2012 Data Protection & Breach Readiness Guide

Developing and advocating best practices to mitigate emerging privacy, identity and security threats to online services, government agencies, organizations and consumers, thereby enhancing online trust and confidence.

January 24, 2012

© 2012 Online Trust Alliance (OTA) All Rights Reserved

Table of Contents

Introduction……..……..page 3
Executive Summary ……..……page 4
Business Impact ……..…….....page 5
Data Incident Plan Framework …… page 6
Data Governance and Loss Prevention……page 7
Data Classification page 7
Audit & Validate Data Access page 8
Forensics, Intrusion Analysis & Auditing page 8
Data Loss Prevention Technologies page 10
Data Minimization page 10
Data Destruction Policies page 11
Inventory System Access & Credentials page 11
Incident Response Planning ……..…….. page 12
Creating an Incident Response Team page 12
Establish Vendor and Law Enforcement Relationships page 12
Create a Project Plan page 13
Determine Notification Requirements page 14
Communicate & Draft Appropriate Responses page 15
Providing Assistance & Possible Remedies page 16
Training, Testing & Budget……...……page 16
Employee Awareness & Readiness Training page 16
Analyze the Legal Implications page 17
Funding and Budgeting page 17
Critique & Post Mortem Analysis page 17
Other Considerations …… page 18
Implement Steps to Help Curb Misuse of Your Brand page 18
International Considerations page 18
Summary……...……..... page 19

Appendix A – Resources……...……..……page 20
Appendix B – Sample Notification Letter …….…… page 22
Appendix C – Cyber Security Liability and Insurance Considerations ……... page 23
Appendix D – Computer Forensics Basics …..…… page 24
Appendix E – Encryption Resources…… page 26
Appendix F – Sample Data Incident Plan Outline……... page 27

Introduction

The 2012 Data Protection & Breach Readiness Guide reflects input from stakeholders across the ecosystem including interviews with companies who have experienced breach and data loss incidents, industry and breach analysis experts. Originally published in January 2009, the 2012 report has been updated and expanded in several areas including:

- Updated data and incident examples
- A new section on data minimization
- Computer forensics tips
- Laptop and mobile device encryption options
- A sample data incident plan

A data breach can have devastating consequences to a business, damaging its brand and causing it to lose customers. The purpose of this guide is to provide prescribe guidelines that help businesses to proactively develop a plan to minimize data collection, enhance data protection and to create a customer-centric incident response plan. By planning in advance, businesses of all sizes can minimize their risks, costs and the impact of a breach to their customers and the reputation of their company and brand.

Support and contributions to the guide reflects input from numerous organizations including the Council of Better Business Bureaus, the Identity Theft Council, the Identity Theft Assistance Center, Javelin Strategy & Research, National Cyber-Forensics & Training Alliance, (NCFTA), Ponemon Institute, Privacy Choice, Privacy Rights Clearing House and the US Chamber of Commerce.

OTA wishes to acknowledge input from the OTA Steering Committee and members including Concise Consulting, Debix, DigiCert, Epsilon, IID, Intersections, LashBack, MarkMonitor, Message Systems, Microsoft, PayPal, Pitney Bowes, Publishers Clearing House, Return Path, Secunia, Star Marketing Group, Symantec Corporation, TRUSTe, TrustSphere and VeriSign Inc.

The Online Trust Alliance (OTA) and its contributing authors and reviewers provide this document as a public service, based on collective expertise and opinion. There is no implied warranty on the guidance in this document. While this document is not meant to be an exhaustive list of all of the steps that need to be taken to prepare for, and deal with, a data breach, it provides links to complimentary resources that provide added detail in several areas such as data classification, data destruction and computer forensics.

Updates of this report will be posted at https://otalliance.org/breach.html. To submit comments or suggestions, please email staff@otalliance.org.

About The Online Trust Alliance (OTA) https:/otalliance.org/

OTA is an independent non-profit with a mission to develop and advocate best practices and public policies which mitigate emerging privacy, identity and security threats to online services, organizations and consumers, thereby enhancing online trust and confidence. By facilitating an open dialog with industry, business and governmental agencies to work collaboratively, OTA is making progress to address various forms of online abuse, threats and practices which threaten to undermine online trust and increase the demand for regulations.

Executive Summary

Few events can damage a company's brand and the trust of its customers more than a data incident, defined as either the loss or misuse of customer data. As stated by Zappos CEO Tony Hsieh following the breach of their 24 million customers, "We have spent over 12 years building our reputation and trust, it is painful to see us take so many steps back due to a single incident."[1]

2011 has become known as the "Year of the Breach" due to the high-profile natures of breaches that were experienced by both large companies such as Sony and smaller organizations such as a Massachusetts non-profit, the eHealth Collaborative. Many of the breaches including Sony, Epsilon, Michaels, RSA and NASDAQ, were due to external attacks, including server exploits and passwords compromised via phishing and forged email. Other data loss incidents resulted from lost notebooks, hard drives and files erroneously sent in email or posted on public sites.

As stated for the past three years in OTA reports, all businesses have to assume they will experience a data loss incident. The costs of these incidents include direct costs (such as providing credit monitoring services to affected customers), the indirect costs of lost productivity, and the complex mosaic of navigating US, Canadian and European law. When combined, the direct plus indirect costs can be staggering.

OTA advocates that businesses create an incident response plan and be prepared for the likelihood that they will experience a breach or data loss. Businesses need to accept three fundamental truths about data: 1) the data they collect includes some form of personally identifiable information (PII) or "covered information"; 2) if a business collects data it will experience a data loss incident at some point; 3) data stewardship is everyone's responsibility. Rather than be lulled into the belief it will not happen to <u>your</u> business, a well-designed plan is an essential part of regulatory compliance, demonstrating that a firm or organization is willing to take reasonable steps to protect data from abuse. Developing a plan can help to minimize risk to consumers, business partners and stockholders, while increasing brand protection and the long-term viability of a business.

2011 Incident Highlights

- 558 breaches
- 126 million records
- 76% server exploits
- 92% avoidable
- $318 cost per record
- $7.2 million average cost of each breach
- $6.5 billion impact to U.S. businesses

This document outlines some key questions and recommendations for businesses to consider integrating into their baseline framework. Depending on your industry, the size of your business, and the type of data collected, your requirements may vary and you should consult with professionals to aid you in your plans.

Since the Privacy Rights Clearinghouse (PRC) began tracking breaches in 2005, 543 million records have been breached, more than one record for every resident of North America.[2] High profile data breaches and cyber security incidents are a reminder that all businesses and government agencies are at risk. In 2011, PRC recorded 558 incidents, and the Open Security Foundation reported 126.7 million records impacted. Equally as alarming are the threats that impacted every sector of the economy. Education (schools and colleges) represented 13% of the incidents, government agencies 15%, health care providers 29% and business 43%.[3] Compared to 2010, the percentage of breaches increased most significantly in the healthcare industry (which holds some of the most sensitive personal data) at 11%, while the number of business incidents decreased 13%.

[1] http://redtape.msnbc.msn.com/_news/2012/01/16/10163952-zappos-says-hacker-may-have-accessed-info-on-24-million-customers?ocid=ansmsnbc11

[2] Source: Privacy Rights Clearing House & DataLossDB.org

[3] http://datalossdb.org/yearly_reports/dataloss-2011.pdf

© 2012 Online Trust Alliance (OTA) All Rights Reserved

This data is the tip of the iceberg since a large number of breaches continue to occur undetected or unreported. Of the data from the Identity Theft Resource Center (ITRC), less than 30% of the incidents were provided via mandatory reporting and 38% did not identify the manner in which the breach was exposed.[4] While OTA encourages self-regulation and reporting, these trends suggest a need for improved voluntary self-regulatory efforts. These efforts include broader transparency and more detailed reporting requirements. Due to the increased sophistication of international crime syndicates, economic uncertainty and the proliferation of data carried on smartphones and tablets, we expect the number and severity of breaches and resulting identity thefts will continue to grow this year.

