Data Breach Response Best Practices
Prepared for Experian

Conducted by
Javelin Strategy & Research
May 2009

Introduction

You Are Not Alone

If your institution experiences a breach, know that your company is not alone. Hundreds of breaches are occurring each year, with the number of breaches in 2009 already totaling 170[1] separate incidents as of April. The volume of breaches peaked in 2008, with the Identity Theft Resource Center's 2008 breach report revealing 656 reported breaches, for a 47% increase over 2007's total of 446.

While businesses and organizations are taking necessary measures to prevent security breach incidents, it has become widely known that even the most "secure" institutions are not immune to data leakage, whether accidental or intentional. Recent breaches involving leading financial institutions, the businesses trusted most by consumers, has proven this point. While the ideal goal is to prevent a data breach from occurring in the first place, the industry is coming to realize that preventative measures, no matter how advanced the security technology is or extensive the resources are – offer no guarantees.

Breaches can also be costly events, especially if the data-loss incident occurs on a larger scale and affects tens of thousands of customers. On average, breaches can cost an organization $4.1 million, or $197 per record breached, when factoring losses such as lost business, fines and litigation costs, lost shareholder value and reputation damage. Overall, 65% of the cost of the data breach is due to lost business.

Clearly, breaches can affect all organizations, regardless of size or perceived strength in security defense resources. Therefore, an institution's response to a data-loss incident makes all the difference. Businesses and organizations can work to protect reputations and customer relationships by ensuring effective, timely and comprehensive assessment of the data exposed, communication with customers and employees, and protection for those individuals who are at higher risk of fraud.

[1] 2009 Breach Stats Report, Identity Theft Resource Center, Accessed April 29, 2009.

Recommendations for Data Breach Response and Planning

Handling a breach can be overwhelming and daunting, especially if the incident is sudden and your company is unprepared. Here are recommendations for immediate post-breach response and planning, notification and long-term breach preparation.

Responding to an Unexpected Breach

If your company is limited in resources (namely staff) and/or time, or not sure how to respond to a data-loss incident, consider consulting with a breach-resolution agency. This may be an option for smaller to mid-size businesses or organizations that have never experienced a breach or may be in the middle of creating a data-breach response and resolution plan. There are a number of breach-resolution providers out there, with some vendors focusing on notification and customer services, and others providing a comprehensive solution that includes everything from forensic analysis to consumer new accounts fraud protection such as credit monitoring for victims.

Once the breach has been detected, engage in a thorough investigation and forensic assessment of the data accessed, individuals who have been affected, and potential causes of the breach. This procedure must be executed immediately in order to take relevant action; in other words, the exact size, scope and severity of the breach must be identified before determining next steps. Again, for smaller companies without dedicated IT security specialists on hand, there are firms specializing in forensic data analysis and risk assessment that can examine the important details of a breach incident.

Notification – How to Notify your Customers

Notify affected customers in a timely, thorough and clear manner. Breach notification should occur immediately after the incident and via more than one channel, depending on the scale and sensitivity of the information compromised.

To the extent that is possible, ensure that notification information is comprehensive enough to cover "who", "what", "when" and "how". "Who" would be the identity of the breached entity; "what" would be the general description of what happened and the specific data that has been exposed; "when'' is the timeframe of the breach; and "how" includes steps that the instiution is taking to address the situation, regardless of where the breach occurred, as well as next steps that victims can take to ensure prevention and detection of possible fraud.

Empathize with your customer to maintain trust and loyalty, and assure your customers they are being protected. If the breach occurred at your institution, consider including an apology in the notification to breach victims, as well as information and tips to protect against identity fraud. More importantly, let your customers know what steps are being taken to protect them.

Recommendations for Data Breach Response and Planning

In the event of a larger-scale breach that occurs internally (and not through a third-party business partner or vendor), establish a Web site with further information and a breach response call center to address inquiries from concerned breach victims. Some customers will prefer different channels, either to read more information or to talk to a bank representative directly to be guided on next steps.

