A COALFIRE PERSPECTIVE

SEC Cyber Risk Disclosure Guidance

by Rick Dakin, CEO/Chief Security Strategist, Coalfire

February 2012

DALLAS | DENVER | LOS ANGELES | NEW YORK | SEATTLE

877.224.8077 | info@coalfire.com | www.coalfire.com

SEC Cyber Risk Disclosure Guidance

The crazy aunt is now out of the closet. Companies, in general, have some level of unrecognized cyber risk and have not fully disclosed those risks and risk management plans to boards or external stakeholders to include clients, partners and shareholders. Now, publicly-traded companies have to disclose cyber risks in financial statements. On October 13, 2011 the Securities and Exchange Commission (SEC) Division of Corporation Finance released a guidance document that assists registrants in assessing what disclosures should be made in the face of cyber security risks and incidents.

While cyber risk for financial records has been part of the financial audit and reporting process since the early SOX 404 days, these new requirements for disclosure represent a broader impact to operations and a more stringent standard for analysis and reporting. The guidance provides an overview of disclosure obligations under current securities laws emphasizing that registrants should disclose the risk of cyber incidents "if these issues are among the most significant factors that make an investment in the company speculative or risky." Registrants are expected to evaluate security risks, and if a registrant determines that disclosure is required, the registrant is expected to "describe the nature of the material risks and specify how each risk affects the registrant," avoiding generic disclosures.

The SEC indicated that in analyzing cyber security risks and whether that risk should be reported, registrants should take the following into account:

- prior cyber incidents and the severity and frequency of those incidents;
- the probability of cyber incidents occurring and the quantitative and qualitative magnitude of those risks, including the potential costs and other consequences resulting from misappropriation of assets or sensitive information, corruption of data or operational disruption; and
- the adequacy of preventative actions taken to reduce cyber security risks in the context of the industry in which they operate and risks to that security, including threatened attacks of which they are aware.

Additionally, the guidance advises registrants to address risks and incidents in their MD&A "if the costs or other consequences associated with one or more known incidents or the risk of potential incidents represent a material event, trend, or uncertainty that is reasonably likely to have a material effect on the registrant's results of operations, liquidity, or financial condition or would cause reported financial information not to be necessarily indicative of future operating results or financial condition." Other situations requiring disclosure include if one or more incidents has materially affected a registrant's "products, services, relationships with customers or suppliers, or competitive conditions" and if an incident is involved in a material pending legal proceeding to which a registrant or any of its subsidiaries is a party. Registrants are also expected to disclose certain security incidents on financial statements, as well as the effectiveness of disclosure controls and procedures on filings with the SEC. As a result, most public company breach notification and incident response plans will have to be updated.

The guidance will likely cause companies to more carefully forecast and estimate the impact of cyber incidents and the consequences of failing to implement adequate security. This analysis will go well beyond the current focus on privacy-related security issues and require analysis of key operational issues impacted by security breaches. It will be interesting to see how this affects the internal corporate dynamics between CIOs and their business counter-parts.

In some organizations, the general counsel will ask the CIO how the security program is operating and the CIO may provide an operations-level report that may not fully address this requirement. The risk management discussion must include not only technical controls but also other process controls, which could be outside the direct oversight of the CIO. This is truly a cross-functional requirement that will include the CIO as well as other members of the executive team. Some scoping questions that are inherent in the SEC guidance to manage risk have been listed below.

- What types of sensitive data does the company collect, process, store or transit?
- What critical operations are supported by IT that may cause significant damage to third parties (i.e. critical infrastructure)?
- How does the organization map its data flows to determine critical segments for enhanced protection?
- What process does the company use to manage risk identification and risk management planning and what reports are generated to provide transparency to company governance structure?
- When is the last time the executive team participated in the company Incident Response and Data Breach Notification exercise process? Do you know where to get a copy of the Incident Response Plan?

Many companies, to include Heartland Payment Systems, thought they were managing risks commensurate to industry standards only to incur a significant data breach. Sony, TJ Max and others were in the same situation. Clearly, their risk management plans were not adequate and the transparency of both the risk and control effectiveness was not reported in a manner where executive oversight was possible. At Heartland, the company had implemented several security programs that were audited and reported to be compliant with industry standards. In short, the company was not completely unprepared. In fact, Heartland was operating a security program that was well above most programs today. Unfortunately, the lack of oversight from the top resulted in sub-optimized performance at the operations level and residual risks were present. Those risks resulted in a data breach that likely could have been prevented. This disclosure requirement is intended to help identify those risks and inform key stakeholders on the effectiveness of management control of the risks.