As organizations accumulate and rely on vast amounts of sensitive and personal data, the importance and challenges of data stewardship have increased dramatically. Compounding these challenges is the increased use of outsourcing and cloud services and evolving definition of privacy. Today, businesses need to not only validate and monitor their own policies and practices, but also their vendors. As the definition of Personally Identifiable Information (PII) and covered information is rapidly evolving, businesses need to take a broader view of the data they retain. Historically PII refers to information that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a user and can apply to all data collected including email addresses, names, street addresses, etc. Independent of point of collection (online or offline), all data is at risk and should be incorporated in a business' data loss plan.

Business Dynamics & Technical Landscape

- On and Off Line Data Collection
- Evolving Definition of Covered Information, beyond PII
- Complex Regulatory Framework
- Increased Reliance on Outsourcing & Cloud Services
- Multiple Devices & Platforms
- Portability of Storage & Devices
- Increase Sophistication & Resiliency of Cybercrime

Business Impact

According to the Verizon 2011 Data Breach Notification report, 50% of all data breaches were through hacking (up 10% over 2010) and 49% incorporated malware (up 11% over 2010). Most alarming is that 96% were avoidable through simple steps and internal controls.[5] This report provides further insights into where to focus counter measures, revealing that while hacking constituted 50% of the breaches, these incidents represented 76% of the records. Surprisingly, physical attacks (where the attacker is using a computer at one of your locations, as opposed to a remote, or "cyber" attack) continue to rise significantly, with 29% of breaches involving physical attacks (up 14% over 2010).

Small and large companies alike run the risk of a data breach, and the implications of a breach to the organization can be grave. For example, after an employee of Massachusetts General Hospital left 192 patient records on a subway, the hospital was fined $1M by the US Health and Human Services.[6] Similarly, the Massachusetts eHealth Collaborative, a 35-person non-profit, experienced a single laptop theft that cost them over $300,000 in legal, private investigation, credit monitoring and media consultancy fees. Employees also spent over 600 hours dealing with the damage that the breach caused to their brand and reputation.[7] Additionally, Sony expected its breach to incur upwards of $171 million in cleanup costs.[8]

[4] http://www.idtheftcenter.org/ITRC%20Breach%20Report%202011.pdf

[5] http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf

[6] http://www.hhs.gov/ocr/privacy/hipaa/news/mghnews.html

[7] http://www.nytimes.com/2011/12/19/technology/as-patient-records-are-digitized-data-breaches-are-on-the-rise.html?ref=massachusettsgeneralhospital

[8] http://informationweek.com/news/security/attacks/229625379

Such incidents not only harm a company's brand, but typically increase scrutiny and liability exposure, risking a negative impact to a business's bottom line. According to the Ponemon Institute, malicious or criminal attacks are the most expensive cause of data breaches and are on the rise. In 2010, more than 31 percent of data breach cases involved malicious attacks with an average cost of $318 per record, up from $214 with the average breach costing $7.2 million.[9]

Key operations may be impacted during a data breach if criminals change passwords or delete key files. If your business outsources some of its operations to other organizations, a breach of your data at that other organization can directly impact your operations and customers as well. Planning for incidents and physical disasters in advance helps to identify your potential exposure to both internal and external threats. Developing a plan for protecting both your hard and soft assets can help provide effective prevention, recovery and system integrity.

Incident planning incorporates both data breaches and disaster planning as a part of an organization's learning effort to help reduce operational risks, improve information security and corporate reputation risk management practices. Just like first responders for a physical incident, data managers and cyber responders must be trained, equipped and empowered to deal with the incident. Planning is the key to maintaining online trust and the vitality of the Internet, while helping to ensure the continuity of business.

Data Incident Plan Framework

An effective Data Incident Plan (DIP) includes a playbook that describes the fundamentals of a plan that can be deployed on a moment's notice. Organizations need to be able to quickly determine the nature and scope of the incident, take immediate steps to contain it, ensure that forensics evidence is not accidentally ruined and immediately initiate steps to notify regulators, law enforcement officials and the impacted users of the loss.

Scope of a DIP

- Consumer & Partner Data
- Intellectual Property
- Brand Reputation & Protection
- Regulatory Compliance
- Stockholder & Investment Community
- Business Continuity

The following working framework is designed as an aid to businesses, non-profits and governmental agencies in creating their DIPs. It recommends prevention, containment, and reactive operational practices. Once developed, the DIP should be distributed and communicated to all relevant employees, data partners and vendors to help ensure an effective 24/7 incident response capability.

Risk Assessment/Prevention

To help maximize business continuity, organizations are encouraged to self-audit their level of preparedness by surveying key management leaders the following questions:

1. Do you know what sensitive information is maintained by your company, where it is stored and how it is kept secure?
2. Do you have an accounting of all stored data including backups and archived data?
3. Do you have a map of data workflows both within your organization and your vendors' organizations to identify points of vulnerability?
4. Do you have a 24/7 incident response team in place?
5. Is management aware of the regulatory requirements related specifically to your business?

DIP Components

- Preventative
- Discovery
- Containment
- Mitigation
- Recovery
- Critique

[9] http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=ponemon Updated figures will be published in March 2011.

6. Have you conducted an audit of your data flows across your company and vendors, including a privacy and security review of all data collection and management activities?
7. Are you prepared to communicate to customers, partners and stockholders during an incident?
8. Do you have access credentials in the event key staff is not available?
9. Do you have a employee contact list to contact in the event of a breach, and is updated with contact information on a quarterly basis?
10. Are employees trained and prepared to notify management in the case of accidental data loss or a malicious attack? Are employees reluctant to report such incidents for fear of disciplinary action or termination?
11. Have you coordinated with all necessary departments with respect to breach readiness? (*For example information technology, corporate security, marketing, governance, fraud prevention, privacy compliance, HR and regulatory teams)*.
12. Do you have a privacy review and audit system in place for all data collection activities including that of third-party/cloud service providers? Have you taken necessary or reasonable steps to protect users' confidential data?
13. Do you review the plan on a regular basis to reflect key changes? Do key staff members have hard copies of the plan readily accessible in their offices and homes?

Data Governance and Loss Prevention

An organization's responsibility for data governance is dynamic and continually redefined and broadened, and varies not only between countries but between U.S. states. If your organization does not currently have a DIP it is not alone, but the plan needs to be developed now. The following sections are designed to help an organization understand the data they are responsible for protecting, limit access to that data, store only necessary data, and prevent common causes of data loss.

1. **Data Classification**

The first step in a DIP is to understand the type of data your organization is collecting and storing and to classify it according to the level of criticality and sensitivity, a process known as data classification. There are a variety of data classification schemes, ranging from the US government's *top secret/secret/confidential/public* scheme to a *high/moderate/low business impact* scheme. The scheme your organization chooses is less important than the exercise of making sure the data that is being collected is understood and what the potential impact of losing that data might be. The scheme should include details about data ownership, the definition of the security controls in place to protect it and any data retention and destruction requirements for the data. Federal Information Processing Standard (FIPS) publication 199 is a good guide for your data classification exercise.[10]

Data Classification

- Types of data
- Sensitivity level
- Owner of the data
- At motion/at rest

Once the data has been classified, it is also important to note whether or not the data is in use (accessed as a normal part of business), in motion (taken outside of your location), or at rest (archived). Data in motion has a particularly high risk of being lost, as that data could be on PCs, tablets, or mobile phones that are often lost or stolen. PII data that is in motion should be encrypted if possible (see Appendix E for encryption options). However, data that is at rest or in use, even if not stored on mobile devices, is still at risk of being breached. Even data that only resides on company servers may be breached due to hacking. Breaches ranging from the hacking of Subway restaurant Point of Sale systems to Epsilon involved server hacking, making auditing and validating data access especially important, as detailed in the next section.

