DATA BREACH INCIDENT RESPONSE

WORKBOOK

CYBERCECURITY

DEFENDING YOUR ASSETS

Notice to Readers

This workbook is not intended as legal advice and Cybercecurity encourages all companies to seek legal advice regarding issues discussed in this document.

This document is a work in progress–Cybercecurity is continually seeking suggestions for improvement or areas where clarification is needed. If you have a suggestion for this publication, please email rh@Cybercecurity.com. Your feedback is appreciated and important to us.

Version 4.0

Copyright

Trademarks

Using this Workbook

This workbook is intended to provide general guidance and assistance in developing security standards appropriate for individual businesses. No one solution fits all businesses. Measures will vary depending on factors including the size and complexity of the business, the industry, and sensitivity of data.

The information in this workbook should not be regarded as a substitute for a company's self-assessment of security procedures or for legal advice.

Data Breach Incident Response Workbook

by Cybercecurity www.cybercecurity.com

Table of Contents

1 The World We Live In

Since 2005, over 863,860,240 records have been compromised from 4,211 publicly reported data breaches.1 With an ever increasing threat landscape, it is more important than ever for organizations to be prepared for data loss. Some laws in effect across the country now include notification requirements for populations over 500, breaches involving logins/email addresses, and shortened notification windows – as little as 5 days. The notification process involves writing/ producing the notification letter, setting up the call center, and mailing the letters to the affected parties. There has also been a marked increase in Regulator inquiry lawsuits. Regulators include the Attorney General, HHS, Medicare, Medicaid, DHS, and more. According to a Ponemon Institute Study released in 2014, the average cost of a data breach to a business was $201 per record lost, much of which is attributed to customer churn as the result of a breach.2

Consumer awareness of identity theft and the security of personal information is at an all-time high. With data breaches continuing to make daily headlines, publicity of large-scale breaches has caused an outrage among consumer advocacy groups, as well as adversely affected organizations such as banks and issuers. Some incidents have led breached institutions to be stricken with time-consuming and expensive class-action lawsuits.

According to the Identity Theft Resource Center (www.idtheftcenter.org), in 2013 there was a 30% increase over the total breaches tracked in 2012, distributed across these industries:

- Banking/Credit/Financial 3.7%
- Business 33.9%
- Educational 9%
- Government/Military 10.2%
- Medical/Health Care 43.1%3

Damage to the reputation of the breached institution may be even more difficult to prevent than any financial losses because it is heavily dependent upon the company's image, brand, and its relationships with customers.

In fact, Javelin Strategy & Research found that consumers avoid doing business with a breached organization at an alarming rate:

- 33 percent of consumers will shop elsewhere if their retailer of choice is breached
- 30 percent of patients will find new health-care provider if hospital/doctor's office is breached
- 24 percent of consumers will switch bank/ credit card provider if institution is breached 5

While data breaches can cost tens of millions of dollars to repair because of fines, security upgrades, and notification efforts, reputation is one asset that may not be fully restorable.

A key finding from a Ponemon survey of breach victims highlights the importance of a well-planned data breach response effort:

> "The most profitable investments companies can make seem to be an incident response plan, a strong security posture, the involvement of business continuity management and the appointment of a CISO with enterprise-wide responsibility."
>
> *Source: Ponemon 2014 Cost of a Data Breach Study*

Key findings on how consumers were affected by the way the organization responded to the security breach:

> "In addition to the increase in cost, companies are losing more customers following a data breach. The average abnormal churn rate between 2013 and 2014 increased by 15 percent. Certain industries, especially financial services, continue to be most susceptible to high churn in the aftermath of a material data breach."

> "According to this year's benchmark findings, data breaches cost companies an average of $201 per compromised record – of which $ 134 pertains to indirect costs including abnormal turnover or churn of customers."

The consequences of data breaches are higher than ever, and are no longer limited to the privacy department – accountability has moved to C-level executives and board members. Greater consequences mean that business need to be prepared to execute an effective incident response quickly and thoroughly.

The impact of a botched response is now significant. As McKinsey & Co. says "Much of the damage results from an inadequate response to a breach rather than the breach itself." Given the high stakes and challenging decisions a breach response calls for, it is imperative to have active engagement from across your company, supported by the CEO and other C-level executives, to create and follow a comprehensive incident response plan.

This Data Breach Incident Response Workbook is designed to provide an

outline and recommendations for planning a well-orchestrated response to a data compromise.

This workbook is a start, and the next step is engaging external stakeholders including a cyber insurer, attorney/breach coach, and notification & remediation vendor (ie, Cybercecurity) to ensure your plan is well-documented and tested so when the time comes, your response is financially and operationally sound.

