2014
DATA PROTECTION & BREACH
READINESS GUIDE

The Online Trust Alliance's mission is to enhance online trust and empower users while promoting innovation and the vitality of the Internet.

OTA
Online Trust Alliance

Updated April 7, 2014

© 2014 Online Trust Alliance (OTA)
All Rights Reserved

TABLE OF CONTENTS

© 2014 Online Trust Alliance (OTA) All Rights Reserved

INTRODUCTION

As society and business become increasingly reliant on data, the threat landscape continues to exponentially expand. Online services introduce stronger and more innovative defenses against cybersecurity threats with each passing year. Unfortunately, cybercriminals simultaneously create new techniques and deceptive tactics that outpace such efforts. The result underscores the need for businesses to make security and data protection a priority, and to be prepared for a breach incident.

The **2014 Data Protection & Breach Readiness Guide** (Guide) has been developed to help organizations of all sizes in both the public and private sector. Content has been included to help aid a broad range of stakeholders ranging from business and technical decision makers and privacy and security professionals to web and app developers. The goal is to help readers better understand the issues and solutions which can enhance their data protection practices and enable them to develop readiness plans in the event they incur a data loss incident.

This Guide reflects input from a broad group of stakeholders, industry and breach analysis experts as well as interviews with companies who have experienced data loss incidents. New to the 2014 report is an expanded discussion on a breach's impact to a business, including contractual obligations to customers, how crimes of opportunity target unsuspecting organizations and the resulting "business shock." In addition, the report outlines current best practices in data security and brand protection.

Even the most cyber-savvy organizations have found themselves exposed and ill prepared to manage the effects of a data breach. The best defense is implementing a broad set of operational and technical best practices that helps protect your company and your customers' personal data. The second step is to be prepared with a data lifecycle plan that allows a company to respond with immediacy. Ultimately, industry needs to understand that effectively handling a breach is a shared responsibility of every functional group within the organization. A key to success is moving from a compliance perspective to one of stewardship. This perspective recognizes the long term impact to a brand, the importance of consumer trust and implications and considerations with vendors and business partners.

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 includes links to resources that provide added detail in several areas such as data classification, data destruction and computer forensics.

Report updates and resources are posted at https://otalliance.org/breach.html. To submit comments please email editor@otalliance.org.

© 2014 Online Trust Alliance (OTA) All Rights Reserved

EXECUTIVE SUMMARY

Breaches and data loss incidents have become a fact of life for organizations of every size and throughout the public and private sectors. There is no perfect defense from a determined cybercriminal, but the best practices advocated by OTA and outlined in this paper, can reduce a company's attack surface and vulnerabilities.

Since OTA's first report in 2009, we have learned that no organization is immune from the loss of confidential and sensitive data. As larger quantities of diversified data are amassed on a range of devices and third party service providers are increasingly relied upon, every business must be prepared for the inevitable loss. 2013 culminated with Target's breach, which is estimated to impact upwards of 110 million credit and debit card accounts. This incident was a "perfect storm", highlighting how breaches can occur at the worst time, catching a business off guard, paralyzing management and creating consumer remorse.[1] Victims include not only the consumer, but also the business breached and the banks whose credit and debit cards have been compromised.

It is yet to be determined if Target adequately protected their systems. The long-term impact to their profitability and customer loyalty will not be known for some time while Target faces a range of lawsuits from banks, consumers and shareholders.[2]

Whether the result of an online attack, in-store breach, internal theft, malware, or accidental loss of data incident, such incidents can have significant financial impact and can have devastating consequences on the value of a company's brand.

While businesses may be aware of this threat, they are not necessarily equipped to respond effectively. Businesses must acknowledge the company-wide panic and disruption that can occur. Viewing breaches as a "technical issue" is a recipe for failure. Instead, they need to recognize that every department within an organization needs to play a part in readiness planning. Those that prepare in advance will not only be postured to survive the data breach, but also retain their reputation with their customers.

2013 INTERNATIONAL INCIDENT HIGHLIGHTS*

OTA

89% COULD HAVE BEEN PREVENTED

OPEN SECURITY FOUNDATION

31% DUE TO INSIDE THREATS

21% PHYSICAL LOSS / THEFT

40% OF THE LARGEST BREACHES RECORDED OCCURRED IN 2013

2013 VERIZON DBIR

76% WEAK OR STOLEN CREDENTIALS

29% VIA SOCIAL ENGINEERING

Companies need to not only be prepared for a breach, but equally as important have a plan to appropriately respond to third party notification of a potential vulnerability. As observed with Snapchat in early 2014, the lack of a process appropriately respond has damaged their reputation and opened them up for potential lawsuits and regulatory scrutiny.

The alarming growth in data incidents highlights the challenges business leaders are facing. Based on analysis of data provided by the Open Security Foundation and RiskBased Security, it is estimated over 823 million records were exposed in 2013, including credit card numbers, email addresses, log in credentials, social security numbers and other related personal information.[3] Year-end data for 2013 identified 2,164 incidents. OTA's analysis of these breaches revealed 31% were due to lack of internal controls resulting in employees accidental or malicious events and 37% the result of actual hacks. The balance of incidents were primarily attributed to lost or stolen devices (12%) and fraud (11%). Lost, stolen, or misplaced documents accounted for 9% of all incidents.[4]

[1] http://www.chicagotribune.com/news/sns-rt-us-target-breach-20131218,0,3434295.story
[2] http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=d88fff5b-210d-4ade-aa0f-6b5233578102
[3] https://www.privacyrights.org/data-breach and http://datalossdb.org/statistics
[4] http://datalossdb.org/statistics

© 2014 Online Trust Alliance (OTA) All Rights Reserved

Based on the 2013 Verizon Data Breach Investigations Report, 76% of network intrusions were due to exploited weak or stolen credentials and 29% used social engineering, increasing 4-fold in one year. These incidents are often a crime of opportunity, which cannot be prevented by technology alone. Inappropriate actions, such as bringing work materials home via personal e-mail accounts or on USB drives, and "low tech-events," such as sending sensitive documents to the wrong recipients, can have the same effect as breach incidents caused by outside parties.[5]

These trends suggest a need for increased commitment and adoption of voluntary best practices. These include broader transparency and more detailed reporting requirements. As the result of the increased sophistication and tenacity of international crime syndicates, combined with the proliferation of data stored on mobile devices, OTA expects the number and severity of breaches and resulting identity thefts will continue to grow.

OTA advocates that every organization handling customer data, ranging from email addresses to personally identifiable information (PII), create a data management strategy and incident response plan that evaluates data from acquisition through use, storage and destruction. A key to successful data lifecycle management is balancing regulatory requirements with business needs and consumer expectations. Success is moving from a perspective of compliance, the minimum of requirements, to one of stewardship where companies meet the expectations of consumers.

Business leaders need to recognize if they collect sensitive data, they will realize a data loss incident. NOT being prepared is a recipe for failure, and loss of consumer trust.

DATA LIFECYCLE MANAGEMENT & STEWARDSHIP

A well-designed, actionable data stewardship plan is an essential factor in compliance, demonstrating that a firm or organization is willing to take reasonable steps to protect data from abuse. Furthermore, developing a plan can help to minimize risk to consumers, business partners and stockholders, while increasing the value of brand protection and the long-term viability of a business.

Be it a PC, mobile device, corporate network or data center, companies must strive to protect their data no matter where it resides. Business leaders must continually review their notification, collection and use practices when new products, services and marketing partnerships are developed and expanded. The definition of "privacy" and the composition of PII continue to evolve. Applying yesterday's rules may no longer be applicable in today's data driven economy.

FUNDAMENTALS OF A DATA LIFECYCLE STRATEGY

1. Privacy and Terms of Use policies need to be continually reviewed and updated.
2. The data a business collects include some form of Personally Identifiable Information (PII) or "covered information."
3. The realization that if a business collects data, it will inevitably experience a data loss incident.
4. Data stewardship is everyone's responsibility.

[5] 2013 Data Breach Investigations Report http://www.verizonenterprise.com/DBIR/2013/

© 2014 Online Trust Alliance (OTA) All Rights Reserved

While consumers are realizing significant benefits, complex data analytics and data appending applications have created a set of complex policy and regulatory concerns regarding the use, control and sharing of data.

This Guide identifies key questions and recommendations for businesses to consider when creating a baseline data protection framework. Depending on your industry, size of your business, and the type of data collected, your requirements may vary.

The designation and appointment of chief data protection officers and creation of virtual teams of privacy professionals, security specialists and operational managers are becoming commonplace in U.S and regulated in other geographies.

Figure 1: Data Stewardship

All organizations in both the public and private sector are faced with key considerations when it comes to their data collection practices. As illustrated in Figure 2, data may be collected, used, transmitted and shared in multiple dimensions. Information is gathered from multiple devices and platforms, both online and offline, including retail point of sale, in-store mailing lists to event registrations and ecommerce shopping carts. A major challenge is the evolving definition of "covered" or "sensitive" information. Organizations need to continually inventory the data attributed they have collected and compare against the evolving definition of covered information. User rights access and the blurring of the workplace, further exacerbates the risk of unintended exposure and unauthorized access. Whether it be rogue employees or sophisticated cyber criminals, it is imperative that companies take steps to protect their data from abuse and protect their infrastructure from compromise.

As a best practice, companies need to adopt leading security and privacy practices, including implementing a BYOD and device management policies. In addition all organizations should designate a data protection officer who understands today's complex security and privacy regulatory framework and technological landscape.

