2015
DATA PROTECTION & BREACH
READINESS GUIDE

Providing businesses with prescriptive advice to help optimize their data privacy and security practices to prevent, detect, contain and remediate the risk and impact of data loss incidents and breaches.

OTA
Online Trust Alliance

February 13, 2015

TABLE OF CONTENTS

WHAT'S NEW

The 2015 Data Protection & Breach Readiness Guide (Guide) has been developed to help organizations of all sizes in both the public and private sector better protect their data and detect, contain and remediate an incident. The Guide includes content to help aid a broad range of stakeholders ranging from business and technical decision makers to privacy and security professionals to web and app developers. The goal of the Guide is to help readers better understand the issues and solutions which can enhance their data protection practices and enable them to develop effective data loss incident readiness.

Even the most cyber-savvy organizations have found themselves exposed and ill prepared to manage the effects and impact of a data breach. The best defense is implementing a broad set of operational and technical best practices that help protect your company and your customers' personal data. The second step is being prepared with a data breach response 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 an organization and requires a strong guiding hand from senior executives.

A key to success is moving from a compliance perspective to one of data stewardship. This perspective recognizes the long term impact to a brand, the importance of consumer trust and the implications of a data breach incident on vendors and business partners. While there is no perfect defense from a determined attacker, the best practices advocated by OTA and outlined in this Guide can help to greatly reduce a company's attack surface and impact of a data loss incident.

New to the 2015 Guide is an expanded discussion on the importance of completing security and privacy assessments and annual audits of vendors and cloud providers. The report provides a framework of key risk questions for businesses to consider, including vendor contractual obligations. Additional discussion has been included on the importance of sharing not only breach data with law enforcement but also threat intelligence including attempts and suspicious activity. The 2015 Guide includes an expanded section on security best practices to help prevent, detect, contain, and remediate the impact of a data loss incident.

The Online Trust Alliance (OTA) and its contributing authors and reviewers provide this document as a public service, based on collective expertise and opinion. This is provided "as is" without any representation or warranties and is not, nor intended to be legal advice. 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. To submit comments please email the OTA at admin@otalliance.org.

EXECUTIVE SUMMARY

There is no doubt that 2014 has overtaken all previous years as the year of the breach. According to Risk Based Security, the first nine months of 2014 resulted in 904 million records being exposed, which is a 95% increase from the same period of time in 2013. 2014 ended with a bang as a result of the massive breach of Sony by Guardians of Peace (GOP). The Sony breach resulted in not just consumer information being leaked, but also their intellectual property including movies and scripts, employee data, executive salaries and a plethora of other sensitive data. Though Sony may be remembered most for the embarrassing leaked emails regarding Hollywood stars and pulling the movie "The Interview" from theaters. Yet the impact to Sony's brand and organization may have significant long-term consequences.

Combined with broadened news and social media coverage, data breaches in 2014 have touched nearly every household and business in North America, Europe and other regions of the world. But the real news is not the number of credit cards or social security numbers compromised, but the increased growth and precision of targeted attacks against high-net worth targets, ranging from consumers to corporations. These attacks are not the product of script kiddies, but instead are sophisticated criminal activities being orchestrated by a blend of underground cybercrime networks and nation states.

> *"There is simply no good news when it comes to breaches, businesses are overwhelmed yet all too often fail to adopt security basics."*

While some may claim these breaches are the result of highly technical and sophisticated efforts, the data reported by the FBI and other organizations continually report more than 90 percent were avoidable had widely accepted best practices and security controls been applied. 2014 revealed the emergence of micro-targeting to higher net worth targets accomplished by sophisticated social engineering and malicious tactics including forged email and the use of targeted malvertising.[1]

When combined with the revelations of Snowden, it is no surprise consumers are increasingly concerned regarding the collection, use and sharing of their data and online activities. According to the Pew Research Internet Project report released in November 2014, 91% of adults "agree" or "strongly agree" that consumers have lost control over how personal information is collected and used by companies. Additionally, nearly 90 percent "agree" or "strongly agree" that it would be very difficult to remove inaccurate information about them online.[2]

