consider this increased risk of a regulatory challenge in developing adequate plans.

b. Other Federal & State Enforcement Activities

Other federal agencies, including the Department of Treasury and New York State agencies are also aiming to implement regulations to enforce board involvement in cybersecurity. In an Advance Notice of Proposed Rulemaking

("ANPR"), the U.S. Department of Treasury sought public comment on standards that would require the nation's largest banks to improve their cybersecurity governance, including board-level approvals and "expertise in cybersecurity."[16] The comment period ended January 17, 2017, and bank regulators will use information collected from the ANPR to develop a more detailed proposed rule that will be published for public comment at a later date. A new proposed rule is still forthcoming.

New York's Department of Financial Services has implemented cybersecurity regulations with unprecedented requirements that exceed existing federal and state cyber regulation. These requirements include a board review of a required 14-point comprehensive cybersecurity policy and written certification from a senior corporate officer.[17] New York's recent adoption of these regulations demonstrates an ongoing shift in public policy towards a more expansive approach to cybersecurity. It is anticipated that other states will implement similar regulations in the near future.[18]

c. Litigation

Many shareholder derivative lawsuits have been filed against directors and officers alleging claims for breach of fiduciary duty, or even securities fraud, relating to the data breach.[19] The claims typically follow a similar fact pattern in which the plaintiff alleges that the company breached its fiduciary duties by failing to implement a system of internal controls to protect customers' personal and financial information, and by causing or allowing the company to conceal the data breaches from investors. The Chamber of Commerce reports that four law firms, including Edelson PC and Lieff Cabraser Heimann & Bernstein LLC, are asserting the majority of the privacy and cybersecurity-related lawsuits against boards in an effort to take advantage of this evolving legal landscape.[20] Many plaintiffs' claims have been dismissed for failing to meet the required standard of care because the defendant companies were found to have made reasonable business judgements regarding cybersecurity. These judgments include having security measures in place pre-breach, changes enacted post-breach, and management's reports to the board's audit committee and corporate responsibility committee covering the company's data security measures.

III. Analyses to Date of Cyber Board Issues

Over the past three years, organizations like ISACA, Korn Ferry, SpencerStuart, and World Economic Forum have taken a particular interest in the board's role in cybersecurity. The following reports analyze how comfortable boards currently are with cybersecurity and what their role is as leaders of a company.

a. 2014 ISACA Report

In 2014, ISACA and The Institute of Internal Auditors Research Foundation issued the report *Cybersecurity: What the Board of Directors Needs to Ask.* The report was prompted by the Institute of Internal Auditors Audit Executive Center's "Pulse of the Profession 2014" survey which indicated that while 65% of board members perceive cybersecurity as a high risk, only 14% of board members reported that they were actively involved in specific actions related to cybersecurity.[21] The report highlights that board members need to be aware of potential cyber threats, and how to properly defend against them.

According to the report, boards should be familiar with the management of security governance, and the company's incident response protocol.[22] Boards also need to be aware of the company's security framework (i.e. HIPAA, PCI-DSS, etc.), and persistent internal and external cyber threats.[23] Potential cyber threats include: employees bring their own device ("BYOD") and smart devices, disaster recovery and business continuity, periodic access reviews, and log reviews.[24]

Cloud computing and third party outsourcing are also risks that the board should be aware of. Cloud computing includes internet solutions that the company uses day-to-day. The solutions may be salesforce.com, box.net, or Microsoft 365.[25] Instead of cloud computing, companies may outsource critical business processes, like payroll, accounts payable, and accounts receivable to a third party. Boards should be aware that the lack of control surrounding third-party services can pose a serious cybersecurity risk to the company.[26]

The ISACA report also introduces the three lines of defense concept. This concept helps the board and company defend against potential cyberattacks.[27] There are two actors responsible for the three lines of defenses, the senior management and the board. The senior management is on the first line of defense. They are responsible for the implementation of cybersecurity policies and standards, and the day-to-day monitoring of the networks and infrastructure.[28] The CISO is in the second line of defense. The CISO is responsible for governing the financial control, security, risk management, quality, inspection, and compliance of the company. They must ensure that the appropriate monitoring, reporting, and tracking are being performed by IT operations. [29] Finally, both the senior management and the board are on the third line of defense. Both of these actors are responsible for the internal audit that ensures that the first and second lines of defense are functioning properly.[30] It is important that the senior management and the board should work together to implement the internal audit.[31]