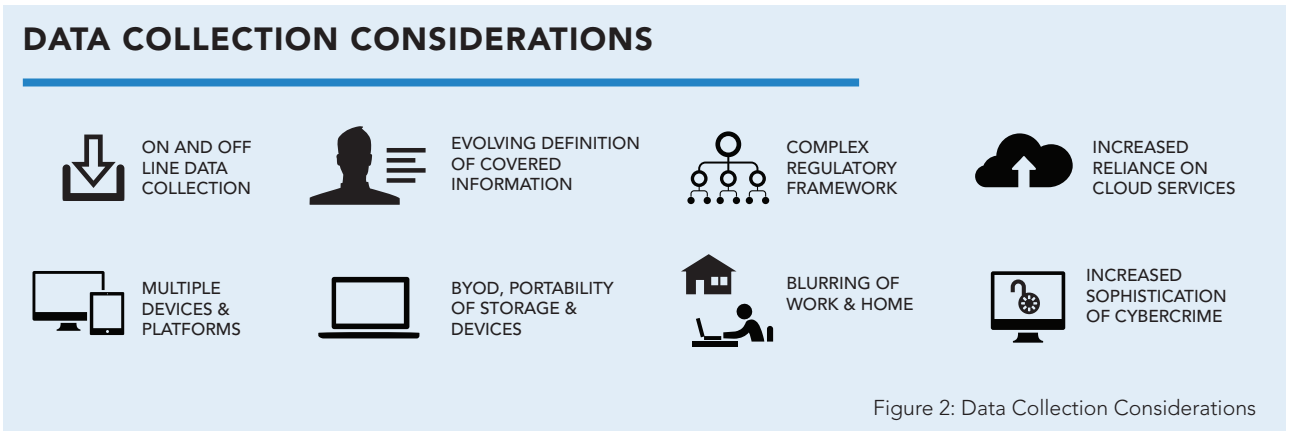

Figure 2: Data Collection Considerations

© 2014 Online Trust Alliance (OTA) All Rights Reserved

BUSINESS IMPACT

A breach can impact every facet of a business. The **"business shock"** can paralyze operations, damage relationships with vendors and partners and tarnish consumer trust. Costs and financial losses associated with such an incident can be significant and take years to recover from.

Small and large companies alike run the risk of a data breach, and the implications of a breach to the organization can be grave. The business shock can be compounded by lack of accurate reporting of an incident, compromising an organization's integrity and trust. Combined, the lack of planning and adequate security and privacy practices can harm a company's brand, increase liability exposure, and engender a negative impact to a business' bottom line.

Often overlooked is the impact a breach has on business relationships and contracts with third parties. For instance, an incident can bring negotiations to a grinding halt and derail a merger. Companies need to understand the contractual obligations of their customers, partners and service providers which may include penalties, right to audits and related downstream effects. An internal review and inventory of all contracts is highly recommended, calling out notification requirements. Such third party clauses may include audit provisions and other remedies to be paid by the businesses experiencing the loss. This information needs to be incorporated into the communication plan outlined in **Incident Response Planning: Communicate & Draft Appropriate Responses, page 19**.

An incident plan that incorporates both disaster planning and training sessions for potential breaches helps reduce operational risks, improves information security practices and reduces the risk to a corporation's reputation. Just like first responders to a fire or accident, data managers and cyber responders must be trained, equipped and empowered to deal with the data loss incident. Conversely, service providers are increasingly being held accountable and named in legal actions. 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 (DIP) FRAMEWORK

An effective Data Incident Plan (DIP) is a playbook that describes breach fundamentals that can be deployed on a moment's notice.

A key requirement for the DIP is having understanding how data is collected, retained and destroyed. Organizations must be able to quickly determine the nature and scope of an incident, take immediate steps to contain it, ensure that forensics evidence is not accidentally ruined and subsequently notify regulators, law enforcement officials and the impacted users of the loss. The scope of an organization's plan should include impact assessment regarding the loss of intellectual property, brand reputation, regulatory compliance, and business continuity.

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.

SCOPE

- CONSUMER & PARTNER DATA
- INTELLECTUAL PROPERTY
- BRAND REPUTATION
- REGULATORY COMPLIANCE
- STOCKHOLDER IMPACT
- BUSINESS CONTINUITY

© 2014 Online Trust Alliance (OTA) All Rights Reserved

THE 10 QUESTIONS OF RISK ASSESSMENT:

The following questions are provided to help complete a self-audit.[6]

1. Do you understand the international and local regulatory requirements related specifically to your business based on where the customer or consumer resides?[7]
2. Do you know the specific data attributes you maintain for all customers? How and where are these data stored, maintained, and archived (include your vendors and third-party/cloud service providers)?
3. Is the original business purpose for collecting this data still valid and relevant? Can you Identify points of vulnerability and risk?[8]
4. Are your encryption and de-identification processes representative of best practices?
5. Do you have a 24/7 incident response team in in place? Do employees have reporting process?
6. Are you prepared to communicate to employees, customers, stockholders, and the media during an incident?
7. Do you follow generally accepted security and privacy best practices? If not, are you prepared to explain why?
8. Does your privacy policy reflect your data collection and sharing practices, including use of third-parties? Have you audited your site to confirm you are in compliance?
9. Do you know who to contact in the event of a breach? Are you prepared work with your law enforcement authorities such as the FBI, Secret Service and State Attorney General Office? Or will you have to resort to making these contacts in the "heat of the battle" on an ad hoc basis?
10. Are you willing to sign off on your DIP and be accountable that you have adopted best practices to help prevent a breach?

SECURITY & PRIVACY ENHANCING BEST PRACTICES

It is no longer "optional" to have adequate controls in place and implement data and infrastructure best practices. To maximize consumer trust, businesses need to focus efforts in the three-pillars on consumer protection; 1) Brand Protection, 2) Security and 3) Privacy. The companies looking at these issues holistically are best equipped in protecting their brand from a significant incident.

On the other hand, the lack of sound privacy practices and brand protection controls negatively impacts consumer trust and increases legal risk. To help provide prescriptive advice and benchmark reporting, OTA annually publishes an Online Trust Audit and Honor Roll which evaluates the adoption of such practices by leading brands.[9] (See figure 3) OTA's analysis of nearly 500 breaches in the first

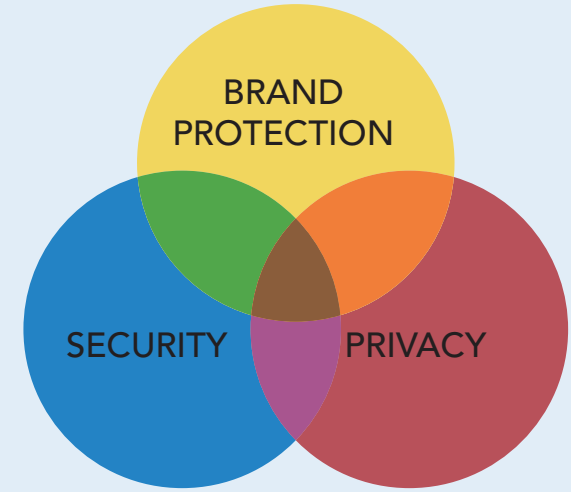

Figure 3: Keys to Consumer Trust

[6] Note these questions are not intended to address specific requirements such as those required for Payment Card Industry (PCI) or the Health Insurance Portability and Accountability Act (HIPAA). See Appendix A, page 26 for additional resources.
[7] Including a review of Canadian and European Union (EU) regulations.
[8] Data minimization should be a central operating principle. If data is not collected, and/or is destroyed when it is no longer needed, the potential for data breaches is significantly reduced.
[9] https://otalliance.org/HonorRoll.html

© 2014 Online Trust Alliance (OTA) All Rights Reserved

half of 2013, revealed that 89% could have been avoided had simple controls and security best practices been implemented. These results are consistent with past research published by Verizon showing that such practices would have helped prevent up to 97 percent of data breaches in 2011.[10] As the dependency on outsourcing has increased, businesses are acquiring and storing increasing amounts of data, relying on the service provider to keep their data secure.

While no direct fault of their own, businesses can face significant financial and reputation harm as a result of a service provider's data loss incident. Both the business and service provider must contend with a matrix of obligations governing the disclosure of personal information under federal and state laws and regulations, privacy principles and industry guidelines and standards.[11]

Therefore, a business must put in place appropriate contractual protections with each of its service providers having access to the personal information to: (1) specify the service provider's standard of care and its obligations with respect to the treatment of personal information and (2) minimize the risks and liabilities associated with a service provider's security breach or the unauthorized use of personal information. Such contractual provisions should stipulate notification requirements, material notice changes, and a provision for audits and be annual revaluations.[12] Internal privacy and security teams should periodically review contractual terms and conditions and consider including applicable best practices as part of a vendor onboarding process.

SECURITY BEST PRACTICES

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 internet domains and creation of bogus web sites are on the rise. Such exploits may result in the installation of malware and keystroke loggers via trojans and deceptive downloads.

With the rise of social engineered based exploits, data sniffing of unencrypted data and drive-by downloads via malvertising, application white-listing and related controls as outlined should be implemented on all systems.

1. **Email authentication** checks inbound email to help detect malicious and deceptive email including spear phishing and forged email targeting unsuspecting users, with the primary goals to comprise their PC or device with malware. All businesses should implement SPF, DKIM and DMARC to maximize the protection for these threats to customers and internally to employees, allowing ISPs and internal networks the ability to detect and block such fraudulent email.[13] Email authentication implemented on outbound email will help improve your organizations' ability to protect its brand. These standards are proven to aid organizations in managing inbound email for threats, it also helps ISPs and other organizations accepting your email to do the same. Authenticating your outbound email ensures that your email is less likely to be identified as spam, that your legitimate email is delivered to recipients' inboxes, and email forged in your organization's name will be filtered or blocked.
2. Implement Secure Socket Layer (SSL) for all data collection. Include "**Always on SSL (AOSSL)**" for all web services to help prevent eavesdropping on data being transmitted between client devices, wireless access points and intermediaries.[14]

[10] http://www.verizonenterprise.com/DBIR/2012/
[11] Some of these laws, including California and Massachusetts law, require that non-affiliated service providers contractually agree to take reasonable or appropriate measures to protect shared personal information.
[12] For a general template to assist in preparing data security clauses used in a services agreement see: http://www.kelleydrye.com/publications/articles/1502/_res/id=Files/index=0/Rosenfeld_Hutnik_Data%20Security%20Contract%20Clauses%20for%20Service%20Provider%20Arrangements%20(Pro-customer).pdf
[13] https://otalliance.org/eauth.html
[14] In light of the recent breaches include wireless snooping and government agencies leading search providers, social networking sites and web email providers have migrated to Always On SSL, (AOSSL). https://otalliance.org/AOSSL.html

© 2014 Online Trust Alliance (OTA) All Rights Reserved

3. Upgrade to **Extended Validation SSL (EVSSL)** certificates for all commerce and banking applications. EVSSL provide users a higher level of assurance the site owner is who they purport to be by the display of a green address bar and other trust indicators.[15]

4. Review all **password management policies** including enabling support of two-factor authentication. Rotate passwords on all business clients and servers every 90 days. Passwords should use a long passphrase, including a combination of upper and lowercase alphabetic characters, symbols, and numbers and should not permit the use of any dictionary words.