[10] http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

2. Audit & Validate Data Access

A DIP should address employee access to all customer, business confidential and sensitive data and should include:

- Validating appropriate employee use and data access.
- Scanning of outbound email for content.
- Scanning of data copied to removable media and backup systems.
- Auditing of data repositories such as third party data shares and storage sites.
- Managing devices, including encrypting, limiting, tracking or remote wiping of data on external storage devices.
- Establishing provisions to automatically revoke all employee or vendor credentials upon termination or resignation.

Limiting data access helps to minimize the scope of potential losses and can provide an increased level of accountability and auditing capabilities. Equally important is the deployment of policies addressing appropriate use and access. Policies should include a device management plan which addresses all removable drives, media, USB keys, mobile devices, notebooks and respective encryption requirements. See Appendix E for a description of encryption options. All sensitive data shared with third parties and all wireless connections should be encrypted using industry best practices and standards. Policies concerning uploading such documents containing sensitive data to the "cloud" or external storage sites should be balanced for business need and convenience versus risk and exposure.

Employee & Vendor Access
- Management & Oversight
- Safeguarding
- Deter, Detect & Defend
- Education & Training
- Personnel & Physical Security

Companies doing business with governmental bodies should review the appropriate government requirements. In the recent wake of WikiLeaks, the US Executive Office of the President, Office of Management and Budget (OMB), published a self-assessment program for user data access. While developed for government agencies and contractors, this document reinforces the importance of detection, deterrents and defense from unauthorized employee and contractor disclosure.[11]

Critical Logs
- Transaction
- Database server
- Application server
- Operating system

A critical step in developing policies is to review all Web applications and third-party content being served on internal and external-facing sites. More and more frequently, applications, add-ons, and third party scripts are becoming intrusion opportunities and aid in the distribution of malware. Intrusion testing, application vulnerability scanning and preventative web application scans for iframes, cross-site scripting (XSS) vulnerabilities, clickjacking, malvertising and other threats including trojans, key loggers, and sniffers need to be part of an organization's arsenal to combat online threats**.**

3. Forensics, Intrusion Analysis & Auditing

An essential element of an incident response plan is the approach to take for computer forensics to help determine the source of a breach. A forensics investigation is best left to the experts, as it is extremely easy to render forensics evidence inadmissible in court by accidentally modifying it or taking actions that disrupt the chain of custody. It is critical for your affected systems, and the appropriate logs, to be in the proper state for law enforcement or other forensic experts to do an investigation that will hold up in court.

[11] https://otalliance.org/docs/OMB_Self-Assessment.pdf

Top suggestions to help accomplish this goal include:

- Secure and protect the integrity of the evidence and ensure that any systems affected by a breach are only accessible to internal investigators and law enforcement.
- Isolate suspected servers and client workstations from the network, unplugging network cables or disconnecting the workstations from wireless access points as appropriate. Note that law enforcement may request that your organization put affected systems back online if they feel that it gives them the opportunity to monitor the actions of the attacker.
- Contact law enforcement and your attorney. It is critical that forensics be performed by experts, and that your organization does not do anything to taint or compromise the data. If you have trained in-house security response capabilities, do an internal investigation prior to contacting law enforcement.
- Do not change the state of the systems in question. If the systems are on, leave them running and if they are off, unplug them.
- Do not try to image the affected systems or make copies of data. Simply copying data off a system will not provide investigators with the same level of evidence that can be obtained by experts using forensic toolkits and imaging utilities.
- Do not attempt to run programs, including antivirus and other utilities, on the affected systems without the help of experts. It's very easy to accidentally destroy evidence.
- Do not plug external storage devices, removable media, etc. into the affected systems.
- Document the employees who have access to the affected systems and obtain the names of all new hires and employees who have been recently terminated.
- Preserve all relevant logs on all affected systems, including web, client and server operating systems, application, firewall, mail, and intrusion detection system logs.
- Document everything that has been done on the affected systems since the incident was detected for law enforcement personnel.

As noted above, logs are a fundamental component of forensic analysis to determine the scope and customer impact of the incident. It is critical to enable logging prior to the occurrence of a breach; otherwise, your organization risks missing the trail that leads to the cause of the breach. Once a breach occurs, your organization will need to isolate and review logs from the compromised systems, including network devices, routers and access control systems. Your business may have a number of log types--transaction, server access, application server, firewall, and the client operating system. They can all provide valuable information to retrace what occurred. Since it is well-known to attackers that logs are of great value to investigators, it is important that your organization protect the logs from attack and routinely back them up. Additionally, your organization will want to keep copies of logs before, during, and after an incident to assist investigators.

A primary goal of log analysis is to understand what data has been compromised and to determine whether or not that data is PII. As your organization review logs look for queries that match the data known to have been exported. If your organization does not have any evidence to match against, the database administrator, application developer, and other key IT staff should be able to provide "normal" application and database activities. This should include anomalies such as unusual queries that applications or administrators would not normally make. Look for authentication attempts that appear out of place, both successful and unsuccessful. If file-level auditing was enabled by the system admin for the server OS, check if files were created in any unusual directory. This could be evidence of a database dump or copy. After you determine the type and sensitivity of data that has been

compromised, speak with your attorney to understand your reporting obligations. The laws for reporting vary widely by US state and country and you will need to work with an expert to ensure that you're following the appropriate laws that apply to your data. See Appendix D for further information on forensics and logs.

4. Data Loss Prevention Technologies

The increased complexity of internal systems and use of outsourcing, temporary employees, contractors and remote workers increases the risk of a breach. There is a wide array of technologies to help identify accidental, unauthorized and/or illegal transfers of data and documents, yet often the basics of security are overlooked. The referenced security best practices are recommended for every organization.

Beyond these security best practices, other technology solutions include intrusion and loss detection, data access control, and automated breach notification. Some solutions provide the ability to classify and monitor data which may be within an email, application or data store, and can monitor data while at rest, in use or in motion. Other solutions can perform contextual inspection of data as it is edited or sent out. Rules can be configured to notify the appropriate employees and can perform varied levels of prevention and remedial actions from simple notification to active blocking. They provide mechanisms for classifying information, including data matching, data fingerprinting to rule-based expressions, key words and watermark recognition. When implemented they have the ability to aid in the handling, control and transmission of sensitive data.

Use of new technologies is being driven by the increased regulatory and compliance requirements, internal requirements and governance, as well as, general business awareness of data management. For larger companies with IT security expertise, content-aware Data Loss Prevention (DLP) solutions offer capabilities to identify data at risk and apply remedial actions to help ensure that data is appropriately protected, along with forensics and remediation capabilities.[12]

Security Best Practices

- Use of Secure Socket Layer (SSL) for all data collection forms; ideally use "Always on SSL" for best data protection
- Extended Validation SSL certificates for all commerce and banking applications *
- Data & disk encryption
- Multilayered firewall protection
- Encryption of wireless routers
- Default disabling of shared folders
- Security risks of password re-set and identity verification security questions
- Upgrading to browsers with integrated phishing and malware protection
- Email authentication to help detect malicious and deceptive email **
- Automatic patch management for operating systems, applications & add-ons
- Inventory system access credentials
- Remote wiping of mobile devices

5. Data Minimization

There is a key rule of thumb when it comes to collecting data: if your organization does not have the data, it cannot lose it. While that statement seems obvious and easy to follow, it is also potentially in conflict with the marketing needs of the organization. Marketing teams want to have the necessary data to understand their customers and present them with attractive offers for the company's products. When it comes to customer information, keep the data that provides

[12] See Gartner Magic Quadrant for Content-Aware Data Loss Prevention - http://www.gartner.com/reprints/?id=1-16XZCGC&ct=110811&st=sb
*Extended Validation SSL Certificates - https://otalliance.org/resources/authentication/index.html
** Email Authentication - https://otalliance.org/resources/authentication/index.html

your organization with a competitive advantage and discard the rest. For example, Wharton marketing professors recommend that rather than maintaining data on individual users, aggregate data that can answer questions such as, "Among all people who bought five times or more, how many times are they likely to buy in the next year?"[13] Maintaining this aggregated data, and discarding PII data, in many cases can give your organization the necessary marketing information about your customers while reducing the reporting requirements, and potentially the severity of, a breach. Of course, in industries such as healthcare and financial services, organizations will end up with sensitive customer information, and need to maintain it, in the normal course of business.