The challenges of data security have become a challenge for businesses worldwide as they deal with the increased complexity of not only their own infrastructure, but also the vendors and cloud service providers on which they are increasingly reliant. Patching systems from widely known threats such as Heartbleed[3] and vulnerabilities in WordPress and Drupel website content management platforms has been a significant challenge for organizations of all sizes.[4] As if Heartbleed was not enough, Secure Sockets Layer (SSL 3.0) was exposed to Poodle, a major vulnerability impacting banking and commerce sites worldwide.[5]

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 of data. In addition to Sony, other high profile breach victims in 2014 included Home

[1] Malvertising typically involves injecting malicious or malware laden advertisements into online advertising networks and webpages..

[2] http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/.

[3] http://heartbleed.com/.

[4] https://www.drupal.org/SA-CORE-2014-005.

[5] http://www.symantec.com/business/support/index?page=content&id=TECH226102.

Depot, JP Morgan Chase, eBay, Apple (iCloud), and SnapChat. And, 2014 did not go out with a whimper; the DDoS attacks against Microsoft's Xbox Live service and Sony's PlayStation network by LizardSquad resulted in both companies' online gaming networks crashing during the Christmas holidays.

The Open Security Foundation (OSF) identified over 1,100 breaches involving the loss of personally identifiable information (PII) occurring in 2014.[6] OTA's analysis of this preliminary year-end data found 29% were due to lack of internal controls resulting in employees' accidental or malicious events and 38% the result of actual hacks. The balance of incidents was primarily attributed to lost or stolen devices (12%) and fraud (11%). Lost, stolen, or misplaced documents accounted for 9% of all incidents.

2014 Breach Highlights

90% Could have been prevented - OTA
37% Due to inside threats - OSF
19% Physical loss/theft - OSF
40% of the largest breaches OSF
91% increase in targeted attacks - SYMC

Sources: OTA - Online Trust Alliance,
OSF - Open Security Foundation, SYMC - Symantec

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 devastating consequences on the value of a company's brand and consumer perception. 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, starting with responsible data privacy and collection practices and extending to the security of its own and its vendors' systems. Those that prepare in advance will not only be postured to survive a data breach, but also are more likely to retain a positive reputation with their customers.

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

These trends suggest a need for increased commitment and adoption of responsible privacy and voluntary security best practices. This includes broader transparency and more detailed reporting requirements. As a result of the increased sophistication and tenacity of international crime syndicates and state sponsored attackers, 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.

Data Privacy Fundamentals

- Privacy policies need continual review
- All businesses collect some form of PII
- Everyone will realize a breach or loss
- Data stewardship and privacy is everyone's responsibility
- Every organization needs to have a current and tested breach plan

OTA advocates that every organization handling customer data, ranging from email addresses to PII, create a data lifecycle management strategy and incident response plan that evaluates data from acquisition through use, storage and destruction. A key to a successful data lifecycle management program 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.

[6] http://datalossdb.org/statistics.

DATA BREACH COSTS

According to the 2014 Cost of Data Breach Study: Global Analysis conducted by the Ponemon Institute and sponsored by IBM, the average cost to an organization to investigate, notify and respond to a data breach was $3.5 million.[7] On the other hand, the study found that on average survey respondents would like to see the investment on cyber security double from an average of $7 million to $14 million.

The post breach impact on a company's customers can also be significant. According to creditcards.com, 45 percent of shoppers are likely to avoid stores that have suffered a data breach. In an article about data breaches scaring away consumers, Fortune.com revealed that post breach Target's earnings dropped 62% for the second quarter of 2014.[8] Target is also facing more than 90 lawsuits that have been filed by customers and banks concerning the breach. Total costs to Target to respond to the breach are now estimated at over $140 million, not including pending lawsuits.[9]

> *"There will never be perfect security. A breach or accidental loss can and will occur. All organizations need to make data stewardship part of every employees role."*

Small and large companies alike run the risk of a data breach, and the implications of a breach to the organization can be grave. Based upon their study, the Ponemon Institute estimates that there is a 22% probability that an organization will suffer from a material data breach in the next two years.[10] The business shock of a breach can be compounded by the 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 significantly 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 an organization's communication plan as part of their overall incident response planning.