5. **Data & disk encryption**. All sensitive data including email lists should be encrypted, including hashed passwords. (**Appendix 7**)

6. **Encrypt communication with wireless devices** such as routers, including point of sale terminals and credit card devices. Keep all "guest" network access on separate servers and access devices with strong encryption such as WPA2 or use of an IPSec VPN.

7. **Client devices need to be hardened**, including default disabling of shared folders, multilayered firewall protection, including both PC-based personal firewall and WAN-based hardware firewalls. In addition, automatic patch management for operating systems, mobile apps, web applications and add-ons should be enabled. All ports should be off to incoming traffic by default.

8. **Create a BYOD Plan & Policy.** The lack of a coherent approach to BYOD introduces a complex set of technical and operational policies, can put an organization at risk. User devices are a threat to pass malware and viruses on to company platforms, compromising valuable company information. Businesses need to formally develop and implement a mobile device management program. This includes conducting an inventory of all employee personal devices used in the workplace, installing of mandatory remote device wiping tools and procedures for to delete company data on lost devices.[16]

DATA GOVERNANCE AND LOSS PREVENTION

If your organization does not currently have a formal readiness plan, it is highly recommended a plan be developed. The following sections are designed to help organizations better understand the data they are responsible for protecting. By limiting access and retaining only what data is necessary can help mitigate the risk and impact of data loss incidents.

DATA CLASSIFICATION

A simplistic but often overlooked approach is:

- **What is important?** (What data do you care about protecting and why?)
- **Where is the data stored?** (data inventory / mapping)
- **How is it controlled?** (controls and access analysis)
- **How do you know that those controls are working?** (monitoring / auditing)
- **What Is important?**

CLASSIFICATION
TYPES
SENSITIVITY
OWNER
STATUS

The first step is determining the type of data your organization is classifying. It should be classified according to the level of criticality and sensitivity. There are a variety of data classification schemes. The scheme should include details about data ownership, what security controls are in place to protect it and any data retention and

[15] https://otalliance.org/resources/EV/index.html
[16] For a review of best practices on BYOD, see: http://www.citrix.com/content/dam/citrix/en_us/documents/oth/byod-best-practices.pdf

© 2014 Online Trust Alliance (OTA) All Rights Reserved

destruction requirements.[17] What scheme your organization chooses is less important than is the actual exercise of making sure the organization understands what data is collected and what the potential impact of losing that data might be.

Where is the data?

Once the data has been classified, the organization must then define whether or not the data is in use (accessed as a normal part of business), in motion (network traffic of the data both internally and externally), or at rest (in a database store and or archived on servers and client devices).

Data in motion has a particularly high risk of being lost, as that data could be on PCs, tablets, or mobile devices. Personal or covered information (including but not limited to PII) that is in motion should be encrypted (see **Appendix F, page 37** for encryption options). However, data that is at rest or in use - even if not stored on mobile devices - is at risk of being compromised. Steps to encrypt should be considered. Data that only resides on company servers or transmitted to service providers may be breached, especially if the service provider does not have adequate controls. Such breaches involving third parties are costly due to the added complexity of their infrastructure and legal issues, which can be triggered during an audit. Last year's hacking of Target underscores the need for auditing and validating data access of every step of the data's lifecycle: from collection, through device transmittals and server storage.[18]

What is PII?

As the definition of Personally Identifiable Information (PII) and covered information is rapidly evolving, businesses need to take a broader view of the sensitivity 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. Increasingly states and international bodies have expanded the definition to apply to virtually all data collected including usernames, passwords, email addresses, names, street addresses, etc.[19] Irrespective of the source of data collection (online or offline), all collected data is at risk and should be incorporated in a business' data loss plan.

VALIDATE & AUDIT EMPLOYEE DATA ACCESS

A DIP should address employee access, including read, write and retrieval access to all data classified as critical or sensitive. **This should include**:

- Validating appropriate employee use and data access (including revoking of employees credentials);
- Scanning of outbound email for protected content (Data Loss Prevention);
- Digital Rights Management (DRM), to control and limit access of proprietary or copyrighted data (if applicable);
- Auditing or confirming that cloud storage complies with the company's data governance requirements (including employee use of third party data shares and storage sites). Include services such as Google Docs, Microsoft OneDrive, Dropbox and others;
- Managing devices, including encrypting, limiting, tracking or remote wiping of external storage devices;
- Establishing provisions to automatically revoke all employee or vendor credentials upon termination or resignation;
- Scanning of removable media and backup systems.

Companies should deploy policies that demarcate appropriate use and access controls. These policies should include a device management plan that audits, inventories and addresses all removable drives, media, USB keys, mobile devices and outlines their respective encryption requirements. See **Appendix F, page 37** for a description of encryption options. All sensitive data shared with third parties and all wireless connections should be encrypted using industry

[17] Federal Information Processing Standard (FIPS) Publication 199 is a guide to aid in data classification. http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf; In addition, FIPS Publication 200 addresses the specification of minimal security requirements for federal information and information systems: http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf

[18] http://krebsonsecurity.com/2013/12/cards-stolen-in-target-breach-flood-underground-markets/

[19] Infra, note 19.

© 2014 Online Trust Alliance (OTA) All Rights Reserved

best practices and standards. Policies concerning the uploading or sharing of such documents containing sensitive data to the "cloud" or external storage sites should be balanced for business needs and convenience versus risk and exposure.

A critical step in developing policies is to review all internet-enabled applications and third-party content being served on internal and external-facing sites. More and more frequently, website applications, add-ons, plug-ins and third-party scripts are becoming intrusion opportunities and aid in the distribution of malware. Part of an organization's arsenal to combat online threats must include: intrusion testing; application vulnerability scanning and preventative web application scans for iframes, cross-site scripting (XSS) vulnerabilities, clickjacking, malvertising, trojans, key loggers, and sniffers. Companies doing business with governmental bodies should review the appropriate government requirements.

In response to last years WikiLeaks, the Executive Office of the President, Office of Management and Budget (OMB), published a self-assessment program for user data access. This document reinforces the importance of detection, deterrents and defense from unauthorized employee and contractor disclosure.[20]

FORENSICS, INTRUSION ANALYSIS & AUDITING

An essential element of a response plan is performing forensics to help determine the source and magnitude of a breach. A forensics investigation is best left to experts. 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 imperative that your impacted systems and the appropriate logs be in the unmodified state for law enforcement or other forensic experts to do an analysis that will hold up in court. Increasingly, reports from forensics firms are being subpoenaed.

Companies may want to consider retaining outside legal counsel and/or third parties to help conduct such analysis. Having your attorney retain forensics investigators should be considered since their reports may be "attorney client privileged" and deemed confidential and legally not discoverable.

Suggestions on what you should do:

- Secure and protect the physical integrity of the evidence and ensure that any systems impacted are only accessible to internal or hired investigators and law enforcement. Make sure you track the chain of custody of all evidence.
- Isolate suspected servers and client workstations from the network, unplugging network cables or disconnecting the workstations from wireless access points as appropriate.
- Preserve and store all critical log files in a secure location, including web client and server operating systems, application, mail, firewall, IDS, VPN and network flows. Due to rotation schedules, the saving of critical logs need to happen as soon as possible.
- Contact law enforcement and your attorney. It is critical that forensics be performed by experts, and that your organization does not do anything to compromise the data or chain of custody.
- Disk image capture/evidence preservation should strongly be considered before placing machines back online for law enforcement monitoring purposes.
- Review internal remediation plans and policies (discovery as a result of DLP)
- Document everything that has been done on the impacted systems since the incident was detected.
- Document the employees who have access to the impacted systems including the names of all new hires and employees who have been terminated in the past 90 days.

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

© 2014 Online Trust Alliance (OTA) All Rights Reserved

Suggestions on what you should NOT do:

- Do not change the state of the systems in question. If the systems are on, leave them running (but disconnect from your network) and if they are off, unplug them.
- Do not shut down or unplug any server or device.
- Do not try to image the impacted 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 utilities, on the impacted systems without the help of experts. It's very easy to accidentally destroy evidence.
- Do not plug storage devices, removable media, etc. into the impacted systems.

CRITICAL LOGS

Logs are a fundamental component of forensic analysis to determine the scope and impact of the incident. Businesses may have a number of log types- transaction, server access, application server, firewall, and the client operating system. Attackers understand the value of logs, so it is important to protect the logs from attack and routinely back them up. Also, 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 or other types of regulated data. A best practice is to examine all logs in advance, include those generated by internal systems as well as those of your vendors / service providers to assure they are configured correctly to capture data to meet your business and regulatory requirements. A security event manager (SEM) is highly recommended. A SEM is a tool for data networks to centralize the storage and interpretation of logs to help decipher trends and identify abnormalities. Learning after the fact the logs were not capturing the appropriate data or archiving data can negatively impact a business's ability to fully understand the scope of the data loss incident. In addition, all servers and logs should have time zones synchronized, to facilitate data analysis throughout an organization's global infrastructure.

As your organization reviews logs, look for queries that match the data believed to have been compromised. If your organization does not have any evidence to match against, IT staff should be able to provide "normal" application and database activities. This should include anomalies such as unusual queries. 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 or if ZIP, TAR or other typically unused compressed files were created. This could be evidence of a database dump or copy.

CRITICAL LOGS

- FIREWALL
- TRANSACTION
- DATABASE SERVER
- APPLICATION SERVER
- OPERATING SYSTEM
- NETFLOW / VPN

After you determine the type and sensitivity of data that has been compromised, speak with your attorney or Chief Privacy Officer to understand your reporting obligations. Ultimately, 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 as well as identifying all impacted systems. Indeed, your organization will need to isolate and review logs from the compromised systems including network devices, such as routers and access control systems once a breach occurs.

