wiley

NEWSLETTER

Key Steps in Responding to Security Breaches

July 2016

Security breaches remain big news, virtually every day. Companies in all industries still deal with stolen laptops and mobile devices. Hackers are engaged in ever more brazen schemes, to gather personal and proprietary information. Data thieves are using personal information for identity theft and tax fraud. Insiders steal or mis-use data for a wide range of purposes, including health care fraud, sale of celebrity details to tabloids and other inappropriate purposes. In addition to personal information, companies face theft of the most sensitive corporate information, including intellectual property, strategic planning and client information. The latest concern —soon to be replaced by something even newer—involves "ransomware," where data (of virtually any stripe) is held hostage, without a company's ability to access or use it.

Each breach incident stands on its own. Companies try to develop protocols that fit these problems into categories, but the details of each situation matter a lot. Nonetheless, in the event of any kind of security breach, there are some key questions that always need to be asked. Following these steps will enhance your company's ability to respond and address any kind of security breach, and deal effectively with the legal and operational implications of these breaches.

Identifying the problem

The first question is figuring out what happened. This needs to take place in both an immediate "triage" sense, and in a short term but more thoughtful approach, depending on the situation. Some incidents will be revealed quickly to be small or one-time events (a specific lost device or misdirected package). Other incidents (e.g., a hacking attack) may require a more comprehensive immediate and

Practice Areas

Privacy, Cyber & Data Governance

ongoing effort to evaluate and contain.

One key tip—make sure your employees know where to go if they become aware of a potential problem and that they know to go there fast (and without doing too much investigation on their own). One consistent problem for companies involves failures to report potential breaches, with time delays causing a broad variety of problems. Your people can't go home for the weekend hoping that a device will be found.

Determining the cause of the problem

Once you have a handle on the problem, why did it happen? Was there a training issue? Were your procedures inappropriate? Did you have an information security protection that didn't work the way you anticipated? Determining this cause will go a long way toward both fixing the problem and making sure it doesn't happen again.

Evaluating any potential harm from the problem

What kinds of problems could result from the breach? Did it involve "only" corporate information, where the potential harm is to your company or a client, rather than individuals? Was the information personal data and, if so, was it in the "more sensitive" areas, such as social Security Number or credit card information, or health care information regulated by the HIPAA rules? What might happen to individuals as a result of the breach? Such harm issues can dictate some of the immediate mitigation steps, greatly impact your notification obligations, and may lead to much more significant legal concerns related to a breach.

Stopping the bleeding from the problem

Another key question is whether you can stop any potential harm—or make sure it doesn't get worse. Some breaches will be revealed to be "over"—the full extent of the breach has happened, and there's nothing else to do other than work through the impact. That's pretty unusual though. In most situations, there are steps that can be taken to reduce or mitigate potential harm. If information was lost, can it be found? Can you make sure that nothing happened to it? Can you cut off a hacker's access to your data? Can you stop sending data to a vendor that has a problem?

All such steps require thought and quick action. If there are actions that can reduce or mitigate harm, they need to be taken quickly and aggressively.

Evaluating appropriate changes (if any)

In any breach, there are lessons to be learned. It is clear that enforcement agencies both want changes made right away when there are problems, and will be more aggressive if problems are not fixed or problems recur because changes are not made. It is critical that fixes be implemented—even if it turns out that the potential incident was not a big problem. I have found repeatedly that companies that do an investigation and determine that no notification of individuals is required often do not do a good job of fixing the

underlying problems. That's risky—mainly because the next time might be much worse.

Determining any legally required steps (or appropriate business steps)

Once you have a good handle on what happened with the breach and what you need to do to address the specific incident, you need to make sure that your company has evaluated the legal obligations and business implications resulting from the breach. Do you have an obligation to notify customers? Regulators? Law Enforcement? Does it make sense to do so anyway? Did the breach involve corporate information, with implications for ongoing business activities or transactions? There are many laws that address obligations to customers if the data is personal data – there are fewer legal obligations related to corporate information, but the potential implications for your business from a corporate breach may be greater. Think broadly both of what you are required to do by law, and what you should do for the sake of your business operations (including contractual commitments that go beyond your formal legal obligations and "doing right" by individuals).

Are you required to (or should you) notify individuals?

The most focused legal question involves notice obligations to individuals. This is the area most highly regulated by law, particularly for the range of sensitive information covered by state breach laws (such as SSNs, credit cards and bank account numbers), along with the array of health care information regulated by the HIPAA rules. Based on too much experience, many companies are becoming familiar with these obligations, but individual notification remains both complicated and risky. The details of the laws are expanding, the range of data covered by them is growing, and the plaintiffs' bar seems to be pouncing on every meaningful breach notification letter. For regulated industries, particularly under HIPAA, a reported breach leads to an investigation that will cover a broad range of overall compliance practices. The notice dilemma involves an evaluation of both the legal requirements and appropriate judgments about notification implications. Pay close attention to these details, get appropriate advice, and don't always just follow what you have done in the past.

What Else?

These questions and issues are highly likely to be relevant in every potential breach situation. It is critical to have a team in place that can address these matters thoughtfully and efficiently. At the same time, it is always critical not to treat this situation "just like the others." Resist the temptation to shoehorn this into a prior approach. Each breach needs to be treated on its own. Is there something particular that is different about this one? We know it likely involves different data and a different root cause than the last one, but what else? Should law enforcement be involved? Was this an insider issue? Could this have been easily prevented? Did this involve the same problem that happened before? How does this event fit with your prior breach history? Is this a recent acquisition that requires immediate attention? Make sure that you are considering these broader issues, even in the context of a need to act swiftly and thoughtfully to address the situation.

Breaches remain challenging. They are stressful, often require quick action in challenging times, and may have substantial implications for the business activities of the company along with significant legal and reputational risk. Make sure that you have a plan in place that covers these key issues—and that you have a good team ready to act quickly if you have one of these situations (as virtually all companies will).