Notification should include:	
√	General description of what happened
√	Specific description of the personal information breached
√	Information about what you have done to prevent further unauthorized access of the individual's personal data
√	Exactly what you will do to assist the individual, including your toll-free number and personalized Web site for more information. If fraud does occur, the victim will need resolution services.
√	Steps the individual can take to prevent and detect fraud

Notification Checklist

Protecting Breach Victims Who Are at Higher Risk

If Social Security numbers are among the pieces of data that has been exposed, consider providing identity-protection services to reduce the risk of new accounts fraud. There are a variety of identity fraud protection solutions such as credit monitoring and fraud alerts that **are** specifically designed to prevent or detect new accounts fraud (usually perpetrated by stolen Social Security numbers). In order to mitigate the risk of new accounts fraud occurring among customers with exposed SSNs, offer a complimentary subscription to an identity-protection service.

Long-Term Data Breach Response Preparation

Establish a structured data breach response plan that can adapt to the evolving data security environment. Generally, institutions handling sensitive data must have a **formal** policy for breach response, but this policy must be flexible enough to accommodate changing business or operating needs and address new security threats, as well as changing legislation.

Set up a cross-functional data breach response team to handle highly targeted communications as part of your planning. This breach response team is different from the incident response team that must do the forensics on the breach. Instead, this group must take the information from **the** forensics group and rapidly begin the process of

Data Breaches Negatively Impact Customer Relationships

Now that 44 U.S. states are requiring institutions to notify customers when their information has been exposed, consumers are increasingly learning about breach incidents and consequently becoming more aware of the security risks involved in losing sensitive information. Three out of four consumers believe fraud is increasing, according to Javelin consumer data. Notification of a data breach is likely to cause confusion and even fear among those informed. Given the tremendous misunderstanding surrounding identity theft, identity fraud, and security breaches, some consumers may mistakenly assume that exposure of their personal information has resulted in actual fraud.

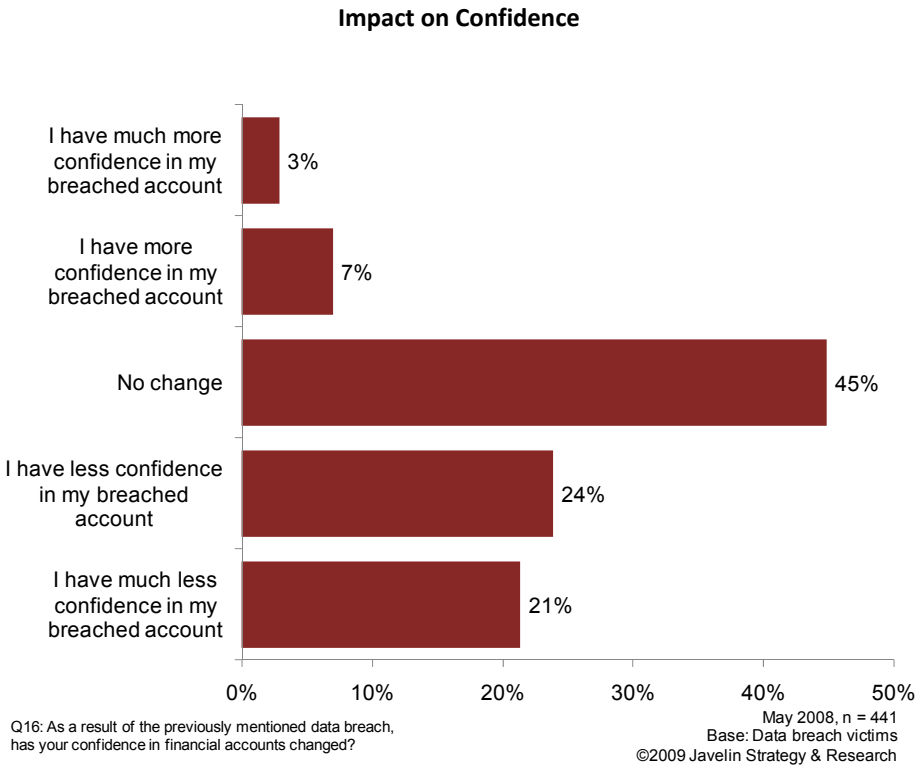
The importance of an institution's response to a data breach then becomes paramount in maintaining customer loyalty and brand security. Clear, thorough and timely notification is an essential obligation of the breached entity, as victims deserve to know when and how they have been affected. Most importantly, victims will want to know the action to be taken by the breached institution to protect victims against potential fraud. In other words, aside from an explanation of the incident and an apology, consumers are questioning what the institution will do to fix the situation for breach victims personally.

