

Finding the Right Balance:

Data Breach Prevention vs. Response

Larissa K. Crum
Executive Vice President
Immersion, Ltd.

Brian Zawada, MBCP
Director of Consulting
Avalution Consulting

No organization expects to have a breach; in fact, most organizations have gone to great lengths and spent tremendous amounts of money to prevent them from happening. However, a strategy is needed to minimize the cost and reputational damage associated with a data breach when proper prevention techniques fail.

Benjamin Franklin stated that “an ounce of prevention is worth a pound of cure”. If Benjamin Franklin was alive today and knew about data breaches, he would likely amend his quote to say “a cup of prevention and an ounce of response are worth a pound of cure”. Since we can’t look to Benjamin Franklin for his wisdom, we have to rely on those who have been involved with data breach planning and response from the beginning.

Kathryn Maginnis created the Veterans Administration’s (VA) first Incident Response Team to continuously monitor and assess all privacy and security breaches throughout the VA. She is currently the Associate Deputy Assistant Secretary for Risk Management and Incident Response in the VA’s Office of Information and Technology. Featured in the Fall 2009 issue of the IANewsletter, she describes one of the lessons learned from a 2006 event where a laptop with considerable personal information was lost. “All data breaches cannot be prevented, but they can be anticipated. Having policies, processes, and personnel in place to report and respond to the breach enables the organization to respond optimally.”

Reported data breaches continue to increase as the world transitions from paper to electronic information – mainly as a result of individuals who inadvertently misplace or lose a laptop, poorly code software, or accidentally post sensitive information on the internet. Unfortunately for organizations, the news media continues to broadcast glaring examples of misplaced proprietary information and security events, such as:

- The Transportation Security Administration (TSA) accidentally posted - on a public website - a manual that contained complete details about its airport screening procedures.
- Health Net of the Northeast’s loss of a hard drive containing seven years worth of unencrypted personal, financial and medical information of approximately 1.5 million of its customers.

“All data breaches cannot be prevented, but they can be anticipated. Having policies, processes, and personnel in place to report and respond to the breach enables the organization to respond optimally.”

No organization expects to have a breach; in fact, most organizations have gone to great lengths and spent tremendous amounts of money to prevent them from happening. However, a strategy is needed to minimize the cost and reputational damage associated with a data breach when proper prevention techniques fail.

Prevention Isn’t Perfect

Every organization has a responsibility to protect the information they’ve been entrusted with -whether that information is Personal Identifiable Information (PII) – which includes full name, social security number, bank account information, credit/debit card numbers and driver’s license numbers – or Personal Health Information (PHI) – which includes medical diagnosis, patient history and medications. However, many organizations only focus on prevention of security breaches and fail to address the response activities needed should a breach occur. While it is logical to focus initially on prevention, response planning cannot be ignored. Since 2005, almost 340 million records containing sensitive personal information have been compromised in security breaches according to the Privacy Rights Clearinghouse.

You Won't Have Time

Each year, new regulations governing data breach response are enacted. While there are forty-five state regulations on PII, two federal laws have received significant attention:

On December 8, 2009, the House of Representatives passed H.R. 2221: Data Accountability and Trust Act, which specifically requires written notification to individuals who have had their PII compromised. If adopted, this will be the first federal requirement relative to PII breach notification and will preempt the existing state statutes.

The HITECH Act of 2009, which went into effect in late September of 2009, requires HIPAA covered entities and business associates to notify individuals who have had their PHI compromised. Enforcement of the HITECH regulations went into effect on February 22, 2010. In addition to the requirements identified in the HITECH Act, an increasing number of states are requiring separate notification and additional compliance measures when PHI breaches occur.

All of these regulations have one common requirement: when a breach occurs, you must respond and notify affected parties as quickly as possible, often within sixty days. Planning and preparation are not only key to meeting regulatory requirements in the event of a data breach, but also to protecting your organization against devastating financial and reputational impacts.

Let's Make a Plan

In a breach response situation, an organization must answer numerous questions in order to effectively respond and manage the event. That is where preplanning comes into play and provides significant value. Having key questions answered upfront saves days and weeks worth of frenzied back and forth following a data breach.

At a high level, it's important to carefully consider each of the following topics when developing a data breach response capability, or assessing a current-state strategy:

- The plan, which summarizes breach management processes, workflows and protocols, as well as notice production and call handling capabilities
- The data breach response team

Let's explore each of these topics in greater detail.

Data Breach Planning, Response and Notification – The 5 Issues You Must Consider

1. Establish Protocols For Discovery, Determination and Escalation of a Data Breach
2. Identify Your Data Breach Response and Notification Obligations (seek legal advice)
3. Establish a Cross-Functional Response Team
4. Document and Test a Plan to Ensure Nothing's Missed
5. Implement a Notification Production and Call Center Capability

Establishing the Response Plan

The first step in planning is to recognize that data breach preparation is a subset of an organization's incident response and business continuity planning efforts. "Siloing" data breach planning is never a cost-effective method of preparedness. Instead, consider integrating data breach response with crisis management and incident response plans, and establishing data breach incident protocols and procedures consistent with the larger preparedness effort.

Most importantly, there must be policies and procedures established to allow a team charged with responding to a breach to make the necessary decisions to minimize impact and stay in compliance with regulatory requirements. There are several issues to consider for inclusion in an organization's incident response plan, as it pertains to data breach response and notification, including:

1. Does the organization have policies and procedures in place to handle the detection and escalation of a breach situation to the appropriate level of management? Are legal and regulatory issues considered in these policies and procedures?
2. Are procedures in place to assess the impact of a breach, and is the organization adequately prepared with proactive crisis communications strategies to notify key stakeholders?
3. Does the organization have the ability to manage a large scale breach and produce quality notification letters representative of the organization's brand and image?
4. Does the organization have the ability to handle a flood of calls from customers responding to the breach notification?
5. Does the organization have a plan to manage all returned, undeliverable notifications?
6. Has the organization identified, or does it have available, proper legal, forensics, and e-discovery guidance needed to handle the breach and prepare for compliance with the various notification requirements?