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 incident responders must be trained, equipped and empowered to deal with a 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.

---

[7] http://www.ponemon.org/blog/ponemon-institute-releases-2014-cost-of-data-breach-global-analysis and http://www-935.ibm.com/services/us/en/it-services/security-services/cost-of-data-breach/.

[8] http://fortune.com/2014/09/25/will-data-breaches-scare-away-consumers/.

[9] http://www.nytimes.com/2014/08/06/business/target-puts-data-breach-costs-at-148-million.html?_r=0.

[10] See note 7 supra.

DATA LIFECYCLE AND STEWARDSHIP

An ounce of prevention is worth much more than a pound of cure when it comes to data breaches. A well-designed, actionable data stewardship program is an essential factor in not only meeting compliance and regulatory obligations, but perhaps more important is to demonstrate to consumers and business partners an organization has taken reasonable steps to protect data from abuse and loss. Furthermore, developing a program 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. The aftermath of a data breach is often costly and can paralyze an organization, disrupting business operations.

Figure 1 - Data Stewardship

An adequate data stewardship program focuses on several fundamentals. First, understanding that privacy policies and practices are not stagnant. As a business is dynamic, privacy policies require ongoing review and updating. Second, every organization should assume that they collect one or more forms of covered or PII. This can range from employee payroll data to consumer birthdays, phone numbers and home addresses. Third, business leaders need to realize there is no perfect security. A breach or accidental loss can and will occur, requiring organizations to make data stewardship every employee's responsibility. These fundamentals underscore the need to continually review your data lifecycle and to develop a breach response plan.

Data lifecycle management ensures the confidentiality, integrity and availability of data collected, used or stored by an organization through the life of the data, including the ultimate disposal at the end of its lifecycle. The objective of the program is to prevent unauthorized disclosure, modification, removal or destruction of data, and interruptions to an organization's activities. The main data lifecycle stages are collect, store, use/process, share, archive and destroy.

Figure 2- Data Lifecycle

Beyond managing the lifecycle of your data, you must be a good steward of your data. The first step is to re-validate the business purpose of any data collected. Ask the questions - is the data required, relevant and does it need to be retained? Be it a client, mobile device, server, corporate network, cloud provider or data center, companies must strive to help protect data no matter where it resides, whether it is stored within a company's internal network or with a cloud service provider. 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, both in the US and abroad. Applying yesterday's rules may no longer be applicable in today's data driven economy.

This Guide identifies key questions and recommendations for businesses to consider when creating a baseline data lifecycle and stewardship framework. Depending on your industry, size of your business, and the type of data collected, your requirements may vary. The key components of a data lifecycle and stewardship program are: Program Governance, Risk Assessment, Controls, Training, Vendor Management, Monitoring, and Incident Response. See Figure 3.

An essential part of creating a data lifecycle and stewardship program is designating a chief data protection officer and creation of virtual teams of privacy professionals, security specialists and operational managers, which are becoming commonplace in U.S. and other geographies. All organizations in both the public and private sector are faced with key considerations when it comes to their data collection practices.

Figure 3 - Data Management Program Elements

As illustrated in Figure 4 below, 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, event registrations and ecommerce shopping carts. A major challenge is the evolving definition of "covered" or "sensitive" information.

Also, it is important for organizations to continually inventory the data they collect and compare it to the ever-evolving definition of covered information. User rights access and the blurring of the workplace further exacerbates the risk of unintended exposure and unauthorized access of covered data. Whether it be rogue employees or sophisticated cybercriminals, it is imperative that companies take steps to identify the data they collect, 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 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.