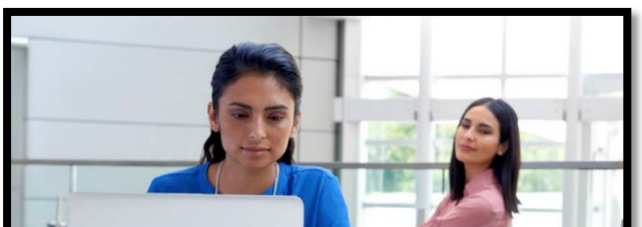
2 Anatomy of a Data Breach

These days, it is almost impossible to be in business and not collect or hold Personally Identifiable Information (PII) that belongs to customers, employees, business partners, students or patients. PII includes (but is not limited to):

- Social Security Number
- Name
- Address
- Date of Birth
- Account Numbers (checking, credit card, etc)
- Email address
- Passwords

If this Personally Identifiable Information falls into the wrong hands, it could put these individuals at risk for identity theft.

Not all personal information compromises result in identity theft, however, and the type of personal information compromised can significantly affect the degree of potential damage.



There are Four Fundamental Ways Data Breaches Occur:

1. Theft or Loss of Physical Equipment

A data breach can result from the theft or loss of physical equipment which stores data, such as laptop computers or memory storage devices.

2. Illegal Access to the Systems or Information A data breach can occur through unlawful access to PII data by technological means such as hacking into existing computer systems or hijacking computers with viruses, worms, or trojans. Once inside a system, criminals can steal data, infect it, or overload computer systems.

3. Insiders

A data breach can be committed by current employees, ex-employees, or even through social engineering where an employee is tricked into providing access or information (phishing is considered to be socially engineered fraud).

4. Oversight

A data breach can result from inadequate security or negligence, so proper precautions were not taken to safeguard the data in the first place.

What Steps Do I Need To Take After A Breach?

STEP ONE: One of the first questions the organization should try to answer is:

- What was the level of harm caused by the data breach exposure?

- In determining the potential for harm it is important to ask some additional questions like:

› Was the data encrypted?

›› What data (PHI, PII, etc.) was included in the breach?

›› Was the data only exposed to another business unit, and if so, was a confirmation received that the information was destroyed?

›› Could this exposed information pose any harm to the affected individuals?

The guidelines indicate that there are three categories of harm that can potentially require consumer notification:

1. Financial Harm
2. Reputational Harm
3. "Other" Harm

Financial harm affects a consumer's credit or finances, such as a breach of a consumer's Social Security number. Reputational harm is the exposure of consumer information that can hurt a consumer, such as the accidental release of a consumer's health history. The definition of "other harm" has been the subject of much discussion. Most industry leaders believe "other harm" to mean an exposure that did not include information such as a Social Security number, or personal health information, but an exposure that may include date of birth, name, address and insurance information. This information could be just as valuable to a thief who could receive medical treatment using the patient's insurance information.

STEP TWO: Document the details of the data exposure and include the level of harm you have determined and why you have assigned that level of harm.

STEP THREE: If it is determined that you need to notify the affected individuals, your next step will be to decide who you will notify, how you will notify, and what level of remedy to provide.

You should always consult with your legal counsel as to what level of notification is required.

General Notification Guidelines for HIPAA and HITECH Data Breaches:

- If you have disclosed information to a HIPAA-compliant entity or a business associate and have been able to ensure the information was not viewed, it has not been stored and you can confirm it has been destroyed, you usually do not have to notify.

- If the lost information was protected by strong encryption, you usually do not need to notify.

- However, if you do not know the status of the information that has been compromised, then in general you must notify.

- Determine who you need to notify. Possibilities may include:

» Affected Consumers

» Department of Health and Human Services (HHS)

» State regulatory authorities, for example Department of Health in California

» State Attorneys General Offices (If SSN was involved)

» Local newspapers and /or your corporate website (If there are more than 10 consumers who need to be notified and you do not have a valid current address

3 Preparing For A Data Breach

While theft prevention should be the primary goal of any organization, proactive planning can minimize the impact when a breach does occur. Most businesses tend to hope they will never fall victim to a security crime or disaster – but "hope" is not a good foundation for a business plan – being prepared is.

There are two main things to keep in mind when the time comes to respond to a data breach:

1. It is important to move swiftly and follow your completed Data Breach Incident Response Plan, and

2. It is important to document all ongoing events, all people involved, and all discoveries into a timeline for evidentiary use.

The following is a list of actions to take when a breach occurs: (Reminder, you should always consult with legal counsel in the event of a data breach.)

- Identify how the breach happened, contain the breach, and implement a solution to help prevent a recurrence
- Notify appropriate people within the company
- Engage a Forensics Investigator
- Engage a Breach Notification & Remediation Partner for notification, call center, and consumer protection
- Notify External Agencies, within required time frames, such as:
  - › Law Enforcement
  - › Affected vendors, suppliers
  - › FTC
  - › State Attorneys General (where applicable
  - › Notify affected individuals

Be Prepared for a Data Breach

The top recommendation of any company that has experienced a data breach is to have a response plan in place. The plan should include written emergency contact lists, a clear understanding of which law enforcement agencies must be contacted and involved, and a time frame for notification – internal SLAs should be established.