Additionally, a comprehensive annual audit should be conducted to understand what data is being collected, and whether it should be retained, aggregated, or discarded. This audit should be conducted by representatives of both marketing and IT. The company may re-validate the business need for its collection and retention and can discuss whether aggregation might be used to minimize the amount of PII data that is being retained. Data retention and destruction policies should dictate how long information needs to be retained and how to destruct data once past its retention period

6. Data Destruction Policies

Since a common area for data breaches is on archived media or computers that are no longer in use, many new privacy laws require businesses to securely destroy data when it reaches end of life. Formatting a hard drive or deleting files using built-in operating system features leaves the files open to being recovered by a third-party with simple tools. In fact, a British research study of 300 hard drives purchased from eBay and computer fairs showed that 34 percent of drives had data identifying the particular individual or organizations where the drives had been in use.[14] Any sensitive data no longer in use needs to be securely decommissioned either by overwriting, degaussing, encryption, or physical destruction of the storage medium. Whether a business is donating a system to a charity, selling or giving it to an employee for personal use, or simply disposing of it, the secure deletion step needs to be performed. The National Institute of Standards and Technology (NIST) has published documentation with the guidelines for securely destroying data.[15]

7. Inventory System Access & Credentials

Having a list of key systems, access credentials and key contacts is essential to mitigating threats and minimizing the impact on business operations. This list should be kept secure yet accessible at all times to respond to not only data incidents, but to physical disasters or the loss of key personnel. Such a list should include but not be limited to:

- Registrar, including DNS access
- Server hosting provider, including IP address
- Cloud service providers including data backup, email service providers and others
- Payroll providers
- Merchant Card processor
- Company bank accounts and credit cards

[13] http://knowledge.wharton.upenn.edu/article.cfm?articleid=2186
[14] http://www.dailymail.co.uk/news/article-1178239/Computer-hard-drive-sold-eBay-details-secret-U-S-missile-defence-system.html
[15] http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf

Incident Response Planning

Organizations must be prepared to react on several fronts when confronted with a data loss or breach. To be prepared, it is critical to have an orchestrated response and vendor relationships in place with an appropriate project plan which is well documented and assures the appropriate personnel have been trained. The organization should be prepared to notify all appropriate parties, (including regulatory bodies and law enforcement), communicate timely, accurate information and consider offering remedies to those affected.

8. Creating an Incident Response Team

Data breaches are by nature interdisciplinary events that require coordinated strategies. Every functional group within an organization needs to be represented, including but not limited to Information Technology, Information Security, Compliance or Risk Management, Human Resources, Operations, Legal, Public Relations, Finance, and Customer Service. In addition, Sales, Business Development, Procurement and Investor Relations groups all should be included to fully anticipate the ramifications to business continuity. As a first step organizations should appoint an executive, with defined responsibilities and decision making authority with respect to data breach response. It is suggested this role be assigned to a Board member, corporate officer or high-level employee, as this individual could be required to provide Board briefings and needs to be equipped with decision making authority. Equipped with a project plan, every relevant employee should know who is in charge, who to call and what to do. Time is critical; avoid redundancy and any ambiguous responsibilities. Breach team criteria should include:

- An executive with broad decision making authority
- Representation of all key internal organizations
- "First responders" available 24/7, in the event of an after-hours emergency
- Spokesperson trained in media and who has a deep understanding of operations and security
- A team of appropriately trained employees
- Someone who has access and authority to key systems for analysis and back-up
- The appropriate authority and access to management for actions which may require higher level approvals.
- A summary of key contacts with after hour numbers for both internal and external contacts including outside legal counsel and PR agency.

Plan Fundamentals

- Create & empower a team
- Assign 24/7 "First Responders"
- Develop vendor and law enforcement relationships
- Create & document a plan
- Create a notification "tree"
- Create communication templates & scripts
- Develop on-call resources & remedies
- Employee training
- Regulatory & legal review
- Funding
- Ongoing critique

9. Establish Vendor and Law Enforcement Relationships

We recommend pre-selecting service providers for functions including legal, public relations, notification activities and forensics services. Utilizing such services will help preserve consumer trust and brand loyalty. In addition, brands should consider domain monitoring and take-down services to help reduce the exposure from malicious and phishing sites and to audit outbound email for compliance to the latest email authentication protocols.[16] Other third parties to be considered include credit monitoring and identity theft management companies, as well as call centers to accommodate the anticipated spikes in call volumes. In selecting vendors, the following attributes should be considered;

[16] For email authentication resources visit https://otalliance.org/resources/authentication/index.html

- Subject matter expertise in the relevant industry
- Bonding, indemnification & insurance
- Experience handling the type of events and constituents
- Multi-Lingual language proficiencies
- Ability to speak to the media, customers and partners on the company's behalf.[17]

If your organization has existing insurance coverage, check with your carrier to see whether they have recommended providers to estimate your potential exposures and define an acceptable level for your risk tolerance and provide preferred rates.

Vendor agreements should include standard security risk management language and a risk assessment of their access to or storage of your data. Audit validation processes and performance benchmarks are essential parts of any agreement. In addition, clauses should be included addressing responsibility in the event of a security breach. Provisions should include the allocation of costs and responsibility for notification.

Building a relationship with law enforcement prior to an incident is also a best practice. In the U.S., federal and state agencies can both handle computer crime and there may be a regional task force for high technology crimes in your area. Becoming active in the local chapter of InfraGard, an information sharing and analysis effort between the FBI and the private sector, is a good way to build relationships with both law enforcement and data breach experts[18].

10. Create a Project Plan

A full project plan that includes a timeline and process flow is a critical tool for managing the pressing demands resulting from a breach. It is not uncommon to find public relations, sales, law enforcement, regulators, consumers and media with competing priorities. It is important to anticipate the needs and manage the expectations of each group, which is very difficult to do without a realistic and comprehensive timeline. Plans need to have the ability of being "activated" 24/7, including holidays and weekends, as criminals do not necessarily work a standard workweek. Your plan should address some key questions:

- What is the overall impact?
- What are the regulatory obligations and should law enforcement be notified?
- How will the breach be communicated?
- Who needs to be informed and what is the timing of each notification (internally and externally)?
- What data do you or your partners hold and how have you protected it?
- What changes need to be made to your internal processes and systems to help prevent a similar breach from reoccurring?
- How damaging will the loss of confidential data be to your customers or partners?
- How damaging will it be to your business and employees?
- What information needs to be collected if there is third party notification of an attack? Key information such as the person's name, organization, return contact information, and details on what they know about the incident is critical.[19]
- Are your answers above the same for all of your customer segments?

[17] Brand and domain management resources may be found at https://otalliance.org/about/Members.htm
[18] To find a local InfraGard chapter visit http://www.infragard.net/chapters/index.php?mn=3
[19] http://www.antiphishing.org/reports/APWG_WTD_HackedWebsite.pdf

11. Determine Notification Requirements

Business decision makers need to be familiar with the disclosure requirements of the regulations which govern their industry including not only digital data but the controls over respective paper documents and redress procedures. It is equally important to review your contracts with customers and partners as they may have notification requirements which exceed regulations.

Key Communication Plan Considerations

- Internal Communications
- Partner Communications
- Phone scripts
- On-hold messages
- Spokesperson Training
- Email & Letter Templates
- Web site and FAQ
- Multi-Lingual Support
- Media Monitoring Services

It is important to note that some state laws conflict with one another so it is very important to be intimately familiar with all requirements. If your organization has customer data, that data more than likely includes information from customers in other countries or U.S. states than your own. As of January 2012, in the U.S. there are forty-seven states which govern disclosure of PII or health-related information. It is very difficult to keep up with the reporting regulations for all of the states and countries where your organization has customers. Thus, it is important to have a business relationship with an attorney who is well-versed in the various data breach reporting laws. Different types of data loss events may require different responses – e.g., the theft of important confidential corporate information by a former employee would be handled differently than the loss of thousands of employees' Social Security numbers, customer credit card numbers, or an email list with millions of records, all of which could trigger obligations under the law. In most scenarios, the reporting messaging should include how the incident occurred, the scope of the incident, what steps are being taken to help individuals from becoming victims of identity theft and what is being done to prevent a reoccurrence. All communications should be carefully coordinated with legal counsel and law enforcement to ensure legal compliance and prevent the perpetrator from knowing that a breach was detected, thus preserving forensics.