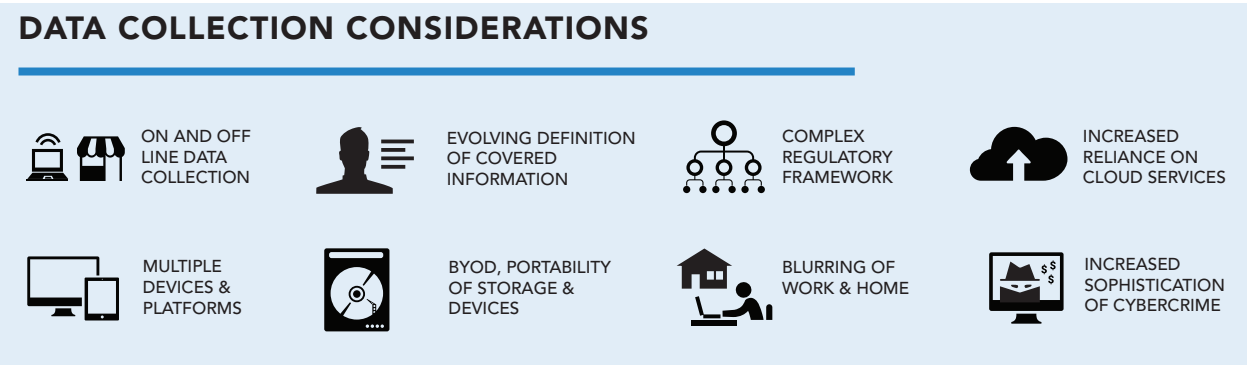

Figure 4 - Data Collection Considerations

Data Governance

If your organization does not currently have a formal data lifecycle and stewardship program, it is highly recommended a program 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, a data governance strategy can help mitigate the risk and impact of data loss incidents. Key components of a data governance program are discussed below.

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 your controls are working and practices are being followed?

Classification Criteria

- Types of Data
- Criticality and Sensitivity
- Ownership
- Controls and Status

The first step is determining the type of data your organization is classifying. Data 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 the data and any data retention and destruction requirements.[11] What scheme your organization chooses is less important than is the actual exercise of making sure the organization understands what data is collected and the potential impact of a data loss incident.

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 clients, tablets or mobile devices. Personal or covered information (including but not limited to PII) that is in motion should be encrypted (see Appendix F 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 is 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.[12]

As the definition of 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 user names, passwords, email addresses, names, street addresses, etc.[13] 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.

---

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

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

[13] 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://oag.ca.gov/ecrime/databreach/reporting.

Inventory System Access & Credentials

Having an inventory of key systems and 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 not only to 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
- Event Registration sites
- Bank accounts and merchant card processor(s)
- Company bank accounts and credit cards

Employee Data Access Controls

An organization should promulgate and deploy appropriate controls concerning employee and third party access to systems and data, and this includes ensuring appropriate read, write and retrieval access to all data classified as critical or sensitive. For third party vendor and cloud service providers, an organization should periodically audit access and take any necessary steps to ensure only those persons with a legitimate need to access an organization's systems and data are granted. Best practices include:

- Validating appropriate employee use and data access and those of third party vendors and cloud service providers;
- Scanning of outbound email for protected content (Data Loss Prevention solutions);
- Digital Rights Management (DRM), to control and limit access of proprietary or copyrighted data (if applicable);
- Auditing or confirming that cloud storage complies with an organization's data governance requirements (including employee use of third party data shares and storage sites). This includes any web-based file or content hosting services such as Google Docs, Microsoft OneDrive, Dropbox, etc.;
- Managing devices, including encrypting, limiting, tracking or remote wiping of external storage devices and mobile devices;
- Establishing provisions to automatically revoke all employee or vendor credentials upon termination or resignation; and
- 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 and mobile devices as well as outline their respective encryption requirements. See Appendix F for a description of encryption options. All sensitive data shared with third parties and all wireless connections should be encrypted using industry best practices and standards. Policies concerning 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 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.

Data Loss Prevention Technologies

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 Data Loss Prevention Technologies (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 Fundamentals

- Data at Rest
- Data in Motion
- Data in Use

DLP solutions work in conjunction with existing security and anti-virus tools that companies have deployed on servers, clients 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.[14]

[14] See Symantec DLP Overview http://www.symantec.com/data-loss-prevention.