b. 2015 Korn Ferry Report

With cyberattacks on the rise, Korn Ferry issued the report, *Navigating the Digital Age: The Definitive CyberSecurity Guide for Directors and Officers,* to help boards prepare for cybersecurity.[32] Cybersecurity is a new role for directors, many of whom feel unequipped to deal with it because it does not relate to traditional areas of director expertise. Therefore, it is important that companies ensure that everyone on the board is speaking the same language when it comes to cyber threats and security.[33] Once cyber threats have been identified as a critical risk, it must be managed with the same rigor and processes applied to other risks and remain visible on director's dashboards, with key, comprehensible metrics.[34] The board's most important role lies in asking the right questions, which may require business smarts and good old-fashioned common sense but not necessarily technical cybersecurity expertise.[35] The right questions can help ensure that there is alignment from the top and that the company has a firm grasp on cybersecurity.[36]

Besides asking the right questions at board meetings, there are three other practical ways that boards can be on the front lines of cybersecurity. First, when appointing new board members, boards should look at candidates who are knowl-

edgeable in cybersecurity.[37] Secondly, the board should be involved when senior management creates and employs robust prevention, detection, and response plans.[38] Finally, boards should stay in communication with the executive level management and continue to monitor cybersecurity in metrics.[39]

c. 2016 SpencerStuart Survey

In 2016, SpencerStuart released their inaugural *2016 Global Board of Directors Survey.* The comprehensive survey looks at what board directors think when it comes to the company's risks, and board's strengths and weaknesses. Board directors are taking a more strategic, dynamic, and responsive role with the proliferation of cyberattacks.[40] These attacks, which can cause a company financial loss and reputational damage, increase the scope of risk oversight.[41] The key findings of the SpencerStuart survey include what boards think their awareness and readiness for cyberattacks are, the political issues most relevant to the board, and challenges the board faces in achieving strategic objectives.

Board directors globally express the most concern about regulatory and reputational risk, followed by cybersecurity. This is compared to their concerns about activist investors and supply chain risk.[42] When asked to indicate the level of concern and level of readiness the company has in place on a scale from 1-5, companies on average rate the risk and readiness of cybersecurity to their company as a 3.2.[43] This means that on average companies view cyberattacks as a moderate to great threat. Similarly, on average, companies are moderately to greatly prepared for cyberattacks.[44] Furthermore, the average board rates their board processes for cybersecurity as a 3.0.[45] Meaning the board views their board process for cybersecurity as average.

Board directors indicated that cybersecurity is one of the three most relevant political issues. 39% of board directors viewed cybersecurity as a relevant political issue.[46] That is third to the regulatory environment (59%) and the economy (65%).[47] Interestingly enough, only 9% of board directors view cybersecurity as a challenge in achieving the company's strategic objectives.[48] This is compared to attracting and retaining top talent, which 41% of directors view as a challenge.[49]

d. 2017 NACD Director's Handbook on Cyber-Risk Oversight

Due to the increased focus on the board's role in cybersecurity oversight, the National Association of Corporate Directors ("NACD") published an updated handbook with guidance for officers and directors on managing cybersecurity risks.[50] The NACD identified five action items it believes all corporate boards should consider as they seek to enhance their oversight of cyber risks. These action items include:

1. Understand and approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue.
2. Understand the legal implications of cyber risks as they relate to their company's specific circumstances.
3. Gain adequate access to cybersecurity expertise, and discussions about cyber-risk management should be given regular and adequate time on the board meeting agenda.
4. Set the expectation that management will

establish an enterprise-wide cyber-risk management framework with adequate staffing and budget.

5. Board-management discussion of cyber risk should include identification of which risks to avoid, accept, mitigate, or transfer through insurance, as well as specific plans associated with each approach.[51]

e. 2017 World Economic Forum Report

With companies now using technology and the internet to meet their business needs, the World Economic Forum has been working to ensure business leaders are aware of the inherent risks of such technology.[52] The World Economic Forum believes in two main ideas when it comes to cybersecurity. The first idea is that leadership has a vital role in securing resilience against cyberattacks. Secondly, company leaders need a mindset that goes beyond cybersecurity to build a more effective cyber strategy and incorporate it into the overall strategic plan.[53] In the report, *Advancing Cyber Resilience Principles and Tools for Boards,* the World Economic Forum gives boards 10 principles to effectively deal with cyber challenges and to implement cyber resilience.

