Effectively Managing a Data Breach

By Eric Samore

Introduction

There are many ways a business may experience a data breach. Employees are human who sometimes mishandle protected information and/or fail to secure devices. International cyber criminals operate outside the reach of the US justice system. Chances of a breach have increased due to the explosion of: (a) internet traffic, mobile devices, software applications, and cloud based data traffic used by businesses; and (b) sensitive data handled by employees.

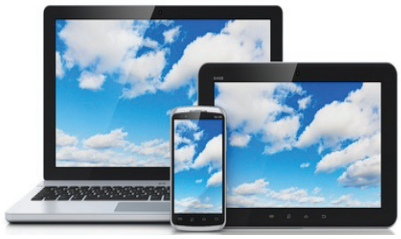
"There are only two types of companies: those that have been hacked, and those that will be," according to the former FBI director Robert Mueller. The costs associated with a data breach will vary depending upon the character of your response. Handling an incident poorly will diminish reputation, sales, earnings and profit. Advance preparation for a data breach is central to limiting the scope of losses. Preparation includes a written breach response plan, which identifies the key individuals with responsibilities for responding to an incident. Studies have documented that a response plan reduces the cost of a breach.

A data response plan should include the procedures for limiting the exposure, preservation of evidence and communicating your plan to business partners and customers. A response team needs to be clearly identified before there is any breach. The plan should include procedures and processes to be taken to see that the breach is limited and does not spread.

Choose Your Response Team

The response team should consist of technology, management, risk management, legal, public relations and others depending on where and how the breach occurred. Within your organization, all necessary decision makers should be included. There should be a clear channel of authority akin to the military in responding to a breach. The team needs to be identified and deployed rapidly. Time is critical. Rapid deployment will be facilitated if your organization has practiced and rehearsed the response in accordance with the plan.

Because of the importance of preserving evidence, you will promptly want to consider retaining a forensics expert to determine if his or her involvement is required. Most organizations do not have IT departments with forensic expertise, and experience in making sure that all relevant evidence is preserved. Internal IT departments typically do not have the qualifications to make sure that the systems has been forensically copied and preserved during an investigation. An outside consultant should be specifically trained in preserving evidence in the process of responding to a breach.



You will also want to immediately talk to your insurance broker to report the claim to trigger coverage if you have insurance. Insurers work with experienced professionals who can step in immediately to address the breach.

At the same time, you will need to consider retaining outside counsel. Outside counsel can supervise the investigation in a way that maintains confidentiality of communications. They will determine your reporting obligations so as to reduce fines, penalty, and regulatory investigations. Outside counsel can also provide advice for a consistent message that minimizes the public relations fallout.

Identify What Information Has Been Breached

Valuable evidence is often inadvertently lost after a breach has been discovered. It is critical to preserve all relevant evidence. Otherwise, for example it may be impossible to trace the hacking that occurred.

Ascertaining what kind of data has been breached and who owns that data is a basic threshold inquiry. Is it the protected data such as social security numbers, credit card numbers, names and addresses? Who are the owners of that data and where do they live. These are the basic questions that have to be answered in order to comply with your legal obligations.

Communicate to Comply With the Law and To Restore Customer Trust

Counsel should be hired to determine your reporting obligations in accordance with all applicable state statutes and federal regulations. Notification obligations may extend to affected individuals, law enforcement and administrative agencies. Data breach reporting laws vary depending in part on the residency of the person's whose information is at risk. The time constraints imposed by the states varies from jurisdiction to jurisdiction.

Above and beyond your legal reporting obligations and of equal importance are the concerns of your customers. Your customers are concerned with what measures have been put in place to protect them and what steps will be taken to improve the security of their information. Customers will want to know if they can trust continuing to do business with you. Credit monitoring and identity restoration services can provide the security that customers are looking for which can also reduce the chance of litigation.

Try to speak to the media with one voice. Do not communicate a data exposure estimate to the media until you are confident regarding its accuracy. Communicating different estimates over a period of time serves to prolong and exacerbate the bad news in the eyes of the public. Convey that you are taking steps to protect your customers and their information.

Conclusion

If a data breach occurs, keep your cool. Keep your mind focused and clear on the tasks at hand: assemble your team; preserve evidence; identify the information at risk; identify the owners of the information; comply with reporting obligations; and maintain public trust. If the incident is handled properly, the consequences to your bottom line may be surprisingly limited.

for further INFORMATION, please contact
Eric Samore
312.894.3251
esamore@salawus.com

150 N. Michigan Avenue, Suite 3300
Chicago, IL 60601