IDENTITY GUARD®
BUSINESS SOLUTIONS

6 Steps
to Data Breach Preparation

888-283-1725
IDENTITYGUARDBUSINESS.COM

IDENTITY GUARD®
BUSINESS SOLUTIONS

TABLE OF CONTENTS

888-283-1725
IDENTITYGUARDBUSINESS.COM

More than 9 billion records have[1] been lost or stolen as a result of breaches since 2013.

This guide will help you put a plan in place that will take care of customers and minimize damage to the brand in the event a data breach 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.

Despite enormous investments in prevention, breaches continue to occur with alarming regularity.

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. And as the number of data breaches rise, identity theft crimes have increased; the Federal Trade Commission reports that identity theft is the second largest complaint category[2].

Because of the prevalence of data breaches and the far reaching possible effects of the loss of data, it's important to put together a plan to quickly respond should your company experience a breach.

[1] Identity theft resource center source: BreachLevelIndex.com, Gemalto NV, 2017
[2] FTC "Consumer Sentinel Network Data Book" March 2017

1 Assign Responsibility

Having an incident response team already established ensures the response and actions that follow are timely, coordinated and effective.

Knowing who needs to be consulted and who the decision maker is can help put your organization 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 so if you already have one, leveraging one of those teams to manage your breach response activities could be a great start.

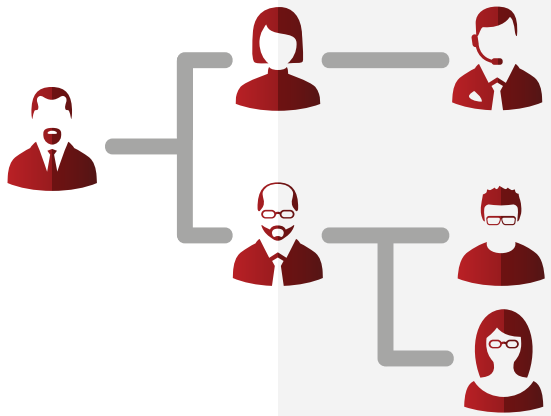
Most Valuable Players in an Incident Response Team

When creating your incident response team, each team should have an Incident Response Lead to direct and manage the IRT members. The most effective teams will have members representing the following departments:

- Executive Management
- Information Technology
- Legal
- Compliance & Privacy
- Customer Relations
- Communications

Identify the following key success factors when building your incident response team:

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



2 Understand Your Regulatory and Legal Requirements

Data breach notification laws and regulations vary widely by industry, state and type of breach.

For example, there may be different laws to follow when the breach is caused by criminal incursion, such as when a hacker accesses your databases, versus an accidental data loss, such as when an employee loses a laptop with sensitive data.

Forty-eight states, plus the District of Columbia, Guam, the U.S. Virgin Islands and Puerto Rico all have their own laws stipulating who must be notified in certain breach situations[3].

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 policy makers 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. Certain states have strict laws about notification and disclosure of the nature of a breach, while others prohibit disclosing too much information in order to prevent copycat crimes.

Staying current in this ever changing environment is an important part of your Data Breach Readiness program.

Every breach event is different - consult a qualified attorney who understands your organization's unique circumstances can adequately advise you on your legal and regulatory obligations.

[3]NCSL "Security Breach Notification Laws", 2017

3 Develop a Data Breach Readiness Strategy

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 might receive a highly legalistic notification letter letting them know they are a victim of a breach, and urging them to "be wary". While this may satisfy the legislative standard, it can be a poor customer experience.

Organizations that retain customer's personal information should take the time to construct a Breach Readiness strategy that is suited for their unique circumstances.

The response strategy must include fulfilling any legal or regulatory obligations, but can also explore a much richer set of questions.

Questions to explore when developing a strategy:

- 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 negative 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 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?

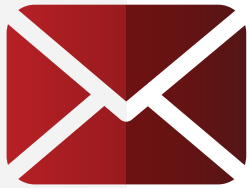
Partner with a company that can provide personalized communications and solutions to help mitigate damages to customer retention after a breach.