The first principle is taking responsibility for cyber resilience. The board should take on ultimate responsibility for oversight of cyber risk and resilience. The board may decide to delegate the oversight committee to an existing committee, or to a new committee.[54]

The second principle is taking command of the subject. When new board members join, they should receive cyber resilience training and ongoing updates on threats and trends. Board directors should also receive advice and assistance from an independent expert at the board's request.[55]

The third principle is appointing an experienced accountability officer. This officer is responsible for reporting to the board the company's capabilities, management, and implementation of cyber resilience.[56]

The fourth principle is integrating cyber resilience into the company's strategic plan. This includes integrating cyber resilience into the budget and resource allocation.[57]

The fifth principle is assessing and being aware of the company's risk appetite and tolerance. It is important that the risk appetite is aligned with the company's strategic plan, regulatory requirements, and the appropriate industry benchmarks.[58]

The sixth principle is holding management responsible for assessing and reporting risks, threats, and events. This should be a standing agenda item during board meetings.[59]

The seventh principle is to ensure that management supports the accountability officer with the creation, implementation, testing, and ongoing monitoring of cyber resilience plans. All of which should be reported regularly to the board.[60]

The eighth principle is creating a community with the company's stakeholders. It is important management collaborates with stakeholders appropriately to ensure systemic cyber resilience.[61]

The ninth principle is ensuring that an independent review is carried out annually.[62]

Finally, the tenth principle is reviewing the

board's performance in implementing cyber resilience to ensure effectiveness.[63]

IV. Board of Directors Cybersecurity Readiness Checklist

The average board is uncomfortable with the topic of cybersecurity. However, being familiar with the topic is crucial in an age where cyberattacks carry a significant risk. Below is a checklist of what boards should do to help them be proactive and secure in the cyber world.

1. Ensure Knowledge Among the Board and Staff

- Does the company have a staff that is the company's security lead?
- Does our Board of Directors have at least one director that has knowledge and expertise in cybersecurity?

2. Understand Current and Potential Resources

- What is IT's budget?
- What does the IT management team look like?
- Would the company benefit from having a privacy committee?

3. Assess Risk

- What information does the company collect from its customers, suppliers, etc.?
- What is the company's IT infrastructure?
- Does the company use IT outsourcing? If so, how is the information handled by third parties?
- What are the IT benchmarks and regulations in the company's industry?
- What is the risk exposed to the information we collect both internally and externally?
- What are the holes that need to be patched to ensure that the information we collect is secure?
- Conduct an on-going risk assessment

4. Implement New Policies

- Writing and implementing policies and procedures
  - Write and implement a prevention plan
    - How will the company protect the information the company collects from cyberattacks?
    - What are the specific strategies and procedures that will be/are implemented?
  - Write and implement an incident response plan
    - How will the company handle a cyberattack?
    - What are the specific strategies and procedures that will be/are implemented?

5. Review Insurance Coverage and Insure Liabilities Relating to Cyber Attacks

- Does the company's insurance policy cover data privacy breaches?
- Does the company's insurance policy cover cybersecurity risks?
- Try to secure "business interruption coverage" which includes:
  - Systems Failure

- Cyber Extortion
- Digital Asset Restoration
- Contingent Business Interruption Coverage

ENDNOTES:

[1] Ellen Nakashima, *The NSA has linked the WannaCry computer worm to North Korea*, Washington Post (1970), http://wapo.st/2s2G1Gg?tid=ss_tw-bottom&_utm_term;=.50891976d352 (last visited Aug 11, 2017).

[2] *Ransomware cyber-attack threat escalating - Europol*, BBC News (2017), http://www.bbc.com/news/technology-39913630 (last visited Aug 11, 2017).

[3] Jonathan Berr, *"WannaCry" ransomware attack losses could reach $4 billion*, CBS News (2017), http://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/ (last visited Aug 11, 2017).

[4] *Ransomware Damage Costs $5 Billion in 2017, Up from $350 Million in 2015*, Cybersecurity Ventures (2017), http://cybersecurityventures.com/ransomware-damage-report-2017-5-billion/ (last visited Aug 11, 2017).

[5] Joann S. Lublin & AnnaMaria Andriotis, Boards Seek Bigger Role in Thwarting Hackers The Wall Street Journal (2018), https://www.wsj.com/articles/boards-seek-bigger-role-in-thwarting-hackers-1515596400 (last visited Jan 17, 2018).