Some risk may not be economically mitigated. That accepted risk has to be disclosed to shareholders or investors as a part of the Management Discussion in financial statements going forward. The inherent risk of each company's exposure to cyber risks can be easily stated. However, the adequacy and effectiveness of risk mitigation or compliance efforts will take a higher level of analysis and reporting that likely occurs today in many organizations. These changes to corporate governance may be minor in some organizations and significant investments in others. However, the path is clear. Accountability for cyber risk has fully migrated from the data center to the boardroom.

About the Author

Rick Dakin, CEO, Co-Founder and Chief Security Strategist

Mr. Dakin provides strategic management IT security program guidance for Coalfire and its clients. He has more than 25 years of experience in senior management with leading IT firms. Mr. Dakin combines an in-depth knowledge of IT controls with a comprehensive understanding of organizational needs and the rapidly emerging legislation affecting IT security. Prior to co-founding Coalfire, he was President of Centera Information Systems, a leading eCommerce and systems integration firm. He is a past president of the FBI's InfraGard program, Denver chapter, and a member of a committee hosted by the U.S. Secret Service and organized by the Joint Council on Information Age Crime.

Appendix A – SEC Cyber Risk Disclosure Guidance

Division of Corporation Finance

Securities and Exchange Commission

CF Disclosure Guidance: Topic No. 2

Cybersecurity

Date: October 13, 2011

Summary: This guidance provides the Division of Corporation Finance's views regarding disclosure obligations relating to cyber security risks and cyber incidents.

Supplementary Information: The statements in this CF Disclosure Guidance represent the views of the Division of Corporation Finance. This guidance is not a rule, regulation, or statement of the Securities and Exchange Commission. Further, the Commission has neither approved nor disapproved its content.

Introduction

For a number of years, registrants have migrated toward increasing dependence on digital technologies to conduct their operations. As this dependence has increased, the risks to registrants associated with cyber security[1] have also increased, resulting in more frequent and severe cyber incidents. Recently, there has been increased focus by registrants and members of the legal and accounting professions on how these risks and their related impact on the operations of a registrant should be described within the framework of the disclosure obligations imposed by the federal securities laws. As a result, we determined that it would be beneficial to provide guidance that assists registrants in assessing what, if any, disclosures should be provided about cyber security matters in light of each registrant's specific facts and circumstances.

We prepared this guidance to be consistent with the relevant disclosure considerations that arise in connection with any business risk. We are mindful of potential concerns that detailed disclosures could compromise cyber security efforts -- for example, by providing a "roadmap" for those who seek to infiltrate a registrant's network security -- and we emphasize that disclosures of that nature are not required under the federal securities laws.

In general, cyber incidents can result from deliberate attacks or unintentional events. We have observed an increased level of attention focused on cyber attacks that include, but are not limited to, gaining unauthorized access to digital systems for purposes of misappropriating assets or sensitive information, corrupting data, or causing operational disruption. Cyber attacks may also be carried out in a manner that does not require gaining unauthorized access, such as by causing denial-of-service attacks on websites. Cyber attacks may be carried out by third parties or insiders using techniques that range from highly sophisticated efforts to electronically circumvent network security or overwhelm websites to more traditional intelligence gathering and social engineering aimed at obtaining information necessary to gain access.

The objectives of cyber attacks vary widely and may include theft of financial assets, intellectual property, or other sensitive information belonging to registrants, their customers, or other business partners. Cyber attacks may also be directed at disrupting the operations of registrants or their business partners. Registrants that fall victim to successful cyber attacks may incur substantial costs and suffer other negative consequences, which may include, but are not limited to:

- Remediation costs that may include liability for stolen assets or information and repairing system damage that may have been caused. Remediation costs may also include incentives offered to customers or other business partners in an effort to maintain the business relationships after an attack;
- Increased cyber security protection costs that may include organizational changes, deploying additional personnel and protection technologies, training employees, and engaging third party experts and consultants;
- Lost revenues resulting from unauthorized use of proprietary information or the failure to retain or attract customers following an attack;
- Litigation; and
- Reputational damage adversely affecting customer or investor confidence.

Disclosure by Public Companies Regarding Cyber security Risks and Cyber Incidents

The federal securities laws, in part, are designed to elicit disclosure of timely, comprehensive, and accurate information about risks and events that a reasonable investor would consider important to an investment decision.[2] Although no existing disclosure requirement explicitly refers to cyber security risks and cyber incidents, a number of disclosure requirements may impose an obligation on registrants to disclose such risks and incidents. In addition, material information regarding cyber security risks and cyber incidents is required to be disclosed when necessary in order to make other required disclosures, in light of the circumstances under which they are made, not misleading.[3] Therefore, as with other operational and financial risks, registrants should review, on an ongoing basis, the adequacy of their disclosure relating to cyber security risks and cyber incidents.

The following sections provide an overview of specific disclosure obligations that may require a discussion of cyber security risks and cyber incidents.