Since many state, federal and foreign regulations require prompt notification, it is important to determine in advance how impacted individuals need to be contacted. Knowing this in advance will significantly improve your organization's ability to mitigate consumer angst and increase compliance. Considerations include the number of individuals impacted; the specific data elements exposed; the risk to the affected constituents from such exposure; regulatory requirements; and law enforcement jurisdiction. Speed and accuracy are equally important. Consumers increasingly expect timely and clear notification delivered in a manner appropriate to their needs, and depending on the type of data that was breached, may have an expectation for your organization to provide them with credit monitoring services free of charge.

Regulations vary not only by state, but also by country, industry and type of breach, requiring businesses to be familiar with a broad set of regulations. The regulatory landscape is rapidly expanding with the draft Data Breach Notification Act legislation introduced in September 2011 by Senator Dianne Feinstein, which is intended to provide a consistent set of data breach rules for U.S. businesses.[20]

[20] http://www.gpo.gov/fdsys/pkg/BILLS-112s1408is/pdf/BILLS-112s1408is.pdf

A data loss plan should be familiar with or address applicable requirements including but not limited to the following:

- Individual state laws where a business has nexus or customers including state data breach notification and employee data protection laws.
- Individual country laws if any of the lost data pertains to residents of countries other than the US.
- Payment Card Industry Data Security Standards (PCI DSS).
- Sarbanes-Oxley Act.
- HITECH Act of 2009, including the HITECH Breach Notification Rule [21]
- Health Insurance Portability and Accountability Act (HIPAA), including the HIPAA Privacy and Security Rules.
- Gramm-Leach Bliley Act, including the Safeguards Rule, and the interagency guidance on response programs for unauthorized access to customer information and customer notice.
- Fair Credit Reporting Act
- Federal Trade Commission Guidelines and Requirements
- Children's Online Privacy Protection Act (COPA)
- Basel II Accord
- Fair & Accurate Credit Transactions Act, Red Flags Rule (FTC)[22]
- Federal Financial Institution's Examine Council (FFIEC) Guidelines

Organizations found to be in breach of laws could face significant fines and penalties. *Readers are encouraged to work with a qualified attorney or firm who specializes and regulatory obligations. In addition, a firm's insurance policy should be reviewed for coverage. See Appendix C for insurance policy considerations.*

12. Communicate & Draft Appropriate Responses

Customers, employees, investors, regulators, and other key stakeholders will lose confidence and trust in an organization if it does not communicate effectively. This lost confidence can have a direct impact on the bottom line – from lost revenues (and increased marketing expenses to recapture those revenues) to additional legal, compliance and public relations expenses. The communications component of a plan needs to address three critical components: 1) internal communications 2) communication to impacted parties and 3) communication to applicable regulatory parties. A well-executed communications plan not only minimizes harm and potential legal liability but can actually enhance a company's overall reputation.

Spokesperson(s) need to be prepared to respond to media inquiries. The plan should anticipate the need to provide access to services and information to help impacted individuals. In addition to email, written correspondence, and web site postings, companies should monitor the use of social networking sites such as Facebook, Twitter and blogs to track consumer sentiment. Companies may consider using social networking sites for controlled, scripted and moderated postings, but need to be prepared for the debate or dialog, which may follow.

The communications component of the DIP should have a set of pre-approved web pages and templates staged, phone scripts prepared and frequently asked questions (FAQ's) drafted and ready for posting. Staff needs to anticipate call volumes and steps to minimize hold times and to consider the need for multi-lingual support.

[21] http://hitechanswers.net/about
[22] Red Flag' Requirements for Financial Institutions and Creditors Will Help Fight Identity Theft http://www.ftc.gov/bcp/edu/pubs/business/alerts/alt050.shtm

In the possibility of a phishing exploit to be the cause or contribute to the incident, it is suggested organizations create a phishing warning page and FAQ in advance and to post and replace the deceptive site as a teachable moment for end users.[23]

Most organizations realize too late or in the heat of the incident that there are subsets of the population that require specific communication. It may be appropriate to consider separate messages and methods of delivery for the company's most important relationships, such as its highest-value customers or most senior employees, or for categories of individuals that may be particularly sensitive, such as the elderly, the disabled and minors. Remember to consider all applicable laws before determining how to notify. Tailoring communications by geographic region and the unique characteristics of the population, including ethnicity and age of the audience, may be appropriate.

Key questions to include in external communications:

- Incident description including what, how and when, (*the more facts the better*).
- What type of data was lost or compromised?
- Who was impacted including estimate of the number and type of customers?
- What action is the business offering to assist affected persons or organizations?
- What steps are being put in place to help assure it will not happen again?
- What are you doing to help ensure your customers are not a victim of identity theft?
- Where will your customers go for information? (Contact info and toll free number)?
- How the organization keep customers informed and what are the next steps (critical in the early stages when all of the information may not be known)?

13. Providing Assistance & Possible Remedies

While the actual occurrences of identity theft from data breaches may be low, the threat to consumer trust of your brand can be significant. A DIP should evaluate what, if any remedy should be offered to affected individuals (or businesses). Offering remedies can help to offset any inconvenience and damage or the negative perception to an organization's brand. The incident may impact not only your customers but also business affiliates and partners. Offering a remedy can provide the opportunity to turn a potentially bad situation into a positive brand experience. Typical offers have included credit report monitoring, identity theft protection, and website gift certificates. Customers want companies to take responsibility and protect them from potential consequences of identity theft. It is recommended the design of such plans include mechanisms, both on and off line, for a customer to accept and enroll since their level of trust may be tarnished.

Training, Testing and Budget

A DIP will ultimately fail to be executed if the employees charged with its administration are not adequately trained. Organizations must have the foresight to allocate staff time and budget for the proper execution of their DIP. In order for a DIP to be successful, it is critical that the plan be reviewed by key stakeholders, fully tested, and updated regularly (consider quarterly) to address changes in the company or in the threat landscape.

14. Employee Awareness & Readiness Training

Providing baseline privacy training, defining PII (or covered information based on your businesses and regulatory requirements), sensitive and internal confidential data, is a good step in preparing employees for a breach. It is recommended that employee training include (but not be limited to) data collection mechanisms, retention policies, handling and sharing policies as well as data loss reporting procedures. Company personnel who are part of the

[23] For examples of teachable moments visit APWG http://www.apwg.org/reports/APWG_CMU_Landing_Pages_Project.pdf or OTA's sample phishing page https://otalliance.org/resources/samplephishgpage.html

response team should be prepared to both investigate and report findings and to communicate with media and regulatory authorities. Employees should be required to review plans upon hire and annually. In addition, companies may wish to consider background checks for all employees before they are provided with access to sensitive data. Employee completion of required training should be documented and reported to management for internal policy compliance. In addition, it is recommended that the training discuss the importance of unique strong passwords and safe computing recommendations.[24] *Plans should include an employee "call-tree" including cell phone and home numbers for critical employees and vendors that need to be contacted. In the event of a breach, forensics specialists should be on call to aid in preservation of evidence, determining the extent of the loss and who was potentially impacted.*

15. Analyze the Legal Implications

Prepare for the possibility of litigation. Preservation of all relevant information, communications and systems logs is essential. Lost or missing data could create additional scrutiny and brand damage. A legal review of all service providers' policies and business practices should be conducted annually and prior to their selection.