[6] Office of Compliance Inspections and Examinations ("OCIE"), *OCIE's 2015 Cybersecurity Examination Initiative*, Volume IV, Issue 8, Sept. 15, 2015, *available at* https://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf

[7] Alex et al., Why 'WannaCry' Malware Caused Chaos for National Health Service in U.K. NBCNews.com (2017), http://www.nbcnews.com/news/world/why-wannacry-malware-caused-chaos-national-health-service-u-k-n760126 (last visited Aug 16, 2017).

[8] *Genesco, Inc. v. Visa U.S.A., Inc.*, 302 F.R.D. 168 (M.D. Tenn. 2014).

[9] Reed Smith developed a first-of-its-kind tool designed to help companies clarify their notification strategy in response to a data loss incident. For more information, please visit: www.BreachRespondeRS.com.

[10] Carmen Germaine, *SEC Poised To Turn Cybersecurity Focus Into Enforcement,* LAW 360 (Jul 17, 2017, 4:18 PM), https://www.law360.com/articles/937197/sec-poised-to-turn-cybersecurity-focus-into-enforcement.

[11] Clayton Backs Improvements to Cybersecurity Disclosures, Thomson Reuters Tax & Accounting (2017), https://tax.thomsonreuters.com/media-resources/news-media-resources/checkpoint-news/daily-newsstand/clayton-backs-improvements-to-cybersecurity-disclosures/ (last visited Aug 11, 2017).

[12] Id.

[13] SEC Nominee Jay Clayton Defends Prior Work Lawyer Goldman Sachs, Mar 23 2017, C-SPAN.org, https://www.c-span.org/video/?425840-1%2Fsec-nominee-jay-clayton-defends-prior-work-lawyer-goldman-sachs&_start;=7116 (last visited Nov 28, 2017).

[14] *SEC Charges Investment Adviser With Failing to Adopt Proper Cybersecurity Policies and Procedures Prior To Breach*, SEC (Jul. 2.3, 2017, 4:18 PM), https://www.sec.gov/news/pressrelease/2015-202.html.

[15] Id.

[16] Alejandro H. Cruz, Craig A. Newman & Michael F. Buchanan, *Cyber in the Board Room: Balancing Risk and Oversight,* PATTERSON BELKNAP (Jul. 18, 2017, 4:28 PM), https://www.pbwt.com/privacy-and-data-security/data-security-law-blog-2/cyber-board-room-balancing-risk-oversight/.

[17] *Id.*

[18] Michael Krimminger & Cleary Gottlieb Steen, *New York Cybersecurity Regulations for Financial Institutions Enter Into Effect*, HARVARD LAW SCHOOL FORUM ON CORPO-

RATE GOVERNANCE AND FINANCIAL REGULATION (Jul. 26, 2017, 2:58 PM), https://corpgov.law.harvard.edu/2017/03/25/new-york-cybersecurity-regulations-for-financial-institutions-enter-into-effect/.

[19]*See, e.g.*, *Palkon v. Holmes*, 2014 WL 5341880 (D.N.J. 2014).

[20]Engineered Liability: The Plaintiffs' Bar's Campaign to Expand Data Privacy and Security Litigation, Institute for Legal Reform, http://www.instituteforlegalreform.com/research/engineered-liability-the-plantiffs-bars-campaign-to-expand-data-prviacy-and-security-litigation (last visited Nov 21, 2017).

[21]THE INSTITUTE OF INTERNAL AUDITORS RESEARCH FOUNDATION 6, CYBERSECURITY: WHAT THE BOARD OF DIRECTORS NEEDS TO ASK (2014).

[22]*Id.* at 14.

[23]Id.

[24]*Id.*

[25]*Id.* at 9.

[26]Id.

[27]*Id.*

[28]*Id.* at 16.

[29]Id.

[30]*Id.*

[31]Id.

[32]KORN FERRY, Navigating the Digital Age: The Definitive CyberSecurity Guide for Directors and Officers (2015).

[33]*Id.* at 2.

[34]*Id.*

[35]*Id.* at 3.

[36]*Id.* at 2.

[37]*Id.* at 5.

[38]Id.

[39]Id.

[40]SPENCERSTUART, 2016 GLOBAL BOARD OF DIRECTORS SURVEY 2 (2016).

[41]*Id.*.

[42]*Id.*at 18.

[43]*Id.*

[44]Id.

[45]*Id.* at 21.

[46]*Id.* at 16 - 17.

[47]Id.

