SFG | SHARED ASSESSMENTS

Briefing Paper

The Board's Role in Realizing Effective Risk Management

Executive Summary

- Recent Equifax and Facebook incidents demonstrate the extent to which some boards are failing in their responsibilities to provide the last line of defense by assuring that critical risk management processes are fully functional within the organization. The Equifax board ignored signals that its risk management capabilities were clearly inadequate.[i] Facebook misled its customers about the extent to which the company's third parties could access and utilize their personal information.[ii]
- Boards can take the following actions to assure effective risk management oversight:
  - Ensure that board members understand why and how robust risk monitoring is required to achieve organizational strategic goals and overall success.
  - Nominate board executive(s) with appropriate risk management background.
  - Establish a board risk committee or group that oversees all risk management activities enterprise-wide and advises the full board around risk-related decisions.
  - Designate a Chief Risk Officer (CRO) to represent the risk committee and oversee risk-related issues.
  - Regularly review all aspects of risk monitoring processes to ensure they are effectively and efficiently meeting organizational needs.

Introduction

In practice, company governing boards are the last line of defense in ensuring that critical risk management processes are fully functional within the organization. However, best practices dictate that boards more actively evaluate risk management practices to ensure that enterprise risk management programs are effective. Recent high profile incidents, such as those at Equifax and Facebook, highlight the important role that the board must play to mitigate risks. These events serve as a stark example of why boards must become proactive in their risk management oversight role.

Moody's May 2019 downgrade of credit reporting agency Equifax from "stable" to "negative" should serve as a wake-up call to boards everywhere. In the case of Equifax, an engaged board should have recognized key risk monitoring gaps and directed the organization to take steps to better manage cybersecurity risks, reduce the likelihood of a data breach and improve response time and resiliency when a breach occurs.

Important news for boards, beyond the recent $5 billion Federal Trade Commission (FTC) penalty against Facebook, are the requirements in the consent order that stipulate a restructuring of the company's board to compensate for previous oversight lapses and to hold the company accountable for its privacy practices. [iii] Crucially, industry experts see the FTC's 20-year settlement order with Facebook as the new model for future offenders. Engaged boards should ensure that the organization's risk monitoring strategies and tactics are appropriate to protect the organization.

Cases In Point - Equifax and Facebook

Equifax Settlement

The Equifax board had ample warning that its cybersecurity risk management processes were substandard. One full year before Equifax disclosed the 2017 breach that compromised the private information of 145.5 million consumers, Morgan Stanley Capital International (MSCI), one of two major and independent index providers, warned of signs that Equifax was failing to protect its credit reporting data.

MSCI analysts reviewed Equifax company records and found no evidence of regular cybersecurity audits, employee training to recognize risks or management plans to respond to a risk event. Equifax scored "zero" on MSCI's privacy and data security measures and was removed from the family of MSCI indexes that select stocks use to base how well companies perform. The Wall Street Journal (WSJ) reported that MSCI's report concluded that Equifax was ill-prepared to face the "increasing frequency and sophistication of data breaches."[iv]

On July 20th 2019, a federal court in Atlanta gave preliminary approval regarding a settlement by Equifax of up to $650 million, which is the largest ever settlement specific to a single data breach by the Federal Trade Commission. The agreed upon settlement resolves pending class-action lawsuits and federal and state investigations tied to the breach.[v] This settlement is in addition to the estimated hundreds of millions of dollars that Equifax has already spent on improving technology systems and on free credit report monitoring services for individuals impacted by the breach. The data breach and the company's handling of the incident also led to Equifax's Chief Executive leaving the company and seriously damaged the company's reputation.

Figure 1: MSCI ESG Rating Timeline of Equifax Before the Data Breach

Source: Used with permission from The Wall Street Journal, WSJ.com. Copyright 2019. Dow Jones & Company, Inc. All rights reserved.
Note: ESG is an acronym for "Environmental, Social and Governance."

