CLIENT EMERGENCY CALL:

OUR DATA HAS BEEN STOLEN!

Important Steps Before That Call

By Benita Kahn

Receiving a call that your client's company is the common point of purchase[1] or discovering that the database where your client's employee information is maintained has been hacked starts the beginning of a long journey. Most articles focus on the journey that starts with this call. This article, however, will focus instead on what should be in place before that call is ever received – a well prepared incident response plan. This plan will lay out the step by step process to be followed on this data breach journey. Having a plan in place will provide your client's company the advantage of considering each step included in the plan as it is executed after the event, rather than reacting and creating while in the midst of a public relations crisis.

Many companies have incident response plans in place that have been created by their Information Technology group. However, often those plans are technology-specific and can miss some of the more practical steps that should be considered. An important first step is to create a simple escalation process. When creating this process, the company should consider use of an already familiar means for employees to report their suspicion of a data breach. For example, consider whether the company has a help desk that might be trained to take these types of employee calls as well.

Whatever group is selected to provide intake for the initial internal call, the individuals in that group should be trained to know what additional information should be obtained, how to conduct an initial evaluation of the severity of the risk involved and who receives the escalation of this information. Regardless of the severity, there must be a means to quickly pass on the information to those who will be making decisions about the event.

This leads to the next step in the escalation process for suspected data breaches, which is consideration of the formation of a committee in advance that includes all the possible stakeholders for such an event. This could include possible "owners" of the information, legal (in house and outside counsel), public relations, information technology, risk management. It is important to designate one of these individuals as the person to receive the call from the initial intake, to further evaluate who the necessary stakeholders are for the specific event and to determine the means by which these individuals will be contacted. For example, if employee information has been stolen, HR would be the "owner" of the information, but if customer information is stolen that might involve a different set of "owners."

This committee will then need to quickly start making decisions on such issues as: i) next steps for further investigation, including a determination of what type of data was stolen (e.g. paper or electronic, specific personal information taken) and whether outside forensic assistance is required, ii) if a breach has occurred, the means to end the outflow of stolen data; iii) how to control communication about the investigation, iv) whether third party contracts impose notice, forensic or other obligations in the face of a data breach, v) whether individuals must be notified and how; vi) if the secret service should be contacted; vii) how to ensure that business can continue as usual in the face of correcting for the data breach, and viii) how to immediately begin limiting the company's liability exposure.

Notification obligations become a significant part of an incident response plan. Forty-six states have now enacted laws that require notifications when a data breach involves what is defined in the statutes as personal information. The incident response plan should prepare for these notification requirements. Generally, "personal information" is defined as first name or initial and last name combined with a social security number, or driver's license number or financial account number (e.g. credit or debit card, bank account, investment account number). In most states, the notice laws only apply to unauthorized access to electronic personal information,[2] but fortunately exclude notification if the electronic personal information is encrypted.[3] Some states allow an evaluation of risk of harm before notice is required, so this will need to be considered by the committee that is formed. Several states require notification of affected individuals within 45 days, which is very quick when your client is in the midst of a crisis. Unfortunately, the information that must be included in a notice letter to affected individuals is not the same for every state. It is recommended that draft letters be prepared in advance and be part of the incident response plan.

In addition to notifying individuals whose information was stolen, a dozen states[4] require notification of state officials such as the Attorney General or consumer protection department and many state laws require notification of the three major consumer reporting agencies (Experian, Trans Union and Equifax). All of the necessary contact information should be included in an incident response plan.

Continued on Page 28

Fraudsters

Continued from Page 27

In addition to the states, if healthcare information is involved in the data breach, then the regulations enacted by Health and Human Services for protected health information (PHI) and by the Federal Trade Commission for personal health record information (PHR) must also be considered. Both regulations have specific requirements and very short fuses for notification (60 days from discovery of the breach, which is defined as when the company should have known of the breach). While encryption is a "safe harbor" for these notice obligations, the regulations of these federal agencies require a specific type of encryption.[5] Prepared draft notices and address information for the notices should also be a part of a complete incident response plan if the company retains either PHI or PHR information.

When reviewing the list of considerations for the incident response committee and the various notice of breach laws, it is easy to see that making decisions on all of these issues in the middle of a crisis can easily lead to more mistakes. Having a written information response plan, training people with roles in the plan and updating the plan regularly will help your client reduce, and hopefully eliminate, additional mistakes in the face of the discovery of a data breach.

---

1. This means that counterfeit credit card numbers have been tracked back to a common legitimate use at your client's company.
2. Alaska, Arkansas (medical information), Delaware (medical information), Hawaii, Indiana (if computerized data is transferred to paper, including microfilm), Maryland, Massachusetts, North Carolina, South Carolina, Utah, and Wisconsin apply their notice laws to paper data breaches as well.
3. However, in several states notice is still required if the encryption key is also stolen.
4. Hawaii, Louisiana, Maine, Maryland, Massachusetts, Missouri, New Hampshire, New Jersey, New York, North Carolina, South Carolina, Virginia.
5. So far, two specific examples of encryption have been deemed to meet the requirements: (1) for data at rest, encryption consistent with National Institute of Standards and Technology Special (NIST) Publication 800-111 and; (2) for data in transit, encryption that complies with Federal Information Processing Standard 140-2.

bakahn@vorys.com

Benita Kahn,
Vorys Sater Seymour and Pease