Kevane Grant Thornton
An instinct for growth™

Advisory Alert: The audit committee's role in cybersecurity

By now, most senior-level executives have heard that either you have had a data breach or you just don't know that you've had a data breach. Cyberattacks are now as much a part of doing business as taxes and financial statements and they are getting expensive. According to the *2015 U.S. Cost of a Data Breach* Study[1] by the Ponemon Institute, in 2014 there was an 11% increase in the total cost of a data breach, to a $217 average per lost or stolen record, a clear reminder that organizations need to make a priority of addressing cybersecurity risks. For those companies with audit committees, that subset of the board has seen its role expand as it works to identify key areas of risk. After all, cybersecurity risks are no different from any other kind of enterprise risk, and the audit committee's charter is to understand a business and its objectives, then identify suitable ways to address risks that threaten the business or its goals.

That said, cybersecurity is a daunting arena, so audit committees should educate themselves about cyberrisks in the same fashion that they educated themselves about addressing risks as required by the Sarbanes-Oxley Act, drastic changes to a given market or product, or any major category of risk facing the enterprise. Specifically, audit committees should become aware of their obligations and ask probing questions about the control environment that may jeopardize those obligations.

The audit committee is uniquely positioned to assess risks that threaten the enterprise. Indeed, a proper contemplation of cybersecurity risk necessitates that it be treated like another category of enterprise risk. Put differently, audit committees should leverage existing protocols (such as enterprise risk assessments, risk analyses, training protocols, monitoring and reporting mechanisms, and the like) to ensure that these risks are adequately addressed. To illustrate just one of these points, the audit committee already interacts with the CFO regularly for other risk management discussions; it should continue to do so for cybersecurity risk. This is especially true, given that the CFO is (statistically speaking) the officer most

[1] Ponemon Institute. U.S. Cost of a Data Breach Study, May 2015

Contact us
For assistance in this matter, please contact us via ojel.rodriguez@pr.gt.com

Adding true value means exceeding our clients' expectations, anticipating their needs and being proactive and innovative in the accounting profession.

Through the **Kevane Grant Thornton business and tax application for mobile devices** you will have access to our Alerts, Tax News and other related matters, plus a customized tax calendar for individuals, businesses and other entities, thus providing an excellent tool to manage filing and payment due dates with government agencies in Puerto Rico.

Download for free the application. Available for iPhone, Motorola and all tablets.

Google play App Store

Follow us on and

March 13, 2017

commonly associated with leading cybersecurity efforts. (Grant Thornton LLP recently collaborated with the Financial Executives Research Foundation on a study focused on the CFO's role in cybersecurity, which revealed that 38% of all cybersecurity initiatives are actually run by the CFO).

Prevention and incident response

While the primary cybersecurity consideration for any organization remains prevention, more and more companies recognize that a security compromise is eminently more likely than it used to be. Accordingly, being prepared to respond to a security compromise or breach is quickly becoming of equal importance. An audit committee can and should play a strong role in both prevention and incident response, but to do so require a certain level of baseline understanding combined with the ability to ask detailed questions to management about the processes and controls in place.

Basic fact-finding questions might include the following:

- Where is our sensitive data stored?
- Are we including payment information, health information, intellectual property, R&D, and customer and vendor information in our definition of sensitive data?
- What data leaves the company, how does the data leave, and to whom is it transmitted?
- Have we performed a vulnerability assessment to identify our information security exposures?
- Have we evaluated our third-party vendors and partners for exposure to sensitive data?
- Who is authorized to log into our network and from which platforms?
- What measure of insurance has the company secured, and which department(s) completed and reviewed those applications for coverage?
- What are our policies and procedures related to employees' use of personal devices to access company systems and sensitive data?
- How does the organization educate its employees on their obligations related to the handling of sensitive information?

In terms of how well an organization is positioned to respond to a security incident, such as the protocols to follow if sensitive data is compromised, the audit committee should ask three basic questions to management to assess risks:

1. Does the company have an incident response plan or program?
2. If the answer is yes, has the company ever tested the plan (before it's needed in a live-fire situation)?
3. If that answer is a yes, what is the company doing to ensure that its plan remains current and adequate to the risk it faces as an industry and a regulated entity?

Within each of those questions are several nuances. Moreover, the answers to these questions allow for a proper series of follow-up questions related to insurance (i.e., insurable versus uninsurable), the treatment of third parties that handle sensitive data, the applicability of the attorney-client privilege, technology investments and ongoing management, policy and procedure considerations, training and awareness issues,

and other key considerations. All these elements need to be aligned to enable a company to cope properly with cybersecurity risk.

Cybersecurity and the SEC

An audit committee needs to be conversant with any matters that might require disclosure in SEC filings, especially in light of the recent news that cybersecurity has been listed by the SEC as a top examination priority during 2015. Indeed, the SEC staff has stated that investors cannot make informed investment decisions without knowing about material actual or potential cyber threats facing a given registrant. Audit committees would do well to increase their scrutiny of cybersecurity in the following areas related to financial statement filings:

- Forms 10-K and 10-Q and other SEC filings regarding risk factors: If risks are deemed significant enough to make investment in a registrant speculative, they must become part of the disclosure regimen. Cybersecurity risks should be considered as a category within this regimen, and the SEC appears from recent decisions to be less accepting of generic risk statements in this area. Some care should be taken to delve into the probability of cyber incidents, the impact of such incidents if they were to occur and the level of preventive measures undertaken by the registrant to deal with the same.
- Management's discussion and analysis portion: Registrants that do not outline what they are doing in this arena risk facing tough questions from regulators and potential litigants, especially if they are experiencing and defending against material cyberattacks and/or incurring material costs to prevent such attacks.
- The legal proceedings section of the Form 10-K: This area would have to include any material litigation or regulatory incidents related to cybersecurity incidents.
- Various other financial statement disclosures: Additional areas for consideration include but are not limited to remediation costs, reputational damage, liability for stolen information, increased preventive costs (insurance, technology investments and the like) and so on.

Newer issues: Insurance and the law

Issues regarding the topic of cybersecurity, like methods of cybersecurity, are ever-changing. The case law related to cyber insurance, for example, is still developing, yet a pattern is emerging that merits attention by organizations obtaining cyber insurance policies. Simply put, great care should be paid to the policy application itself, including any warranties presented to the underwriter that are related to internal controls in place to address information security. A recent court decision (Columbia Casualty Company v. Cottage Health System) highlights this issue clearly. There, an underwriter cited an exclusion that precludes coverage because of the policyholder's "failure to follow minimum required practices." According to the underwriter's complaint, the defendant "permitted anonymous user access, thereby allowing electronic personal information to become available to the public via Google's Internet search engine," thereby voiding the coverage provided by the insurer.

The case reflects the care that companies must undertake to ensure that policy applications be scrutinized carefully for

inaccuracies and misstatements. Any daylight between the warranties provided and facts that later reveal a deficient practice might result in a claim that falls outside of coverage.

In summation

With the SEC heightening its scrutiny of organizations' cybersecurity processes and new technologies also creating new channels for cyberattacks, the need is greater than ever for audit committees to be a more integral part of cybersecurity management efforts. Involving the audit committee after a data breach severely limits its ability to add value to the process and puts the organization at a tremendous disadvantage. Cybersecurity risk has evolved to the level where it should be addressed every bit as seriously as any other substantial enterprise risk, such as a change to the regulatory environment or a sweeping industry mandate.

We are committed to keep you updated of all developments that may affect the way you do business in Puerto Rico. Please contact us for assistance in relation to this or any other matter.