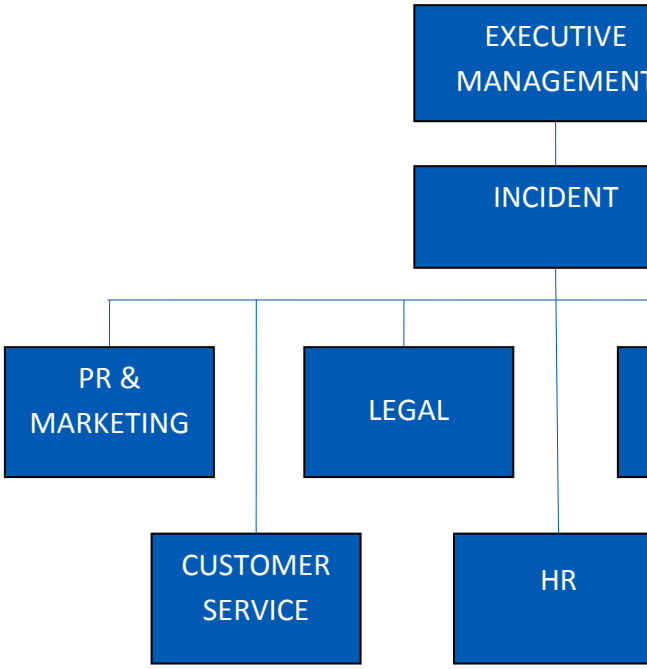
Additionally, vendor contracts should be in place with a mail-house for notification letters, a call center that specializes in breach response and consumer identity protection, and finally, to have pre-negotiated rates for fraud protection in the event your company needs to notify those affected. It can be difficult to negotiate these contracts during an emergency situation.

Use the worksheets in this book to create a formal written plan of how you would respond to a data breach situation. Your incident response team should meet monthly to update contact information, discuss any changes in the organization, review any incidents that may have occurred, and evaluate the response process. The incident response team should practice responding to a data breach at least annually and preferably quarterly.

- Risk Management and Security
- Compliance and Audit
- Legal
- Privacy
- Public Relations

It is important to assign an Incident Lead to direct and manage the internal response team, as well as to act as the go-between for management and the response team. This individual (and their backup) should be considered to be the project lead for the breach response.

RESPONSE TEAM S



4 Build a Strong Internal Response Team

Build your Incident Response team with the right mix of expertise with representation from:

- Executive Management
- Information Technology
- Customer Service

The other members of the response team have specific responsibilities to protect your company and customers, but all should report directly to the Incident Lead during a breach response.

Executive Management needs to be kept up-to-date during a data breach incident. The Incident Lead will run tactical, day-to-day operations of the data breach as well as regularly update management. The Incident Lead is typically someone from the legal department or a Chief Privacy Officer and their role is primarily that of a project manager and needs to be in frequent contact with the primary decision-maker for the incident. This person will coordinate efforts among all groups, notify all the appropriate people within the company and externally, and create the documentation and timeline of activities, identify key tasks, and estimate costs.

PR and Marketing personnel must be involved in the breach incident. A decision will need to be made very early in the event to determine whether or not it is appropriate to notify affected individuals of the incident. If required, it is critical to begin notification in a timely manner and PR/Marketing need to ensure that consistent messages are shared throughout the response (see Chapter Six: Data Breach Notification).

Legal, Privacy, and Compliance personnel will work with counsel to find out what is required in the response. These individuals will be responsible for determining whether or not affected individuals should be notified and the legal requirements around the content of the notification (see Chapter Six: Data Breach Notification). Additionally, this team or person is also responsible for determining which external organizations should be contacted. For example, in the event of a data breach of credit card information, credit card associations (Visa, MasterCard, American Express, and Discover) should be notified, as well as the acquirer through which the merchant processes. If the company who suffered the breach loses client information, the client will need to be notified and involved in the plan.

Security & IT teams will work with forensics investigators to help identify what information was actually compromised. A word of caution, though – many IT individuals may be under the impression that they possess the skill set and training to conduct forensic investigations on the data compromise (identification of how the breach happened, impact to any other systems, analysis of what was taken, ensuring the damage has stopped, etc). Unless specifically trained for this work, it is important to hire certified data forensics experts, who possess this specialized skill set.

By having an untrained team working on the system, the chances of information

being tampered with or corrupted are increased which makes it significantly more difficult to investigate.

RECOMMENDATION:

Hire an outside certified data forensics team in every incident where a computer intrusion has occurred.

Customer Service and Human Resource (HR) personnel will play a critical role in the incident if employee or customer notification is determined to be a requirement. HR will be involved when the breach has impacted employee information and Customer Service will be called into action if the data breach impacts customers.

Because the notification of clients will create high volumes of calls, most companies will also create a telephone hotline dedicated to handling the breach incident.

A consumer website should also be created and provide clear, detailed instructions about steps consumers may take to protect themselves. Also include a Frequently Asked Questions section as well as any other publicly available information regarding the breach.

