

# Data Breach & Incident Readiness Planning Guide



*Creating an online trust community, promoting business practices and technologies to enhance consumer trust and the vitality of interactive marketing, ecommerce, and online financial and governmental services*

*In collaboration with the Anti-Phishing Working Group (APWG), the Direct Marketing Association (DMA), the Association of the German Internet Industry, Internet Security Alliance (ISA), Merchant Risk Council (MRC), Direct Marketing Association of Singapore (DMAS), US Chamber of Commerce and OTA Member Companies*

January 27, 2010

## Introduction

Cybersecurity threats, misguided business practices, and online crime continue to grow in sophistication, frequency and magnitude, contributing to the growing levels of loss of sensitive and personal data. According to the Identify Theft Research Center, data breaches involving personally identifiable information (PII) increased over 600% this past year with over 222 million records being compromised.<sup>1</sup>

As organizations accumulate vast amounts of user data, the responsibilities of data stewardship and governance have increased dramatically. Recent high profile data breaches and cybersecurity incidents have shown that financial institutions, retailers, health care providers, educational institutions, government agencies and others are susceptible and at risk.

Few if any other events or incidents can damage a company's reputation and consumer's trust more than a breach of personal, sensitive or corporate data which impacts not only a company's customers but also their partners, stockholders and employees. High profile breaches risk scrutiny from consumer advocates and regulators, not to mention fines and loss of business resulting in a negative impact to stock holder value.

While regulatory mandates have historically been the top driver for developing plans, the possible negative impact on a corporate brand's reputation, consumer trust and costs are becoming a significant driver. In the 2010 Data Breach Survey published by SC Magazine, 76% of respondents stated regulatory pressures and 75% cited the possible negative risk to their brand as the main influences for developing their plans.<sup>2</sup> According to the 2009 Cost of Data Breach Report published by the Ponemon Institute, data breach incidents cost U.S. companies \$204 per compromised customer record, compared to \$202 in 2008. The average total per-incident costs in 2009 were \$6.75 million.<sup>3</sup>

Be proactive and be prepared. Planning ahead is the key to maintaining online trust and the vitality of the internet, while helping to ensure the continuity of business. It is an organization's opportunity and obligation to its constituents including customers, citizens, employees, and stockholders. Having a plan is a business imperative.

Companies need to proactively plan for the worst case understanding the focus is not if a data loss will occur, but when! An effective Data Loss Plan (DLP) includes an orchestrated playbook including the fundamentals of a readiness plan, to be deployed on moment's notice. Such a plan helps to maximize a state of preparedness where all of the key decision makers have been identified, responsibilities defined, key support relationships have been put in place, and applicable legal and regulatory requirements have been assessed. Organizations need to be able to quickly determine the nature and scope of the incident, take immediate steps to contain and control it and initiate steps to notify regulators and the impacted consumers.

The framework is designed for businesses, non-profits and governmental agencies and is recommended to include but not be limited to preventative, containment, and reactive operational practices. Once developed, the DLP should be distributed and communicated to all employees and data partners, to help ensure an effective 24/7 incident response.

Visit <https://www.otalliance.org/resources/Incident.html> for updates and resources.

---

<sup>1</sup> Identify Theft Resource Center. Data for 2009 included the Heartland Payment System breach including 130 million records. Netting out this specific incident, breaches increased 259% from 2008 to 2009. [http://www.idtheftcenter.org/artman2/publish/lib\\_survey/ITRC\\_2008\\_Breach\\_List.shtml](http://www.idtheftcenter.org/artman2/publish/lib_survey/ITRC_2008_Breach_List.shtml)

<sup>2</sup> SC Magazine <http://www.scmagazineus.com/guarding-against-a-data-breach-survey-minding-data/printarticle/159965/>

<sup>3</sup> Ponemon Institute 2009, published January 2010. <http://www.encryptionreports.com/costofdatabreach.html>

## Data Governance and Data Loss Prevention

An organization with responsibility for data must consider ways to govern and protect that data. The following sections advise an organization on how to: understand the data they are responsible for, limit the risk of access to that data, store only necessary data, and prevent common methods of data loss.

