SQUIRE PATTON BOGGS

CYBERSECURITY CONCERNS UNDERPIN CONTINUED PUSH IN THE REGULATORY AND LEGAL ARENAS

While Congress continues its aggressive push on cybersecurity legislation, regulatory oversight and legal efforts continue across the spectrum of industries effectively filling the gap in addressing now every day concerns over cybersecurity, data protection, data security and privacy issues.

The daily updates on wide-ranging cybersecurity attacks are creating a new and increased regulatory, legal and compliance focus on companies and what actions are being taken to protect consumers and shareholders. While the recently issued Cybersecurity Framework is voluntary, it makes clear that the C-Suite and Boards/Directors have a specific responsibility to be involved in the oversight and implementation of cybersecurity risk management.

As a result, we are seeing increased activity from a host of key regulatory institutions including:

- Securities and Exchange Commission (SEC) and the SEC Investor Advocate Office
- Federal Financial Institutions Examination Council (FFIEC)
- Federal Trade Commission (FTC)

The Securities and Exchange Commission Continues Call for Increased Cybersecurity Efforts From the C-Suite:

SEC Commissioner Calls on Direct Engagement from Boards of Directors on Cyber Risks

The SEC continues to steadily deliver the message to all boards and Directors that cybersecurity is a responsibility for all corporations. SEC Commissioner Luis A. Aguilar recently delivered a speech at the New York Stock Exchange titled "Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus" and, speaking in his personal capacity, expressed his belief that proper risk management of emerging cyber-threats is the responsibility of corporate boards of Directors. He also noted that the SEC will become increasingly interested in how boards respond to these threats. Given the severity of the risk, boards must go beyond the minimum industry standards to develop proactive policies to address cyber-threats.

In response to these new and emerging cyber-threats, Commissioner Aguilar suggested that boards learn from the National Institute of Standards and Technology's (NIST) "Framework for Improving Critical Infrastructure Cybersecurity" as well as:

- Promote mandatory education for all board members;
- Require a certain number of board members with technological expertise;
- Create a separate, cyber-threat risk committee similar to the risk committees required for financial institutions under the Dodd-Frank Act; and
- Fund management positions dedicated to privacy and cybersecurity, such as a chief information security officer.

Furthermore, he established that having a clear, well-developed cyber-risk policy and management structure will help companies respond effectively and quickly when cyber-attacks occur. He also reiterated that the SEC's responsibility is to protect "the integrity of the capital markets infrastructure," which cyber-attacks and the threat of cyber-attacks endanger.

SEC Calls for Comments Following Cybersecurity Roundtable

As a follow-up to the SEC Cybersecurity Roundtable earlier this year, the SEC issued a call for comments from the private sector. The SEC is still collecting comments about the issues and challenges that cybersecurity raises for market participants and public companies and how they are addressing these concerns. Interestingly, comments from industry were relatively limited but focused on the benefits of sound internal controls and procedures to limit companies' exposure to malware and viruses, as well as the need to raise awareness of cyber risk and the inherent business risk associated with not having strong cybersecurity systems in place.

Investor Advocate Office Will Review Cyber-Threat Protections

The Dodd-Frank Wall Street Reform and Consumer Protection Act established the Office of the Investor Advocate at the SEC (the "Office"). The Office is tasked with promoting the interests of investors, including how they are impacted by and may benefit from changes to SEC or other self-regulatory organization regulations.

In its inaugural report to the Congress on its annual objectives released on June 30, the Office acknowledged that "[a]s markets and financial services have become increasingly automated, investor protections have not kept pace with technological evolution." During Fiscal Year 2015, the Office plans to:

- Survey efforts by the SEC, the Financial Industry Regulatory Authority, the stock exchanges, alternative trading systems, and other market participants to protect investors from cyber-threats;
- Examine the SEC's Regulation Systems Compliance and Integrity (SCI), a proposed rule requiring key market participants to establish comprehensive policies and procedures regarding their technology systems; and
- Consider other improvements that may benefit investors and protect them against cyber-threats.