Facebook Actions (SEC, FTC and EU)

Public companies are required to identify and consider material risks to their business and maintain procedures to ensure disclosures are accurate in all material respects. On July 24th, the Securities and Exchange Commission (SEC) announced charges and a settlement of $100 million against Facebook for making misleading disclosures regarding the risk of user data misuse.[VI]

Also on July 24th, the FTC announced it had fined Facebook $5 billion for "misleading users about the extent to which third-party application developers could access users' personal information and ... deceiving users about their use of this and additional sensitive information." Significantly, the FTC's settlement also requires that Facebook create an independent committee of its board of directors to oversee privacy practices, including regular independent third party assessments of the effectiveness of the company's privacy program.[VIII, IX]

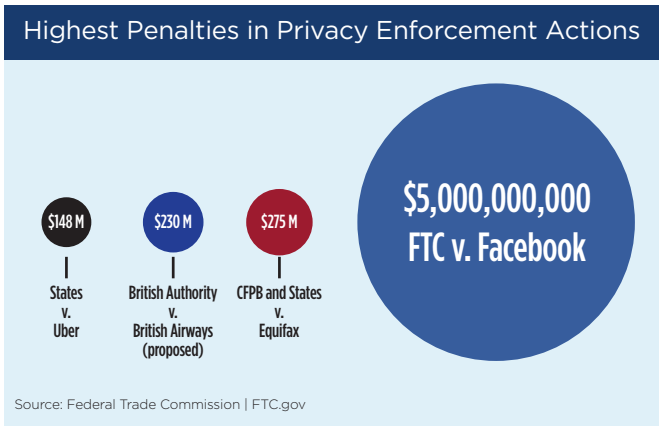

Figure 2: Penalty Amounts by Relative to Current Actions

In addition to these record fines, the European Union (EU), led by Ireland's Data Protection Commission, is nearing the end of its investigations into 11 cases under the General Data Protection Regulation (GDPR). Notably, EU rules give privacy regulators "more expansive powers than the FTC to order changes in behavior."[X] Depending on actions resulting from these investigations, there could be repercussions that go well beyond the impacts on Facebook. Although there may be additional Facebook fines as a result of the Commission's findings, what should matter to boards is the EU's heightened ability to force changes in the way companies do business, some of which, in Facebook's case, may "go to the heart of [its] business model."[XI]

Benefits of Engaging the Board in Risk Management Processes

Regulators around the world have recognized the criticality of board engagement in risk management processes for decades and the associated guidance on risk management practices has been increasingly prescriptive. For example, in March 2019 the Monetary Authority of Singapore (MAS) issued draft guidelines which would require boards to review and endorse, at least annually, a financial institution's critical business functions, business continuity objectives and the level of residual risk the company is willing to accept.

The Shared Assessments longitudinal Vendor Risk Management Benchmark Studies validates that board involvement in cybersecurity risk management is linked to an organization's Third Party Risk Management (TPRM) practice maturity.[XII] Study results show a strong correlation between organizations with high levels of engagement around cybersecurity risk issues and improved practice maturity of TPRM programs.

Shared Assessments' Vendor Benchmark Study

The Benchmark study uses the Shared Assessments' Vendor Risk Management Maturity Model (VRMMM) Tool to determine the current state of TPRM programs among organizations, measuring TPRM program maturity across eight different categories:

1) Program Governance;
2) Policies, Standards, Procedures;
3) Contract Development, Adherence and Management;
4) Vendor Risk Assessment Process;
5) Skills and Expertise;
6) Communication and Information Sharing;
7) Tools, Measurement and Analysis; and
8) Monitoring and Review.

The VRMMM maturity levels scale range from one to five with:

- Levels four and five designating organization that are operating fully mature or advanced TPRM programs;
- Level three for organizations with transitional TPRM programs that are not yet fully functional; and
- Levels zero to two for organizations that demonstrate either only ad hoc or no TPRM program activity.

DEGREE OF BOARD ENGAGEMENT WITH AN UNDERSTANDING OF THIRD PARTY RELATED CYBERSECURITY ISSUES			
PROGRAM MATURITY (Not showing "Don't Know" responses)	**HIGH LEVEL** (32% of survey respondents)	**MEDIUM LEVEL** (41% of survey respondents)	**LOW LEVEL** (20% of survey respondents)
Fully-Functional and Advanced TPRM Programs	57%	37%	25%
Transitional TPRM Programs	25%	30%	24%
Programs with Ad-Hoc or No TPRM Activities	18%	33%	51%

Figure 3: Strong Relationship Between Board Engagement and TPRM Practice Maturity

The Board's Role in Risk Management Processes

It is critical for an organization's board to provide effective oversight of risk monitoring processes. Many organizations have a designated board-level risk committee, or other established group, that oversees risk management activities and advises the full board on current and emerging issues to inform risk decision making.