Data Minimization & De-Identification

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. When it comes to customer information, a good policy which OTA recommends is to 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, de-identified or discarded.[15] Organizations may need to re-validate their business need and decide whether aggregation can be used to minimize the amount and storage length of retained PII. Data retention policies should dictate how long information needs to be retained.

For any sensitive data where there is a valid business reason to retain, consider de-identifying the data. Data de-identification is essentially removing identifiable elements of personal data, so that a particular individual's identity cannot be established from the analysis of the data. It is worth mentioning that data de-identification is not perfect and researchers have been able to re-identify individuals in several instances with supposedly de-identified data.[16]

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.[17] 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 simply disposing of it, a secure deletion step needs to be performed.[18]

---

[15] 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.

[16] https://www.cippguide.org/2010/09/21/de-identification-re-identification/.

[17] http://www.dailymail.co.uk/news/article-1178239/Computer-hard-drive-sold-eBay-details-secret-U-S-missile-defence-system.html.

[18] The National Institute of Standards and Technology (NIST) guidelines for media sanitization. http://www.nist.org/nist_plugins/content/content.php?content.52.

SECURITY BEST PRACTICES

Data loss and identity theft occur from an ever-increasing level of deceptive practices. Social engineering, forged email, malvertising, phishing, and fraudulent acquisition of internet domains are on the rise. Through a multi-stakeholder input process, OTA has developed a list of recommended best practices, which are easy to implement and manage across all industry sectors. In addition, organizations are encouraged to review other controls including the Critical Security Controls for Effective Cyber Defense, published by the Council on Cyber Security. Combined with OTA's best practices outlined below, these controls are a recommended set of actions that provide specific methods to help prevent, detect and contain today's most pervasive threats.[19] For updates visit https://otalliance.org/2015BestPractices.

OTA recommends that all organizations implement the following best practices:

1. **Enforce effective password management policies**. Attacks against user credentials including brute force, sniffing, host-based access and theft of password databases, remain very strong attack vectors warranting the use of effective password management controls. Businesses should review the National Strategy for Trust Identities in Cyberspace, as an alternative for password management.[20] Best practices for password management include:
    a. Use multi-factor authentication (e.g. one-time PINs) for access to administratively privileged accounts. Administrative privileges should be unique accounts monitored for anomalous activity and should be used only for administrative activities[21];
    b. Require users to have a unique password for external vendor systems and refrain from reusing the same password for internal system and personal website logins;
    c. Require strong passwords comprised of an 8 character minimum, including a combination of alphanumeric characters and force password changes every 90 days with limited reuse permitted;
    d. Deploy a log-in abuse detection system monitoring connections, login counts, cookies, machine IDs, and other related data;
    e. Avoid storing passwords unless absolutely necessary and only store passwords (and files) that are hashed with salt or are otherwise encrypted;
    f. Remove or disable all default accounts from all devices and conduct regular audits to ensure that inactive accounts can no longer access your infrastructure; and
    g. Remove access immediately for any terminated employees and any third parties or vendors that no longer require access to your infrastructure.
2. **Least privilege user access (LUA)** is a core security strategy component, and all accounts should run with as few privileges and access levels as possible. LUA is widely recognized as an important design consideration in enhancing data security. It also provides protections against malicious behavior and system faults. For example, a user might have privileges to edit a specific document or email campaign, but lack permissions to download payroll data or access customer lists. Also, LUA controls help to minimize damages from exposed passwords or rogue employees.
3. **Conduct regular penetration tests** and vulnerability scans of your infrastructure in order to identify and mitigate vulnerabilities and thwart potential attack vectors. Regularly scan your cloud providers as well for potential vulnerability points and risk of data loss or theft. Deploy solutions to detect anomalous flows of data which will to help detect attackers staging data for exfiltration.

---

[19] The Critical Security Controls align with the NIST's Security Controls for Federal Information Systems and Organizations (Special Publication 800-53 Rev. 4, April 2013). http://www.counciloncybersecurity.org/critical-controls/.