16. Funding & Budgeting

Responding to an accidental loss, or data breach incident is often an unbudgeted expense, including less tangible costs such as loss of business, an increase in insurance costs, and higher merchant card processing fees. The heat of a crisis is not the best time to make vendor selections. Consider pre-contracting services for affected individuals. Offering of credit monitoring services, fraud resolution, and/or ID theft insurance can help minimize the impact and reduce the chance of customer defections or lawsuits. Many organizations have business continuity and interruption insurance to cover the costs of an incident, including the hiring of a crisis public relations firm, notifying regulators and affected parties, and providing monitoring and identity theft remediation services to affected individuals. Annually review your insurance coverage to ensure it is keeping pace with regulatory requirements and your business and data collections practices. (See Appendix C for a partial list of cyber-insurance considerations).

Budgeting Considerations

- Security & Monitoring Software & Services
- Forensic Specialists
- Employee Training
- PR & Crisis Management Resources
- Remediation Programs
- Call Center Capabilities
- Legal Review
- Equipment Replacement
- Lost Revenue
- Insurance

17. Critique & Post Mortem Analysis

Organizations should carefully analyze past events to improve their plan and minimize the possibility of future recurrences. Conducting "fire drills" and annual audits can be an essential part of testing a crisis management plan. Ideally, plans should be tested regularly during the year including weekends and critiqued to remediate any deficiencies.

Any breach should also include a post mortem analysis where you gather key team members to analyze the breach and document corrective actions. This phase is especially important to keep structured and documented for regulatory compliance and for Board review. Key questions to ask and document in the post mortem phase include:

- Did we follow our plan, or did we have to discard it and start over during the incident?
- What lessons have we learned?
- What can we do better next time?[25]

[24] See the Department of Homeland Security program; Stop, Think Connect http://www.dhs.gov/files/events/stop-think-connect.shtm

[25] https://otalliance.org/resources/security/OTA_Email_Security_Guidelines.pdf

Other Considerations

18. Implement Steps to Help Curb Misuse of Your Brand, Domain & Email

Data loss and identity theft occur not only from accidental physical loss, but also from an ever- increasing level of deceptive practices. Forged email, malvertising, phishing, deceptive acquisition of domains and creation of bogus web sites are all on the rise. Such exploits may result in the installation of malware and keystroke loggers via trojans and deceptive downloads. Steps are to be taken to mitigate these exploits. Businesses should authenticate all email with declarative policies to help detect email spoofing, lock all domains from potential transfer, monitor domain registration, and implement Extended Validation Secure Socket Layer (EV SSL) Certificates. Combined with other key practices such as DNSSEC, these practices help to establish reasonable security measures[26]. Conversely, the absence of such practices may be viewed as a failure to adequately protect their customers. [27, 28]

19. International Considerations

US-based businesses need to be aware of the data breach notification laws and guidelines for all of the countries in which their customers reside, providing they are holding PII data on those customers. Given the number of people that relocated between countries, businesses that maintain customer data also need to make an effort on an ongoing basis to confirm the location of customers for whom they hold PII data. Contacting customers twice a year to confirm there residency, and thus under the same breach notification rules, is a best practice.

In the European Union (EU), the current data protection laws were enacted in 1995, before widespread adoption of the internet, smartphones, social networking, or even laptops. The existing EU laws do not require data breach notification, though some EU member countries such as the UK do have data breach laws. It is anticipated the EU data privacy directive will be finalized by March 2012. The proposed bill is reported to provide EU national data protection authorities the ability to levy fines up to 5 percent of a company's annual sales for data protection violations.[29] In January 2012 the European Data Protection Supervisor identified the following strategic issues.[30]

- Revision of the EU data protection framework
- Review of the Data Retention Directive
- Negotiations on agreements with third countries on data protection

Canada implemented the Personal Information Protection Act (PIPA) in 2004. While PIPA is focused on ensuring that businesses obtain consent before personal information is collected, used or disclosed, an amendment was passed in May 2010 (O.C. 122/2010) with provisions for notice regarding services providers outside of Canada and notice regarding security breaches, specifically for the province of Alberta. This amendment states that written notice must be provided to the Commissioner and include information including a description of the breach, an estimate of the number of individuals impacted by the breach, an assessment of the risk posed to individuals affected by the breach, and a description of the steps the organization has taken to reduce the risk of harm to affected individuals, among other information. Businesses that maintain PII on residents of Canada are recommended to be familiar with PIPA and its appropriate amendments.[31]

---

[26] DNSSEC - http://www.dnssec.net/

[27] Email Authentication including (SPF/SenderID and DKIM) as well as EV SSL Certificates may be found at http://otalliance.org/resources/ Many OTA Members who provide such services may be found at http://otalliance.org/about/Members.htm

[28] See OTA Online Principles and Business Guidelines https://otalliance.org/resources/principles.html

[29] http://www.businessweek.com/news/2011-12-06/eu-s-data-protection-reform-should-inspire-u-s-reding-says.html

[30] http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2012/EDPS-2012-01-Inventory_2012_EN.pdf

[31] http://servicealberta.ca/pipa/legislation/amendments.cfm

Summary

Data protection and privacy along with an organization's preparedness for the likelihood of a data loss incident are significant issues every business owner and executive must recognize. This risk has been elevated by several factors including the collection of vast amounts of digital information and the increasing levels of cybercrime and online malice.

As supported by the data reviewed in this document, data loss incidents can happen to businesses of all sizes, non-profits and government organizations. It is prudent to assume that over time all businesses will suffer a breach or loss of data. Such events can range from a lost laptop, a misplaced document to a system breach by a hacker. Whether you are a Fortune 500 businesses with a large IT security staff and chief privacy officer or a local merchant, hospital or non-profit, if you collect data you are at risk.

It is critical for all businesses including those who may not have an online presence; to acknowledge that the data they collect is not only a powerful marketing tool and business asset, but equally as import this contains sensitive personal data. Business and government leaders need to consider the following key principles to maximize their preparedness;

- Acknowledge the data they collect contains one or more forms of PII or sensitive data.
- Accept they will experience a data loss incident or breach.
- Understand they may fall under multiple government regulations requiring notice and remedies.
- Being unprepared can significantly add to the direct and indirect costs including management resources and lost productivity.
- A data incident can result in significant damage to a business's brand reputation.

It is critical for all businesses to be fully prepared with a data protection and breach incident plan to help protect their data, detect a loss and quickly mitigate the impact. A key is to instill data security and privacy as part of an organization's culture. The responsibility cannot be siloed with one group or individual and needs to be considered every employee's responsibility. Following the guidance in this document will help ensure that businesses are not caught off guard and are ready to take the appropriate steps to minimize the damage to their customers and brand in the event of a data loss incident.

Equally as important is to complete a audit of all business practices, products and services including third party vendors to validate the business reason for the collection of all data. Site visitors and customers must have clear, discoverable and comprehendible notices. Rather than being written by attorneys for attorneys, such notices need to be easily understood by the target audience. Addressing the mounting calls for self-regulation, provisions must be in place for consumers to have the ability to permanently opt-out of all data collection with notice on the use and sharing of any such data.

Conversely, consumers have a shared responsibility to understand they may be exchanging their online data for the use of advertising supported services ranging from free content, news and email to the hosting and storage or their documents and photos. As with businesses they need to take steps to protect their data and devices including ensuring they are using the most current browser technologies, automatically patching and updating their software and applications to think before they indiscriminately click on links and accept downloads from unknown sites.

OTA encourages all businesses, non-profits and government organizations to make a renewed commitment to data protection and privacy. Being prepared for a breach and data loss incident is good for your business, your brand and most importantly your customers.