4 Establish Breach Response Operations

Once your organization has a strong Breach Readiness strategy plotted out, the focus should shift to executing the plan when a breach occurs.

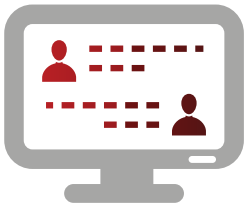
This process can cause additional questions to surface about the detailed tasks a Breach Response includes, such as:

- Who will print the legally required notification letters?
- What exactly will they say?
- Who will answer the calls from concerned customers?
- What will our public relations approach be?
- Who will be responsible for speaking to the press?
- How will the customers enroll in the breach response products?



These detailed tasks can be a challenge for many organizations that do not retain the internal staff that can facilitate large scaled letter printing, breach related customer service and breach response product enrollment.

The majority of organizations choose to utilize an outside resource to facilitate the Breach Response, engaging them in advance of a breach so they can react quickly in a crisis situation. Additionally an exterior Breach Response program can help provide an expedited and uniformed operation based on previous experience in supporting other companies in their Breach Response efforts.



Engage and negotiate agreements with breach response partners ahead of time to discover what operational tasks they can perform efficiently in the event of a breach.

5 Select an Identity Protection Partner

Customers want companies that will 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 organization is real and long lasting. Offering identity theft protection services to your customers provides you with an opportunity to turn a potentially bad situation into a positive brand experience.

Researching identity theft protection partners before a breach occurs is a good idea. It can help the organization to confidently determine which identity protection provider will best uphold your commitment to safeguarding your customers' data and your image.

When you're evaluating a provider, here are some questions to cover:

- How do I purchase the service for my customers?
- Is there a minimum or a maximum to how many customers you service?
- What is the enrollment process for my customers?
- How much does the service cost – are the fees charged per impacted customer or as customers enroll?
- What customer service is available for my customers?
- Does the service include breach response operations, such as letter printing?
- Does the service include victim assistance for customer who experience identity theft?
- How long does it take to get my program set up?

6 Create a Breach Response Communications Plan

When a breach occurs, organizations need to have a communications plan in place, for both internal and external communication.

Internal communications to your organization's executives, legal team and other important parties is your first priority when responding to a breach, except in extreme cases where information about the breach has been leaked to the media, which may accelerate the overall communications plan. Your organizations executives, customer-facing employees, suppliers, and public relations all need to know the details behind the breach event and response.

After informing all the necessary parties internally, it's time to strategically release the information to the public. Affected consumers will be concerned about how the breach occurred and what information was stolen, plotting out the organization's detailed communications plan before a breach occurs is vital to responding to their concerns. Their ability to receive that information is an 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.

With answers to the basic questions 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.

Researching the appropriate partner to fulfill your needs is better done in advance than during the middle of the crisis. For example, partner with an identity protection service that can help provide appropriate language and letters to help your organization communicate the incident and the solution to affected customers.

About Data Breach Readiness

There is no silver bullet when it comes to protecting yourself from the threat of data breaches, but being ready matters.

Small to mid-sized organizations don't always have the same resources to help protect their information and react appropriate if a breach occurs, that's where Data Breach Readiness by Identity Guard can help. With a network vulnerability scan, business data monitoring, security awareness training, and a comprehensive Data Breach Readiness Guide to assist you in creating your plan, Data Breach Readiness can help your organization be more aware of how to prevent data breaches and be prepared in the event that one happens.

About Identity Guard:

Identity Guard is one of the leading providers of data breach response services. We have implemented hundreds of programs for companies of all sizes 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 and hospitality, have been able to reduce the extensive costs of a data breach from consumer attrition, legal liability and negative public reactions.

We've serviced breaches with as many as 40 million affected customers and have on-boarded more than 2 million members in less than 4 weeks.

Identity Guard is provided by Intersections Inc. (NASQ: INTX), a leader in the identity protection industry with over 20 years of experience and award-winning products you can count on.

IDENTITY GUARD® BUSINESS SOLUTIONS

888-283-1725
IDENTITYGUARDBUSINESS.COM