- 1. Data Classification.** A preventative and mitigating first step is identifying and classifying data which is 1) in use, 2) at rest (archived or stored) and 3) in motion. Organizations need to apply a value to such data, determine the useful life, level of sensitivity and the applicable regulatory requirements. It is advisable to have legal counsel, including those trained in discovery review your classification policies. Typically “data in use” is highly exposed as it is being used on client desktops or mobile devices often susceptible to vulnerable applications, viruses and malware along with unprotected external devices. Data “at rest” is equally challenging since a great deal of data is often stored on servers in multiple geographic locations, without documentation of its existence. The use of offsite storage and archiving with third parties needs to be incorporated into the plan.

Last but not least is “data in motion”. Examples include customer lists, suppression files, and other data that might be uploaded to cloud applications, connection from remote locations, or to third party service providers. Virtual private networks (VPNs), Transport Layer Security (TLS) and Secure Sockets Layer (SSL), are cryptographic protocols that help provide security, and should be adopted where feasible or regulated.<sup>4</sup>

- 2. Audit & Validate Data Access.** A comprehensive DLP plan needs to address employee access to all customers, business confidential and sensitive data including; 1) validating appropriate employee use and data access, 2) scanning of outbound email for content, 3) audit data repositories such as third party data shares and storage and 4) device management.

Limiting data access helps to minimize potential losses and can provide an audit trail. Equally important is the deployment of policies addressing appropriate use and access. Policies should consider a device management plan requiring all removable drives, mobile devices, media and USB keys as well as notebooks be fully encrypted.<sup>5</sup> Additionally, all data shared with third parties containing sensitive data and 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 validated for business need vs. risk and a user’s convenience.

A critical component to mitigate data loss and breaches is to review all web applications and third party content being served on both internal as well as external facing site. More and more frequently, applications, ad-ons, and third party java script are becoming jumping off points for intrusion and distribution of malware. Intrusion testing, application vulnerability scanning and preventative web application scans for iFrame, cross-site exploits (XSS), click jacking, and other threats including trojans, key loggers, and sniffers need to be part of an organization’s arsenal to combat online threats.

---

<sup>4</sup> See OTA Principles number 1 and 7. <https://www.otalliance.org/resources/principles.html>

<sup>5</sup> For an overview on Full-Disk Encryption (FDE) see [http://en.wikipedia.org/wiki/Full\\_disk\\_encryption](http://en.wikipedia.org/wiki/Full_disk_encryption). Windows BitLocker drives encryption helps to protect from threats of data theft, accidental disclosure from lost, stolen or inappropriately decommissioned PC hardware. BitLocker helps to prevent a thief who boots another operating system or runs a software hacking tool from breaking into a system or performing offline viewing of the files stored on the protected drive. <http://www.microsoft.com/windows/windows-vista/features/bitlocker.aspx> Similar solutions are available for Apple users from PGP, CheckPoint and others.

3. **Data Minimization & Destruction Policies.** A comprehensive audit and “discovery” is required to understand what data is collected, and to re-validate the business need for its collection and retention. Existing retention periods need to be validated for regulatory compliance and then determine what if any data destruction is required. As storage prices have decreased dramatically and data recovery tools have become more sophisticated, the physical destruction of drives should be considered. Reducing the storage and retention, reduces the scope and impact of potential breaches.
4. **Implement Steps To Help Curb Misuse Of Your Brand, Name, Domain & Email.** Data loss and identity theft occur not only from breaches and physical loss, but from an increasing level of deceptive practices including forged email, illegally diverting or acquiring a domain and creating phishing or bogus web sites to capture consumer personal data. In the process they increasingly attempt to install malware and keystroke loggers via trojans and deceptive downloads. Proven steps to mitigate these exploits include; authenticating all outbound email with declarative policies to help detect email spoofing; locking of domains from potential transfer, domain registration monitoring, adoption of email authentication, and implementation of Extended Validation Secure Socket Layer (EV SSL) Certificates. These need to be considered part of the arsenal to counter data abuse. Combined with other key practices, they help to demonstrate reasonable security measures and are critical to help insuring consumer trust. Conversely their absence is increasingly being viewed as an organization’s failure to adequately protect their customers.<sup>6, 7</sup>

### Data Loss Response Planning

Organizations must be prepared to react on several fronts when confronted with a data loss or breach. It is critical to have the right team coordinated, the right vendor relationships in place, and an appropriate project plan developed before a breach occurs. In reaction to a data breach the organization should be prepared to notify the appropriate stakeholders and regulatory bodies, communicate the right information, and offer possible remedies to those affected.