© 2012 Online Trust Alliance (OTA) All Rights Reserved

APPENDIX A
Resources

Online Trust Alliance

Data Breach Resources - https://www.otalliance.org/resources/Incident.html

Anti-Malvertising Guidelines - https://otalliance.org/resources/malvertising.html

Domain Name System Security Extension (DNSSEC) - https://otalliance.org/resources/dnssec.html

Draft Privacy & Data Statement - https://www.otalliance.org/privacy_demo.html

Email Authentication - https://otalliance.org/resources/authentication/index.html

Extended Validation SSL Certificates - https://otalliance.org/resources/EVresources.htm

Phishing Warning Page - https://www.otalliance.org/resources/samplephishgpage.html

Browser Updates - Why Your Browser Matters - https://otalliance.org/browser

Data Privacy Day - https://otalliance.org/dataprivacyday.html

---

Executive Office of the President, Office of Management & Budget (OMB)
Self-Assessment Program for User Access to Classified Information
https://otalliance.org/docs/OMB_Self-Assessment.pdf

Federal Trade Commission
Dealing with a Data Breach
http://www.ftc.gov/bcp/edu/microsites/idtheft/business/data-breach.html

Business Data Breach Publications
http://www.ftc.gov/bcp/edu/microsites/idtheft/business/publications.html

Protecting Personal Information: A Guide for Business
http://business.ftc.gov/sites/default/files/pdf/bus69-protecting-personal-information-guide-business.pdf

Information Compromise and the Risk of Identity Theft: Guidance for Your Business
http://business.ftc.gov/documents/bus59-information-compromise-and-risk-id-theft-guidance-your-business

Illinois State Attorney General Office - Identity Theft & Data Breach Hotlines
http://illinoisattorneygeneral.gov/consumers/hotline.html

Washington State Attorney General Office - Identity Theft & Privacy
http://www.atg.wa.gov/ConsumerIssues/ID-Privacy.aspx

© 2012 Online Trust Alliance (OTA) All Rights Reserved

APPENDIX A
Resources Continued

American National Standards Institute (ANSI) & Internet Security Alliance: The Financial Management of Cyber Risk - http://webstore.ansi.org/cybersecurity.aspx

Anti-Phishing Working Group guidance for a hacked website - http://www.antiphishing.org/reports/APWG_WTD_HackedWebsite.pdf

Identity Theft Assistance Center (ITAC) - http://www.identitytheftassistance.org/

Identity Theft Resource Center (ITRC) - http://www.idtheftcenter.org/index.html

Identity Theft Council - http://www.identitytheftcouncil.org/

InfraGard – http://www.infragard.net

Javelin Strategy & Research - https://www.javelinstrategy.com/

National Cyber-Forensics & Training Alliance http://www.ncfta.net/

Open Security Foundation DateLossdb - http://datalossdb.org/

Ponemon Institute - http://www.ponemon.org/index.php

Privacy Clearing House, Chronology of Data Breaches - www.privacyrights.org/data-breach

TRUSTe – Privacy Best Practices - Protecting Customer Information Online http://www.truste.com/why_TRUSTe_privacy_services/privacy_best_practices

US Chamber of Commerce - http://www.uschamber.com/issues/technology/privacy-issues-overview

US Council of Better Business Bureaus Data Security Guide- http://www.bbb.org/data-security/

Appendix B

SAMPLE LETTER TEMPLATE

Dear [Name of User or Patient]:

I am writing to you with important information about a recent breach of your personal information from [Name of Organization]. We became aware of this breach on [Insert Date] which occurred on or about [Insert Date]. The breach occurred as follows:

(Describe event and include the following):

1. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.
2. A description of the types of unsecured information that were involved in the breach (such as whether full name, Social Security number, date of birth, home address, account number, diagnosis, disability code or other types of information were involved).
3. Steps the individual should take to protect themselves from potential harm from the breach.
4. A brief description of what the organization is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches.
5. Contact procedures for individuals to ask questions or learn additional information, which includes a toll-free telephone number, an e-mail address, Web site, or postal address.

Optional Considerations:
To help ensure that this information is not used inappropriately, [Name of Organization] will cover the cost for one year for you to receive credit monitoring. To take advantage of this offer, [Need to document the process for how this would work]. We also advise you to immediately take the following steps:

- Call the toll-free numbers of anyone of the three major credit bureaus (below) to place a fraud alert on your credit report. This can help prevent an identity thief from opening additional accounts in your name. As soon as the credit bureau confirms your fraud alert, the other two credit bureaus will automatically be notified to place alerts on your credit report, and all three reports will be sent to you free of charge.

    - Equifax: 1-800-525-6285; www.equifax.com.
    - Experian: 1-888-EXPERIAN (397-3742); www.experian.com
    - TransUnion: 1-800-680-7289; www.transunion.com

- Order your credit reports. By establishing a fraud alert, you will receive a follow-up letter that will explain how you can receive a free copy of your credit report. When you receive your credit report, examine it closely and look for signs of fraud, such as credit accounts that are not yours.

- Continue to monitor your credit reports. Even though a fraud alert has been placed on your account, you should continue to monitor your credit reports to ensure an imposter has not opened an account with your personal information.

We take very seriously our role of safeguarding your personal information and using it in an appropriate manner. [Name of Organization] apologizes for the stress and worry this situation has caused you and is doing everything it can to rectify the situation.

We have established a toll-free number to call us with questions and concerns about the loss of your personal information. You may call [Insert Toll Free Number] during normal business hours with any questions you have.

We have also established a section on our Web site with updated information and links to Web sites that offer information on what to do if your personal information has been compromised.

[Insert Closing Paragraph Based on Situation]

Sincerely,
[Insert Applicable Name/Contact Information]

APPENDIX C

CYBER SECURITY LIABILITY AND INSURANCE CONSIDERATIONS

The following is a partial list of criteria a company may wish to consider when reviewing cyber security liability policies and coverage including both first and third party protection. For your specific needs contact your legal and insurance professionals.

1. Coverage for Loss resulting from Administrative or Operational Mistakes – extends to acts of the Employee, Business Process Outsourcing (BPO) or outsourced IT provider.
2. Cyber Extortion reimbursement costs for a range of perils including a credible threat to introduce malicious code, pharm and phish customer systems or to corrupt, damage or destroy the Insured's computer system.
3. Electronic Media peril broadly defined to include infringement of domain name, copyright, trade names, logo, service mark on internet or intranet site.
4. Interruption expenses include additional costs associated with rented/leased equipment, use of third party services, additional staff expenses or labor costs directly resulting from a covered Loss of Digital Assets claim.
5. Personally identifiable information (PII) broadly defined to include an individual's name in combination with social security number, driver's license number, account number, credit or debit card or any non-personal information as defined in any privacy regulation.
6. Knowledge provision includes Board of Directors, President, Executive Officer, Chairman, Chief Information Officer, Chief Technology Officer, Risk Manager or General Counsel.
7. Broad coverage for Damages to third parties caused by a breach of network security.
8. Breach of Privacy coverage – includes Damages resulting from alleged violations of HIPAA, state and federal privacy protection laws and regulations.
9. Regulatory Expense coverage to comply with an alleged breach notice order issued by a regulatory agency against the Insured.
10. Coverage for expenses resulting from a breach of consumer protection laws including, but not limited to, the Fair Credit Reporting Act (FCRA), the California Consumer Credit Reporting Agencies Act (CCCRAA) and the EU Data Protection Act.
11. Public Relations Expenses coverage available to repair your reputation as a result of a data breach.
12. Customer Breach Notice Expense Coverage (via sub-limit) – reimburses for costs to notify and remediation costs including but not limited to credit monitoring.
13. Coverage for acts of a rogue employee causing intentional damage to the Insured's Computer Network.
14. Customer Notification Expenses include legal expenses, credit monitoring expenses, postage and advertising costs.
15. Privacy Breach definition extends to acts of the Insured and acts of a Service Provider acting on behalf of the Insured.
16. Punitive and exemplary damages coverage provided on a most favorable venue basis.