Companies with a Chief Risk Officer benefit from having an executive leader integrated with board risk committees who:

1. Oversees risk monitoring activities across the organization.
2. Has a direct reporting line to the organization's board and C-suite and works with the board risk committee chair to ensure that the risk committee stays abreast of risk-related matters.
3. Engages in executive and corporate strategy meetings to ensure risk strategy, risk appetite and risk culture expectations are appropriately considered.
4. Communicates findings to the board risk committee with a frequency that will give risk committee members sufficient time to consider issues and resolutions before meetings with the full board.

Improving the Involvement of Boards in Risk Monitoring Processes

The board should set a tone that conveys the importance of a widely embraced risk culture and its value to the health and prosperity of the company. It is important that the organization's risk culture, objectives and values are effectively communicated and used appropriately to inform risk decision making.

A risk appetite statement serves as a starting point to develop a complete risk appetite framework. Risk appetite frameworks incorporate risk tolerance metrics at all levels within an organization and assure a coherent understanding of risk tolerance at the business unit level. The Chief Risk Officer has a key role, through board review and approval, in updating and maintaining the company risk appetite framework and associated metrics.

Boards can take the following actions to ensure effective risk management oversight:

- Ensure that board members understand why robust risk monitoring is important to achieving organizational strategic goals and overall success.
- Nominate executive(s) to the board with appropriate risk management backgrounds and expertise.
- Establish a board risk committee or sub-group to oversee all enterprise risk management activities and advise the full board regarding risk-related decisions.
- Designate a Chief Risk Officer to represent the board risk committee and oversee risk-related matters throughout the organization.
- Ensure that board members understand and document approval of enterprise risk monitoring processes, including the board-approved risk strategy, risk appetite statement and the development of a company-wide enterprise risk management framework.
- Ensure that the organization's identified risks are consistent with organizational objectives, operating strategy and risk culture.
- Develop and maintain direct communication channels between risk committees and senior managers to discuss and stay abreast of risk-related matters. Chief Risk Officers should be afforded unimpeded access to board risk committees.
- Regularly review all aspects of risk monitoring processes to ensure they are effectively and efficiently meeting organizational needs. Ensure that risk reporting metrics are relevant, conducted at the right frequency and communicated effectively among all key stakeholders.

Many organizations conduct board-directed assessments or reviews using a qualified, external third party to provide an arm's length perspective of current risk management practices. This is a best practice and may be required by regulators.

Conclusion

Governing boards should play an active role in ensuring that risk monitoring processes meet the needs of the organization and are carried out effectively. Organizations with boards actively engaged in risk monitoring processes are far more likely to implement and maintain an effective enterprise risk management program. Board engagement helps organizations to be more responsive to real-time risk developments and to maintain a higher level of resiliency.

Five key steps boards should take to help their organizations develop and maintain effective enterprise risk management programs include:

1. Actively engage in risk management (including cybersecurity risk management) processes.
2. Ensure that the organization's risk management strategies and operations align with the strategic objectives of the organization.
3. Establish a board risk committee (or designated group) to oversee and keep the board abreast of risk management activities. Confirm that there is an appropriate level of risk management expertise on the board.
4. Designate a Chief Risk Officer who takes the lead to ensure that the board receives timely information about current and potential risks and risk monitoring processes.
5. Charter regular, arm's length assessments of risk management programs and use the associated reports to ensure timely program improvements as necessary.

Endnotes

i A Warning Shot on Equifax: Index Provider Flagged Security Issues Last Year. Wall Street Journal, Oct. 6, 2017. Accessed at: https://www.wsj.com/articles/a-warning-shot-on-equifax-index-provider-flagged-security-issues-last-year-1507292590

ii Facebook to Pay $100 Million for Misleading Investors About the Risks It Faced From Misuse of User Data. U.S. Securities and Exchange Commission press release, July 24, 2019. Accessed at: https://www.sec.gov/news/press-release/2019-140

iii Stipulated Order for Civil Penalty, Monetary Judgment, and Injunctive Relief. U.S. District Court acting on authorization to the Attorney General by the Federal Trade Commission. Accessed at: https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_order_filed_7-24-19.pdf

iv A Warning Shot on Equifax: Index Provider Flagged Security Issues Last Year. Wall Street Journal, Oct. 6, 2017. Accessed at: https://www.wsj.com/articles/a-warning-shot-on-equifax-index-provider-flagged-security-issues-last-year-1507292590

v Equifax Is Said to Be Close to Reaching Deal in Huge '17 Data Breach. New York Times, July 19, 2019. Accessed at: https://www.nytimes.com/2019/07/19/business/equifax-data-breach-settlement.html