Contacting the Team

Create and distribute an Incident Response Phone List that is updated at least quarterly. Include the employee's role on the Incident Response Team, their name, work/cell/home phone numbers, and e-mail address. Every person should have a backup contact as well.

Internal Response Team Considerations:

- In order for a company to have a strong data breach prevention plan, concern and focus on data security must come from top management so that fiscal and personnel resources are included in budget allowances year-round.
- Data breaches often must involve the CEO, CFO, CPO, CIO, CMO and General Counsel; you should include them in the Internal Response Team and Plan from the outset of the project.
- Upper management involvement in data breach preparedness is necessary in order to integrate the concern for information security as a core value in a company.
- Re-evaluation of security systems and policies should be conducted on an ongoing basis in order to remain up-to-date on the latest technologies and criminal trends.
- Training and practice of your Data Breach Incident Response Plan should occur on a regular basis.

5 Data Breach Checklist

With a data breach, **timing is everything.**

Document everything that happens, everything you discover, and turn it into a timeline!

Within the first few hours after discovering a potential data breach, it is important to begin running through the following checklist:

Implement Data Breach Incident Response Plan

- Alert & Activate Incident Response Team. Refer to the Internal Contact List.
- Collect and/or review the incident response plan
- Verify known facts
- Alert appropriate external and internal contacts
- Consult legal counsel upon discovery of a breach
- Review cyber insurance coverage, if any in place
- Review response vendor contracts, if any in place
- Restrict information until there is a communication plan in place and legal counsel is involved – keep it on a need-to know basis only

Include the following information in an ongoing written summary:

- Current date and time of any updates to the summary
- Date/Time of discovery of data breach
- Name of person reporting data breach (could be anonymous)
- Details of how the data breach was reported

- Type of data breach: theft, illegal access, insiders, oversight
- Identify how the breach happened and de-scribe what happened
- Was the breach contained (how and when)?
- What was/will be implemented so this same breach cannot happen again?
- Keep a list of all external officials and individuals contacted and involved in the incident. Refer to the External Contact List Template

Begin Identification of the Problem

- How many records are affected?
- What type of PII was potentially compromised? Be specific "Did every record lost include an SSN? Did the list include family member SSNs?" Potential PII lost:
  - Name
  - Address
  - Social Security number
  - Date of Birth
  - Account Numbers (checking, credit card, etc.)
  - Email address
  - Passwords

What is the type of incident?

- Network/server breach
- Hardware loss, theft, or destruction
- Software loss, theft, or destruction
- Hacking/unauthorized third-party access to system
- Unauthorized websites that publish sensitive corporate information not approved for public consumption
- Other

- Maintain a complete chain of evidence: identification, collection, analysis, storage, preservation, transportation, returned to who, when and where

Begin the Process of Reporting the Incident

- Limit communication
- Use discretion when sharing information with employees, law enforcement, vendors, business partners, etc.
- Be especially careful when communicating with breach victims and the media
- Notify law enforcement at the discretion of upper management. Consider these factors when deciding to contact law enforcement:
- Severity of the incident
- Scope of the compromise

- Recommendations of your lawyer regarding disclosure and notification
- Legal counsel should be present in all meetings with law enforcement
- Do not include confidential information in any communication unless necessary
- Identify and communicate with key regulators, as guided by legal counsel. State regulators are very active in breaches as your customers are their citizens.
- If the breach is found to be noticeable, en-gage response vendor for notification, call center, and consumer protection services.

If the data breach could result in harm to a person or business, contact local police:

- Report the situation and be clear about the potential risk for identity theft
- Contact the local FBI office or the U.S. Secret Service if your local police are not familiar with investigating data breaches
- Mail theft: Contact the U.S. Postal Inspection Service

Create an Executive-Level Incident Summary Report that includes:

- High-level description of the incident and its scope
- Impact on the company
- Actions taken to prevent further occurrences "" Recommendations for further action

Create a Technical Incident Summary Report that includes:

- Detailed information about the event
- Detailed information about the investigation
- All conclusions reached

6 Data Breach Notification

Determining if notification is necessary and/ or legally required is a complex issue impacted by confusing state laws governing jurisdictions where breach victims reside. The considerations below are presented as an overview and are not intended to be inclusive of all issues to be considered. Some examples of how State Laws differ include the definition of personally identifiable information, who must be notified (State Agencies, Law Enforcement, the Credit Reporting Agencies), the timing of the notification to the individuals, and the content of the letter. ***You should always consult with your legal counsel as to what level of notification is required***.

Not every incident is going to require the notification of customers and other businesses, depending upon the assessment of the severity, scope, and nature of the data that was

compromised. If the situation does warrant notification of customers and other businesses, the following information should be taken into consideration:

Notifying Affected Individuals

If you determine you are going to notify a set of individuals in one state because of a specific law, you should notify all individuals affected in the breach. The general guideline is to treat all affected breach populations equally. There are many examples where individuals were not treated equally in a data breach and there were legal consequences to the organization. Additionally, even if the individuals identified are overseas, while there is little notification law, it is also recommended that overseas notification is included.