Risk Factors

Registrants should disclose the risk of cyber incidents if these issues are among the most significant factors that make an investment in the company speculative or risky.[4] In determining whether risk factor disclosure is required, we expect registrants to evaluate their cyber security risks and take into account all available relevant information, including prior cyber incidents and the severity and frequency of those incidents. As part of this evaluation, registrants should consider the probability of cyber incidents occurring and the quantitative and qualitative magnitude of those risks, including the potential costs and other consequences resulting from misappropriation of assets or sensitive information, corruption of data or operational disruption. In evaluating whether risk factor disclosure should be provided, registrants should also consider the adequacy of preventative actions taken to reduce cyber security risks in the context of the industry in which they operate and risks to that security, including threatened attacks of which they are aware.

Consistent with the Regulation S-K Item 503(c) requirements for risk factor disclosures generally, cyber security risk disclosure provided must adequately describe the nature of the material risks and specify how each risk affects the registrant. Registrants should not present risks that could apply to any issuer or any offering and should avoid generic risk

factor disclosure.[5] Depending on the registrant's particular facts and circumstances, and to the extent material, appropriate disclosures may include:

- Discussion of aspects of the registrant's business or operations that give rise to material cyber security risks and the potential costs and consequences;
- To the extent the registrant outsources functions that have material cyber security risks, description of those functions and how the registrant addresses those risks;
- Description of cyber incidents experienced by the registrant that are individually, or in the aggregate, material, including a description of the costs and other consequences;
- Risks related to cyber incidents that may remain undetected for an extended period; and
- Description of relevant insurance coverage.

A registrant may need to disclose known or threatened cyber incidents to place the discussion of cyber security risks in context. For example, if a registrant experienced a material cyber attack in which malware was embedded in its systems and customer data was compromised, it likely would not be sufficient for the registrant to disclose that there is a risk that such an attack may occur. Instead, as part of a broader discussion of malware or other similar attacks that pose a particular risk, the registrant may need to discuss the occurrence of the specific attack and its known and potential costs and other consequences.

While registrants should provide disclosure tailored to their particular circumstances and avoid generic "boilerplate" disclosure, we reiterate that the federal securities laws do not require disclosure that itself would compromise a registrant's cyber security. Instead, registrants should provide sufficient disclosure to allow investors to appreciate the nature of the risks faced by the particular registrant in a manner that would not have that consequence.

Management's Discussion and Analysis of Financial Condition and Results of Operations (MD&A)

Registrants should address cyber security risks and cyber incidents in their MD&A if the costs or other consequences associated with one or more known incidents or the risk of potential incidents represent a material event, trend, or uncertainty that is reasonably likely to have a material effect on the registrant's results of operations, liquidity, or financial condition or would cause reported financial information not to be necessarily indicative of future operating results or financial condition.[6] For example, if material intellectual property is stolen in a cyber attack, and the effects of the theft are reasonably likely to be material, the registrant should describe the property that was stolen and the effect of the attack on its results of operations, liquidity, and financial condition and whether the attack would cause reported financial information not to be indicative of future operating results or financial condition. If it is reasonably likely that the attack will lead to reduced revenues, an increase in cyber security protection costs, including related to litigation, the registrant should discuss these possible outcomes, including the amount and duration of the expected costs, if material. Alternatively, if the attack did not result in the loss of intellectual property, but it prompted the registrant to materially increase its cyber security protection expenditures, the registrant should note those increased expenditures.

Description of Business

If one or more cyber incidents materially affect a registrant's products, services, relationships with customers or suppliers, or competitive conditions, the registrant should provide disclosure in the registrant's "Description of Business."[7] In determining whether to include disclosure, registrants should consider the impact on each of their reportable segments. As an example, if a registrant has a new product in development and learns of a cyber incident that could materially impair its future viability, the registrant should discuss the incident and the potential impact to the extent material.

Legal Proceedings

If a material pending legal proceeding to which a registrant or any of its subsidiaries is a party involves a cyber incident, the registrant may need to disclose information regarding this litigation in its "Legal Proceedings" disclosure. For example, if a significant amount of customer information is stolen, resulting in material litigation, the registrant should disclose the name of the court in which the proceedings are pending, the date instituted, the principal parties thereto, a description of the factual basis alleged to underlie the litigation, and the relief sought.[8]

Financial Statement Disclosures

Cyber security risks and cyber incidents may have a broad impact on a registrant's financial statements, depending on the nature and severity of the potential or actual incident.

Prior to a Cyber Incident

Registrants may incur substantial costs to prevent cyber incidents. Accounting for the capitalization of these costs is addressed by Accounting Standards Codification (ASC) 350-40, *Internal-Use Software*, to the extent that such costs are related to internal use software.

During and After a Cyber Incident

Registrants may seek to mitigate damages from a cyber incident by providing customers with incentives to maintain the business relationship. Registrants should consider ASC 605-50, *Customer Payments and Incentives*, to ensure appropriate recognition, measurement, and classification of these incentives.