It is important your contracts with third party data providers and vendors provide access to such logs, including stated provisions outlining access as well as to the inclusion logs of other related servers and historical data. Consider including a provision on documenting what logs are collected and how they are maintained. This should preferably be done on separate or centralized logging systems with good audit trails for access. Also specify the minimum retention period these vendors keep the logs as possible. See **Appendix E, Commuter Forensics Basics, page 35** for further information.

© 2014 Online Trust Alliance (OTA) All Rights Reserved

DATA LOSS PREVENTION TECHNOLOGIES (DLP)

Organizations are finding themselves subject to an increasing number of data protection requirements that obligate them to protect employee or, consumer data against hazards from within and outside of their organizations. In addition to protecting regulated data, many organizations are also looking to help protect intellectual property and other sensitive data within the organization that may pose a threat to their enterprise but where protection is not being required by any external driver.

Information security vendors have introduced various technology solutions that allow organizations to address protection of data across the data lifecycle stages – Collection, Storage, Use, Transfer and Disposal. These solutions enable enforcement of data protection policies and provide data discovery, data encryption, event monitoring and quarantine of sensitive data. Due to the multiplicity of solutions and options available for protecting sensitive data, organizations today are faced with a challenge to determine the solution that best addresses their specific data protection needs.

Implementation of DLP can help identify vulnerabilities in advance of potential exposure and aid in the creation and implementation of controls and processes to minimize and remediate the threat. Such solutions can be an early warning of data flowing out of an organization, being stored on mobile devices and unauthorized employee access. While such actions may be benign and identify lapses of adherence of company policies, they can help identify the need for employee training.

DLP solutions work in conjunction with existing security tools and anti-virus tools that companies have deployed both on servers, clients (for example, laptops and tablets) and on their network. Leading DLP solutions address data protection by environments such as:

- **Data at rest** – Data stored within the network perimeter on large data stores such as databases, network file servers and data warehouses.
- **Data in motion** – Data transmitted over the internet through multiple protocols (http, SMTP, FTP, etc.) to locations outside the enterprise domain as well as between divisions and geographies of the same company.
- **Data in use** – Typically defined as data being created, modified, and stored on removable media devices, such as laptops and tablets.

DLP solutions are shipped with hundreds of pre-defined data protection policies. These policies contain rule sets for the identification of common sensitive data elements. In addition, most vendors are willing to create custom policies based on enterprise requirements.[21]

DATA MINIMIZATION

A key rule of thumb when it comes to collecting data: if your organization does not have the data, it cannot lose it. While this statement seems obvious and easy to follow, it is also potentially in conflict with the marketing and business needs of an organization. Marketing and operation teams often 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 your organization with a competitive advantage and discard the rest.

Additionally, a comprehensive annual audit should be conducted to understand what data is being collected, and whether it should be retained, aggregated, or discarded.[22] Business may need to re-validate its business need and decide whether aggregation can be used to minimize the amount of retained PII. Data retention policies should dictate how long information needs to be retained.

[21] Symantec DLP Overview http://www.symantec.com/data-loss-prevention
[22] Data aggregation is any of a number of processes in which information is gathered and expressed in a summary form, for a variety of purposes.

© 2014 Online Trust Alliance (OTA) All Rights Reserved

DATA DESTRUCTION POLICIES

A common target for data breaches and accidental disclosure is archived media, files and computers that are no longer in use and/or discarded Increasingly, privacy laws require businesses to securely destroy data when it reaches end of life. Formatting a hard drive or simply deleting files leaves the data open to be discovered by the cybercriminal.

To this point, a British research study of 300 hard drives purchased from eBay and computer fairs showed that 34% of drives had data identifying a particular individual or organization where the drives had been in use.[23] Any data no longer in use needs to be securely decommissioned either by overwriting using industry-standard data erasure practices, degaussing, encryption, or physical destruction of the storage medium. Whether a business is donating a system, selling or or simply disposing of it, the secure deletion step needs to be performed.[24]

INVENTORY SYSTEM ACCESS & CREDENTIALS

Having an inventory of key systems, access credentials is essential to mitigating threats and the impact on operations. This list should be kept secure yet accessible at all times with hard copies 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:

- Registrars, including DNS access, domain and SSL certificates
- Server hosting providers, including IP addresses
- Cloud service providers including data backup, email service providers and others
- Payroll providers
- Bank accounts and merchant card processor(s)
- Company bank accounts and credit cards

INCIDENT RESPONSE PLANNING

Organizations must be prepared to react on several fronts when confronted via a data loss incident or breach. It is critical to have an orchestrated response plan including relationships with key vendors and law enforcement. A well-documented plan is only as good as the training and readiness of the incident team.

Organizations need to be prepared to notify all appropriate parties, (including regulatory bodies and law enforcement), communicate timely, accurate information and consider offering remedies to those affected.

Data breaches are interdisciplinary events that require coordinated strategies and responses. Every functional group within an organization needs to be represented.[25]

As a first step, organizations should appoint an executive, with defined responsibilities and decision-making authority with regarding data breach response. It is suggested this role be assigned to a corporate officer or high-level employee, as this individual could be required to provide Board briefings and needs to be empowered 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; and the need to avoid redundancy and any ambiguous responsibilities is essential.

[23] http://www.dailymail.co.uk/news/article-1178239/Computer-hard-drive-sold-eBay-details-secret-U-S-missile-defence-system.html
[24] The National Institute of Standards and Technology (NIST) guidelines for media sanitization. http://www.nist.org/nist_plugins/content/content.php?content.52
[25] This includes, but not limited to: Information Technology; functional groups including Risk Management, Human Resources, Operations, Legal, Public Relations, Marketing, Finance, and Customer Service need to be integrated. In addition, Sales, Business Development, Procurement and Investor Relations groups should be included to fully anticipate the ramifications to business continuity.

© 2014 Online Trust Alliance (OTA) All Rights Reserved

Breach Response Team Selection Criteria:

- An executive with broad decision making authority.
- A representative from each internal organization.
- "First responders" available 24/7, in the event of an after-hours emergency.
- Spokesperson trained in media who has a deep understanding of operations and security.
- A team of appropriately trained employees (technical and policy).
- Staff with access and authority to key systems for analysis and back-up.
- A single individual (and a delegate) with the authority and access to management for actions which may require higher level approvals.
- A summary of internal and external contacts with after hour numbers including outside legal counsel, PR agency and law enforcement.

PLAN FUNDAMENTALS

Create & empower a team
24/7 "First Responders"
Develop vendor & 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

ESTABLISH VENDOR AND LAW ENFORCEMENT RELATIONSHIPS

Service providers should be considered for critical functions including public relations, notification activities and forensics services. Utilizing such services for incident response can help ensure an effective response. 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.[26] Other third parties to consider are credit monitoring and identity theft management companies, as well as call centers to accommodate anticipated spikes in call volumes.

Vendor selection considerations:

- Subject matter expertise in the relevant industry
- Bonding, indemnification & insurance
- Experience handling sensitive events and constituents
- Multi-lingual language proficiencies
- Ability to speak to the media, customers and partners on the company's behalf.[27]

Vendor agreements should include standard security risk management language and a risk assessment of access or storage of your data. Audit validation processes and performance benchmarks are essential parts of any agreement. In addition, include terms that address responsibility in the event of a breach. These provisions should include the allocation of costs, such as potential audit costs, as well as responsibility for notification.

[26] For email authentication resources visit https://otalliance.org/eauth.html
[27] Brand and domain management resources may be found at https://otalliance.org/about/Members.htm

© 2014 Online Trust Alliance (OTA) All Rights Reserved

If your organization has existing insurance coverage, check with your carrier to estimate potential risk tolerance and preferred rates for recommended providers.

Prior to a data loss incident, reach out to regulators such as state Attorney Generals, Secret Service and FBI. In addition, there may be a regional task force for high technology crimes in your area. Become active in the local chapter of InfraGard, an information sharing and analysis effort between the FBI and the private sector; this can help build relationships with both law enforcement and data breach experts.[28] Regulators prefer to hear "bad news" from you first – a courtesy phone call can go a long way. When speaking with the authorities, don't inflame the situation by being defensive. Instead, focus on what you are doing to help citizens in their jurisdiction.

CREATE A PROJECT PLAN

A comprehensive project plan includes a timeline and process flow. This 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 thus important to anticipate these various needs and manage the expectations of each group, which is very difficult to do without a realistic and comprehensive timeline. The project plan must have the ability to be "activated" 24/7, including holidays and weekends, as criminals often strike on holidays, weekends and during high volume business times, when staff may be limited. As observed in the case of Target 2013 breach, the sheer volume of holiday transactions help to masked their activity and was a "perfect storm."

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 are the notification requirements (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? Critical information includes the person's name, organization, return contact information, and details on what they know about the incident.
- Are the above answers the same for all of your customer segments?

DETERMINE NOTIFICATION REQUIREMENTS

Business decision makers must be familiar with the regulations that govern their industry. This includes not only digital data, but also the controls over respective paper documents and redress procedures. The failure to notify the appropriate government agency can result in further inquiries and substantial fines. It is equally important to review your contracts with customers and partners; they may have notification requirements that exceed regulations and may vary based on customer size and jurisdictions.

As of January 2014, there are forty-eight states, plus the District of Columbia, Puerto Rico, and the Virgin Islands with laws that govern data disclosures. Compounding the mosaic of laws is the fact that businesses may not know where a consumer resides and the respective notification

[28] InfraGard chapters: https://www.infragard.org/FbTty4cyYBFFAj3Spx5ms%25252BxhvOgLbrLQDorlo3ju04Y%25253D!

© 2014 Online Trust Alliance (OTA) All Rights Reserved

requirements.[29] Note that some state laws conflict with one another, so become intimately familiar with all requirements. If your organization has customer data, it likely includes information from customers in other countries or U.S. states than your own. A best practice is to periodically request customers to update their user profiles. This aids marketing as well as compliance efforts.

