



Seven Steps to
DATA BREACH
Readiness



DATA BREACH READINESS



Few events can damage a company's reputation more than losing the personal confidential information entrusted to a business by its customers - a data breach. Even before factoring in the negative impact to employee morale, business partner relationships and regulatory dialogues, a data breach can be very costly if not handled properly. Customers have shown a propensity to stop doing business with companies that cannot protect their confidential information, and do not take care of their customers when a breach occurs.

Recent high profile data breaches have shown us that financial institutions, retailers, health care providers, educational institutions and others are all susceptible to losing data.

Despite enormous investments in prevention, breaches continue to occur with alarming regularity. According to the Identity Theft Resource Center (ITRC), in 2010 there were 662 data breaches that exposed more than 16 million records, of those, 5.9 million were attributed to two large data breaches. Also, based on the March 2011, "Consumer Sentinel Network Data Book" released by the Federal Trade Commission (FTC), more than 1.3 million consumer complaints were received in 2010, with identity theft being the number one complaint category at 19% of the overall complaints.

Clearly prevention efforts are not enough. Companies also need to proactively plan for the worst case scenario that a breach actually occurs. "Breach Readiness" is a state of preparedness where all of the key decision makers have been identified, the key support relationships have been put in place, the applicable legal and regulatory requirements have been assessed, and the plan for action is ready to execute in the unfortunate event that a data breach occurs.

Intersections Inc. has been a leader in the fight against identity theft for over a decade. We have protected the identities of 32 million consumers and helped tens of thousands of individuals recover after a verified case of identity theft. We understand the harm that a corporate breach event can cause for companies and their customers, and we offer a full line of Breach ReadinessSM products and services to provide both peace of mind and a compelling brand experience.

The purpose of the "Seven Steps to Data Breach Readiness" guide is to help organizations get started on the path toward taking care of customers when a data breach occurs.

1

ASSIGN RESPONSIBILITY FOR BREACH READINESSSM

Data breaches are by nature interdisciplinary events that require coordinated activities from numerous functional departments such as IT, Operations, Legal, Public Relations, and Customer Service. When a breach occurs, companies quickly find themselves wrestling with questions such as:

- How did this happen?
- Who does it impact?
- What are our legal and regulatory obligations?
- How will this impact our bottom line?
- What should we do?
- Who is in charge?

Having a Crisis Management team already established ensures the response and actions that follow are timely, coordinated and effective. Just knowing who needs to be consulted and who gets to make decisions puts companies ahead of the game when a breach occurs.

Many companies already have incident response teams as a part of their technology, operations, security or business continuity teams. Leveraging one of these existing teams to manage data breach response activities is a great way to ensure that your Breach ReadinessSM plans are implanted when an event occurs. Key success factors to look for in developing a crisis management team for breach response include clearly identifying the following:

- Who is responsible for the success of your breach response
- How to declare a data breach has occurred
- Who needs to be informed of a data breach
- Decision makers and their levels of authority

DEVELOP A BREACH READINESSSM STRATEGY

“If you don’t know where you are going, any road will get you there.”

– *Lewis Carroll*

The same is true for breach response. Far too often, the road taken by institutions experiencing a breach is simply to follow the legislative and regulatory requirements for notification of impacted customers. In this type of response, impacted customers typically receive a highly legalistic notification letter letting them know they are a victim of a breach, and urging them to “be wary”. This may be the appropriate breach response for some companies despite the poor customer experience. However, it certainly does not represent the highest order of strategic planning for such a critical moment in your relationship with your customers.

Ideally, institutions in possession of customer confidential information should take the time to explicitly decide upon a Breach ReadinessSM strategy that is right for their unique circumstances. The response strategy must include fulfilling any legal or regulatory obligations, but can also explore a much richer set of issues. Questions to explore in this strategic dialogue include:

- What data do we possess and how do we protect it?
- How damaging will the loss of confidential data be to our customers?
- Are we more concerned about the cost of breach response or the cost of lost business from a poor response?
- How damaging will negative public and regulatory relations be to our business?
- Do we want to offer a complimentary breach response product to impacted customers as a means of retaining their business?
- What tone do we want to take in our breach related customer communications?
- Are our answers above the same for all of our customer segments?

Thoughtfully answering the questions above will help companies choose the right road to Breach ReadinessSM.

3

UNDERSTAND YOUR REGULATORY AND LEGAL REQUIREMENTS

Data breach notification laws and regulations vary widely by industry, state and type of breach (for example, criminal incursion versus accidental data loss). Forty-six states, plus the District of Columbia, the U.S. Virgin Islands and Puerto Rico all have their own laws stipulating who must be notified in certain breach situations. The number of laws will continue to grow and there continues to be much discussion regarding federal regulations as well. Industry regulators, voluntary associations, internal policies and others impose additional requirements that may or may not conflict with a company's legal obligations.