Cyber incidents may result in losses from asserted and unasserted claims, including those related to warranties, breach of contract, product recall and replacement, and indemnification of counterparty losses from their remediation efforts. Registrants should refer to ASC 450-20, *Loss Contingencies*, to determine when to recognize a liability if those losses are probable and reasonably estimable. In addition, registrants must provide certain disclosures of losses that are at least reasonably possible.

Cyber incidents may also result in diminished future cash flows, thereby requiring consideration of impairment of certain assets including goodwill, customer-related intangible assets, trademarks, patents, capitalized software or other long-lived assets associated with hardware or software, and inventory. Registrants may not immediately know the impact of a cyber incident and may be required to develop estimates to account for the various financial implications. Registrants should subsequently reassess the assumptions that underlie the estimates made in preparing the financial statements. A registrant must explain any risk or uncertainty of a reasonably possible change in its estimates in the near-term that would be

material to the financial statements.[9] Examples of estimates that may be affected by cyber incidents include estimates of warranty liability, allowances for product returns, capitalized software costs, inventory, litigation, and deferred revenue.

To the extent a cyber incident is discovered after the balance sheet date but before the issuance of financial statements, registrants should consider whether disclosure of a recognized or non-recognized subsequent event is necessary. If the incident constitutes a material non-recognized subsequent event, the financial statements should disclose the nature of the incident and an estimate of its financial effect, or a statement that such an estimate cannot be made.[10]

Disclosure Controls and Procedures

Registrants are required to disclose conclusions on the effectiveness of disclosure controls and procedures. To the extent cyber incidents pose a risk to a registrant's ability to record, process, summarize, and report information that is required to be disclosed in Commission filings, management should also consider whether there are any deficiencies in its disclosure controls and procedures that would render them ineffective.[11][11] For example, if it is reasonably possible that information would not be recorded properly due to a cyber incident affecting a registrant's information systems, a registrant may conclude that its disclosure controls and procedures are ineffective.

Endnotes

---

[1] Cyber security is the body of technologies, processes and practices designed to protect networks, systems, computers, programs and data from attack, damage or unauthorized access. Whatis?com available at http://whatis.techtarget.com/definition/cybersecurity.html. See also Merriam-Webster.com available at http://www.merriam-webster.com/dictionary/cybersecurity.

[2] The information in this disclosure guidance is intended to assist registrants in preparing disclosure required in registration statements under the Securities Act of 1933 and periodic reports under the Securities Exchange Act of 1934. In order to maintain the accuracy and completeness of information in effective shelf registration statements, registrants may also need to consider whether it is necessary to file reports on Form 6-K or Form 8-K to disclose the costs and other consequences of material cyber incidents. See Item 5(a) of Form F-3 and Item 11(a) of Form S-3.

[3] Securities Act Rule 408, Exchange Act Rule 12b-20, and Exchange Act Rule 14a-9. Information is considered material if there is a substantial likelihood that a reasonable investor would consider it important in making an investment decision or if the information would significantly alter the total mix of information made available. See Basic Inc. v. Levinson, 485 U.S. 224 (1988); and TSC Industries, Inc. v. Northway, Inc., 426 U.S. 438 (1976). Registrants also should consider the antifraud provisions of the federal securities laws, which apply to statements and omissions both inside and outside of Commission filings. See Securities Act Section 17(a); Exchange Act Section 10(b); and Exchange Act Rule 10b-5.

[4] See Item 503(c) of Regulation S-K; and Form 20-F, Item 3.D.

[5] Item 503(c) of Regulation S-K instructs registrants to "not present risks that could apply to any issuer or any offering" and further, to "[e]xplain how the risk affects the issuer or the securities being offered." Item 503(c) of Regulation S-K.

[6] See Item 303 of Regulation S-K; and Form 20-F, Item 5. A number of past Commission releases provide general interpretive guidance on these disclosure requirements. See, e.g., Commission Guidance Regarding Management's Discussion and Analysis of Financial Condition and Results of Operations, Release No. 33-8350 (Dec. 19, 2003) [68 FR 75056] Commission Statement About Management's Discussion and Analysis of Financial Condition and Results of Operations, Release No. 33-8056 (Jan. 22, 2002) [67 FR 3746]; Management's Discussion and Analysis of Financial Condition and Results of Operations; and Certain Investment Company Disclosures, Release No. 33-6835 (May 18, 1989) [54 FR 22427].

[7] See Item 101 of Regulation S-K; and Form 20-F, Item 4.B.

[8] See Item 103 of Regulation S-K.

[9] See FASB ASC 275-10, *Risks and Uncertainties.*

[10] See ASC 855-10, *Subsequent Events*.

[11] See Item 307 of Regulation S-K; and Form 20-F, Item 15(a).