

TEXAS LAWYER

APRIL 7, 2014

An ALM Publication

www.texaslawyer.com

4 QUESTIONS IN-HOUSE COUNSEL CAN ASK TO UNDERSTAND HOW TO PROTECT PROPRIETARY INFORMATION

BY JULIE MACHAL-FULKS

Many executives view management and protection of internal data and intellectual property as an information technology or a security issue. Many corporate attorneys are not involved in data security functions at all. This is a recipe for trouble.

To minimize the risks associated with losses of proprietary data, corporate counsel need to take an active role in developing the policies designed to protect the data. An executive sponsor needs to ensure that employees charged with management of the data receive appropriate training and reinforcement regarding protection of the data.

Here are four questions in-house counsel can ask to understand how to protect proprietary information.

1. What constitutes proprietary data that should receive protection? Every attorney representing corporations should work with the individual business teams to identify what types of proprietary data the business owns, uses or controls.

For instance, the company might control data for third parties that include personally identifiable or financial information for customers (retail and financial organizations) or for patients (health care providers). Most



midsize-to-large organizations maintain personally identifiable information for their employees including name, address and Social Security numbers, financial and retirement account information, and medical claims history.

The corporation might own protectable information in addition to employees' or clients' information. This would include trade secrets, pricing formulas, customer lists and other intellectual property. Corporate counsel must ensure that the company protects proprietary data from disclosure by employees and subcontractors as well as from discovery or misuse by business partners and third parties.

2. How can the company secure the data entrusted to it? When clients and customers provide their protectable data to a company to manage, they expect the company to take appropriate steps to secure the data. Counsel representing these companies need to review the agreements with the customers and clients to ensure that company employees are aware of the contractual obligations and can adhere to the guidelines for protecting the data.

Counsel should work with the company's chief security officer or other security workers to identify and address risks in client-facing agreements. Counsel should not rely

exclusively on the assurances of the technology or security departments but should ensure that they can conduct independent reviews of the policies and procedures.

3. How can the company protect proprietary data from disclosure by employees? The Ponemon Institute 2013 Cost of a Data Breach Study indicates that for U.S. companies, the causes of a security incident are as follows: human error (35 percent), a system glitch (29 percent) and a malicious attack (37 percent). That means that human errors and system glitches combined are almost twice as likely to cause a security incident as a malicious attack.

Because human error continues to cause a large number of security incidents, companies need to reinforce training around security issues. Employee training should include two critical components designed to protect data from disclosure by employees: 1. realistic policies that consider and balance customers' needs for information with the company's need for security, and 2. vigilant reinforcement and training to enforce the carefully designed policies.

To help give employees the tools they require to do their part to protect data, counsel needs to consider the following:

- Where will the company list the policy?
- Can employees easily access the policy?
- Is there a clearly articulated chain of command from which the employees can seek answers quickly at all times of the day or night?

- Does the policy present common scenarios that the persons who interact with the protectable data might encounter?

- Do policies provide physical safeguards as well as technical protections?

All too often, customer service representatives have little or no guidance regarding how to respond to customer requests while maintaining security and privacy. Frequently, they inadvertently violate corporate policies by sending unencrypted, unsecured data over email or providing information over the phone. These practices subject organizations to countless data and privacy risks.

4. Ensure that business partners protect proprietary data. Subcontractors and other business partners often have access to proprietary data. Companies need to ensure that their agreements contemplate protection of the data to which they have access.

Primarily, the business associate and subcontractor agreements need to include provisions that the business partners and/or subcontractors have sufficient physical and technological protections in place to protect proprietary data, particularly if the partner is a technology services company that will store data on its servers.

Counsel should ensure that the service provider, subcontractor or business partner has sufficient insurance coverage at appropriate limits to cover a potential loss, in the event that those protections fail. Finally, the company regularly should audit its vendors'

compliance with the agreements to ensure that vendors are taking appropriate steps.

Companies evaluating potential relationships with third parties should include noncircumvention agreements, which can reduce the risk that the potential business partner will use proprietary data, including intellectual property, for its own benefit.

Lawyers play a critical role in ensuring that their client companies reduce the risks associated with protectable data, regardless of whether that data belongs to customers and clients or to the company itself. Companies need to evaluate their current practices to confirm that there is a multidepartmental approach to data security.

Corporate counsel should consider implementing programs to evaluate compliance with internal security protocols, ensure adequate insurance coverage and, to the extent possible, include provisions in the agreements with customers, clients, subcontractors, and business partners designed to protect data entrusted to the company.

Julie Machal-Fulks is a partner in Scott & Scott in Southlake, where she leads a team of attorneys in representing and defending clients in legal matters relating to information technology.