[20] http://www.nist.gov/nstic/.

[21] Multi-factor authentication adds a second layer of security to username/password authentication by requiring an additional verification method typically from either a trusted device (e.g. a one-time PIN texted to a mobile device) or biometrics. See http://azure.microsoft.com/en-us/documentation/articles/multi-factor-authentication/.

4. **Harden client devices** by deploying multi-layered firewall protections (both client and WAN-based hardware firewalls), using up-to-date anti-virus software, disabling locally- shared folders by default and removing default accounts. Enable automatic patch management for operating systems, applications (including mobile and web apps) and add-ons. All ports should be blocked to incoming traffic by default and disable auto-running of removable media (e.g. USB drives, external drives, etc.). Whole disk encryption should be deployed on laptops, mobile devices and systems hosting sensitive data.
5. **Require email authentication on all inbound and outbound mail** streams to help detect malicious and deceptive email including spear phishing and spoofed email.[22] All organizations should:
   a. Authenticate outbound mail with SPF and DKIM, including parked and delegated sub-domains;
   b. Adopt a DMARC reject or quarantine policy once you have validated that you are authenticating all outbound mail streams;
   c. Implement inbound email authentication to check for SPF, DKIM, and DMARC;
   d. Encourage business partners to authenticate all email sent to your organization to help minimize the risk of receiving spear phishing and spoofed email; and
   e. Require end-to-end email authentication using SPF and DKIM with a DMARC reject or quarantine policy for all mail streams managed or hosted by third parties.
6. **Implement a mobile device management program** requiring authentication to unlock a device, locking out a device after 5 failed attempts, using encrypted data communications/storage, and enabling remote wiping of devices if a mobile device is lost or stolen.
7. **Continuously monitor in real-time** the security of your organization's infrastructure including collecting and analyzing all network traffic in real time, and analyzing centralized logs (including firewall, IDS/IPS, VPN and AV) using log management tools, as well as reviewing network statistics. Identify anomalous activity, investigate, and revise your view of anomalous activity accordingly.
8. **Deploy web application firewalls** to detect/prevent common web attacks, such as cross-site scripting, SQL injection and directory traversal attacks. Review and mitigate the top 10 list of web application security risks identified by the Open Web Application Security Project (OWASP).[23] If relying on third party hosting services, require deployment of firewalls.
9. **Permit only authorized wireless devices** to connect to your network, encrypt communications with wireless devices such as routers, printers, 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 with AES encryption or use of an IPSec VPN.
10. **Implement Always On Secure Socket Layer (AOSSL)** for all servers requiring log on authentication and data collection. AOSSL helps prevent sniffing data being transmitted between client devices, wireless access points and intermediaries.[24]
11. **Review server certificates for vulnerabilities** to assess the risk of your domains being hijacked. Attackers often use "Domain Validated" (DV) SSL certificates to impersonate e-commerce websites and defraud consumers. Sites are recommended to upgrade from DV certificates to an "Organizationally Validated" (OV) or "Extended Validation" SSL (EVSSL) certificates. OV and EVSSL certificates are validated by the Certificate Authority to ensure the identity of the applicant. EVSSL certificates offer the highest level of authentication and verification of a website. EVSSL provides users a higher level of assurance that the site owner is who they purport to be, presenting the user a green trust indicator in a browser's address bar.
12. **Develop, test and continually refine a data breach response plan**. Regularly review and improve the plan based upon changes in your organization's information technology, data collection and security posture. Take the time after an incident to conduct a post-mortem and make improvements to your plan. Conduct regular tabletop exercises testing your plan and personnel.

[22] Email authentication standards and resources https://otalliance.org/eauth.

[23] See OWASP www.owasp.org.

[24] EV SSL Certificates https://otalliance.org/EVSSL.

