

August 4, 2008

Prepare a formal plan to respond to data breaches

By Brad Gow

The rash of recent high-profile privacy breaches in U.S.-based companies continues. According to the Privacy Rights Clearinghouse, at least 100 organizations have reported losing the sensitive information of more than 9.4 million people so far in 2008.

Increasingly sophisticated hacking techniques combined with new identity-theft legislation have created a potential minefield for companies maintaining consumer information on their networks. In addition to the public relations headaches companies experience following a privacy crisis, they may also face the direct costs of notifying customers, litigation initiated by affected individuals and financial institutions, Federal Trade Commission fines and penalties, and even directors and officers liability lawsuits.

Recent well-publicized breaches by prominent retailers have focused senior management attention on the need to prepare for data breaches arising out of network hacking, misplaced files and lost computer equipment.

Priority one is keeping sensitive information secure.

The initial focus of any plan is to prevent the data breach in the first place. A comprehensive information security plan, incorporating controls around people, processes and technology, should be drafted on a macro level. As most litigation stemming from data breaches alleges negligence in the handling of sensitive customer information, formal plans and demonstrated security investments will help your organization defend itself in court, if necessary.

In addition to assigning formal management responsibility for privacy to a single individual, organizations should create internal working groups to coordinate the risk management, legal, information technology and human resources functions. Effective information security can't be accomplished merely with new equipment in your server room. In most cases, people are the weakest link.

Priority two is being prepared for the inevitable with the use of crisis management planning.

No data is completely secure given the complexity and changing nature of today's corporate networks. Despite the implementation of comprehensive information security measures, companies must be prepared to quickly and effectively respond in the event of a privacy breach. The last thing a CEO needs after a serious privacy event has occurred is to have his senior team react to the crisis in 'panic mode.' A moderate amount of preparation can go a long way, and should include the following components:

- Identify a specific individual to manage the crisis and direct operations. There should be no question about who is in charge once the crisis team is assembled.
- Preapprove third-party forensic specialists to be called in immediately. In addition to providing triage and securing the network, these technicians should be trained in mirroring compromised servers and protecting the evidentiary chain of custody for potential legal action against the perpetrators. Specialists are required for this important job; in-house IT staff should not

be used. Properly mirroring servers and network equipment and maintaining and documenting a proper chain of custody so that evidence can be used in court is a detailed process and can easily be mismanaged by those individuals who are not used to performing this function on a daily basis.

- Agree upfront on a policy of honest, open communication. Organizations in crisis mode must balance the desire to minimize potential liability with the need to dictate and control their media story. Information concerning a privacy breach is eventually going to come out. You can choose to release it yourself and control the message, or allow the media and blogging community to spin the story for you.

- Commit to immediately involving the FBI in the event of a hack or extortion attempt. If the data loss is not accidental, law enforcement should be notified. Identify the FBI Internet Crime Bureau contact in your city or state and incorporate this into your crisis management plan. In some cases, engaging law enforcement can also be grounds for delaying public notice of the event.

- Identify a single individual, preferably a senior executive, to communicate with the media. The individual should be well-versed in the crisis management plan. Depending on the organization, it may also be wise to preapprove a third-party crisis management communications company with experience in data breaches to assist that individual.

- Develop contingency plans for different types of breaches to which your organization may be susceptible. Predrafted letters to customers and business partners (with noncontroversial technical detail to be inserted) should be prepared and approved in advance so time-consuming reviews and sign-offs in the middle of a crisis are not necessary.

- Purchase privacy liability insurance coverage. If your company maintains a large amount of sensitive customer information on its networks, purchasing insurance can be a good idea. The coverage available in the market today is much more comprehensive, and affordable, than ever.

Remember Watergate. If it's not the crime that gets you into trouble, it's the cover-up. Reasonable people understand that accidents occur. Companies should be prepared to provide detailed information about a breach as soon as they have confirmed its accuracy. The data has already been lost. You can use the crisis as an opportunity to communicate openly and honestly with your customers, or you can alienate them by withholding information and relying on self-serving technicalities. Instituting a formal plan and reacting in an appropriate and responsible manner during the crisis will pay off in the long run.

Brad Gow is vp of ACE USA's Professional Risk division in Philadelphia.