Federal Financial Institutions Examination Council's (FFIEC) Cybersecurity Assessment Program Benefiting Smaller Institutions

The FFIEC has taken seriously its role in addressing cybersecurity concerns and has embarked upon a series of efforts to address these issues. In its interagency role working with the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Consumer Financial Protection Bureau (CFPB), and other bodies, the FFIEC recently announced a series of actions:

- In June 2014, the FFIEC created a Cybersecurity and Critical Infrastructure Working Group "to enhance communication among the FFIEC member agencies and build on existing efforts to strengthen the activities of other interagency and private sector groups."
- The FFIEC has also embarked on an effort that includes "assessing and enhancing the state of industry preparedness and identifying gaps in the regulators' examination procedures and training that can be closed to strengthen the oversight of cybersecurity readiness."
- The FFIEC has also announced the launch of its cybersecurity assessment pilot program, aimed at 500 community banks. The assessments will be conducted by state and federal regulators during regularly scheduled institution examinations, including of those banks with less than US$10 billion in total assets, as well as limited-purpose chartered institutions. The assessments will focus on:
  - Threat intelligence and collaboration;
  - Cybersecurity controls;
  - Service provider and vendor risk management; and
  - Cyber-incident management and resilience.

Third Circuit to Review FTC's Authority to Regulate Data Security Practices in Latest *Wyndham* Case Development

The Federal Trade Commission (FTC) has long engaged in enforcement activities against companies for alleged lapses in their data security controls and violations of their privacy policies, under its FTC Act, Section 5 authority to regulate "unfair" and "deceptive" trade practices. However, the FTC's authority to do so has come under increasing scrutiny. Most prominently, Wyndham Hotels and Resorts LLC has taken action in federal court challenging such enforcement activities against it and several related entities, stemming from a series of cyber-attacks and data breaches that allegedly resulted in some US$10.6 million in payment card fraud.

Just recently, on July 29, the Court of Appeals for the Third Circuit agreed to hear Wyndham's interlocutory appeal from the U.S. District Court of New Jersey regarding two key issues: (1) whether the FTC's Section 5 authority can support an unfair practices claim based on data security practices; and (2) whether the FTC is obligated to formally promulgate data security regulations before bringing such claims. When granting Wyndham leave to seek the immediate appeal, the District Court emphasized the lack of current legal authority and "the nationwide significance of the issues in this action-which indisputably affect consumers and businesses in a climate where we collectively struggle to maintain privacy while enjoying the benefits of the digital age." On the same day, District Court Judge Esther Salas rejected Wyndham's request to dismiss claims against Wyndham Worldwide Corp. and two additional entities, holding that at this stage the FTC's "allegations support a common-enterprise claim."

Seeking "much needed clarity," timely resolution, and greater certainty regarding data security regulation, several prominent business groups filed an *amici curiae* ("friend of the court") brief that urged the Third Circuit to take up these business-critical issues, including the Chamber of Commerce of the United States of America, the American Hotel & Lodging Association (AH&LA), and the National Federation of Independent Business (NFIB).

The *Wyndham* case will undoubtedly impact a variety of organizations (and their affiliates) and could embolden further data security actions by the FTC. Moreover, if the FTC is not required to promulgate specific data security regulations, then a clear understanding of the Commission's past data security enforcement actions, along with current cybersecurity best practices, will be even more critical to any organization's establishing and maintaining a data security program that regulators and courts are willing to view as "reasonable."

Contacts

Norma M. Krayem
T +1 202 457 5206
E norma.krayem@squirepb.com

Samuel Rosenthal
T +1 646 557 5185
E samuel.rosenthal@squirepb.com

Mel M. Gates
T +1 303 894 6111
E melodi.gates@squirepb.com

Ludmilla L. Savelieff
T +1 202 457 5125
E ludmilla.savelieff@squirepb.com

Amy F. Davenport
T +1 202 457 6528
E amy.davenport@squirepb.com

Samantha A. Martin
T +1 202 457 6314
E samantha.martin@squirepb.com