TX Office: (817) 416-6842
NV Office: (702) 565-2727

Kral Ussery
Certified Public Accountants
Advisors - Litigation Support - Internal Audit

Governing Cybersecurity

Cybersecurity committees on the rise

By Ron Kral, CPA, CMA, CGMA
Partner of Kral Ussery LLC

Cybersecurity risks pose grave threats to investors, our capital markets, and our country.[1] This is the opening sentence of the SEC's Interpretive Guidance on Public Company Cybersecurity Disclosures dated February 21, 2018. While the SEC's focus is primarily on effective disclosure controls and procedures for accurate and timely disclosures of cyber risks and material events, the magnitude of this topic has deep operating and compliance ramifications. The big question in boardrooms is who precisely should be responsible for cybersecurity oversight?

Many companies rationalize that cybersecurity oversight should reside with their audit committee since there are SEC disclosure ramifications. However, does this make sense considering that cyber risks extend well beyond financial reporting and SEC disclosures? While there is no single correct answer considering the large array of risk environments, industries, organizational sizes and operating models, it is clear that cybersecurity committees are becoming more popular. A search of recent proxy statement filings with the SEC revealed twelve companies disclosing cybersecurity committees, five of which were created in the last year. This article sheds some light on these filings, as well as some considerations for cybersecurity governance.

A Growing Trend of Cybersecurity Committees

The following table captures the twelve (12) companies disclosing cybersecurity committees in proxy statements filed with the SEC over the last three months:

Ticker Symbol	Industry	Filing Date	Date Committee Formed	Committee Structure
CALX	Technology	4-3-18	June 2017	Standing board committee
CPSI	Healthcare	3-16-18	October 2017	Executive committee[2]
CVLY	Financial	4-6-18	Not disclosed	Standing board committee
ELLI	Technology	4-4-18	Not disclosed	Standing board committee
GM	Automotive	4-27-18	November 2017	Standing board committee

[1] Page 1 of RELEASE NOS. 33-10459; 34-82746; US Securities and Exchange Commission; February 21, 2018.
[2] Reports to the Company's Chief Operating Officer.

MOBL	Technology	4-27-18	April 2018	Standing board committee
MOH	Healthcare	3-19-18	Not disclosed	Standing board committee
NATR	Manufacturing	3-26-18	Not disclosed	Executive committee[3]
NTGR	Technology	4-20-18	June 2017	Standing board committee
PFSW	Services	5-18-18	Not disclosed	Standing board committee
TECD	Technology	4-26-18	Not disclosed	Standing board committee[4]
WIFI	Technology	4-24-18	Not disclosed	Standing board committee

Keep in mind that the above table only captures those companies filing recent proxy statements with the words "cybersecurity committee." Many other companies also address cybersecurity risks through risk committees, technology committees, IT committees, etc., that have similar scopes to the twelve identified cybersecurity committees. Calix, Inc (CALX) discloses that their *Cybersecurity Committee oversees Calix's management of risks associated with cybersecurity threats and reviews with management at each meeting the Company's assessment of cybersecurity threats and risks, data security programs, and management and mitigation of potential and any actual cybersecurity and information technology risks and breaches*.[5] They also elaborate on more specific responsibilities.

Many of the other twelve companies also disclose the scope and duties of their cybersecurity committees, as well as make available their committee charters via their websites. General Motors (GM) noted a key responsibility of reviewing *the Company's controls to prevent, detect, and respond to cyberattacks and breaches involving GM's electronic information, intellectual property, sensitive data, connected products, and the connected ecosystem.*[6] Verifying that well-designed controls are operating effectively is a critical responsibility in successfully addressing cyber risks.

Companies are recognizing the need to create independent oversight of cyber risks, including management's responses due to increasing exposures. Hence the upward trend to dedicate oversight responsibility to a board committee as five of the twelve companies have established their cybersecurity committees within the last year. GM disclosed that their *Board established a new Cybersecurity Committee to enhance the Board's oversight of GM's evolving cybersecurity risks.*[7] MobileIron (MOBL) disclosed their committee was formed *in response to the growing complexity of cyber security risks*

[3] Reports directly to the Audit Committee
[4] Undated name in fiscal 2018 to CyberTech Committee
[5] Page 11 of Calix, Inc. proxy statement filed with the SEC on 4-3-18,
[6] Page 24 of GM's proxy statement filed with the SEC on 4-27-18.
[7] Page 22 of GM's proxy statement filed with the SEC on 4-27-18.

affecting information security infrastructure domestically and internationally as well as specific risks and cyber security threats.[8]

Independence is arguably the most important single theme for effective boards and committees. It is the central lynchpin in fulfilling duties objectively in the best interest of investors who entrust directors to act solely on their behalf. Of the twelve cybersecurity committees ten are standing board committees made up entirely of independent directors. Independent directors should be unbiased in their oversight role of management's response to cyber risks, and thus in a stronger position to provide independent perspectives.