Some situations call for immediate customer notification to help prevent misuse of confidential information and additional monetary losses. Other situations require absolute confidentiality to give investigative resources the opportunity to identify suspected bad actors. Some states require notification and disclosure of the nature of a breach. Other states prohibit disclosing too much information in order to prevent copycat crimes. Of course, all of this only describes the lay of the land in breach laws at the time of writing this guide. By the time you read it, most likely, someone somewhere will have already enacted new rules that change your obligations in response to a data breach.

Staying current in this ever changing environment is an important part of your Breach ReadinessSM program. Since facts and circumstances are different in every breach event, only a qualified attorney who understands your unique circumstances can adequately advise you on your legal or regulatory obligations. However, industry primers such as *Intersections' Data Breach Consumer Notification Guide* can help start you on the path to successfully navigate this complex environment.

CHOOSE A HIGH QUALITY IDENTITY THEFT PROTECTION PRODUCT FOR IMPACTED INDIVIDUALS

When a breach occurs, your customers can feel betrayed and at risk. Certainly, recovery from a breach involves expenses for legal professionals, IT staff, public relations and many other out-of-pocket costs. However, third party studies have shown that the biggest cost to businesses from a data breach is the loss of future business from impacted customers. How well you manage the breach response directly affects your future revenue line.

Offering breach response services to your customers provides you with an opportunity to turn a potentially bad situation into a positive brand experience. Customers want companies to take responsibility for the breach and protect them from the potentially damaging consequences of identity theft. While the actual incidence of identity theft from a data breach is low, the threat to your brand is real and long lasting.

Research has shown that customers expect a lot from a breach response service, including:

- Knowledgeable staff who can answer questions about the breach in plain language
- Victim assistance services that cover the costs of actual identity theft and help the customer restore their good name
- Access to their credit reports and monitoring of credit report changes to help prevent identity theft

However, even this level of service will not fully protect your customers. For example, credit bureau monitoring may help stop the creation of new loan accounts, but does little to identify account takeovers or new non-credit accounts for services such as mobile phones or utilities. Worse still, many breach response product providers have highly effective marketing materials that claim to provide great levels of protection, backed by less than substantive actual operations.

Well-prepared companies research breach response services and their options before a breach occurs. With the right information in hand, you can confidently determine which breach services provider will best uphold your commitment to safeguarding your customers' data and your image in the event of a crisis. Contact Intersections at Partner@Intersections.com to allow us the opportunity to explain the marketplace and your options for Breach ReadinessSM products.

5

ESTABLISH BREACH RESPONSE OPERATIONS

You have made all of the strategic decisions and know what you are willing to invest to retain your best customers. You are well on your way to Breach ReadinessSM, but you are not quite at the finish line. Numerous detailed questions remain to be tackled, such as:

- Who will print our legally required notification letters?
- What exactly will they say?
- Who will answer the calls from concerned customers?
- Will we issue a press release?
- How will customers enroll in our breach response products?

Most companies find these detailed implementation issues far more challenging than the strategic questions related to breach response. It is frequently clear from the beginning that companies want to maintain their customers by offering compelling breach response products. However, companies typically do not have the internal staff available for letter printing, breach related customer service and breach response product enrollment. Negotiating agreements with partners to handle these operational tasks is better done far in advance of a breach rather than during the heat of a crisis situation.

Strategic choices also play a critical factor in establishing breach operations. Some companies offer breach response products to their impacted customers, but make it quite difficult for customers to understand the offer and enroll in the service. Other companies encourage their customers to enroll by making the offer clear and compelling, and following up with one step enrollment options both via the internet and via a professionally staffed and trained call center. Your breach response operations need to be matched with your customer service philosophy and breach response strategy. Make sure you understand how your customers will be treated before signing any contracts for breach response operations services.

Intersections is a full service Breach ReadinessSM firm offering not only a wide-range of the best breach response products in the industry, but also a full complement of breach operations services such as notification letter templates, letter fulfillment, online and offline enrollment, and customer service support.

CREATE A BREACH RESPONSE COMMUNICATIONS PLAN

When a breach occurs, numerous internal and external constituents may need to know the details of the situation. Executives, customer-facing employees, customers, suppliers, press and regulators all may have legitimate needs to know some or all of the details behind the breach event and response. Disseminating this information in a controlled manner requires detailed planning of the messages, audiences and communication channels. This way, when a breach occurs you are ready to update customer service lines and websites, contact media outlets and regulators, and inform senior executives quickly.