#### 5. Create a team with accountability & decision making authority.

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 IT, security, compliance, risk management, human resource, operations, legal, public relations, and customer service. In addition sales, business development, procurement and stockholder relations need to be included to fully anticipate the ramifications to business continuity. As a first step organizations need to appoint a single executive, with clearly defined responsibility and decision making authority. It is suggested such a role be assigned to a Board member or corporate officer, as they will likely be required to provide Board briefings. Combined with a project plan, every employee should know who is in charge, who to call and what to do. Time is critical.

Avoid redundancy and any ambiguous responsibilities. Key team criteria include:

- Corporate officer or executive with board decision making authority
- Representation of all key internal organizations
- Available 24/7
- Appropriate training
- Access and authority to key systems for analysis and back-up
- Appropriate authority and timely access to management for actions which may require higher level approvals

---

<sup>6</sup> Email Authentication including (SPF/SenderID and DKIM) as well as EV SSL Certificates may be found at <http://otalliance.org/resources/index.html>. Many OTA Members who provide such services may be found at <http://otalliance.org/about/Members.htm>

<sup>7</sup> See OTA Online Principles and Business Guidelines <https://www.otalliance.org/resources/principles.html>

**Establish Relationships with Vendors.** We recommend pre-selecting and contracting external service providers for legal, public relations and notification activities. Highly visible brands should consider domain monitoring and take-down services to help reduce the exposure from malicious and phishing sites and audit outbound email for compliance to the latest email authentication protocols.<sup>8</sup> Other third parties to be considered include credit monitoring and identity theft management companies as well as outsourced call centers to accommodate spikes in call volumes. They can help design compensatory packages for affected geographies and market segments. Attributes of appropriate vendors would include deep knowledge of the relevant industry, bonding, insurance, experience in handling the type of events and constituents anticipated by the plan, language proficiency and the ability to speak to the media, customers and partners on the company's behalf.<sup>9</sup> If you have existing insurance coverage, check with your carrier if they have recommended or required providers to estimate your potential exposures and an acceptable level for your risk tolerance level.

Vendor agreements should include standard security risk management language and a risk assessment of their access to, and or storage of your data. Audit validation processes and performance benchmark are an essential part of any such agreements.

**6. Create a Project Plan.** A plan including a timeline and process are critical tools 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 conflicting 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, independent of holidays and weekends when such exploits are increasingly executed. A plan needs to address what is the impact, what needs to be done, what are the legal and regulatory obligations. The plan should be able to estimate the impact to the bottom line and quickly determine and state of how the breach occurred. Organizations need to publish the plan and procedures and post for employee reference.

Key questions to be addressed are recommended to include:

- Who needs to be informed and the timing of each (internally and externally)?
- What data do you or your partners hold and how have you protected it? (see #1)
- What changes need to be made to your internal processes and systems to help prevent it 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?
- Are your answers above the same for all of your customer segments?

**8. Determine Who Needs to Be Notified, How & When.** Be familiar with the disclosure requirements of the regulations which govern your industry. Different types of data loss and cyber security events require different responses – e.g., the theft of important confidential corporate information by a former employee would likely be handled quite differently than the loss of thousands of employees' Social Security numbers, credit card data, or an email list with millions of records. In most scenarios, messaging should include how the incident occurred, the scope of the incident, what steps are being taken to help individuals and what is being done to prevent a re-occurrence. All must be carefully coordinated with legal counsel and law enforcement to prevent tipping the hand of the online criminal and to preserve forensics.

---

<sup>8</sup> For email authentication resources visit <https://otalliance.org/resources/authentication/index.html>

<sup>9</sup> Brand and domain management resources may be found at <https://otalliance.org/about/Members.htm>

Since many state, federal and foreign regulators require prompt notification, it is important to determine in advance how individuals need to be contacted. In cases of a breaches involving personally identifiable information (PII), designing a system to quickly determine who is affected is critical. Considerations include the size of the affected population, the specific data elements exposed, risk to the affected constituents from such exposure, and predicted response of the affected constituents, regulatory requirements and law enforcement jurisdiction. Speed and accuracy are both important. Consumers increasingly expect timely and clear notification delivered in a manner appropriate to their needs.

