Why Your Organization Needs a Cybersecurity Compliance Plan

Compliance officers are not necessarily expected to be cybersecurity experts, but are expected to ask questions to assure that risks are addressed.

By Theodore Banks | Contact | All Articles
Law Technology News | December 10, 2013

Image: Clipart.com

Over the years, we've all heard stories about hackers getting access to credit card information. In addition to the financial cost of those security breaches, many state laws require 1) notification of persons whose data has been compromised, 2) financial restitution, and 3) credit monitoring for a certain period of time.

Since 2000, the FTC has brought 21 actions against the hacked companies (i.e., the "hackees"), asserting that the lack of security is a violation of §5 of the FTC Act, which states that "Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful." The FTC has been successful in other data breach cases. In 2006, the FTC obtained a $10 million penalty from ChoicePoint Inc. regarding a data breach involving more than 180,000 stolen card numbers. The agency has also gone after Twitter, HTC, and Google for data breaches, and these actions, like practically all such cases, resulted in fairly quick out-of-court settlements.

In 2008-09, hackers repeatedly broke in to Wyndham Hotel's internal network because of weak spots in the security of a franchisee-owned hotel in Arizona. The breach allowed access to more than 619,000 card accounts, many of which landed in a domain registered in Russia, with fraudulent charges to the tune of more than $10.6 million. In 2012, the FTC sued the hotel chain on the grounds that it had engaged in unfair and deceptive practices because it allegedly assured customers that it was using industry-standard practices to protect their data online, when in fact, the agency argued, that was not the case. See: **http://at.law.com/LTN13129**.

Rather than settling, Wyndham decided to fight. Attorneys for Wyndham Worldwide appeared in federal court in Newark on Nov. 7, 2013, and argued that the company shouldn't face a lawsuit under the FTC Act because of alleged cybersecurity lapses. Counsel argued that the FTC doesn't have the legal authority to tell companies how they must store customer information online.

Wyndham argued that the FTC's role in this area is limited because Congress never granted it broad powers over cybersecurity matters, but instead ordered it to oversee more targeted issues, such as protecting children online and people's personal information at financial institutions. Even if it had the authority, Wyndham argued, it has never given the industry notice of requirements through regulations or interpretative guidance. Wyndham did not challenge the assertion that its data security was deficient, but instead argued that the FTC had no expertise in this area, and should be going after "thieves and deceivers."

Find similar content
Companies, agencies mentioned
Key categories
Most viewed stories
1 No Disclosure: Why Search Terms Are Worthy of Court's Protection
2 Four Tell-Tale Signs of Insider Data Theft
3 A Glimpse at the Legal Profession's Future
4 New Legislation Adds Risks to Robo-Calling, -Texting
5 HIPAA Compliance With HP Autonomy iManage v9.0

The FTC's position is that Congressional silence on the agency's broader authority does not limit its ability to pursue breaches in corporate cybersecurity, particularly in cases where consumers have been substantially harmed. The FTC argued that companies can look to both its previous enforcement actions and a handbook it issued in which it stated that firms need to have "reasonable" measures in place to protect customer data. Wyndham, asserted the commission, did not comply with these "rudimentary" **guidelines**.

The Real Question

It will be interesting to see where the court comes out on this case, but for a compliance officer, the message is: it doesn't matter! The real question to be faced is whether there is an adequate cybersecurity system in place for customer data. Although there is a strong legal argument to be made that following the "industry standard" payment card industry protocol in the United States should be enough to avoid legal liability to the government, as a practical matter this should not be considered sufficient if sites that follow the PCI rules are penetrated.

As a compliance officer, you are not necessarily expected to be a cybersecurity expert, but you are expected to ask questions to assure yourself that risks faced by your company are addressed. So, when it comes to security of customer credit card data, make sure that your risks assessment includes the following:

- Does the organization follow the best practices from the **PCI Security Standards Council**, including the recently-released **version 3** of the PCI Data Security Standard?
- Does the cybersecurity program cover all of the 20 points included in the standards published by the SANS Institute (**www.sans.org**)?
- Does the program follow the 35 prioritized mitigation strategies from the **Australian Defence Signals Directorate**?
- Does the company have insurance to cover financial exposure—and the mechanics of remediation—from a breach? In addition to covering possible financial exposure, the process of going through the exercise of trying to get quotes from underwriters would reveal where gaps might exist, which can be quite useful.

The bottom line for compliance people is that cybersecurity should be part of your risk assessment, whether or not there is a risk of FTC enforcement. There are significant financial risks—and probably legal risks—for any company that fails to take adequate steps to protect its data, including third party data.

Sources: The Newark Star Ledger, The Wall Street Journal, Federal Trade Commission, Bloomberg Business Week, and the American Bar Association Antitrust section's publication, Secure Times.

*Chicago-based **Theodore Banks** is a partner at Scharf Banks Marmor and president of Compliance & Competition Consultants.*

PREVIOUS
The Software Act Seeks to Monitor Technology

NEXT
Nexidia Audio and Video Search Tools Integrate With Symantec

Type your comment here...

Comments are not moderated.
For more information, please see our **terms and conditions**.
To report offensive comments, **Click Here**.

REVIEW POST

Reader Comments

Lindsey Jaeger
December 10, 2013 11:37 AM

For all interested in participating in the larger conversation about cyber defense strategies and responsibilities for business and industry, consider attending the Law Informatics Symposium on Feb. 28, 2014 at NKU Chase College of Law in Greater Cincinnati. http://lawandinformatics.org/2014symposium.php

Comments are not moderated. To report offensive comments, click here.

Post a Comment »