Establishing and training the right team members, and getting buy-in from senior management, are critical in order to develop, maintain and implement an appropriate data breach response strategy.

Having a plan isn't always enough. The organization must explore the extreme details of its breach management and response strategy in order to protect its reputation. For example, if your organization cannot provide appropriate answers to such questions as: "Who is signing the notification letter?", "Is the customer address file current?", "Has a toll free number been obtained that can be referenced in the notification letter?", then it is likely that your organization has over-allocated its resources to prevention and under-allocated its resources to response and preplanning. In that case, additional effort will have to be put forth to answer these and other similar matters in order to be prepared for the worst.

Establishing the Response Team

Establishing and training the right team members, and getting buy-in from senior management, are critical in order to develop, maintain and implement an appropriate data breach response strategy. Due to the nature of a breach and the various state and federal requirements, it is often necessary to include representatives from Operations, Information Technology, Public Relations, Marketing, Legal, Customer Service, Privacy and Risk (as well as others, depending on an organization's circumstances). Each team member holds a key piece of information and a differing perspective relative to the development of an effective data breach response. Each team member may contribute in multiple ways, including impact assessment techniques, authoring the notification letter, coordinating media relations, or vendor management. Each link in the chain is critical. Knowing who is performing which response procedure is imperative in the event that a breach occurs.

Who Should Own the Planning Effort?

Clearly, a cross-functional team should be charged with responding to a data breach event. But who should “own” the planning effort? The answer to this question isn’t as important as the recognition that a qualified individual should take a leadership role in the planning and plan maintenance effort. No one person will have all of the competencies and experiences necessary to address this issue alone. As a result, the person charged with leading the planning effort must be a skilled facilitator with knowledge of other organizational preparedness efforts. It is also important for that person to understand the organizational structure and culture, and be respected by those who must contribute to data breach response strategy design and decision-making.

Summary

Individuals responsible for preparedness efforts have the opportunity to help navigate organizations through this relatively complex issue. It will be important to deliver the message to senior management that optimal preparedness will require a balance of prevention and preplanning / response efforts. Organizations wrestling with data breach response planning and preparation are faced with three key challenges:

1. Understanding the multiple federal, state, customer and other organizational requirements that influence the design and implementation of response and notification strategies
2. Enhancing existing strategies and plans in order to capture data breach response needs
3. Implementing adequate notification and call-handling capabilities that satisfy the organization’s regulatory obligations

Overall, the approaches and concepts outlined in this whitepaper will contribute to the improvement of organizational preparedness and regulatory compliance. With what’s at stake, the proposed federal regulation on the horizon, the HITECH Act already in effect, and the forty-five diverse state statutes, there is a unique opportunity to be “out-in-front” to better prepare your organization for a crisis event with significant financial, regulatory and reputational consequences. A data breach or an inadvertent disclosure of PII or PHI is an event that may very well impact your organization in the future regardless of investment in prevention.

No one person will have all of the competencies and experiences necessary to address this issue alone. As a result, the person charged with leading the planning effort must be a skilled facilitator with knowledge of other organizational preparedness efforts.

To learn more about data breaches and planning approaches for such a threat please refer to the following resources:

- ❑ **Self-Assessment:** [Data Breach Response Preparedness](#)
- ❑ **Web Article:** [Data Breaches: A Sidewalk Sale of Consumer and Personal Information](#)
- ❑ **Webinar:** [Data Breach - The Missing Piece in Your Business Continuity Program](#)
- ❑ **News Article:** [Ponemon Institute Study – Data Breach Costs](#)



Avalution Consulting specializes in business continuity strategy design, development, implementation and long-term solution maintenance. Our team excels at implementing customized business continuity

programs and enabling in-house personnel to execute and maintain continuity plans through effective knowledge transfer processes and compelling training concepts. Avalution is also recognized as a participant BSI Americas Associate Consultant Program (ACP). As a certified firm, Avalution assists in preparing organizations for BS 25999 certification as well as assessing readiness for the certification process.

In addition, Avalution offers The Planning Portal (TPP), a completely customizable, web-based business continuity software that delivers an easy-to-use set of tools and processes to assist any organization, regardless of size, with developing and maintaining business continuity and disaster recovery-related information – including analyses, plans, awareness content and exercise results.

www.avalution.com | www.theplanningportal.com | 866.533.0575



When Data is Breached

Immersion, Ltd. is based in State College, PA in Penn State's Innovation Park. Immersion provides a comprehensive data breach notification service - **InfoLaunch®**.

InfoLaunch® offers its customers a package of pre-data breach readiness and post-breach printing, mailing and call center services. InfoLaunch® provides businesses with valuable assistance in complying with both the existing 45 state data breach notification laws and the new HIPAA-protected health information breach notification requirements contained in the HITECH Act. InfoLaunch® helps a company that has experienced a data breach, whether of personally identifiable information or of protected health information, to communicate its informative message quickly and effectively to its customers and employees who have had their personal and confidential information compromised in a data breach incident. These incidents are happening with increasing frequency and scope. Such carefully crafted written communication helps a business not only comply with state and federal legal notification requirements but also to protect the organization's brand reputation and shareholder value from erosion due to the breach.

www.useinfolaunch.com | www.immersionltd.com | 866.377.8210