Breaches are not "invitation only" events - any regulator can play. Whether or not a regulator has official jurisdiction, businesses need to consider neighboring state requirements as well as jurisdictions with a high number of customers. Since many state, federal and foreign regulations require prompt notification, it is important to determine in advance how to contact impacted individuals. A best practice is to take the most stringent state requirement as the "highest common denominator" and build compliance to meet that standard. For example, California and Massachusetts are viewed as having the most stringent breach notification requirements.[30]

Knowing these requirements in advance will significantly improve your organization's ability to mitigate consumer angst and increase compliance, while reducing regulatory inquiries, fines and potential lawsuits. 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 expect timely and clear notification delivered in a manner appropriate to their needs, and depending on the data that was breached, may have an expectation to be provided remediation and credit monitoring services free of charge.

Due to the changing landscape of breach notification laws, requirements amongst different jurisdictions vary and sometimes conflict, creating a significant compliance challenge for companies suffering a data security breach. Businesses should review the breach notification laws for each relevant State where individuals whose personal information is held by the business reside. One strategy, however, is to draft a single template letter that meets the requirements of most of these states; then add one or more additional template letters to address relevant states that have conflicting or more restrictive requirements. **Tips on writing a good breach notification letter include**:

- Take responsibility and apologize. If you just lost your friends wallet and their personal information, wouldn't you say you were sorry in some form or fashion?
- Be clear and unassuming. Most people today understand identity theft, but data breach is still a foreign word. Explain what happened, be transparent and honest. Otherwise, it is going to come back and cause problems. And just like anything in life, you will have to remember who you said what to, and what really happened.
- Write at a sixth grade level, for everyone to understand. Consider language options or offer bilingual support.
- Explain their options without scaring them. Provide them a phone number and resource if they are concerned and want assistance.
- Remember that you are a company and they are a single person, a person simply trying to protect themselves in this big scary world.
- Explain steps your company is taking to help make sure this type of incident doesn't happen again.
- Lastly, apologize again and mean it.

The Guide provides a sample breach notification letter in **Appendix B, page 29** as a general template to assist in preparing data breach notice letters for affected individuals in connection with state data breach notification requirements. Regularly check that the contact information provided in the sample letter for federal and state agencies as well as the national consumer reporting is up to date. Remember, it must be tailored to reflect your company's particular circumstances and to address the specific legal requirements.

[29] See, Intersections Consumer Notification Guide (November 2013) http://www.intersections.com/library/IntersectionsBreachConsumerNotificationGuideFinal_Nov2013.pdf

[30] http://oag.ca.gov/ecrime/databreach/reporting. Effective January 1, 2014, California amended its law so that the definition of "Personal Information" now includes "a user name or email address, in combination with a password or security question and answer http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798.80-1798.84

© 2014 Online Trust Alliance (OTA) All Rights Reserved

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. Have on hand the relevant laws, data breach reporting requirements, and contact info for relevant data protection authorities for all jurisdictions your organizations conducts business.[31] The regulatory landscape is rapidly expanding with the proposed State and national legislation for national breach notification legislation, mobile privacy and geo-location related services.[32] See **Appendix C, page 32** for regulations that may affect your business in the event of a breach.

Organizations found to be in violation of laws could face significant fines and penalties. It can be 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 or service provider who is well-versed in the various data breach reporting laws.[33] *Readers are encouraged to work with a qualified attorney or firm who specializes in regulatory obligations. In addition, a firm's insurance policy should be reviewed for coverage. See* ***Appendix C, page 32*** *for insurance policy considerations.*

COMMUNICATE & DRAFT APPROPRIATE RESPONSES

Effective communication 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. Depending on your industry and businesses the messaging and order of communications may vary. A well-executed communications plan not only minimizes harm and potential legal liability, but it can also enhance a company's overall reputation.

The communication plan needs to address six critical audiences:

1. Internal teams (including Board and major investors),
2. Key partners and customers,
3. Regulators and reporting agencies,
4. Law enforcement,
5. Impacted parties, and
6. Press, media and analysts.

Figure 4: Audiences & Messages

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

[31] For a great resource summarizing the reporting requirements for 43 countries, see: http://www.theworldlawgroup.com/files/file/WLG%20Global%20Data%20Breach-Nov%2027.pdf See, also supra note 27
[32] See, Data Security and Breach Notification Act of 2013 (S. 1193). https://www.govtrack.us/congress/bills/113/s1193/text
[33] Different types of data events may require different responses. 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.

© 2014 Online Trust Alliance (OTA) All Rights Reserved

Spokesperson(s) must be prepared to respond to media inquiries. The plan should anticipate the need to provide access to service and information that helps impacted individuals; this includes emails, written correspondences and website postings.[34] Companies should monitor the use of social networking sites such as Facebook, Twitter and blogs to track consumer sentiment.

Most organizations realize too late or in the heat of the incident that there are subsets of the customers and partners requiring customized communications. Consider separate messages and methods of delivery for the company's most important relationships, such as its highest-value customers or senior employees. This may also include categories of individuals that are particularly sensitive such as the elderly, the disabled, minors, and other "at-risk" segments.

Review all applicable laws before determining how to notify. Companies should consider their customer demographics as well as multi-lingual responses and communications. Tailor communications by geographic region and the unique characteristics of the population, including ethnicity and age of the audience may be appropriate.

Key facts 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 taking to assist affected persons or organizations?
- What steps are being put in place to help assure it will not happen again?
- What is being done to minimize the impact of identity theft for your customers?
- Where can your customers go for information? (contact info and toll free number)?
- How will 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)?

PROVIDING ASSISTANCE & POSSIBLE REMEDIES

Typical offers include credit report monitoring, identity theft protection, and website gift certificates. Some companies have limited their remediation measures to incidents involving loss of credit card and social security numbers; however, these offers are increasingly being provided for a broader range of data loss scenarios. Customers want companies to take responsibility and protect them from potential consequences such as identity theft. The design of such plans should include mechanisms, both on and off line, for a customer to easily accept and enroll into any offered services.

It's a daunting fact that 25% of those affected by breach become victims of identity theft.[35] A DIP should evaluate what, if any, remedy should be offered to affected individuals (or businesses). To ascertain pricing and service concessions, negotiate in advance services to offer affected customers. Remedies can help offset user inconvenience and thus mitigate damage to an organization's brand. The incident may impact not only your customers, but also business affiliates and partners. Remedies can provide the opportunity to turn a potentially bad situation into a positive brand experience.

[34] For instance, with the possibility of a phishing exploit as a cause or contributor to an 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. For more 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

[35] http://www.businesswire.com/news/home/20131029005261/en/Study-Connects-Data-Breaches-Alarmingly-High-Rates ("By breaching the data stores of businesses in the financial, healthcare and retail industries, criminals can obtain the fuel they need to execute various fraud schemes, and these crimes have crippling consequences," Javelin Strategy & Research. "Identifying and protecting the sensitive information typically stored by these industries is essential for mitigating the risk of a data breach and, therefore, the risk of financial loss to data custodians, consumers and third-party businesses.").

© 2014 Online Trust Alliance (OTA) All Rights Reserved

TRAINING, TESTING AND BUDGET

A DIP will fail to be executed if employees charged with its administration are not adequately trained. Organizations must allocate staff time and budget to properly execute 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 review) to address changes in the company or in the threat landscape. A best practice includes running quarterly desk-top drills to help identify potential areas of risk, while training new employees within your organization as well as your PR and communication vendors.

EMPLOYEE AWARENESS & READINESS TRAINING

Providing baseline privacy training is an important step in preparing employees for a breach. Employee training should include (but not be limited to) data collection mechanisms, retention policies, handling and sharing policies as well as data loss reporting procedures.

Data Loss Prevention services and software can help identify processes and topic areas to include in employee and vendor training. Company personnel who are part of the response team should be prepared to both investigate, report findings, communicate with media and regulatory authorities. All employees and resources involved in incident response should be prepared in advance as part of the planning process so they are not coming in cold in the event of an incident. Employees should be required to review plans upon hire and annually thereafter. 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, the training session should discuss the importance of unique strong passwords and safe computing recommendations.[36]

ANALYZE THE LEGAL IMPLICATIONS

Prepare for the possibility of litigation and have an established data-security response plan with documentation of employee training to help mitigate damages. Preservation of all relevant information, communications and actions taken both before and after the incident combined with 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.

Increasingly, the Federal Trade Commission (FTC) has exercised its authority regarding data protection and security. The Commission has settled nearly four dozen cases alleging that a failure to have "reasonable" data security constitutes an unfair or deceptive trade practice.[37]

The FTC mainly relies on its Section 5 "deception" authority, punishing companies that violate their privacy promises.[38] Recently, the FTC has begun to utilize its Section 5 "unfairness" authority to combat instances of inadequate data protection. For instance, Wyndham Hotels experienced significant security oversights including three data breaches in less than two years, resulting in $10.6 million in fraud losses. Not only is the company's brand reputation under attack, but they are also facing a complex set of legal challenges.

As data breaches continue apace, so do enforcement action and litigation. For example, retail TJX Companies Inc. disclosed that its systems were hacked in 2007.[39] The company determined that cybercriminals accessed the store's unencrypted wireless networks to access

[36] See the Department of Homeland Security program; Stop, Think Connect http://www.dhs.gov/files/events/stop-think-connect.shtm
[37] http://www.business.ftc.gov/legal-resources/29/35
[38] http://www.ftc.gov/about-ftc/what-we-do/enforcement-authority
[39] http://www.washingtonpost.com/wp-dyn/content/article/2007/09/25/AR2007092500836.html

© 2014 Online Trust Alliance (OTA) All Rights Reserved

systems and data from more than 45 million customer credit and debit cards.[40] The total cost to the company was an estimated $246 million, including a $40.9 million settlement with Visa and other banks, as well as a $9.76 million settlement to a multi-jurisdictional group of 41 attorney generals.[41] [42] [43] TJX also settled FTC charges that it failed to provide reasonable and appropriate security measures for sensitive consumer information; the company is required to implement a comprehensive data security program and obtain audits by independent third-party security professionals for the next 20 years.[44] As with the settlements of the other pieces of litigation stemming from the TJX data breaches, retailers and others that come into possession of non-public personal information should continually re-evaluate their own data security programs.