Generally, early notification of individuals whose personal information has been compromised, allows them to take steps to mitigate the misuses of their information.

Should notification be warranted, in determining what type of protection to offer in the notification, consider the nature of the compromise, the type of information taken, the likelihood of misuse, and the potential damage arising from misuse. For example, thieves who have stolen names and Social Security numbers can use this information to cause significant damage to a victim's credit record.

Always consult legal counsel as most states require that consumers are notified. As of the date of this publication, 47 states, the District of Columbia, Puerto Rico, Guam and the Virgin Islands have data breach notification laws in place. Many states also require notification of the Attorney General's office and other regulators.

When notifying individuals, the FTC recommends that you:

- Consult your law enforcement contact about the timing of the notification so it does not impede the investigation
- Designate a contact person within your organization who will be in charge of releasing information (this should be designated by your Incident Lead). Give the contact person the latest information about the breach, your official response, and how individuals should respond. Consider sending letters (see example below), posting websites and toll-free numbers as methods of communication with those whose information may have been compromised.

It is important that your notice to consumers clearly describes what the company knows about the compromise. Include as much as permitted by applicable laws about how the incident happened, what information was taken (if known), how the thieves have used the information, what actions the company has already taken to remedy the situation, and what responses may be appropriate for the type of information that was compromised. Explain how to reach the contact person within your organization (see Model Letter below).

Consult with your law enforcement contact on exactly what information to include in the consumer notification so your notice does not hamper the investigation. Provide contact information for the law enforcement officer working on the case (as well as your case report

number, if applicable) for victims to use, as they can often provide important information about the crime. Be sure to alert the law enforcement officer working your case that you are sharing this contact information. Breach victims should request a copy of the police report and make copies for creditors who have accepted unauthorized charges. The police report is important evidence that can help absolve a victim of fraudulent debts.

The notification should also encourage those who discover that their information has been misused to file a complaint with the FTC at http://www.consumer.ftc.gov/articles/0341-file-complaint-ftc or at 1-877-ID -THEFT (877-438-4338). Information entered into the Identity Theft Data Clearinghouse, the FTC's database, is made available to law enforcement.

Is your organization exempt from notifying consumers?

Organizations may not have to notify affected consumers in the following situations:

Encrypted data: Some states do not require notification if the compromised data is encrypted. State laws become very specific on this subject. For example, the exact level of encryption (128 bit) can affect compliance requirements. It is unclear if these current exemption requirements will remain in place or if increasing risks will push states to require organizations to notify even if information is encrypted.

Questionable Misuse: Some state laws do not require notification unless there is "reasonable belief" that the breached data has been misused.

Public Availability: If the breached information is already publicly available from a government agency, notification may not be required in some states.

Doubtful Use: In some cases where a breach was stopped and there is reasonable doubt that the information was accessed or used by criminals, some states do not require notification.

Is there a risk to your organization of fines, penalties and class action lawsuits if your organization chooses NOT to notify?

Possible Exemptions to Notifying

You should always consult with your legal counsel as to what level of notification is required. Some possible exemptions include:

- Data was 128 Bit encrypted.
- There is no evidence or reason to believe the data has been or will be misused.
- The information compromised is already publicly available.
- There's reasonable belief the information was never accessed.

Once you have decided to notify, follow the best practices for notification.

Notification and Call Center Best Practices

- Once the decision has been made to notify, the notification letter is a critical element of communication. The fundamental rule of a successful letter

is to be open, honest and direct with the consumer.

- Notification information should be well organized and presented in a way that is direct and concise. It should be obvious from whom the notification is coming and exactly what action is required of the consumers.
- All notification letters and documents should be printed on letterhead on high-quality paper and in color, as many recipients are suspicious of notification letter authenticity
- Expect five to ten percent of consumers who receive notification letters to call the company or agency with questions. Typically, these phone calls last from five to fifteen minutes.
- Be sure to hire a call center experienced in data breach response to manage these calls - an experienced team handling these

  calls will minimize anger and questions from those affected
- Call center staffing costs can be minimized by sending notifications in waves.
- Know where you customer data resides and involve appropriate people early in the process to pull the information to prepare the address file for notification
- Many people, affected or not, are concerned after a data breach so be prepared to reassure anyone who calls with concerns

Cleanse the mailing addresses; typically only 80– 90% are deliverable without extra investigation.

- Match against a Delivery Point Validation databases (DPV)
- Match against the Postal Service Change of Address database
- Determine what you intend to do to track down the rest of the addresses and notification

>> Use 3rd party services to find the consumers

  - Use your customer service for outbound calls

- Asses the risk of not notifying this group (not recommended)
- Discuss what to do when you know that individuals' information has been compromised, but you don't yet know exactly what was exposed
- Include an end date in your letter of when any offer of free protection will end
- Mail-in registrations must be post-marked no later than the published deadline date. Typically allow 10 days for receipt after post-mark date.
- Plan for those consumers who state they never received a notification but insist on you providing protection

Other Notification Tips

Notifying Affected Businesses

Information compromises can have an impact on businesses other than the one currently breached, such as banks or credit issuers. If account access information (e.g. credit card or bank account numbers) has been stolen from a company that does not maintain the actual accounts, it is important to notify the institution that does maintain that information so that it can monitor the accounts for fraudulent activity. If personal information is collected or stored on behalf of other businesses, notify those businesses of any information compromise, as well.

