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

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

Governing Cybersecurity Risks – Are you Prepared?

Independent Verification is Wise

By Pete Nassos, CPA, CISSP, CPCU, SOC for Cybersecurity
Cybersecurity Risk Adviser, Kral Ussery LLC

Last year, Ron Kral wrote about the growing interest in developing cybersecurity committees on corporate boards to focus resources to better prepare for governing enterprise cyber risks (see Governing Cybersecurity). Despite the increased attention and investment, the cyber risk landscape has only broadened with more and more breaches being publicized. The opening sentence of the SEC's Interpretive Guidance on Public Company Cybersecurity Disclosures dated February 21, 2018 states, *Cybersecurity risks pose grave threats to investors, our capital markets, and our country*.[1] This guidance stresses the importance of policies and procedures related to cybersecurity risks and incidents. 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.

Ron's prior article addressed the effort of boardrooms to determine governing responsibility to conclude on who precisely should be responsible for cybersecurity oversight? This article continues that discussion and addresses the question: "Is your organization really prepared?"

A Growing Trend of Independent 3rd Party Verification & Reporting

Company boards are recognizing the need for increased independent oversight of cyber risks and managements' response plans due to increasing exposures. There are some technology executives who either are unaware or perhaps untruthful in disclosing realistic risk exposures to their CEO and board. Hence, we are seeing more boards and board committees demanding independent 3rd party verification of management's identification and response to cyber risks. This includes assessing if adequate policies and procedures are in place and being executed in a timely manner. Afterall, who else can reasonably serve as the board's and committees' independent eyes and ears? An independent cybersecurity resource can help protect the board, management and ultimately shareholders.

Granted that even with the best preparation effort, cybersecurity breaches can occur. Just like fire, windstorms, and earthquakes will happen, the emphasis needs to be on

[1] Page 1 of RELEASE NOS. 33-10459; 34-82746; US Securities and Exchange Commission; February 21, 2018.

disaster preparation and response time. Security and data breaches are bad enough; however, the greater liability often lies in a delayed and poor response to such breaches. Reputational damage and adverse litigation often follow.

Over the years, several cybersecurity related industry standards and frameworks have been developed and used to help guide organizations towards combating cyber risks. Today they are well matured and available as a starting point for conducting risk assessments and remediation efforts. Typically, they have been used by larger corporations and technology consulting firms to evaluate selected areas, identify critical gaps and in some cases- to justify significant IT projects. While these industry standards and frameworks can be very helpful, it is interpreting what needs to be done and understanding how to apply them that is crucial. Having an independent and competent advisor can pay big dividends.

In response to board committee and outside investor interests, the AICPA has developed a new reporting framework, 'System & Organization Controls (SOC) for Cybersecurity[2]'. Unlike the SOC 1, 2, 3 reports, the SOC for Cybersecurity effort is geared towards providing a comprehensive cybersecurity review and risk assessment of the target enterprise as opposed to outsourced service provider. Similar to the COSO Internal Control Framework, the SOC for Cybersecurity report includes a section on 'Management Description Criteria' with 19 specific criteria. Typically, completion of this section will leverage a well-known cybersecurity framework or industry standard, such as the National Institute of Science & Technology (NIST) Cybersecurity Framework (CSF) as the basis for the risk assessment evaluation. Other standards and frameworks such as ISO27001, COBIT2019, or HITRUST can also be used as appropriate depending on the application and industry.

By undertaking a comprehensive, independent assessment of cybersecurity preparation, board members will have improved assurance that their organization is on the right track. This effort will help determine if appropriate actions have been taken and the proper alignment of operating risks to business objectives. Evidence of this independent verification will also better position the organization for negotiating cyber risk insurance policies and premiums, along with defending against adverse lawsuits.

For example, recently a shareholder derivative lawsuit caused the insurance carrier for Yahoo (now Altaba, a subsidiary of Verizon Communications) to agree to a settlement[3] to pay $29 million in liability damages related to the 2013 – 2016 massive user data breach that affected over 3 Billion users of the Yahoo mail & services environment. In that situation, Yahoo did not disclose significant data breaches until September 2016. Further, it was determined that there was active cover-up by Yahoo top executives and that a legal investigation conducted was a 'sham' to conceal the massive data breach. In a

[2] AICPA web site: https://www.aicpa.org/press/pressreleases/2017/aicpa-unveils-cybersecurity-risk-management-reporting-framework.html
[3] Superior Court of Santa Clara County California, Case #17CV307054; Order & Final Judgment, Jan. 4, 2019.

separate case, the SEC fined Yahoo $35 million over *the egregious conduct by Yahoo executives*[4] for this incident.