FUNDING & BUDGETING

Responding to an accidental loss, or data breach incident is often an unbudgeted expense. This includes intangible 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 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 coverage to ensure it is keeping pace with regulatory requirements.

BUDGETING CONSIDERATIONS

Security & Monitoring Software & Services
Forensic Specialists
Employee Training
PR & Crisis Management Resources
Remediation Programs
Legal Review
Equipment Replacement
Insurance

*(See **Appendix C, page 32** for a partial list of cyber-insurance considerations).*

CRITIQUE & AFTER ACTION ANALYSIS

Carefully analyze past events to improve future plans and minimize the possibility of future recurrences. Conducting penetration testing of systems, response "fire drills," and annual audits can be an essential part of testing a crisis management plan. Regularly test these plans during the year (including weekends); critique them to remediate any deficiencies. Such evaluation should look to confirm and remedy the root cause of a breach, including any back door that may exist for future exploits.

Any breach should also include a post-mortem analysis in which key team members are gathered 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.

[40] http://www.computerworld.com/s/article/9014782/TJX_data_breach_At_45.6M_card_numbers_it_s_the_biggest_ever
[41] http://www.boston.com/business/globe/articles/2007/08/15/cost_of_data_breach_at_tjx_soars_to_256m/
[42] http://usatoday30.usatoday.com/money/industries/retail/2007-11-30-tjx-visa-breach-settlement_N.htm
[43] http://www.consumeraffairs.com/tj-maxx-data-breach
[44] http://www.ftc.gov/sites/default/files/documents/cases/2008/08/080801tjxdo.pdf

© 2014 Online Trust Alliance (OTA) All Rights Reserved

Key Questions to ask and document:

- Did we follow our plan, or did we have to discard it and start over during the incident?
- What was the customer feedback and impact to sales and customer relationships?
- What lessons have we learned?
- What internal policies and procedures need to change?
- What can we do better next time?[45]

INTERNATIONAL CONSIDERATIONS

Businesses need to be aware of the breach notification laws and guidelines for all of the countries in which their customers reside.[46]

For instance, in January 2012, the European Union (EU) revealed a draft of its European Data Protection Regulation (Proposal) to replace the previous Data Protection Directive (Directive).[46] **The Proposal includes the following strategic objectives:**[47] [48]

- Strengthen individual's rights.
- Harmonize rules and enforcement throughout the EU.[49]
- Promote high standards of data protection in a technology advanced, globalized world.
- Strengthen and clarify the roles of national data protection authorities.
- Extend the rules to include data use by police and criminal justice operations.

Companies that are active in the EU, offer services to EU citizens and handle personal data outside the union are subject to the proposed rules. For instance, the Proposal governs how data is handled creating implications for cloud service providers. This is particularly important where cloud services are employed or in any circumstance where a third party takes charge of data normally held within a company.

The Proposal does benefit businesses by requiring a single point of notification versus notifying over 27 member states. A key provision is EU wide reporting breach notification requirements. The Proposal would supplant the current patchwork of national laws in Europe that have made reporting mandatory in Germany and Spain, but voluntary in Britain and Italy. The scope would apply to service providers including e-commerce platforms, Internet payment gateways, social networks, search engines, cloud computing services, and application stores.

The EU regulation directs member countries to impose penalties on organizations that do not heed the notification rules, and requires them to craft national disclosure laws that are considered appropriate, effective, proportionate and dissuasive.

Concerns cited are that it is heavy handed, over prescriptive and out of touch with the rapid changes in digital communications. While the Proposal is under review and evolving, businesses should consider its implication in to their published privacy policy and in developing new products and services, as the deadline for implementation is early 2015.[50]

[45] https://otalliance.org/resources/security/OTA_Email_Security_Guidelines.pdf
[46] Infra, note 20
[47] http://bit.ly/1jtVR00
[48] http://www.computerweekly.com/guides/Essential-guide-What-the-EU-Data-Protection-Regulation-changes-mean-to-you
[49] The fact that it's called a "regulation" instead of a directive means that it will be directly applicable to all EU member states without a need for national implementing legislation.
[50] http://bit.ly/1hISa5X

© 2014 Online Trust Alliance (OTA) All Rights Reserved

CANADA

Organizations in all Canadian provinces and territories are subject to similar private sector privacy laws that establish rules for the collection, use and disclosure of personal information in the course of commercial activity.[50] However, the requirements for breach notification vary somewhat across the country. In May 2010, the Alberta Personal Information Protection Act (PIPA) became the first private sector privacy law to formally require breach notification. PIPA requires organizations to notify the Alberta Information and Privacy Commissioner without unreasonable delay about any incident involving loss, unauthorized access to or disclosure of personal information wherever a "reasonable person would consider that there exists a real risk of significant harm to an individual."[52] The Commissioner can order an organization to notify individuals where a real risk of significant harm is found. Failure to notify where required by law can result in a fine of up to $100,000.[53]

Although the federal Personal Information Protection and Electronic Documents Act (PIPEDA) does not contain any formal breach notification requirements, the general requirements for accountability and safeguarding personal information can be interpreted to require some form of notification. To this end, the Office of the Privacy Commissioner of Canada has published voluntary guidelines for responding to privacy breaches.[54]

In addition, Canada published its final regulations to the Canada Anti-spam Legislation (CASL) in December 2013, which will become effective July 1, 2014. Combined with directives of the Office of the Privacy Commissioner, businesses should review the data protection responsibilities, including data which may be stored and processed by Canadian service providers and vendors.[55]

[51] The Federal Personal Information Protection and Electronic Documents Act, SC 2000, c 5, applies to the collection, use and disclosure of personal information generally in the course of commercial activity across Canada except for the following three provinces which have passed their own legislation, Alberta: Personal Information Protection Act, SA 2003, c P-6.5; British Columbia: Personal Information Protection Act, SBC 2003, Quebec: An Act respecting the Protection of personal information in the private sector, RSQ, c P-39.1.
[52] Section 34.1.
[53] Section 59(1)(e.1) and (2)
[54] http://www.priv.gc.ca/information/guide/2007/gl_070801_02_e.asp
[55] http://fightspam.gc.ca/eic/site/030.nsf/eng/00273.html

© 2014 Online Trust Alliance (OTA) All Rights Reserved

SUMMARY

Worldwide we are becoming a data-driven society, providing benefits to consumers and businesses alike. Unfortunately, cybercriminals equally recognize the opportunities and the value of targeting unsuspecting companies. This underscores the need for every business to take a holistic view of data security, privacy and brand protection practices.

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 factors such as the increasing levels of cybercrime and online malice, adoption of geo-location applications and the collection of vast amounts of information.
Combined with the explosive growth of big data, mobile devices and reliance of cloud service providers, it is vital that business leaders focus on data stewardship as a key corporate priority and responsibility. Failure to do so puts consumers in harm's way, adding to the regulatory and legal framework that can inhibit growth and innovation.

Data loss incidents can occur in businesses of all sizes, non-profits, educational institutions 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, to a misplaced document to a system breach by a hacker. Whether you are a Fortune 500 company or a local merchant, if you collect data then you are at risk.

All businesses (including those that may not have an online presence) must acknowledge that the data they collect is not only a powerful marketing tool and business asset, but also contains sensitive information. **Industry and government leaders must consider the following key principles to maximize their preparedness:**

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

Data security and privacy must become part of an organization's culture. Be prepared with an incident plan to help protect their data, detect a loss and quickly mitigate the impact. The responsibility cannot be siloed with one group or individual; it is every employee's responsibility. Following the guidance in this document will help ensure that businesses are ready to take the appropriate steps to minimize damage to their customers and brand in the event of a data loss incident.

Equally as important is completing an audit of all business practices, products and services. This includes third party vendors to validate the business reason for the collection of all data. Site visitors and customers must have clear, discoverable and comprehensible notices. 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.

Conversely, consumers have a 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. They need to take steps to protect their data and devices. This includes: 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, app developers, 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.

© 2014 Online Trust Alliance (OTA) All Rights Reserved

APPENDIX A - RESOURCES

ONLINE TRUST ALLIANCE

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

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

Email Security & Authentication - https://otalliance.org/eauth.html

Always On SSL - https://otalliance.org/aossl.html

Extended Validation SSL Certificates - https://otalliance.org/resources/EV/index.html

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

U.S. DEPARTMENT OF COMMERCE & 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

National Strategy for Trusted Identities in Cyberspace (NSTIC)
http://www.nist.gov/nstic/about-nstic.html

U.S. FEDERAL TRADE COMMISSION

Complying with FTC's Health Breach Notification Rule
http://business.ftc.gov/documents/bus56-complying-ftcs-health-breach-notification-rule

FTC Data Security
http://business.ftc.gov/privacy-and-security/data-security

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

Mobile App Developers: Start with Security
http://business.ftc.gov/documents/bus83-mobile-app-developers-start-security

Protecting Personal Information: A Guide for Business
http://www.business.ftc.gov/documents/bus69-protecting-personal-information-guide-business

U.S. FEDERAL COMMUNICATIONS COMMISSION

Small Business Cybersecurity Resource Guide http://www.fcc.gov/cyberforsmallbiz

CALIFORNIA

Top 10 Tips for Identity Protection http://oag.ca.gov/idtheft/facts/top-ten

Recommended Practices on Notice of Security Breach Involving Personal Information
http://oag.ca.gov/sites/all/files/pdfs/privacy/recom_breach_prac.pdf

Business Resources: Recommended Practices www.oag.ca.gov/privacy/business-privacy

Data Breach Reporting www.oag.ca.gov/ecrime/databreach/reporting

California and Federal Privacy Laws www.oag.ca.gov/privacy/privacy-laws

California Privacy Legislation www.oag.ca.gov/privacy/privacy-legislation/leg2013

© 2014 Online Trust Alliance (OTA) All Rights Reserved

NEW YORK STATE ATTORNEY GENERAL'S OFFICE

Identity Theft
http://www.ag.ny.gov/consumer-frauds-bureau/identity-theft

Security Breach & Notification Act
http://www.ag.ny.gov/consumer-frauds/new-york-state-information-security-breach-and-notification-act