Breached institutions are increasingly providing new accounts fraud protection solutions to victims, namely in the case of exposed Social Security numbers (SSNs). Some companies that have experienced a data leakage incident have offered one to two years of credit monitoring, while others are providing annual subscriptions to fraud alerts services. The provision of identity protection services to breach victims with exposed SSNs is becoming a "best practice" of sorts, with progressively more institutions understanding the positive effect this offering has on customer relationships. By offering an actual solution to the problem, the breached organization is assuming full responsibility and going beyond solely admitting fault. Providing a fraud protection solution is also an effective way to address those breach victims who may react strongly to initial notification.

An Investment in Your Brand

Breaches are about more than identity theft or fraud; they can place a company's brand equity and customer loyalty at serious risk. Though difficult to quantify, the loss to an organization's brand becomes evident through lost business and less interaction with customers. An institution's response to a security breach may ultimately worsen or salvage any potential reputation damage left behind by a data-loss incident. How an institution reacts to a breach is a testament to its philosophy on the importance of data privacy and protection, as well as corporate responsibility. A responsible organization that handles sensitive information will thoroughly assess a breach situation, communicate openly and immediately with victims, and offer adequate protection for those who have been placed at risk of fraud.

Data Breaches Negatively Impact Customer Relationships



Data breaches can result in diminished customer confidence, which may ultimately lead to less interaction and therefore less business. The majority of breached accounts involves compromised credit and debit account numbers, and Javelin consumer data shows that 45% of breach victims have less confidence in their financial accounts as a result of being a victimized by a data breach. While credit and debit card numbers are cited by most consumers as being exposed in a breach (38% of breach victims), SSNs are nearly as likely to be exposed, with 37% of breach victims citing SSNs as being lost, stolen or compromised in a data breach. SSNs are used to perpetrate new accounts fraud, the most damaging type of identity fraud, and thus are highly valued by identity criminals.

Consequently, breached institutions must respond aggressively to prevent the loss in customer confidence and potential impact to their bottom line. The notification process should consist of immediate and apologetic communication that clearly describes what happened and how it affects the victim individually, and reassures victims that they are being protected. The most effective way for an institution to demonstrate its sympathy and concern is to proactively offer complimentary fraud protection, in the form of identity protection services such as credit monitoring, fraud alerts, credit freezes and personal information monitoring services.

Conclusion

Data-loss incidents negatively affect consumer confidence, resulting in serious implications for customer loyalty and reputation. Furthermore, consumers seem to have little faith in the ability of organizations to safely process and maintain their information, and many believe that certain institutions need to do a better job of protecting their personal information.

With even the most resource-rich organizations experiencing breaches, institutions need to look beyond simply investing in technology systems and staff in hopes of completely avoiding a potential security breach. Therefore, responding to a data leakage becomes all the more important. Aside from immediate and clear notification, breached institutions stand to benefit by taking action on behalf of the victims. With the exposure of highly sensitive information such as Social Security numbers, breached institutions are expected to go beyond standard notification procedures and demonstrate the steps being taken to safeguard victims against fraud. The most relevant and appropriate action is for the breached institution to offer an identity fraud protection solution, which will address the security concerns of breach victims and minimize the risk of fraud.