Providing Protection for Breach Victims

Once a breach has occurred and a decision to notify has been made, there is a final critical decision that can seriously impact the public's evaluation of how the breach response was handled: "Should your organization provide identity protection for citizens whose compromised information might be used to commit fraud?"

According to Javelin Research, "In 2013, data breaches became more damaging, with one in three people who received a data breach notification letter becoming an identity fraud victim. Encouragingly, the amount criminals stole decreased by $3 billion to $18 billion, reflecting more aggressive actions from financial institutions, identity theft protection providers and consumers."4

Javelin recommends the following measures that address consumer security concerns and expectations, to institutions in the event of a data breach:

- Given the wide variety of fraud protection solutions and varying features out in the market, engage in comprehensive research of the different services available to understand how they play a role in prevention, detection and resolution.

- Select a solution that is convenient and easy for the breach victim, in terms of enrolment and use, with an understanding of the impact on preventing new accounts fraud.

- Understand that offering a breach solution is a best practice from a customer service standpoint; in other words, do not create a situation in which your customers and/or employees have to request fraud protection assistance. Take a proactive approach by offering the assistance up front.

What Identity Protection to Provide the Breached Individuals

It is important in your notification to offer the correct protection to help those affected by a breach, and the right protection may or may not include credit monitoring. Optimize the protection included in your notification by matching the services offered to the risk of the data lost. As evidenced in the Target data breach in late 2013, they were called out by Consumer Reports as giving the affected a "false sense of security" for offering credit monitoring after a credit card breach. Credit monitoring does not monitor for fraud on existing accounts, only on new ones, so it was not the correct choice for Target to offer the affected population. See page 35 for further information on choosing the right protection based on the risk of data lost.6

It is important to note that the regulators do not require purchasing Credit Monitoring for individuals. The best recommendation is to provide the appropriate protection for the risk of the data lost.

- Typically 10-30% of consumers take advantage of a free offering. This number may increase or decrease depending on:

» How the individuals are notified: i.e. email, letter, phone call, or substitute notice via website

» The population of affected individuals: employees, customers, patients…

» Amount of press the incident receives and timing of the press

» How the data was compromised: stolen laptop, hack, …

» Has the data been used by the crooks to steal identities

Sample Notification Letter

The sample notification letter on the following page is an example of how businesses might notify people whose names and Social Security numbers have been stolen. This is not legal advice. Always consult with legal counsel in connection with any potential breach.

Processing Center • P.O Box XXXX • Denver, CO ZIP CODE
[ORGANIZATION LOGO HERE]

<<FirstName>> <<LastName>> <<Date>>
<<AddressLine1>>
<<AddressLine2>>
<<City>>, <<State>> <<ZipCode>>

Dear <<FirstName>> <<LastName>>,
We are writing to inform you of an incident that may have involved your personal information. [Describe the incident, as required by applicable law, such as what happened, the date of the incident, the date of discovery, details of any subsequent investigation (including whether notification was delayed as a result of a law enforcement investigation, if possible) and the types of personal information compromised] [We believe the risk of harm to you is low.] [Delete if not fair statement**.]. [Note: Depending on the state of residence of each individual in your affected population, such state may have specific statutes and regulations regarding notification—please consult counsel for advice with regard to requirements for a specific state]**

We want to make you aware of steps you may take to guard against identity theft or fraud. Please review the enclosed Information about Identity Theft Protection.

As an added precaution, we have arranged to have Cybercecurity protect your identity for «Time» at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next «Time».

Cybercecurity SECURE: The team at Cybercecurity is ready and standing by if you need identity repair assistance. This service is automatically available to you with no enrollment required. If a problem arises, simply call «DID_Phone» and a dedicated investigator will do the work to recover financial losses, restore your credit and make sure your identity is returned to its proper condition. Cybercecurity maintains an A+ rating at the Better Business Bureau.

Cybercecurity PRO: This service offers additional layers of protection including credit monitoring and a $1 million identity theft insurance policy. [Note: If children are affected, include this sentence: For a child under 18 years old, Cybercecurity ChildScan identifies acts of credit, criminal, medical or employment fraud against children by searching thousands of public databases for use of your child's information.] To use the PRO service, you will need to provide your personal information to Cybercecurity. You may sign up online at enroll.Cybercecurity.com or by phone by calling «DID_Phone» using the following redemption code: {Redemption Code}.

Please note: Additional steps may be required by you in order to activate your phone alerts.

We take the protection of your personal information seriously and are taking steps to prevent a similar occurrence. [Insert statement about what steps company is taking to prevent a similar occurrence.]