In this case, both a US Court and the SEC cited a lack of appropriate oversight by a corporate board of directors and its executives over their actions or lack of timely actions related to data breaches, especially related to personal data privacy. As such, these actions signal increased director & officers (D&O) liability related to board oversight of cybersecurity risks. Such awards will likely have a negative effect on future D&O and cyber risk liability insurance premiums.

A Growing Realization that Cybersecurity Risk Mitigation is More Than Just Implementing Technology

The Yahoo and Equifax data breaches, along with many others, continue to prove that corporate culture and "tone at the top" sets the course for how organizations react to or even create cyber risk exposure. An organization that is proactive in providing comprehensive staff cybersecurity awareness training, as well as enforcing proper cyber practices will substantially mitigate exposure. Today, many security officers are promoted from highly technical roles so they naturally gravitate to technical solutions, continually looking to invest in the latest hardware and software solutions to mitigate risk. But this is only part of the solution. Often such technology investment is not productive if it is not focused on mitigating the root causes of risk exposures. Activities that address 'the soft skills' such as company culture, non-technical staff training and financial risk transfer also need to be addressed.

Do You Know Where Your Data Is?

Government regulations, including hefty fines related to the European Union's Global Data Protection Regulation (GDPR), are causing corporations to ponder where their critical data resides, be it financial, proprietary, employee or customer data. Without a comprehensive data classification and management policy, with related documentation as to which systems store what data and where, it is easy to lose track. This can lead to inadvertently losing control and experiencing a costly data breach. This involves not only your internal enterprise systems, but also the processes and data exchanges with your customers, vendors, and business partners. Controls to ensure data privacy cannot be effective without this foundational understanding of data classification and process flows.

Does Your Insurance Policies Really Provide Meaningful Coverage?

Many companies mistakenly believe they have appropriate insurance policy coverage, figuring that their commercial general liability or D&O liability coverage provides adequate reimbursement. However, a closer analysis shows that only corporate property, such as IT equipment, is generally protected from hazard situations. In addition, some insurance coverage may be rescinded in circumstances involving fraud, or war. Data breaches that occur due to government sponsored hacking could potentially be considered "an act of war" and thus could invalidate the policy coverage. Cybersecurity risk liability, especially

[4] Administrative Proceeding, File No.3-18448; US Securities and Exchange Commission; April 24, 2018.

data privacy liability from breaches, is not well covered unless specific cyber risk exposures are identified and appropriate coverage is specifically stated in the policy terms. 'Difference in Condition' and 'Excess Loss' coverages can be helpful to address insurance coverage gaps.

Recent insurance industry financial statistics[5] indicate that insurance carriers have low total loss ratios and are making strong profit margins on their cyber risk policies written. Insurance brokers and carriers typically rely on customer self-assessments for their policy applications, which require substantial technical staff time to complete. Without having an independent 3rd party verification, such as the AICPA SOC for Cybersecurity attest report, underwriters rely on heftier premiums and narrow legal language to protect their business. By leveraging an independent cybersecurity risk assessment, with independent confirmation of cyber policies and practices, corporations can be more confident and transparent about their cyber risks. This enables the insurance broker, carrier and reinsurance underwriters to better understand and evaluate the appropriate risks to be covered leading to an appropriate premium. There is also an opportunity to consider using captive insurance companies to financially reserve major risks when carriers are not providing adequate coverage or require excessive premiums.

Conclusions

Organizations who undertake independent verification of adherence to standards and can show a healthy 'tone at the top', staff training, security controls, and proper investment in security infrastructure will be better prepared in winning the cybersecurity battles. Further, such actions will position the organization for better insurance premiums and coverage. The recent implementation of the European Union's GDPR and hefty fines recently levied against Equifax, Yahoo, Google and others, further draws light to the downsides of not being proactive in addressing and reporting data privacy breaches. Even more important than government regulations and fines is protecting your brand and shareholder value.

*****

Pete Nassos is Cybersecurity Risk Adviser with Kral Ussery LLC, a public accounting firm delivering accounting, IT and SEC advisory services, along with litigation support and internal auditing to US public and private companies. He is a CPA, with a focus on assessing cyber risk and advising companies on appropriate technology investments to best mitigate risk. Contact Pete at PNassos@KralUssery.com or www.linkedin.com/in/petenassos.

Pete also leads two training sessions relating to cybersecurity, Assessing Cybersecurity Risk for executives and boards, and Cybersecurity Awareness for managers.

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

[5] Business Insurance article, "Cyber underwriting profitability varies by segment"; November 30, 2018.

cybersecurity risk advisory services, 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 2019, Number 1, published on February 11, 2019