© 2012 Online Trust Alliance (OTA) All Rights Reserved

Appendix D

COMPUTER FORENSICS BASICS

The most common goal of performing forensics is to gain a better understanding of an event of interest by finding and analyzing the facts related to that event. When you experience a data breach incident, it is important for you to engage an expert in computer forensics to help you discover the source of the breach and to give law enforcement the best opportunity at catching the perpetrator. The intent of this section of the document is to give you an understanding of the basics behind what an expert will be doing to trace a breach. The process for performing computer forensics comprises the following basic phases:

- Collection: identifying, labeling, recording, and acquiring data from the possible sources of relevant data (computer workstations, external storage devices, network servers, logs, etc.), while following procedures that preserve the integrity of the data.
- Examination: forensically processing collected data using a combination of automated and manual methods, and assessing and extracting data of particular interest, while preserving the integrity of the data.
- Analysis: analyzing the results of the examination, using legally justifiable methods and techniques, to derive useful information that addresses the questions that were the impetus for performing the collection and examination.
- Reporting: reporting the results of the analysis, which may include describing the actions used, explaining how tools and procedures were selected, determining what other actions need to be performed (e.g., forensic examination of additional data sources, securing identified vulnerabilities, improving existing security controls), and providing recommendations for improvement to policies, procedures, tools, and other aspects of the forensic process.

An expert will only be able to do an effective investigation if you've put the right processes in place to trace a breach before it occurs. The types of processes you should put into place, if you aren't already doing them, include:

- Performing regular backups of systems and maintaining previous backups for a specific period of time
- Enabling auditing on workstations, servers, and network devices
- Forwarding audit records to secure centralized log servers
- Configuring mission-critical applications to perform auditing, including recording all authentication attempts
- Maintaining a database of file hashes for the files of common OS and application deployments, and using file integrity checking software on particularly important assets
- Maintaining records (e.g., baselines) of network and system configurations
- Establishing data retention policies that support performing historical reviews of system and network activity, complying with requests or requirements to preserve data relating to ongoing litigation and investigations, and destroying data that is no longer needed.

When performing forensics during incident response, an important consideration is how and when the incident should be contained. It is important to ensure that any affected systems are secured against physical access and left running after an incident occurs. The affected systems should be disconnected from any wired or wireless networks to ensure that evidence does not get contaminated, either intentionally by the perpetrator or unintentionally by someone who normally is authorized to access the system. Document all personnel who have access to the affected

© 2012 Online Trust Alliance (OTA) All Rights Reserved

Appendix D

COMPUTER FORENSICS BASICS (continued)

systems, as an investigator will need this information to build the picture of how the breach might have occurred, and these people might have passwords that are needed for the investigator to properly access the systems.

Once you've contacted law enforcement, you will need to be prepared to answer a series of questions from them. The questions from them will likely include the following areas:[32]

1. What evidence do you have that you were victimized?
2. What is the chronology of the event?
3. What is impact to your network?
4. Are your systems still running?
5. Can you still conduct business?
6. When did the incident first occur?
7. When was incident discovered?
8. Who discovered the incident?
9. Is the activity ongoing?
10. What have you done so far?
11. Who do you think is responsible for the incident and why do you suspect them?
12. What is the internal or external IP address for the attacker?
13. Can you provide a complete topology of your network?
14. What first alerted you to the incident regardless of when the attack truly started?
15. Who in the organization has been notified?
16. Who outside the organization has been notified?
17. From this point forward, who does law enforcement contact and who can they speak to if they are contacted?
18. What are your estimated damages?

For a detailed drill-down on computer forensics, see the NIST Guide to Integrating Forensic Techniques into Incident Response.[33].

[32] High Technology Crime Investigation Association, San Diego Chapter: http://www.htcia.org/
[33] http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf

Appendix E

ENCRYPTION RESOURCES

A best practice for helping the minimize the effect of a breach, especially for laptops, tablets, and smartphones, which often contain customer data and are easily lost or stolen, is encryption. This appendix will focus on encryption for laptops, though the highest-volume tablet and phone operating systems, including iOS (iPhone and iPad) and Android tablets running version 3.0 and up, include options for encrypting the data on the device.

Types of encryption

When encrypting files on a laptop, there are two different types of encryption to examine: file and full-disk. File encryption has been built-in at the operating system level since Windows 2000 (Encrypting File System) and Mac OS X (File Vault). It encrypts files and directories on a per-user basis and is useful in preventing end users who share a PC from being able to read the data of other users. However, since it is possible to inadvertently leave unencrypted temp files, page files, etc. on a disk, it is not a good solution for protecting all sensitive data on a lost or stolen system.

Full-disk encryption is the best solution for protecting sensitive data for laptops that may be lost or stolen, as all data on the drive, including user data, temp files, home directories, etc. is encrypted. It helps ensure that customer or sensitive employee data on a lost or stolen system cannot be accessed by a person who steals a laptop or finds one that is inadvertently left in a public location by an employee. BitLocker in Windows Vista/7 (Ultimate and Enterprise SKUs) and FileVault2 in Mac OS X Lion provide full disk encryption that can be enabled either immediately after operating system setup, or at any later time (even after user data has been copied to the disk). In addition, there are a variety of third-party solutions, including TrueCrypt and PGP, which work on both Windows and Mac OS X systems. Links to resources on encryption options are below:

Full disk encryption:

- Truecrypt (multiple operating systems): http://www.truecrypt.org
- PGP (multiple operating systems): http://www.symantec.com/business/whole-disk-encryption
- Windows Vista/7 BitLocker Drive Encryption: http://windows.microsoft.com/en-US/windows7/products/features/bitlocker
- MacOS X Lion, FileVault 2: http://www.apple.com/macosx/what-is/security.html

File encryption:

- Windows (XP through Windows 7), Encrypting File System (EFS): http://windows.microsoft.com/en-US/windows7/What-is-Encrypting-File-System-EFS
- Truecrypt (multiple operating systems), http://www.truecrypt.org
- MacOS X (Panther through Lion) FileVault: http://www.apple.com/pr/library/2003/06/23Apple-Previews-Mac-OS-X-Panther.html

Phone/Tablet encryption

- iOS encryption: http://manuals.info.apple.com/en_US/iPhone_iOS4_User_Guide.pdf
- Android tablet encryption (Version 3.0 and above): http://source.android.com/tech/encryption/android_crypto_implementation.html

Appendix F

SAMPLE DATA INCIDENT PLAN OUTLINE

A sample Data Incident Plan outline is below, modeled on the NIST Special Pub. 800-61 and ISSA Model Plan, Austin-Texas Chapter:

1.0 Introduction

- 1.1 Purpose of this Incident Response Plan
- 1.2 Purpose of Incident Response Team
- 1.3 Objectives of the Incident Response Team

2.0 Incidents

- 2.1 Incident Categories

3.0 Responding to an incident

- 3.1 Organization
- 3.2 Escalation Levels
- 3.3 Escalation Considerations
- 3.4 The Incident Response Process
- 3.5 Incident Response Team Roles and Responsibilities
- 3.5.1 Escalation Level 0
- 3.5.2 Escalation Level 1
- 3.5.3 Escalation Level 2
- 3.5.4 Escalation Level 3
- 3.5.5 Post Incident

Appendix A: Contact Lists

- Internal contacts
- External contacts
- Law enforcement agency contacts

Detailed Incident Plan Resources

- Full ISSA Model Plan, Austin-Texas Chapter: http://www2.dir.state.tx.us/SiteCollectionDocuments/Security/Policies%20and%20Standards/e4.doc

- British Columbia incident checklist: http://www.oipc.bc.ca/pdfs/Policy/Privacy_Breach_Checklist%28June20

© 2012 Online Trust Alliance. All rights reserved.

Material in this publication is for educational and informational purposes only. Neither the publisher, the Online Trust Alliance (OTA), its members nor the authors assume any liability for any errors or omissions nor how this publication or its contents are used or interpreted or for any consequences resulting directly or indirectly from the use of this publication. OTA makes no assertions or endorsements regarding the security or business practices of companies who may choose to adopt such recommendations outlined. For legal advice or any other, please consult your personal attorney or appropriate professional. The views expressed in this publication do not necessarily reflect the views of OTA member companies or affiliated organizations.

OTA MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT. For updates visit No part of this publication may be reproduced or distributed in any form or by any means, or stored in a database, web site or retrieval without the written consent of OTA.