If you have further questions or concerns about this incident, you can find more information on our website, [insert link], or contact [Organization Contact] at [Organization Phone Toll Free number]. We sincerely regret any inconvenience or concern caused by this incident.

Sincerely,

[Organization Contact, Title]
[Organization Name]
[Organization Address]

7 Incident Response Plan

Use this section to start developing a tailored Incident Response Plan. The worksheets serve as a guide to help you properly document events, actions, and timelines.

Maintain this workbook with other documentation so that the source of an incident can be identified and traced and so that the information is immediately available if needed.

IMPORTANT:

Continuously update the information in the contact lists and other documents – don't get caught in an emergency with outdated information!

You should also maintain copies of the following:

- The company's written Incident Response Plan
- The company's Service and Operating Level Agreements
- The PCI Data Security standard document

[illegible] onsibilities for all card levant)

- Complete record of the company's software licensing information
- Current asset and hardware inventory

Quick Plan Overview

¨ **How is an incident reported and documented in your company?**
- Plan in place to document everything
- Forensic Integrity, treat a data breach like a crime scene
- Who contacts law enforcement

¨ **Do you know who you are going to call?**
- Internal Response Team Created
- Internal Response Team Emergency Contact List
- External Response Team/Notification List

¨ **Vendor contracts in place?**
- Forensic investigator
- Mail-house for notification letters
- Call Center
- Consumer Identity Protection

¨ **Process for determining if notification is required?**
- Legal counsel understands laws
- Timeline obligations and specific state laws (based on where individual lives not the company)

¨ **If notification is required is your organization prepared?**
- PR – what will be said to the public

- Who authors and approves the notification letter
- How will it be sent
- What will be provided to protect the individuals
- Call Center Scripts
- Website with FAQ and additional information

¨ **How will this effort be funded?**

- Is there a cyber insurance policy in place?
- If there is a cyber insurance policy in place, what response vendors are approved or covered by the policy?

Internal Contact List Template – Use for Incident Team

Data Breach Internal Contact List

Last Updated ☐
To be Updated Quarterly

Role	Name	Phone	Email
Executives		Work: Home: Cell:	
Incident Lead		Work: Home: Cell:	
Customer Service		Work: Home: Cell:	
Human Resources		Work: Home: Cell:	
Information technology		Work: Home: Cell:	
Privacy		Work: Home: Cell:	
Risk Manager		Work: Home: Cell:	
Audit		Work: Home: Cell:	
Legal		Work: Home: Cell:	
Security		Work: Home: Cell:	
Compliance		Work: Home: Cell:	

Signature	Date:

External Contact List Template – Use for all contacts outside the company that might need to be contacted during an incident

Data Breach External Contact List

Last Updated ☐
To be Updated Quarterly

Role	Name	Phone	Email
Forensics		Work: Home: Cell:	
Police		Work: Home: Cell:	
FBI		Work: Home: Cell:	
Secret Service		Work: Home: Cell:	
Other		Work: Home: Cell:	
Media		Work: Home: Cell:	
Business Partners		Work: Home: Cell:	
Attorney General		Work: Home: Cell:	
FTC		Work: Home: Cell:	
Card Processors		Work: Home: Cell:	
Regulators		Work: Home: Cell:	

Signature	Date:

Incident Log

Incident Number	
How was the incident reported?	
Date of Compromise (if known)	Time of Compromise (if known)
Date of Discovery of Compromise	Time of Discovery of Compromise

Incident Assessment			
☐ Suspected	☐ Confirmed		
Type of Data Breach			
☐ _____	☐ Illegal Access	☐ Insiders	☐ Oversight
Exposure dates			
Start Date _____ End Date _____			
Data Encrypted?			
☐ Yes	☐ No		

Specific Data Compromised?			
☐ Account #	☐ SSN	☐ CID (4DBC/CCV)	☐ PHI Insurance Info
☐ Name	☐ Email	☐ Expiration Date	☐ Other
☐ Address	☐ DL	☐ Passwords	
☐ Magnetic Strip Data	☐ DOB	☐ PHI Medical Records	

Signature	Date:

Incident Log (Cont.)

Incident Number		
Is law enforcement involved?	☐ **Yes**	☐ **No**
Need to contact media?	☐ **Yes**	☐ **No**
Was extortion involved?	☐ **Yes**	☐ **No**
Need to contact customers?	☐ **Yes**	☐ **No**
Is computer forensics required?	☐ **Yes**	☐ **No**
Website operational?	☐ **Yes**	☐ **No**
Did you contain the breach?	☐ **Yes**	☐ **No**
How did you contain the breach?		
When did the containment occur?	Date _____	Time _____
Describe how the containment was implemented		

Signature	Date:

Here are crucial questions to consider for a Notification Strategy. Remember, the most important message to convey to those affected is "You will be taken care of if you have a problem like identity theft after this incident."

