What would you do if you had a data breach?

By John Immordino CIC, CRM, RPLU, CIPP/US

According to recent Symantec research, 60% of small businesses will close within six months of a cyber-attack. Are you prepared to handle a breach?

One of the first questions that I ask clients is "What would you do if you had a breach?" The response is usually along the lines of a glazed over look, followed by eyes rolling into the backs of heads. I usually know at this point that I will need to educate my client. I start by informing them that 60% of businesses fail to recover from a breach. Why? Because those businesses are not familiar with state data breach notification laws, the costs associated with a breach, and the reputational harm that the business will incur.

The majority of business owners consider reputation one of their most important assets. Small business owners work in the same communities that they live, shop, go to church and where their kids go to school. When clients provide their private information, they expect the business to keep it safe. If the client suffers a breach of this information, the client, and, by extension, the local community, lose faith in the business. As a matter of fact, 38% of clients will leave after a breach and 46% of them will advise friends and family to be careful sharing information with that local business.

This is why the number one concern is to help my clients protect sensitive information and prevent a breach from happening. Many insurance carriers will offer risk management web portals as part of their insurance policy. These are excellent resources for companies that need assistance in identifying and protecting the private information they have. These portals also provide useful tools in training the business employees on the importance of privacy. Some of these same carriers will provide the insured with a public relations firm to help them announce the breach in a way that will mitigate their reputational harm.

When it comes to discussing privacy laws, the best approach is to keep it simple. There are numerous state and federal privacy laws that business must comply with, but I usually focus on one: state notification laws. There are currently 47 different state notification laws. In a general sense, these laws state that if a business collects private information on state residents, they are required to protect that information. If the business fails to protect the information and there is a breach, they must notify the affected individuals within a certain time frame. If the residents are not notified within that time period, the business can be assessed civil money penalties.

The challenge is determining when the business has to notify the affected individual and when the clock starts ticking. Most states specify that they must notify "without unreasonable delay." Some states will actually provide a number of days that can range from five to 45 days. The new national legislation being proposed will be 30 days. So, to keep from getting fined up to several hundreds of thousands of dollars, the business must notify the residents as soon as possible.

The notification will consist of three steps: forensics, legal and mailing. The first step is to find a forensic investigator to assess the breach. Forensics will determine what happened and identify the individuals whose private information has been compromised. This list will then go to a legal counsel specializing in privacy laws. Counsel will determine which laws are applicable to the situation, and suggest compliance methods, including how to structure the notification letter.

All states have specific requirements on how these letters need to be written. After the draft is completed, the letters are then mailed to the affected individuals. This is a complex process that must be completed in a certain time period. Because of this, clients that do not have a formalized response plan are best served by being placed with a carrier that will provide one for them. Several carriers will offer turn-key breach responses or otherwise assist an insured through the breach response process.

The costs associated with handling a breach can cripple any business. Depending on the report being reviewed, these costs can range from $1,000 to $13,700,000. The important thing to remember is that the cost of the breach is not relative to the size of a company.

Instead, the cost associated with each breach has to do with the type of information compromised, the regulatory climate and how the information was compromised. According to a 2014 NetDiligence report on 111 actual cyber liability insurance claims, the average claim payout is $733,109. This amount is inclusive of forensics, notification, legal guidance, public relations, legal defense, legal settlement, regulatory defense, regulatory fines and PCI fines. Because the notification costs can vary so greatly, we usually recommend carriers that will respond to the notification obligation on the basis of a record count outside the limit of liability, instead of a set, static dollar value limit.

It has often been said that it is not a matter of if you will have a breach but when. Educating, training and insuring are the key components to helping your organization be part of the 40% survival rate. The MIIAB has partnered with Arlington/Roe® to offer their members the Big "I" Agents Cyber Secure Program. This program was developed for insurance agents to provide them with the tools to reduce their exposures and the insurance to respond to a breach.

John Immordino *is a vice president of professional liability at Arlington/Roe, a wholesale Insurance broker. He is the administrator of the nationally endorsed Big "I" Agents Cyber Secure Program. This program is only available to member agencies through their IIABA state associations. He can be reached at jimmordino@arlingtonroe.com or 800-878-9891, Ext. 8732.*