Interestingly, six of the twelve companies disclosing a cybersecurity committee are in the technology industry. Perhaps they are closer to cyber risks and thus see the need for a dedicated committee more clearly than organizations in other industries.

Audit Committee Overload

While we are seeing an emerging trend of cybersecurity committees being created, there are tradeoffs between housing the responsibilities within the audit committee or forming a new committee. The bottom line is that accountability should be centralized to a single committee, with the full board being debriefed as needed since all directors share equal fiduciary duties.

The role of the audit committee has evolved overtime, especially for publicly traded companies thanks to the Sarbanes-Oxley Act of 2002 (SOX). SOX raised the bar for audit committees regarding the oversight of internal control over financial reporting, appointing independent external auditors, director expertise and director independence. While it is common for boards to delegate these oversight responsibilities to an audit committee, delegating enterprise risk management (ERM), including cyber risks, should be carefully evaluated.

Concerns have surfaced regarding audit committee workloads. For example, Wesley Bricker, SEC's Chief Accountant, stated: *While audit committees may be equipped to play a role in overseeing risks that extend beyond financial reporting, such as cybersecurity and portions of enterprise risk management, I believe it is important for audit committees to not lose focus on their core roles and responsibilities*.[9]

The audit committee may make perfect sense for some organizations to house cybersecurity oversight, but for others the creation of a new committee may be an opportunity to enhance oversight effectiveness. Scope and workloads will be key considerations for deciding upon a governance structure. Of course, with cybersecurity risks on the rise, independent oversight should be top-of-mind for all organizations. GM disclosed that their board *believes the Cybersecurity Committee will be a critical asset as*

[8] Page 15 of MobileIron Inc. proxy statement filed with the SEC on 4-27-18.
[9] Wesley R. Bricker, Chief Accountant, Office of the Chief Accountant, US Securities and Exchange Commission, Remarks before the University of Tennessee's C. Warren Neel Corporate Governance Center: "Advancing the Role and Effectiveness of Audit Committees", March 24, 2017.

cybersecurity becomes increasingly important to GM.[10] Any organization today would be hard pressed not to conclude that cybersecurity is becoming increasingly important. Now is the time to respond to the increased risks with timely risk assessments, as well as preventive and detective controls that keep pace with the evolving risks.

Directors' Skills

It has never been more important to have technology savvy individuals on the board. Just as directors who are financial experts have been in demand for audit committees, directors with IT and data security expertise should be recruited to address cybersecurity oversight. Boards are also encouraged to look at cyber risks as an ERM matter, not just as a technology issue. Understanding the full risks relating to cybersecurity through the lens of ERM will help force the cross-pollinating of conversations between operating, reporting and compliance objectives.

Directors who are comfortable in understanding emerging technologies and cyber risks are essential in ensuring effective oversight. In a PwC survey of 9,500 executives, only 44% of respondents say their boards actively participate in their companies' overall security strategy.[11] When directors are not comfortable with technology and the language surrounding cyber risks, it is difficult for them to contribute to cybersecurity conversation in a meaningful way. Recruiting the right mix of directors coupled with continuing education is prudent.

Conclusions

Keeping cyber risks top-of-mind and having a proactive response should help mitigate the risks of lost revenues, operational disruption, adverse litigation and reputational damage. While the CEO is responsible for ERM activities, including cyber risks, organizations must consider independent board-level oversight of these efforts.

One size does not fit all when it comes to governance structures. However, core responsibilities must be set at both the board and management levels to protect and grow shareholder value. Are you prepared for a cybersecurity incident? It is not a matter of "will this occur?" but rather "will there be strong evidence of a proactive board when a cybersecurity incident occurs and needs to be disclosed?"

*****

Ron Kral is a partner of Kral Ussery LLC, a public accounting firm delivering advisory services, litigation support and internal auditing to US public and private companies. He is an advisor, trainer and catalyst for entities to protect and grow client shareholder value. Ron is a member of 4 of the 5 COSO sponsoring organizations; the AICPA, FEI, IIA, and IMA. Contact Ron at Rkral@KralUssery.com or www.linkedin.com/in/ronkral.

Kral Ussery LLC assists entities with governance and in all matters relating to financial reporting, including SEC compliance, internal controls testing and remediation, IT general

[10] Page 28 of GM's proxy statement filed with the SEC on 4-27-18.
[11] 2018 Global State of Information Security Survey, PwC, October 18, 2017.

controls, IPO readiness, M&A transactions, US GAAP compliance and implementation of new accounting standards. Visit us at www.KralUssery.com.

This is an article from the Governance Issues™ Newsletter, Volume 2018, Number 2, published on May 30, 2018