vi Facebook to Pay $100 Million for Misleading Investors About the Risks It Faced From Misuse of User Data. U.S. Securities and Exchange Commission press release, July 24, 2019. Accessed at: https://www.sec.gov/news/press-release/2019-140

vii Facebook Agrees to Pay $5 Billion and Implement Robust New Protections of User Information in Settlement of Data-Privacy Claims. U.S. Department of Justice. July 24, 2019. Accessed from: https://www.justice.gov/opa/pr/facebook-agrees-pay-5-billion-and-implement-robust-new-protections-user-information

viii FTC Imposes $5 Billion Penalty and Sweeping New privacy Restrictions on Facebook. The Federal Trade Commission, press release, July 24, 2019. Accessed at: https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions

ix Schechner, S. EU Nears Decisions in Facebook Privacy Cases. The Wall Street Journal. August 12, 2019. Accessed at: https://www.wsj.com/articles/eu-nears-decisions-in-facebook-privacy-cases-11565602202?mod=searchresults&page=1&pos=6

x Schechner, S. EU Nears Decisions in Facebook Privacy Cases. The Wall Street Journal. August 12, 2019. Accessed at: https://www.wsj.com/articles/eu-nears-decisions-in-facebook-privacy-cases-11565602202?mod=searchresults&page=1&pos=6

xii Vendor Risk Management Benchmark Study: Running Hard to Stay in Place. The Santa Fe Group, Shared Assessments Program and Protiviti Inc. 2019.

Thank You to Our Contributors

This paper reviews key steps that boards should take to ensure that their organizations are conducting effective risk management programs. We would like to thank the Shared Assessments Continuous Monitoring Risk Committee volunteer members who conducted this effort:

- **John Bree**, Senior Vice President and Partner, Neo Group
- **Angela Dogan**, Executive Team & EVP of Vendor Risk & Compliance Services, Lynx Technology Partners, Inc.
- **Nasser Fattah**, Managing Director, MUFG Union Bank, N.A. (formerly Bank of Tokyo)
- **Rocco Grillo**, Managing Director-Global Risk Services, Alvarez & Marsal Dispute Analysis & Forensics, LLC
- **Suzanne Hartin**, Chief Risk and Security Officer, Early Warning Services, LLC
- **Mark Holladay**, Executive Vice President and Chief Risk Officer, Synovus Financial Corporation
- **Bob Maley**, Chief Security Officer, NormShield, Inc.
- **Shawn Malone**, Founder and Chief Executive Officer, Security Diligence, LLC
- **Maree Moscati**, Chief Executive Officer, Copytalk, LLC
- **Annie Searle**, Principal, Annie Searle & Associates
- **Glen Sgambati**, Vice President, Lead of Customer Success Executives, Early Warning Services, LLC
- **Linnea Solem**, Founder and Chief Executive Officer, Solem Risk Partners, LLC
- **Adam Stone**, Vice President Consulting Services and Chief Privacy Officer, Secure Digital Solutions, Inc.

We would also like to acknowledge The Santa Fe Group, Shared Assessments Program subject matter experts and other staff who supported this project:

- **Catherine A. Allen**, Chairman and Chief Executive Officer, The Santa Fe Group
- **Jessica Calzada**, Project Manager, The Santa Fe Group
- **Bob Jones**, Senior Advisor, The Santa Fe Group
- **Gary Roboff**, Senior Advisor, The Santa Fe Group
- **Wendy McCoy**, Contract Lead Writer
- **Charlie Miller**, Senior Advisor, The Santa Fe Group
- **Sylvie Obledo**, Senior Project Manager, The Santa Fe Group
- **Marya Roddis**, Vice President of Communications, The Santa Fe Group
- **Robin Slade**, Executive Vice President & Chief Operating Officer, The Santa Fe Group

About the Shared Assessments Program

The Shared Assessments Program has been setting the standard in Third Party risk management since 2005. Member-driven development of program resources helps organizations to effectively manage the critical components of the Third Party risk management lifecycle by creating efficiencies and lowering costs for conducting rigorous assessments of controls for cybersecurity, IT, privacy, data security and business resiliency. Program Tools are kept current with regulations, industry standards and guidelines and the current threat environment; and are adopted globally across a broad range of industries both by service providers and their customers. The Shared Assessments Program is managed by The Santa Fe Group (www.santa-fe-group.com), a strategic advisory company based in Santa Fe, New Mexico. For more information on Shared Assessments, please visit http://www.sharedassessments.org.

Join the dialog with peer companies and learn how you can optimize your compliance program. For more information on Shared Assessments, please visit http://www.sharedassessments.org.