Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Basic Steps To Protect Your Co. Against Cyber Perils

Law360, New York (October 10, 2013, 12:25 PM ET) -- According to a 2010 study, companies in the hospitality industry are the no. 1 targets for computer hackers and other thieves of electronic data — with 38 percent of all credit card hacking cases occurring in the hotel industry.

These crimes are not perpetrated only by faraway hackers either. All too often, rogue criminal employees use swipe card skimmers to steal credit card numbers and related data from guests. The risk of losing guests' private data is critical and needs to be managed carefully.

According to another recent survey, about 30 percent of corporate general counsel believe their companies are unprepared to deal with a serious data breach. That's an eye-opening figure that should cause in-house lawyers and risk managers to stop and think about their own company's preparedness for such issues.

While data security presents daunting challenges for most, there are basic steps that you can pursue to protect your company against the worst cyber perils. A smart blend of careful contracting, insurance coverage, due diligence and follow-up with employees can assist greatly in reducing the risks associated with data security breaches.

Risk Management

State attorneys general, the Federal Trade Commission, the U.S. Securities and Exchange Commission and, most recently, the president have all been vocal about the need to address cybersecurity issues. Regulators fully expect that businesses of all kinds will have assessed data security risks in detail — before an incident occurs.

For example, the SEC has provided guidance to registrants as to what disclosure obligations they may face as a result of their cyberexposure. In relevant part, the SEC advises:

determining whether risk factor disclosure is required, we expect registrants to evaluate their cybersecurity 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 cybersecurity 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, cybersecurity risk disclosure 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. 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 cybersecurity risks and the potential costs and consequences
- To the extent the registrant outsources functions that have material cybersecurity 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
- Description of relevant insurance coverage

A registrant may need to disclose known or threatened cyber incidents to place the discussion of cybersecurity risks in context.

For example, if a registrant experienced a material cyberattack 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. (See Division of Corporation Finance, Securities and Exchange Commission, CF Disclosure Guidance: Topic No. 2: Cybersecurity, Oct. 13, 2011.)

This very detailed guidance obviously presupposes that businesses already have made a comprehensive review and assessment of their cyber exposures.

With regard to threats associated with foreign government agents, computer hackers or simply high-tech credit card thieves, regulators and law enforcement will not only expect that businesses are cognizant of the risks they face, but that they institute competent and diligent security procedures to safeguard electronically captured information in order to mitigate the fallout from a breach.

Of course, your customers will expect this too. Thus, a cyberbreach response plan and a cyberbreach team to implement that plan must be constituted before an incident occurs. Developing the plan and building the team after an incident will be too late in most instances.

Below is a checklist of core requirements for protecting any organization's computer systems as well as the data traveling through them:

1. In most instances, data needs to be encrypted — especially when dealing with guest account and personal information, as well as certain categories of employee information.

2. Data security protocols must be established for password protection, encryption, employee mobile devices (so-called BYOD or bring-your-own-device policies), placement of data on thumb drives/laptop hard drives and continuous employee training.

3. Data mapping is essential to know what data you have and on what systems that data resides.

4. Due diligence must be performed on any computer vendors you are considering using (for example, cloud-computing firms).

5. Regular reminders to employees are important to help ensure companywide compliance with security protocols.

Contractual terms with computer vendors (like cloud firms) are important too. Cloud contracts should typically include provisions that:

- establish clear understandings and obligations for the prompt notice of a security breach (even if the breach affects other customers of the vendor);
- provide indemnification and hold-harmless rights from the vendor firm;
- address issues of who pays for breach notification costs and forensic work if a breach does occur;

- address what insurance protection the vendor will maintain as well as additional insured status for the vendor's customer(s); and

- mandate cooperation by the vendor with any law enforcement/regulatory investigation or process that the company may have to deal with in the aftermath of a breach.

Of course, since cloud-hosting vendors have many customers — all of whom may have data compromised in a single hacking event — you should consider the true value of any indemnity or additional insured status provided by a cloud vendor as part of your overall risk management strategy for cyber risks.

In the event that the vendor loses many clients' data to a hacker, it is very possible that its insurance and/or assets will be inadequate to address the losses and needs of all of the vendor's affected customers.

Insurance Coverage

Businesses will also want to make sure that they have insurance coverage for any mishaps that occur in the course of their computing activities. There are now more options than ever to protect against cyberlosses via dedicated specialty insurance.

Also, it is important to examine what coverage the business has under its traditional insurance policies and identify where potential coverage gaps might exist. Make sure as well that coverage will be available (whether under cyberpolicies, business package policies, errors-and-omissions policies or crime bonds/policies) when cloud computing services are used. Most insurance coverage can readily be adapted to expressly cover these risks.

As always, mind the fine print. Insurance companies often revel in contesting claims on the basis of hard-to-digest exclusionary language — which sadly, is not always located in the section of the policy titled "Exclusions." It's important both to use due diligence to avoid buying policies with the most broadly written exclusions, and to be prepared to push back if coverage is denied on the basis of overly broad interpretations of such exclusions.

--By Joshua Gold and Marshall Gilinsky, Anderson Kill PC

Joshua Gold is a shareholder in the firm's New York office. Marshall Gilinsky is a shareholder in its Washington, D.C., office.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

All Content © 2003-2013, Portfolio Media, Inc.