*Risk*MATTERS

5 Cybersecurity Mistakes That Lead to Regulatory & Legal Action

by Michelle A. Reed and Jay K. Tatachar | October 3, 2016
Risk Management Magazine

WITH HACKING INCIDENTS ON THE RISE, more and more companies are being forced to deal with the consequences of their failures to adequately protect data. Although there is no overarching federal law governing cybersecurity across industries, regulators are bringing enforcement actions with increasing frequency. In addition to the danger of regulatory investigation, companies may also face private class-action lawsuits from customers. Given these legal risks, companies need to take proper cybersecurity and data protection measures in order to reduce their liability if a data breach occurs. The following are the five biggest problem areas that need to be addressed in order to avoid investigations, enforcement actions and class-action lawsuits.

1. Avoid collecting unneeded personal information, but if it must be collected, don't use it unnecessarily.

The easiest way to prevent a breach involving personal information is to not collect it in the first place. This may seem obvious, but companies fall into the habit of routinely collecting sensitive information regardless of the whether they actually need it. In its case against RockYou—which operated a website that allowed users to play games and use other applications—the Federal Trade Commission (FTC) revealed that, as part of the registration process, RockYou collected nearly 179,000 children's email addresses and associated passwords, then stored them in clear, unencrypted text. Among other things, the FTC's complaint alleged that RockYou made deceptive claims in its privacy policy by collecting the email addresses and passwords unnecessarily and left its website vulnerable to common hacking methods. To avoid getting into similar trouble, companies should create a plan to periodically assess the sensitive information they are collecting from users and determine whether they actually need it.

Obviously, many situations do call for the initial collection of sensitive information. This does not mean the information must always be used, however. Using the information when it is not needed creates unnecessary risks. In its complaint against Accretive Health, the FTC alleged that the company failed to employ reasonable procedures to ensure that consumers' personal information that was no longer needed was removed from its systems. Accretive even used personal health information in training sessions and failed to remove the data after the training finished, the FTC said. Given that the information was only used for training purposes, there was no need to use actual personal information instead of sample data in the first place.

2. Require authentication and restrict access only to company employees who have a specific business need to access sensitive information.

Another rule of thumb is that the fewer people who have access to the information internally, the less risk there will be of unauthorized access. Two FTC cases are particularly instructive. First, in its action against Twitter, the FTC alleged that the social media platform failed to prevent unauthorized access to administrative control of its system because it did not take reasonable steps to restrict access to only employees whose jobs required it. That is, a majority of Twitter's employees had far reaching power to reset account passwords, view non-public tweets, and even send tweets on a user's behalf. To compound this, the FTC alleged, Twitter failed to enforce periodic changes of administrative passwords and did not suspend or disable administrative passwords after a reasonable number of unsuccessful login attempts. All of these failures, the FTC argued, made Twitter's system vulnerable to multiple hacks between January and May 2009. Accordingly, to reduce the susceptibility to attacks, companies should only allow broad administrative access on a "need-to-know" basis to those who actually require it for their role.

The FTC's investigation of Goal Financial also demonstrates this lesson. In this case, Goal Financial, a student loan company, failed to restrict access to loan applicants' personal information to only authorized employees. As a result, some employees transferred more than 7,000 files with consumer information to third parties without authorization. One employee even sold surplus hard drives to the public that contained the unencrypted information of about 34,000 consumers. The chances of this occurring could have been drastically reduced by only allowing specific employees with real business needs access to the sensitive information.

3. Use industry-accepted methods to store and transmit sensitive information securely, and ensure service providers do the same.

Companies must ensure that personal identification information is maintained securely during all stages of its use. To achieve this, there is no need to reinvent the wheel. Rather, it is often better to use tried and true industry standards to implement safeguards. For example, in the case against ValueClick, the FTC alleged that the online advertiser and its subsidiaries either failed to encrypt the information at all or used non-standard, proprietary encryption with a simple alphabetic substitution system that was subject to vulnerabilities.

Depending on the nature of the data or business needs, personal information may need to be transferred to separate business units. Companies should ensure that all servers used for transmission and storage employ industry-accepted encryption methods. One example would be Transport Layer Security/Secure Sockets Layer (TLS/SSL). It is not enough to use this encryption in just one stage of the data's lifecycle. Superior Mortgage Corporation learned this the hard way. Despite the lender's claims that sensitive personal information collected at its website was encrypted using SSL technology, the FTC alleged the information was only encrypted while it was being transmitted between a user's browser and the website's server. Once the information was received, it was decrypted and emailed to Superior's headquarters and branch offices in clear, readable text.

Hackers will look for vulnerable entry-points along the entire transmission route, regardless of whether the data is controlled by a company or a third-party service provider. The FTC has clearly underscored the importance for companies to utilize industry-accepted, end-to-end data encryption methods.

4. Be prepared by developing a comprehensive incident response plan.

Because the methods used by cyberattackers are constantly evolving, there is always a chance that hackers may be successful in breaching even the savviest company's cybersecurity systems. Therefore, safeguards are just one part of an effective data privacy and cybersecurity policy. Companies must also have a plan in place to quickly identify, respond to, and minimize the effects of any potential breach.

In the consumer class-action context, once breaches occur, plaintiffs may rely on a variety of federal and state law claims to bring actions. Two cases illustrate the two different viewpoints on cybersecurity and incident response plans. First, in the case *In re: Target Corp. Customer Data Breach Litigatio*n, plaintiffs lawyers highlighted "leaked" reports of internal communications highlighting an allegedly flippant attitude among C-level employees regarding cybersecurity. Target has accrued more than $290 million in expenses in connection with the breach, but still faces a few remaining claims almost three years later.

On the other hand, having a previously instituted cybersecurity plan will protect directors and officers, who may be subject to shareholder suits alleging breaches of fiduciary duties in the wake of system breaches. In the *Palkon ex rel. Wyndham Worldwide Corp. v. Holmes* case, for example, the court dismissed a shareholder derivative suit in a data breach case after finding that the directors and officers had not breached their duty: Outside counsel had advised the company not to sue the directors and officers for breach of any duty and the company hired third-party experts to implement post-breach measures.

Companies should have a well-developed and practiced incident response plan that provides the internal processes for responding to a breach and identifies key providers, including outside counsel and IT forensics teams.

5. If there is a data breach, carefully weigh the nature and scope of your notice.

An important part of any incident response plan is the speed and efficacy with which the company communicates the scope of the breach to those who are potentially affected. This is particularly important in states with laws requiring notification within 45 days of discovery of the breach. The decision of what to include in the notification can have serious ramifications. Indeed, a company's notice disclosure can actually work against it in litigation. In *Remijas v. Neiman Marcus Group LLC*, for example, Neiman Marcus followed state laws and disclosed that 9,200 payment cards had experienced fraud and that customers should check their credit reports. The Seventh Circuit then relied on these notice statements in concluding that plaintiffs had established a substantial risk of harm to confer standing for a class action.

In another recent Seventh Circuit case, *Lewert v. P.F. Chang's China Bistro Inc.*, P.F. Chang's quickly announced that it had sustained a data breach before it knew the true scope of the breach. The June 2014 public statement addressed customers who had dined at all stores and admitted that the company did not know how many stores were affected. Within a week of the breach, it discovered that only 33 stores were affected. During the Seventh Circuit appeal, P.F. Chang's argued that the customers in the case had dined at a restaurant not among the 33 affected. The court rejected this argument, however, pointing to the early notice that warned all customers that they were at risk.

In view of these two cases, it would be prudent for companies to determine the precise scope of a breach before issuing any public statements that could be used in future litigation.