American Law Institute CONTINUING LEGAL EDUCATION From ALI CLE's *The Practical Lawyer*

Responding to Security Breaches

Kirk J. Nahra and Edward Brown

Kirk J. Nahra is a partner with Wiley Rein LLP in Washington, D.C., specializing in litigation and counselling related to privacy, data security and cybersecurity in the United States and across the globe. He chairs the Firm's Privacy Practice and co-chairs its Health Care Practice. He represents companies in virtually every industry in navigating the complexities of privacy and security laws and regulations, across industries and jurisdictions. He can be reached at 202.719.7335 or knahra@wileyrein.com.

Edward ("Ted") Brown is an attorney with Wiley Rein LLP in Washington D.C. Mr. Brown represents clients in a variety of civil litigation matters, primarily focused on insurance coverage and commercial litigation before federal and state courts. He regularly counsels insurers in connection with first-party and third-party claims and coverage disputes involving data security and privacy breaches. He can be reached at 202.719.7580 or erbrown@wileyrein.com.

SECURITY BREACHES remain big news, virtually every day. Executives and managers understand it is a question of "when," not "if," their companies will be targeted. Companies in all industries, as well as a host of other organizations, are affected. Hackers are engaged in ever more brazen schemes to gather personal and proprietary information for a variety of motives. Data thieves are using personal information for identity theft and tax fraud. Insiders steal or misuse 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. Laptops or other devices are stolen, lost, or misplaced, often triggering an incident response. A more recent concern—soon to be replaced by something even newer—involves "ransomware," where data (of virtually any stripe) is held hostage, without an organization's ability to access or use its own data. Companies and not-for-profit enterprises are being attacked from virtually every angle.

Each cyber incident stands on its own. Companies try to develop protocols that fit its 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 a company must ask and address. 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.

1. Identify The Problem

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

Tip. Make sure your employees know where to go if they become aware of a potential problem, and make sure that they know to go there fast (and without doing too much investigation on their own). One consistent problem for companies involves their own employees failing to report potential breaches in a timely manner, which leads to a variety of problems. Your people cannot go home for the weekend hoping that a device will be found.

2. Identify Available Insurance

One of the keys to responding to a breach, and one undertaken in parallel with incident response (or prior to a breach in the first place), is to identify potentially responsive insurance coverage. Often, the persons within an organization primarily responsible for data security are not the same persons steeped in insurance matters, so it is crucial to ensure open communication between all functional departments. Further, as discussed below, a detailed incident response plan (improved through a tabletop exercise) can go a long way in reinforcing to the key players the need for a multi-pronged approach.

Tip: In addition to cyber insurance coverage, a company may evaluate other "traditional" coverage lines to identify whether coverage may exist. To the extent a company does not have a cyber policy, it may seek to purchase that coverage as part of its overall data security and risk management strategy. While selecting the proper insurance coverages goes far beyond the scope of this article, a company should be mindful of all needs and risks in securing coverage.

3. Involve your insurer

For myriad reasons, assuming the company has cyber insurance coverage, it will want to involve its cyber insurer at the earliest time possible. Besides complying with its contractual obligations under its policy, this will enable the company to tap into the insurer's vast experience in dealing with all types of data breach scenarios. One of the most critical tasks, vendor selection, is often best performed when made with the input of the company's insurer, which has every incentive to recommend the ideal service provider to efficiently and effectively manage the response. In addition, many insurers have pre-negotiated rates and established relationships with a variety of vendors, the benefits of which inure to the insurer's policyholders.

Tip: Even if your company has a large self-insured retention that is unlikely to be exhausted by a particular event, notify your insurer. As noted above, insurers can often help by providing valuable expertise to help manage the breach. In addition, the size or scope of the breach may (and often does) grow beyond the threat as originally understood. Finally, notifying the insurer may protect the company in the event a claim arising from the incident is later brought against it.

4. Engage Counsel

Another early step a company will undertake is to engage counsel. Even before a company is fully aware of the nature or extent of a breach, counsel can provide invaluable guidance – particularly during the critical early stages. The first stop should be the organization's general counsel. If the company's own legal team does not have the relevant expertise to sufficiently address the matter, it can determine whether outside counsel should be retained to aid in incident response. In addition, engaging counsel early can enhance the likelihood that certain communications will be protected from

disclosure later on.