Once consumers learn of a breach, by whatever means, you can be certain that they will desire more information on both the breach event and what you are doing to safeguard their data. Their ability to get that information is another important component of eliciting a positive assessment of your company's handling of the situation. In order to ensure consistency, most companies find it helpful to drive communications from a set of "frequently asked customer questions" and associated responses. Getting the message right is easy if everyone is working from the same set of facts. Sample, "FAQs" for a breach response include:

- What happened?
- How did it happen?
- Who was impacted?
- What data was lost?
- What have you done to make certain it does not happen again?
- What are you required to do by law?
- What are you doing to help me ensure I am not a victim of identity theft?
- How can I enroll in identity theft protection?

With answers to the questions above in hand, your public relations, regulatory affairs and internal employee communications teams will be well-armed to deliver the appropriate breach response messages. If you do not have internal communications staff, numerous communications firms are well-suited to helping you craft and deliver these messages.

7

TEST YOUR BREACH READINESSSM PLAN

Data breaches demand a coordinated response from multiple departments within your organization. The success of that response depends largely on how well you have planned ahead. The best-laid plans, however, will be ineffective if not implemented correctly. Testing your plan regularly will help ensure that your plan is effective and that the right people within your organization know how to call the plan into action.

Communication and training are critical. Key personnel in each department must be aware of their own authority and responsibilities, but also how their role fits into the larger strategy for Breach ReadinessSM and response. Try using the steps we have already covered in this guide as an outline for corporate Breach ReadinessSM training. Topics covered could include:

1. Roles and responsibilities for Breach ReadinessSM
2. Breach response strategy
3. Laws and regulations impacting breach response
4. Breach response products for our customers
5. Breach response operations
6. Breach response FAQs
7. Breach response testing plans

If your key employees understand your corporate strategies and plans on all of the topics above, you most certainly will have achieved a high state of Breach ReadinessSM. Congratulations!

THE THREAT OF A DATA BREACH IS REAL, IF NOT CERTAIN

Knowing that the threat of a data breach is real, your company needs to be prepared. Planning ahead is the key to maintaining customer faith, complying with required regulation and the ensuring the continuity of your day-to-day business.

PROVIDE PEACE OF MIND TO YOUR CUSTOMERS

Be proactive today. Pre-define your organizational roles and responsibilities to avoid redundancy and mistakes by creating your crisis management team ahead of time. Make sure you are able to fulfill your regulatory reporting by understanding the different requirements across the country. Allow your company to provide assurance to your customers by being ready to respond, offering them protection services that include easy enrollment and making expert representatives available for counsel. Avoid costly mistakes by executing a contract with a breach services provider before a breach occurs. Arrange to have your corporate communications plan, pre-drafted customer notification and call center capabilities established, as well as how you will message the event internally to your employees.

TAKE ACTION TODAY

Well-prepared companies emerge from a breach with a timely, effective response for their customers and the potential for long-lasting damage to their reputation mitigated.

877.983.9850 | PARTNER@INTERSECTIONS.COM
WWW.INTERSECTIONS.COM

ABOUT INTERSECTIONS

Intersections' Breach ReadinessSM is the leading provider of data breach remediation services. We have implemented hundreds of programs to help our clients both proactively prepare for and quickly react to data breach events. Through our wide range of services, our clients, including financial services, health care, education, retail, e-commerce, hospitality, and payment processing companies, have been able to reduce the extensive costs of a data breach from consumer attrition, legal liability and negative public reactions.

Through our exclusive partnership with ITAC, the Identity Theft Assistance Center - a member-supported, non-profit organization founded in 2004 by The Financial Services Roundtable with unique operational ties to fraud prevention departments at major financial institutions - we can directly help resolve your customers' identity theft problems. No other data breach response provider can provide this level of victim assistance.

In 2004, Breach ReadinessSM was launched by Intersections Inc. (Nasdaq: INTX) a leading provider of consumer and corporate identity risk management services, with over \$364 million in revenue in 2010. Eight million consumers are actively protected by Intersections' consumer and breach remediation services offered through North America's leading financial institutions, directly to consumers under its award-winning IDENTITY GUARD[®] brand (www.identityguard.com), and through its exclusive partnership with ITAC, the Identity Theft Assistance Center. Since its inception in 1996, Intersections has protected 32 million consumers.

Call us at 877.983.9850 or email us at Partner@Intersections.com to find out how we can help your company establish a Breach ReadinessSM program.

If you have currently experienced a data breach, call our Breach hotline at 888.283.1725 or email us at DataBreachServices@Intersections.com.





1.877.983.9850 | Partner@Intersections.com

www.intersections.com