[48]*Id.*at 19 - 20.

[49]Id.

[50]NACD Director's Handbook on Cyber-Risk Oversight, NACD - National Association of Corporate Directors (2017), https://www.nacdonline.org/Store/ProductDetail.cfm?ItemNumber=10687 (last visited Nov 21, 2017).

[51]Id.

[52]WORLD ECONOMIC FORUM, ADVANCING CYBER RESILIENCE PRINCIPLES AND TOOLS FOR BOARDS 3, (2017).

[53]*Id.* at 4.

[54]*Id.* at 8.

[55]Id.

[56]Id.

[57]Id.

[58]Id.

[59]Id.

[60]Id.

[61]Id.

[62]Id.

[63]Id.

FROM THE EDITOR

Katie Wechsler

This issue of *FinTech Law Report* offers practical advice and valuable insights for those in the FinTech space.

Cyber and Boards

First, Paul Gupta and Ariana Goodell of Reed Smith focus on how boards of directors should approach cybersecurity. Cybersecurity is a top priority and concern for companies across a wide variety of industries, and that needs to be reflected at the board level, with directors that have working knowledge of cybersecurity along with careful and thoughtful oversight of the company's cyber policies and procedures.

Mr. Gupta and Ms. Goodell focus on six areas related to cyber where a board should provide leadership: (1) make security a team activity; (2) monitor employees' IT access; (3) develop robust data-mapping and data retention plans; (4) think about what you aren't thinking about; (5) maintain IT business continuity plans; and (6) from day one, prepare for litigation. This article also looks at state and federal enforcement and litigation, highlighting the importance of board's involvement in their company's cybersecurity plan. Mr. Gupta and Ms. Goodell highlight three reports from different organization which analyze how comfortable boards currently are with cybersecurity and what their role is as leaders of a company. Finally, if that wasn't enough practical and worthwhile guidance, the article concludes with a board of directors cybersecurity readiness checklist. This article, complete with pragmatic advice, should be required reading for anyone serving or considering serving as a director of a company, as well as for those supporting those directors.

InsurTech

Next, Bridget Hagan of The Cypress Group provides a thorough and thoughtful look at the role of big data and advanced data analytics in the insurance field. Ms. Hagan details ways in which insurance companies are utilizing big data, innovation, and technology to improve outcomes for consumers and industry. While these advancements are positive for insurers and policyholders, as they can improve the customer experience, increase efficiencies, and reduce costs, they are not without cause for concern. The article provides a comprehensive review of what concerns regulators, on a state, federal and international level, have raised, including privacy issues, and the potential for intentional and unintentional discrimination. These concerns need to be understood and carefully thought through and mitigated to ensure big data and analytics can achieve the positive outcomes they promise. This is not just true for those in insurance, but for anyone using or contemplating using big data.

With big data comes big responsibility, and Ms. Hagan's article is useful for those in the insurance field as well as anyone considering the use and implications of big data and analytics.

Regulation and Litigation Update

Finally, this issue features the always comprehensive and thoughtful review of updates in regulation and litigation affecting FinTech by Duncan Douglass and Samuel Boro of Alston & Bird. In this article, Messrs. Douglass and Boro cover a wide range of FinTech issues, including payments, credit cards, digital currency, the federal chartering of FinTechs, and antitrust

issues. As they do in every *FinTech Law Report* issue, the authors parse through a significant amount of litigation and regulation to provide readers with the most important and significant developments.

Editorial Board

FINTECH LAW REPORT

West LegalEdcenter
610 Opperman Drive
Eagan, MN 55123

FIRST CLASS
MAIL
U.S.POSTAGE
PAID
WEST

FINTECH LAW REPORT

West LegalEdcenter
610 Opperman Drive, Eagan, MN 55123
Phone: 1-800-344-5009 or 1-800-328-4880
Fax: 1-800-340-9378
Web: http://westlegaledcenter.com

THOMSON REUTERS

YES! Rush me ***FinTech Law Report*** and enter my one-year trial subscription (6 issues) at the price of $1,020.00. After 30 days, I will honor your invoice or cancel without obligation.

Name _____

Company _____

Street Address _____

City/State/Zip _____

Phone _____

Fax _____

E-mail _____

METHOD OF PAYMENT

❑ BILL ME

❑ VISA ❑ MASTERCARD ❑ AMEX

Account # _____

Exp. Date _____

Signature _____

Postage charged separately. All prices are subject to sales tax where applicable.