Data breach notification laws and regulations vary widely by country, industry, State and type of breach, requiring businesses to be familiar with a broad set of regulations. The plan should address applicable requirements including but not limited to the following:

- Payment Card Industry Data Security Standards (PCI DSS)
- Sarbanes-Oxley Act
- HiTech Act of 2009<sup>10</sup>
- Health Insurance Portability and Accountability Act (HIPAA)
- Gramm-Leach Bliley Act
- Federal Trade Commission
- Those required internationally by the European Union and the United Kingdom.
- Others include individual State regulatory requirements

Organizations that are found to be in breach of these laws can face significant fines and costly remedies. *Organizations are encouraged to work with a qualified attorney or third party firm who specializes in such legal and regulatory obligations.*

**9. Communications & Draft Appropriate Responses.** Customers, employees, investors, regulators, and other key stakeholders will lose confidence and trust in an organization that does not communicate effectively. This 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. Notification to key regulatory bodies is mandated in a growing number of circumstances, and is a courtesy in others. Spokesperson(s) need to be prepared for responding to media inquiries, delivering a clear message to parties affected. The plan should anticipate the need to provide access to services and information to help those impacted. In addition to email, written correspondence, and web site postings, companies should consider the use of social networking sites such as Facebook, MySpace, Twitter and blogs for both communications and the monitoring of media for a pulse on consumer sentiment. A well-executed communications plan not only minimizes harm and potential legal liability but can actually enhance a company's overall reputations. Sample communications may be found in the Resource section of this document.

Customer service representative phone scripts should be prepared, staged and recorded in advance. Staffing need to anticipate call volumes and steps to minimize long hold times. The communications plan should have a set of pre-approved web pages and templates staged, phone scripts prepared and frequently asked questions (FAQ's) drafted. Consider the need of multi-lingual support. In the case of phishing exploits, it is suggested organizations have a phishing warning page created in advance to replace the deceptive site as a teachable moment for users.<sup>11</sup>

---

<sup>10</sup> <http://hitechanswers.net/about>

<sup>11</sup> For examples of teachable moments visit APWG [http://www.apwg.org/reports/APWG\\_CMU\\_Landing\\_Pages\\_Project.pdf](http://www.apwg.org/reports/APWG_CMU_Landing_Pages_Project.pdf) or OTA's sample phishing page <https://otalliance.org/resources/samplephishpage.html>

It may be appropriate to have a different message and method of delivery for the company's most important relationships, such as 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. Most organizations realize too late or in the heat of notification that there are subsets of the population that require specific communication. Such special communication needs may be caused by particularities of a geographic region, unique characteristics of the population, etc.

Key questions to be considered:

- What happened?
- How and when did it happen?
- Who was impacted?
- What data was lost?
- What have you done so it does not happen again?
- What are you doing to help ensure I am not a victim of identity theft?
- Why should I trust you?
- Where do I go for more information?

**10. Providing Assistance & Possible Remedies.** A comprehensive plan should evaluate what if any remedy should be offered to affected individuals (or businesses). Such offers can help to offset any inconvenience and damage or the negative perception to an organization's brand which may impact not only your customers but business affiliates and business partners. Several studies have shown that one of the largest costs resulting from a data breach is the loss of future business. Offering a remedy can provide the opportunity to turn a potentially bad situation into a positive brand experience. Typical offers have included credit reporting monitoring, identity theft protection, and web site gift certificates. Customers want companies to take responsibility and protect them from potential consequences of identity theft. While the actual incidence of identity theft from such breaches has been low, the threat to the consumer's trusting your brand is significant. It is recommended the design of such plans include trusted mechanisms, on and off line, for a customer to accept and enroll as their level of trust and skepticism most likely have already been negatively impacted.

### **Training, Testing and Refinement, and Budget**

A Data Loss Plan will ultimately fail to be executed if the employees charged with its administration are not adequately trained. A successful DLP must be practiced, tested, and refined based on past experience. Organizations must have the foresight to allocate staff time and budget for the proper execution of their DLP.