Notification – Required Services Checklist		
Key Questions	**Preliminary Answer**	**Internal & External Contacts**
What is the total affected population?		
How will you notify: mail, email, or substitute notice?		
How soon do you need to notify?		
Will you handle notifications internally or outsource to a vendor?		
Who will manage returned mail?		
Which team members must approve notification language?		
How confident are you in the validity of the addresses and who has the information and skill to compile an address file?		
Will you offer an identity protection to those affected?		

Signature	Date:

Good communication with those affected is critical to reassure people after a breach. Most victims simply need to know that they have someone to help them if they have a problem.

Call Center & Customer Support – Required Services Checklist		
Key Questions	**Preliminary Answer**	**Internal & External Contacts**
Who can handle the volume and complexity of calls?		
Who is penetrating and approving the FAQs for the call center?		
Who will train and QA the agents?		
How will you manage customer support escalations?		
Do you need US and/or international support?		
Are there factors that will increase call volume such as a concentrated population or high media coverage?		
What are the hours of operation required to support your population?		
Are email and social media support teams ready to respond?		
What is the timing of public notice /press release and live call center?		

Signature	Date:

Offering the right protection to consumers based on the type and risk of data loss is key to a successful breach response. These questions will help arrive at the appropriate type of protection and monitoring services. Remember: Credit monitoring is not the right solution to help people unless SSNs are lost.

Consumer Protection & Monitoring – Required Services Checklist		
Key Questions	**Preliminary Answer**	**Internal & External Contacts**
What is the right protection based on the risk of the data		
For non-SSN incidents, what level of identity protection is appropriate? Note: Refer to the type of data Lost Char for Guidance on the right protection to offer the affected population		
For incident involving SSNs, what level of credit monitoring enrolment do you expect?		
Were minors involved in the breach?		
What is the vendor customer service rating and can you confirm that they will not sell customer addresses (ie. Are not a data broker?)		
Will the vendor engage in upselling?		

Signature	Date:

Consider what FAQs the call center, customer support, social media and email teams will need to answer. These answers should reinforce anything said in public statements and/or press releases.

Sample Notification FAQs Worksheet

Frequently Asked Questions Regarding Notification of Disclosure

1. What specific information was disclosed about me?
2. Where did this happen and why was my information accessible there?
3. Who was responsible for the security of my information?
4. What did you do when the information was accessed?
5. What are you doing about this so it does not happen again?
6. Were there other individuals affected by this breach, or am I the only one?
7. Was my spouse or other family members' information also affected?
8. Has the person who accessed the information or stole the device been caught?
9. Have you notified the police?
10. Will we receive any additional information or update?

What other questions do you anticipate the affected population will ask?

11. _____

12. _____

13. _____

Signature	Date:

Determine the Right Protection to Offer Based on the Type of Data Lost. Use this chart to provide the appropriate protection for your incident based on the risk of the data lost.

TYPE OF DATA LOST				
RIGHT PROTECTION	Healthcare (PHI)	Passwords	Credit Cards	Social Security Numbers
Identity Repair	✓	✓	✓	✓
Identity Theft Monitoring	✓	✓	✓	✓
Card/Account Alerts*			✓	✓
Credit Monitoring**				✓

*Card / Account Alerts are provided free of charge to customers by most banks and credit unions. Cybercecurity will assist affected individuals in setting up these alerts on their credit card and bank accounts.

**If lost SSNs belong to children, offer Cybercecurity ChildScan Monitoring, designed specifically to find child identity theft that regular credit monitoring cannot detect.

Signature	Date:

8 More Resources

For More Information

This publication provides general guidance for a company that is preparing a data breach response plan. For more individualized guidance, you may contact the Cybercecurity Breach Hotline at 1-877-441-3009 or email rh@Cybercecurity.com. To order reprints of this publication, email rh@Cybercecurity.com.

Other Valuable Complimentary Resources:
New Cybercecurity Data Breach Resources page: www.Cybercecurity.com

Online Trust Alliance Privacy & Data Loss Incident Readiness Planning Guide: www.otalliance.org/resources/Incident.html

International Association of Privacy Professionals for information on becoming a Certified Information Privacy Professional: www.privacyassociation.org/certification/

Identity Theft Resource Center:
www.idtheftcenter.org

Sources:

1 Privacy Rights Clearinghouse: https://www.privacyrights.org/data-breach

2 Ponemon Institute:
2013 Cost of a Data Breach Study: United States

3 Identity Theft Resource Center: http://www.idtheftcenter.org/ITRC-Surveys-Studies/2013-data-breaches.html

4 2014 Javelin Identity Fraud Report: https://www.javelinstrategy.com/news/1467/92/A-New-Identity-Fraud-Victim-Every-Two-Seconds-in-2013-According-to-Latest-Javelin-Strategy-Research-Study/d,pressRoomDetail

5 Javelin White Paper: Data At Rest is Data at Risk https://www.javelinstrategy.com/brochure/300

6 Consumer Reports
http://www.consumerreports.org/cro/news/2014/02/ expect-less-and-pay-more-with-target-credit-monitoring/index.htm