Bloomberg BNA

Privacy and Security Law Report®

Cybersecurity Insurance

Before underwriting a cybersecurity risk, an insurance company will want to be certain that its insured's data security and data breach practices are reasonable, effective and defensible. It makes sense for companies to educate themselves on data hygiene best practices because cybersecurity insurers want to know that best practices have been implemented *before* they insure a company for a cybersecurity event, the author writes.

The Connection Between Reasonable Data Security Practices and Cybersecurity Insurance Application Questions

BY: KATHY DELANEY WINGER

If you've applied for cyber insurance recently, you probably had to answer a series of questions about your company's procedures and practices. If you're wondering why your insurer is asking you as many as 50 questions before making its coverage decision, you'd need wonder no more.

As a data security attorney, I keep abreast of the Federal Trade Commission (FTC) and its involvement with companies that have had data breaches. I also reviewed sample applications for cyber insurance. In doing so, I discovered a clear, unmistakable link between certain questions on cyber insurance applications and:

- practices that the FTC has found to be unreasonable in its investigation of companies that have had data breaches; or
- practices that the FTC has required companies to adopt after they have suffered a data breach.

The reason for the connection is fairly clear and makes sense when viewed from the insurance company's perspective. Specifically, before underwriting a cybersecurity risk, the insurance company will want to be certain that its insured's data security and data breach practices are reasonable, effective and defensible. In many cases, one need only look at what the FTC has found to be unreasonable as a basis for determining the exact opposite, i.e., what's reasonable or review conditions that the FTC has imposed on companies after a breach to determine what's reasonable for companies to do before a breach occurs.

Kathy Delaney Winger is the owner of the Law Offices of Kathy Delaney Winger in Tucson, Ariz., where she advises clients on data security matters. She previously was a partner in a law firm and in-house counsel to the credit card division of a national bank and financial services company.

Examples That Illustrate the Connection

AT&T and *UPromise*

When the FTC investigated data breaches that occurred at AT&T Inc. and SLM Corp.'s UPromise in 2012 and several other telephone companies in 2013, it imposed a number of conditions in connection with the resolution of its investigations and its imposition of fines (11 PVLR 61, 1/9/12). One of the conditions was a

requirement that the companies train their employees on data security and privacy issues. The FTC's actions in this regard make it clear that it's advisable for companies to adopt a data security and privacy training program for employees before a breach occurs. In reviewing applications for cybersecurity insurance, I found two questions the speak directly to this issue:

- Do you enforce a company policy governing security, privacy and acceptable use of company property that must be followed by anyone who accesses your network or sensitive information in your care?
- At least once a year, do you provide security awareness training for everyone who accesses your network or sensitive information in your care?

After their breaches, the FTC also required UPromise, AT&T and the other telephone companies to have a written plan describing how they would respond in the event of a data breach. Typically, such a plan will provide for, among other things, a breach response team whose members are assigned specific responsibilities in the event of a breach, i.e., information technology (IT) response, law enforcement, public relations, customer issues and legal issues. Once again, it's safe to assume that companies are well advised to create and implement a response plan before a data breach occurs. Not surprisingly, a cybersecurity insurance company will want confirmation that its potential insured has a written plan and its application, therefore, asks:

Do you have a written procedure that you rehearse at least yearly to ensure that you are proficient in responding to and recovering from network disruptions, intrusions, data loss and breaches of the following types:

- network attacks and incidents (including malicious code, hacking, spy-ware);
- privacy/confidentiality breaches; and
- denial of service attacks.

Home Depot

An action (or more accurately, lack of action) that the FTC found to be unreasonable when it investigated a data breach at The Home Depot Inc. in 2014 was the failure to monitor and log on to networks to detect questionable activities or unauthorized users (14 PVLR 1135, 6/22/15). The takeaway from this finding is that it's reasonable (and, therefore, advisable) for companies to monitor and log on to networks to detect questionable activities or unauthorized users. Cybersecurity insurance application questions whose purpose is to confirm that a potential insured is engaging in this practice include:

- Do you have a way to detect unauthorized access or attempts to access sensitive information?
- Do you control and track all changes to your network to ensure that it remains secure?
- Do you check for security patches to your systems at least weekly and implement them within 30 days?

In its investigation of the Home Depot data breach, the FTC also faulted Home Depot for failing to delete cardholder information after the time period necessary to authorize the transaction. In other words, Home Depot acted unreasonably by failing to properly dispose of or Payment Cardholder Information (PCI), which includes:

- credit or debit account numbers;
- security codes and expiration dates; and
- PINs.