WASHINGTON STATE ATTORNEY GENERAL'S OFFICE - IDENTITY THEFT & PRIVACY

Identity Theft and Privacy Guide for Business:
http://www.atg.wa.gov/businesses.aspx#.Ut38IZGtvjA

Internet Safety http://www.atg.wa.gov/InternetSafety.aspx

Consumer Privacy & Data Protection
http://1.usa.gov/KCmnYh

Identity Theft
http://1.usa.gov/1hdYOk0

OFFICE OF THE CANADIAN PRIVACY COMMISSIONER

Securing Personal Information: A Self-Assessment Tool for Organizations
http://www.priv.gc.ca/resource/tool-outil/security-securite/english/AssessRisks.asp?x=1

Securing the Right to Privacy: 2013 Annual Report to Parliament
http://www.priv.gc.ca/information/ar/201213/201213_pa_e.pdf

ADDITIONAL RESOURCES FROM THE PUBLIC & PRIVATE SECTORS

US Department of Education, Privacy Technical Assistance Center: Data Breach Response Checklist
http://ptac.ed.gov/sites/default/files/checklist_data_breach_response_092012.pdf

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

Anti-Phishing Working Group http://apwg.org/resources/Educate-Your-Customers/

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

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

Identity Theft Resource Center (ITRC http://www.idtheftcenter.org

Infragard https://www.infragard.org/

Internet Crime Complaint Center (IC3) http://www.ic3.gov/default.aspx

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

Open Security Foundation DataLossdb http://datalossdb.org/

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

RiskBased Security https://www.riskbasedsecurity.com/reports/2013-DataBreachQuickView.pdf

© 2014 Online Trust Alliance (OTA) All Rights Reserved

INTERSECTIONS INC.

Data Breach Consumer Notification Guide
http://www.intersections.com/library/IntersectionsBreachConsumerNotificationGuideFinal_Nov2013.pdf

Identity Protection
http://www.intersections.com/IDProtection.html

7 Steps to Breach Readiness
http://www.intersections.com/library/7stepstodatabreach_040611%20FINAL.pdf

Identity Guard Resource Center
http://www.identityguard.com/identity-theft-resources/

PRICEWATERHOUSECOOPERS (PWC)

Data Privacy Survey:
http://www.pwc.com/us/en/risk-assurance-services/publications/2013-data-privacy-survey-results.jhtml

Protecting Your Brand in the Cloud
http://pwc.to/1cQnlHi

Role of Internal Audit in Data Security and Privacy
http://www.pwc.com/us/en/risk-assurance-services/publications/internal-audit-assuring-data-security-privacy.jhtml

10 Minutes on CyberSecurity Realities
http://www.pwc.com/us/en/10minutes/cybersecurity-realities.jhtml

The Global State of Security Survey 2014
http://www.pwc.com/gx/en/consulting-services/information-security-survey/download.jhtml

SYMANTEC

2013 Cost of Data Breach Study: Global Analysis
http://bit.ly/1ekdNZ0

Data Breach Calculator
https://databreachcalculator.com/

TRUSTe

Privacy Best Practices - Protecting Customer Information Online
http://www.truste.com/resources/privacy-best-practices

Privacy by Design
http://www.truste.com/window.php?url=http://download.truste.com/TVarsTf=GA4ZVGYQ-202

Forrester Report - Measure the Effectiveness of Your Data Privacy Program
http://bit.ly/1bOTmno

© 2014 Online Trust Alliance (OTA) All Rights Reserved

APPENDIX B

The following provides a general template to assist in preparing data breach notice letters in connection with regulatory and contractual data breach notification requirements applicable to affected individuals. Regularly check that the contact information provided in the sample letter is up to date and is compliant with applicable regulatory authorities.

Take into account the footnotes in the Appendix for suggestions and legal considerations. Your letter should be tailored to reflect the particular circumstances of your company's breach and it must address the specific legal requirements of the impacted individuals. Typically, a breach's impact goes beyond State boundaries; thus, multiple versions of the notification letter may be required. Concurrent with notifications to individuals, companies should also send copies to the offices of the respective Attorney General. While mandated by some States, such distribution of both draft and final letters in advance is highly recommended.

SAMPLE LETTER TEMPLATE

[*Company Letterhead*]
[*Individual Name*]
[*Street Address*]
[*City, State and Postal Code*]
[*Credit Monitoring Promotion Code*]

[*Date*]
Dear [*Individual Name*]:

We value your business and respect the privacy of your information, which is why we are writing to let you know about a data security incident that [*may involve/involves*] your personal information. We became aware of this breach on [*Insert Date*] which occurred on [*Identify Time Period of Breach*].

The breach occurred as follows: *(Summarize a brief description of what happened, including the data of the breach and the date of the discovery of the breach, if known).*[56] [57]

The data accessed [*may have included/included*] personal information such as [identify types of PII at issue]. To our knowledge, the data accessed did not include any [*identify types of PII not involved*].[58]

[*Company Name*] values your privacy and deeply regrets that this incident occurred. Working with law enforcement and forensic investigators, [*Company Name*] is conducting a thorough review of the potentially affected [*records/computer system/identify other*] [, *and will notify you if there are any significant developments*]. [*Company Name*] has implemented additional security measures designed to prevent a recurrence of such an attack, and to protect the privacy of [*Company Name*]'s valued [*customers / employees / group of affected individuals*].[59]

The company also is working closely with [*major credit card suppliers and*] law enforcement to ensure the incident is properly addressed.

[56] The language in this section must be tailored to reflect the actual circumstances of the breach and legal requirements of the relevant states. Note that Massachusetts law requires that the notice NOT include a description of the nature of the breach NOR specify the number of individuals affected.
[57] Effective as of Jan. 1, 2012, California law also requires that the notice describe whether notification was delayed as a result of a law enforcement investigation if that information is possible to determine at the time notice is provided.
[58] Several state breach notification laws also require that the notice identify the categories of personal information involved such as an individual's: name or address, birth date, phone number, driver's license number, credit card number, bank account number or Social Security number.
[59] Some state breach notification laws require that the notice briefly describe the general actions the business has taken to remedy the situation. This is also consistent with FTC guidance, and may include: containing the breach, implementing additional internal controls and safeguards, and making changes to existing policies. The language in this section must be tailored to reflect the actual actions taken by the company.

© 2014 Online Trust Alliance (OTA) All Rights Reserved

IF SOCIAL SECURITY NUMBER WAS INVOLVED:[60]

Because your Social Security number was involved, we recommend that you place a fraud alert on your credit files. A fraud alert requires potential creditors to use what the law refers to as "reasonable policies and procedures" to verify your identity before issuing credit in your name. A fraud alert lasts for 90 days.

To help ensure that this information is not used inappropriately, [*Name of Company*] will cover the cost for one year for you to receive credit monitoring. To take advantage of this offer, call the toll-free phone number of one of the three credit reporting agencies listed below. This will let you automatically place an alert with all of the agencies. You should receive letters from all three, confirming the fraud alert and letting you know how to get a free copy of your credit report from each.

- 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

- If you find suspicious activity on your credit reports, call your local police or sheriff's office and file a police report of identity theft. [*If appropriate, also give the contact number for the law enforcement agency investigating the incident for you*]. Get a copy of the police report. You may need to give copies of the police report to creditors to clear up your records.

- Continue to monitor your credit reports. Even though a fraud alert has been placed on your account, and if you do not find any signs of fraud upon the initial review of your reports, you should continue to monitor your credit reports to ensure an imposter has not opened an account with your personal data. For more information on identity theft, we suggest that you visit the web site of [*insert link to State Attorney General website*].

- [*In some US states*] You have the right to put a security freeze on your credit file.[61] This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency.

IF FINANCIAL ACCOUNT NUMBER OR INFORMATION WAS INVOLVED:

To protect yourself from the possibility of identity theft, we recommend that you immediately contact [credit card or financial account issuer] at [phone number] to give you a PIN or password. This will help control access to the account. For more information on identity theft, we suggest that you visit the website of [*insert link to State Attorney General website*].

[60] Some states require that the breach notice include information on certain actions affected individuals can take to protect themselves. Consistent with these state law requirements, the FTC recommends that the notice explain the steps affected individuals can take to protect against misuse or disclosure specific to the type of personal information subject to the breach.
[61] Many (but not all) States allow you to place a "security freeze" on your credit file for free or a reduced fee. Massachusetts and West Virginia breach notification laws require that the notice include information instructing affected individuals on how to place a security freeze on their credit files. Many states do have laws allowing individuals to place security freezes on their files, however, the fees to place, lift or remove the security freeze may vary by state. For more info: http://www.equifax.com/credit/fraud-alerts/

© 2014 Online Trust Alliance (OTA) All Rights Reserved

IF DRIVER'S LICENSE OR IDENTIFICATION CARD NUMBER WAS INVOLVED:

Since your [*State*] driver's license [*or State Identification Card*] number was involved, we recommend that you call the DMV Fraud Hotline at [*phone number*] to report it.

IF MEDICAL INFORMATION OR HEALTH INSURANCE INFORMATION WAS INVOLVED:

We recommend that you regularly review the explanation of benefits statement that you receive from [*us, your plan, your insurer*]. If you see any service that you believe you did not receive, please contact [*us, your plan, your insurer*] at the number on the statement [*or provide phone number here*]. If you do not receive regular explanations of benefit statements, contact your provider or plan and request them to send such statements following the provision of services in your name or number.

You may wish to order copies of your credit reports and check for any medical bills that you do not recognize. [*Review paragraph above on contacting credit reporting agency*]. If you find anything suspicious, call the credit reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your medical records. You may want to request a copy of your medical records from [your provider or plan], to serve as a baseline. For information on your medical privacy rights, we suggest that you visit the website of [*insert link to State Attorney General website*].