Tip: Many small and mid-sized companies do not have outside privacy counsel lined up at the time they learn of a breach. As a result, they are often rushed into quickly settling on counsel where, with better preparation, they could have identified the counsel best suited to their particular needs. Many law firms have "privacy experience," but the level of depth and focus across firms in this space is staggering. In addition, certain firms may specialize in certain aspects of data security (such as, for example, experience representing merchants in disputes with card brands), but they have little expertise in dealing with other aspects of a breach that may be required in a given scenario. In addition, engaging with counsel before a breach happens (or before it is discovered) can often be a helpful way to prepare for response activities if (or when) a breach takes place in real life.

5. Determine the cause of the problem

Once you have a handle on the problem, you may ask the questions: 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 the cause will go a long way towards both fixing the problem and making sure it doesn't happen again.

Tip: In determining the cause, it is often important to bring in professionals from a variety of disciplines. Clearly, forensic investigators are an invaluable resource. But there also may be a need to focus on other vulnerabilities, such as physical security or financial control issues. Experienced counsel can help an organization understand the "unknown unknowns" it may be facing, and guide it to uncover those issues.

6. Evaluate Any Potential Harm From The Problem

Another series of questions a company should ask concern the potential fallout from the breach: 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? These issues of harm will dictate some of the immediate mitigation steps, will greatly impact your notification obligations, and will lead to much more significant legal concerns related to a breach.

Tip: Assessing the harm can often be elusive because, in many instances, the full scope of the breach takes time for the company to uncover. There are also many examples where companies inform their customers they have fixed an issue, only to disclose later on that, in fact, they failed to understand the full nature of the event. Thus, both in the company's investigation and in its communications strategy, it is critical to understand both what it knows and what it doesn't.

7. Stop The Bleeding from the Problem

Another key question is whether you can stop any potential harm—or make sure it doesn't get worse. Investigations will prove some breaches to be "over"—meaning that the full extent of the breach has happened, and there's nothing else to do other than work through the impact. But that's pretty unusual. 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 of these steps require thought and quick action. If there are actions that can reduce or mitigate harm, they need to be taken quickly and aggressively.

Tip: Conducting "tabletop" exercises may better prepare companies to respond to a data breach. These exercises, performed by a company (often with outside consultants and counsel) before an actual breach, can often help the key players prepare for a breach response. These exercises

also may reveal potential holes in a breach response plan, and they enable the organization to address these issues before an actual event.

8. Evaluate 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 for a company to implement these fixes—even if it turns out that the potential incident was not a big problem. We 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.

Tip: Implementing recommended changes can also be critical to protecting the company in the event of a subsequent breach. While judges and juries certainly understand that not every data breach is preventable, the argument that the company acted reasonably in protecting its data is far less compelling when it knew of a known vulnerability yet failed to address it. Similarly, insurance policies often afford no coverage for harm resulting from vulnerabilities that were known to the organization yet, for whatever reason, the organization chose not to address.

9. Determine 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 your business operations (including contractual commitments that go beyond your formal legal obligations and "doing right" by individuals).

Tip: While notification is in some instances required, that is not always the case. This leaves the company with a decision—should it notify even in the absence of a legal or contractual obligation to do so? Many organizations will decide (and counsel will advise) to notify. But that can be counterproductive, such as by in confusing customers or damaging the company's reputation unnecessarily. As a result, where there is no legal obligation to notify, a company should think twice before deciding to notify anyway.

10. Are You Required To (Or Should) 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.

Tip: Timely evaluation of the potential harm is critical. Most states will trigger notification

obligations from the date the first harm was discovered. In other words, once the breach is discovered, the company's "clock" is ticking. In addition, most notification statutes require notice within a reasonable time, and consumers have alleged in many instances that even where a company notified its customers within the time set forth by the applicable statute, it still was not timely.

11. 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.

CONCLUSION • 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. For some companies, a data breach represents an existential threat. Make sure that you have a plan in place that covers these key issues – ideally one that has been implemented, at least in a tabletop setting—and that you have a good team ready to act quickly if you have one of these situations (as virtually all companies will).