PCI may also include Personally Identifiable Information (PII), which includes customers' or employees':

- names;
- dates of birth;
- e-mail addresses;
- Social Security numbers;
- ZIP codes;
- financial data;
- phone numbers; and
- driver's license numbers.

In light of this, companies are well advised to have a practice in place that will ensure that PCI and PII is, at all times and in all instances, properly disposed of. To confirm that companies have such a practice in place, a cyber insurance application asks:

Do you retain Non-public Personal Information and others' sensitive information only for as long as needed and when no longer needed irreversibly erase or destroy same using a technique that leaves no residual information?

The Federal Trade Commission's actions in this regard make it clear that it's advisable for companies to adopt a data security and privacy training program for employees before a breach occurs.

Finally, and again, in connection with its investigation of the 2014 Home Depot breach, the FTC found that Home Depot acted unreasonably when it failed to restrict access to cardholder data to those with a business need-to-know. Thus, it's advisable for companies to restrict access to cardholder data on a need to know basis before a cyber breach occurs. In order to confirm that companies are doing this, a cyber insurance application asks:

Do you physically and electronically limit access to sensitive information on a need to know basis and revoke access privilege upon a reduction in an individual's need to know?

  PVLR ISSN 1538-3423

Liability for a Vendor's Breach and Cyber Insurance Application Questions

The FTC has also made it clear that companies should require high standards of security for their vendors, since they can be held liable for their vendor's data breaches and/or security violations. Thus, the FTC has faulted parties for not requiring their vendors to have the same data and security standards as the companies had, if not better. *FTC v. Navone*, 2009 BL 294967 (D. Nev. 2009) (9 PVLR 134, 1/25/10); *In re Goal Fin., LLC*, F.T.C. (2008) (7 PVLR 350, 3/10/08).

To confirm that its potential insured is imposing those standards, a cyber insurance application asks: Whenever you entrust sensitive information to third parties, do you contractually require all such third parties to protect this information with safeguards at least as good as your own?

The FTC has also cautioned companies whose vendors store their customer data, that they should understand exactly how their vendors are securing the information and handling access. *FTC v. Wyndham Worldwide Corp.*, No. 2:12-cv-01365-PGR (D. Ariz. 2012) (complaint) (11 PVLR 1069, 7/2/12).

Not surprisingly, an insurer will want to confirm that its potential insured possesses this understanding by asking:

■ Whenever you entrust sensitive information to third parties, do you perform due diligence on each such third party to ensure that their safeguards for protecting sensitive information meet your standards (e.g., conduct security/privacy audits or review findings of independent security/privacy auditors)?

■ Whenever you entrust sensitive information to third parties, do you audit all such third parties at least once per year to ensure that they continuously satisfy your standards for safeguarding sensitive information?

Finally, companies are also advised to include an indemnification clause in their contracts for losses and damages they suffer as a result of their vendor's failure to protect sensitive information and to require vendors to certify that they have cyber insurance coverage.

Tracking this recommendation, a cyber insurance application asks:

■ Whenever you entrust sensitive information to third parties, do you contractually require them to defend and indemnify you if they contribute to a confidentiality or privacy breach?

■ Whenever you entrust sensitive information to third parties, do require them to either have sufficient liquid assets or maintain enough insurance to cover their liability arising from a breach of privacy or confidentiality?

How Does the Connection Affect Your Business?

There are many more data security practices that have been recommended and/or required by FTC and many more questions about any given company's data security procedures on typical cybersecurity insurance applications.

Most (if not all) of the recommended practices have a three-fold purpose:

1. to provide companies an effective means of helping to prevent data breaches and/or placing companies in the best possible position after a breach;
2. to give companies a better chance of obtaining affordable cybersecurity insurance; and
3. to put companies that adopt these practices and face a data breach in a much better position to defend themselves.

Companies should keep in mind that the FTC not only investigates the breach but can also impose hefty fines on companies involved in breaches if they find a failure to adopt commercial reasonable practices.

For these reasons, it makes sense for companies to educate themselves on the best practices, i.e., those that are reasonable, effective and defensible, and implement them sooner rather than later. It is clear from the results of FTC post-breach investigations that these practices should be in place *before* a breach occurs. Not surprisingly, cybersecurity insurers also want to know that best practices have been implemented *before* they insure your company for a cybersecurity event. The purpose of the sometimes extensive and numerous questions on cybersecurity insurance applications is to confirm that this is the case.