Questions about this Notice:

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

If there's anything that [*Name of Company*] can do to assist you, please call us at [*toll-free phone number*]. 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.[62]

Sincerely,
[*Name*]
[*Title*][63]
[*Contact Information*]

[62] The notice should, and in some states must, include contact information for a company representative who can assist and provide additional information to affected individuals.
[63] The notice should generally be signed by a senior executive of the company. This may help signal to affected individuals that the company is proactive and takes the incident seriously

© 2014 Online Trust Alliance (OTA) All Rights Reserved

APPENDIX C – REGULATORY REQUIREMENTS & CONSIDERATIONS

Organizations found to be in violation of laws could face significant fines and penalties. Businesses need to consider the following;

- Individual state laws where a business has nexus or customers residing[64]
- Country laws if any of the lost data pertains to residents[65]
- Payment Card Industry Data Security Standards (PCI DSS)[66]
- Sarbanes-Oxley Act[67]
- Health Insurance Portability and Accountability Act (HIPAA),[68] including the HITECH Act of 2009, including the HITECH Breach Notification Rule[69]
- Gramm-Leach Bliley Act (GLBA), including the Safeguards Rule, and the Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice[70]
- Federal Financial Institutions Examine Council (FFIEC) Guidelines[71]
- Fair Credit Reporting Act[72], including the Fair & Accurate Credit Transactions Act, Red Flags Rule[73]
- Federal Trade Commission Guidelines and Requirements[74]
- Children's Online Privacy Protection Act (COPPA), (updated)[75]
- International Standards Organization (ISO) security standards[76]

[64] See infra note 18

[65] See infra note 20

[66] Comprehensive standards governing payment card data security process - https://www.pcisecuritystandards.org/security_standards/

[67] A Federal law to improve accuracy and reliability of corporate disclosures made pursuant to the securities laws. Compliance centers on building a sufficient system of internal controls regarding PII. http://www.soxlaw.com/compliance.htm.

[68] Standards and requirements for transmitting certain health information and e-PHI. http://www.hhs.gov/ocr/privacy/

[69] Effective January 2013, the Department of Human Health & Services (HHS) modified the standard that HIPAA-covered entities must use to determine if a breach of protected health information (PHI) has occurred. http://hitechanswers.net/about

[70] Title V authorizes each agencies' governing financial institutions to establish and enforce guidelines to ensure security and protect against unauthorized access to or use of customer data.

[71] Prescribes principles, standards, and report forms financial institutions. http://ithandbook.ffiec.gov/

[72] A federal law that regulates credit bureaus, entities or individuals who use credit reports, and businesses that furnish information to Consumer Reporting Agencies (CRA). http://www.ftc.gov/sites/default/files/fcra.pdf

[73] The "FACT Act" amended FCRA, adding requirements designed to prevent identity theft and assist identity theft victims. http://www.ftc.gov/os/fedreg/2007/november/071109redflags.pdf

[74] Federal Trade Commission's Privacy and Data Security Enforcement under Section 5, http://www.americanbar.org/groups/young_lawyers/publications/the_101_201_practice_series/federal_trade_commissions_privacy.html

[75] A federal rule that applies to "operators of commercial web sites and online services directed to children under 13 http://www.business.ftc.gov/documents/Complying-with-COPPA-Frequently-Asked-Questions

[76] ISO is a non-governmental international body that creates information and communications technology (ICT) standards. http://www.iso.org/iso/iss_international-security-standards.htm

© 2014 Online Trust Alliance (OTA) All Rights Reserved

APPENDIX D – CYBER SECURITY LIABILITY AND INSURANCE CONSIDERATIONS[77] [78]

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 your computer system.
3. Electronic Media peril broadly defined to include infringement of domain name, copyright, trade names, logo, and 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.

[77] http://bit.ly/LNE1d3
[78] See http://www.dhs.gov/sites/default/files/publications/cybersecurity-insurance-read-out-report.pdf

© 2014 Online Trust Alliance (OTA) All Rights Reserved

APPENDIX E – COMPUTER FORENSICS BASICS

The most common goal of 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. They can help you discover the source of the breach, identify all impacted systems, determine if PII or regulated data was compromised and to help provide law enforcement the best opportunity at catching the perpetrator. The following is intended to help provide an understanding of the basics behind what an expert does when tracing 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 accepted 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 preserve relevant data before a breach occurs. The types of processes you should put into place, if you aren't already doing them, include:

- Performing regular backups of systems and logs 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 including both successes and failures.

- 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.

© 2014 Online Trust Alliance (OTA) All Rights Reserved

When performing forensics during incident response, consider how and when the incident should be contained. 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 so 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 systems: these people might have passwords that are needed for the investigator to properly access the systems. In addition, an investigator will need this documentation to build the picture of how the evidence was collected and of how the breach might have occurred, and these people.

Once you've contacted law enforcement, be prepared to answer a series of questions. These will likely include the following areas:[79]

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. What in your sever environment (operating system, server software & applications)?
14. Can you provide a complete topology of your network?
15. What first alerted you to the incident regardless of when the attack truly started?
16. Who in the organization has been notified?
17. Who outside the organization has been notified?
18. From this point forward, who does law enforcement contact and who can they speak to if they are contacted?
19. What are your estimated damages?
20. For data acquisition purposes, can the compromised system(s) be taken offline? If so, for how long? In some cases better data acquisition can be performed on an offline system, which is ideal in a forensic acquisition environment.

For a detailed drill-down on computer forensics, see the NIST Guide to Integrating Forensic Techniques into Incident Response.[80]

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

© 2014 Online Trust Alliance (OTA) All Rights Reserved

APPENDIX F - ENCRYPTION RESOURCES

Encryption is considered a best practice to help minimize the effects of a breach, not only for sensitive files and data stores, but also equally important for laptops, tablets, and smartphones, which often contain customer data and are easily lost or stolen. As encryption standards continually evolve, readers are recommended to check the web site of their device and operating system provider. Additionally, several third party tools are available for added level of system and file encryption.

Encryption is only as strong as the password which decrypts the file or disk. Like all security measures, encryption is subject to the "weakest link," the user's password. Passwords that encrypt files and hard drives should follow the same guidance for account passwords (i.e., complexity, length, regular updates, use a password only once).

When encrypting files, there are two different types of encryption to consider: ***file*** and ***full-disk***.

File encryption encrypts files and directories on a per-user basis. It 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 recommended for protecting all sensitive data on a lost or stolen system.

Full-disk encryption encrypts all the data on a drive, including user data, temp files, home directories, etc. Thus, it is the best solution for protecting sensitive information, as it ensures customer or sensitive data on a lost or stolen system cannot be accessed by others.

Microsoft offers BitLocker in Windows Vista/7 (Ultimate and Enterprise SKUs) and Windows 8 (Enterprise and Professional SKUs) are leading forms of full-disk encryption. BitLocker can encrypt the drive Windows is installed on (the operating system drive) as well as fixed data drives (such as internal hard drives). New files are automatically encrypted when you add them to a drive that uses BitLocker. However, if you copy these files to another drive or a different PC, they're automatically decrypted. You can also use BitLocker "To Go" to help protect all files stored on a removable data drives (such as an external hard drive or USB flash drive.

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 (free/Open Source) and PGP (commercial), which work on both Windows and Mac OS X systems.

Full Disk Encryption:

- Truecrypt (multiple operating systems): http://www.truecrypt.org
- PGP: http://www.symantec.com/business/whole-disk-encryption
- Windows BitLocker Drive Encryption – Window 7
  http://windows.microsoft.com/en-US/windows7/products/features/bitlocker
- Windows BitLocker Drive Encryption Windows 8.1 Pro and Windows 8.1 Enterprise:
  http://windows.microsoft.com/en-US/windows-8/bitlocker#1TC=t1
- MacOS X Lion, FileVault 2:
  http://support.apple.com/kb/HT4790
  http://www.apple.com/macosx/what-is/security.html

© 2014 Online Trust Alliance (OTA) All Rights Reserved

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/MANUALS/1000/MA1565/en_US/iphone_user_guide.pdf
  http://manuals.info.apple.com/en_US/iPhone_iOS4_User_Guide.pdf
  http://www.apple.com/ipad/business/docs/iOS_Security_Oct12.pdf
  https://itunes.apple.com/us/app/encrypt-files/id511330658

- Android Encryption & Security
  http://source.android.com/devices/tech/encryption/android_crypto_implementation.html (v 3)
  http://developer.android.com/about/versions/android-4.3.html#Security (v 4.0)
  http://www.groovypost.com/howto/encrypt-android-smartphone-tablet/
  http://www.abc.net.au/technology/articles/2013/12/19/3914520.htm

© 2014 Online Trust Alliance (OTA) All Rights Reserved

APPENDIX G

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

© 2014 Online Trust Alliance (OTA) All Rights Reserved

ACKNOWLEDGEMENTS

Support and contributions to the Guide reflects input from numerous organizations including the Identity Theft Council, Open Security Foundation (DataLossDB.org), Privacy Choice, and the Privacy Rights Clearinghouse. In addition, OTA wishes to acknowledge input from staff of the Federal Trade Commission, Federal Communications Commission, U.S. Department of Homeland Security, the Federal Bureau of Investigation, U.S. Secret Service and State Attorney General's office of New York, Washington State and the California Department of Justice, Better Business Bureaus (serving Metropolitan New York, Western Washington/Oregon/Alaska & Golden Gate/San Francisco) and members of the InfraGard chapters in New York City, San Francisco, and Seattle.

Special thanks to the support and input from OTA member companies including American Greetings Interactive, AVG, Bounce.IO, Coles, comScore, DigiCert, Epsilon, Listrak, IID, Intersections, Mark Monitor, Message Systems, Microsoft, Pitney Bowes, PwC, Publishers Clearing House, Responsys, Return Path, Sailthru, Simpli.fi, SiteLock, Symantec, TRUSTe, TrustSphere, Verisign and VivaKi. In addition, OTA Advisors Shaun Brown, David Daniels, Mark Goldstein and Joe St Sauver provided invaluable input, strategic direction and technical edits to this report.

ABOUT THE ONLINE TRUST ALLIANCE (OTA)

https://otalliance.org | 425-455-7400 | admin@otalliance.org

OTA is a 501c3, tax-exempt charitable non-profit with a mission to enhance online trust and user empowerment, while promoting innovation and the vitality of the internet. OTA's goal is to help educate businesses, policy makers and stakeholders while developing and advancing best practices and tools to enhance the protection of users' security, privacy and identity. OTA supports collaborative public-private partnerships, benchmark reporting, meaningful self-regulation and data stewardship.

© 2014 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: https://otalliance.org/breach.html 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.