**11. Employee Training.** All company personnel who are part of the response team should be adequately prepared to both investigate and report findings and to communicate with media and regulatory authorities. Legal counsel should review the method and content of any communications to identify potential issues. All employees should be required to review plans annually and upon hire. Employee completion should be documented and reported to management for internal policy compliance. *Plans should include an employee "call-tree" including cell phone and home numbers for critical employees and vendors to be contacted. In the event of a forced breach, forensics specialists should be on call to aid in preservation of evidence, determining the extent of the loss and who will potentially be impacted.*

**12. Develop Processes for Critique & Post Mortem Analysis.** Organizations should carefully analyze past events to improve their plan and minimize the possibility of future recurrences. Conducting “fire drills” is 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. In the event a breach, having plans to triage, react, and recover are crucial. Any breach recovery effort should also include a post mortem analysis stage where you gather your 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.

**13. Funding & Budgeting.** Responding to a cyber security or data breach incident is often an unbudgeted expense, including both hard and less tangible costs including loss of business, increased insurance, and higher merchant card processing fees. In the heat of a crisis is not the optimum to make financial decisions or vendor selections. Consider pre-contracting services to 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 such costs, 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 coverage to ensure it is keeping pace with regulatory requirements and your business and data collections practices.

#### **Resources**

Visit the OTA site for additional resources <https://www.otalliance.org/resources/Incident.html>

[Anti-Phishing Working Group / Carnegie Mellon University Phishing Warning Page](#)

#### **Federal Trade Commission**

[Dealing with a Data Breach](#)

[Business Data Breach Publications](#)

[Information Compromise and the Risk of Identity Theft: Guidance for Your Business](#)

[Identity Theft Resource Center](#) - Data Breaches

[Identity Theft Assistance Center](#)

[Internet Security Alliance - Financial Risk of Cyber Risk](#)

#### **Online Trust Alliance**

[Data Breach Resources](#)

[Proposed Draft Privacy & Data Collection Statement](#)

[Phishing Warning Page](#)

[DataLossdb](#) - Open Security Foundation

[Ponemon Institute](#)

[Chronology of Data Breaches](#) - Privacy Clearing House

[Washington State Attorney General Office - Identity Theft & Privacy](#)

## Updates

A regulatory requirements, best practices and resources evolve, this document will be updated. If you have comments or suggestions, please email OTA at [staff@otalliance.org](mailto:staff@otalliance.org). Updates will be posted at <https://www.otalliance.org/resources/Incident.html>.

## Acknowledgements

The following organizations have participated in the development of this document; the Anti-Phishing Working Group (APWG), Direct Marketing Association (DMA), Direct Marketing Association of Singapore (DMAS), Internet Security Alliance (ISA), Merchant Risk Council (MRC), US Chamber of Commerce and members of the Seattle Chapter of InfraGard. Special thanks to OTA advisors Mike Jones and Ellen Siegel for their input.

## About The Online Trust Alliance (OTA) <https://www.otalliance.org/>

The mission of OTA is to create an online trust community, promoting business practices and technologies which enhance consumer trust and the vitality of interactive marketing, ecommerce and online financial and government services.

OTA is a global non-profit organization addressing online trust and abuse, helping to protect consumers and businesses. OTA promotes self-regulation and best practices by working with the online trust community, a coalition of leading stakeholders. Members include leading interactive marketers, advertisers, technology and solution providers, government representatives, privacy advocates, academics and merchant card processors. OTA supports balanced recommendations in the best interest of the consumer, while being practical and cost effective for businesses.

Through its member companies and organization affiliates, OTA represents over one million businesses and 500 million users worldwide with regional chapters in Asia Pacific, Canada and Europe. OTA is a United States IRS-approved non-profit, governed by a Board and Steering Committee including Bank of America, Adperio, BoxSentry, Cisco Systems, Datran Media, Epsilon, Iconix, Internet Identity, Intersections, LashBack, MarkMonitor, Message Systems, Microsoft Corporation, McAfee, Publishers Clearing House, Return Path, Secunia, Symantec Corporation, TRUSTe and VeriSign Inc.

---

This paper is for informational purposes only. The Online Trust Alliance (OTA) makes no assertions or endorsements regarding the security or business practices of companies who may choose to adopt such recommendations outlined or the OTA Online Trust Principles. OTA MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT. For updates visit <https://otalliance.org/resources/>. Any reproduction or distribution of this document for commercial purposes requires the permission and expressed written consent of OTA.