RISK ASSESSMENT

As an aid to help organizations follow industry and regulatory best practices, an organization should conduct a risk assessment of their infrastructure and privacy practices. In general, there are four steps to risk assessment: threat assessment, vulnerability identification, risk determination and control recommendation. Conducting a risk assessment regularly is critical to proactively identifying and re-mediating risk to your infrastructure. The following questions are provided as a starting point to help an organization develop and customize their own questions and conduct a self-assessment. For updates visit https://otalliance.org/Risks.

1. Do you understand the international and local regulatory requirements and privacy directives related specifically to where your business is based, data resides and where your customer or consumer resides? [25]
2. Do you know the specific data attributes you maintain for all customers? How and where is this data stored, maintained, flowed and archived (including data your vendors and third-party/cloud service providers store or process)?
3. Is the original business purpose for collecting your data still valid and relevant? Can you identify points of vulnerability and risk?
4. Are your encryption, de-identification and destruction processes in alignment with industry accepted best practices?
5. Do you have a 24/7 incident response team and response plan in place? Do employees have reporting and escalation processes?
6. Are you prepared to communicate to employees, customers, stockholders, government regulators and the media during a data loss incident?
7. Do you follow generally accepted security and privacy best practices? If not, are you prepared to explain why? Do you have an audit trail of access to sensitive data, where it is being stored and how it is being used?
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 whom to contact in the event of a breach? Are you prepared to work with your local state and national law enforcement authorities such as the FBI, U.S. Secret Service and Office of the State Attorney General? Or will you have to resort to making these contacts in the "heat of the battle" on an ad hoc basis?
10. Are you (and your Board) willing to sign off on your breach response plan and be accountable that you have adopted best practices to help prevent a breach?
11. Do you understand the security, privacy and notification practices of your vendors?
12. Do you have a data breach response vendor that can have experts on call to assist with determining the root-cause of a breach, identifying the scope of a breach and collect threat intelligence including all data potentially impacted by an incident?

[25] Including a review of Canadian, European Union, and other pertinent country regulations.

THIRD PARTY RISK ASSESSMENT

As businesses innovate with new services and look to decrease costs and add efficiencies, operational units and employees are increasingly relying upon cloud providers and third party vendors to outsource key functions, often involving some of their most sensitive data. Organizations need to conduct risk assessments of any service providers before you entrust your data with them.

Once completed, having an inventory of their policies, practices and notification obligations including an understanding of the implications of any exceptions is essential for business continuity and response, notification, containment and remediation. Reflecting input from dozens of service provider and their clients, the following questions have been developed to help you assess vendors' data security and privacy practices:

1. Please describe what types of data will be stored, what integration offerings are available and will my data be commingled with other customers' data on individual servers?
2. Where physically will you store my data and please describe the physical security of your data centers and offices? Do you use any third parties for services that would impact the service (e.g. for development, QA, help-desk, integration services, etc.) and do any have access to my data?
3. How many staff would have logical access to our data and how are privileged actions monitored and controlled? Please outline your process for background checks on your employees who have access to your data center and critical systems.
4. Please describe the organizational structure for security operations at your company, how often and who conducts risk assessments, and do they include penetration testing?
5. Please provide documentation that you have a comprehensive security program that adhers to a recognized framework (e.g. ISO, COBIT) and is periodically reviewed by a third party? Does this program include third party vulnerability scans and periodic penetration tests on your applications and networks? Please describe how third-party software patches (e.g OS, web apps, database, etc.) are deployed on your systems and how are you protected from DDoS attacks?
6. Do you have any third party certifications or attestations, such as FedRamp, FIPS 140 -2, FISMA and DIACAP, HIPAA, ISO 27001, PCI DSS, TRUSTe or SOC 1/SSAE 16/ISAE 3402?
7. Do you have a security audit report such as SAS70/SSAE16 that we can review and are you hosted in a SAS70/SSAE16 or audited facility?
8. Please describe how your network perimeter is protected, including whether you deploy IPS/IDS, anti-virus (on both service and staff) and have a centralized logging facility?
9. Please provide a description of your disaster and business continuity plans and how often are the plans tested? Do you backup your data and if so, in what form, where and how long do you maintain backups?
10. Please describe your security incident management process and describe any security breaches or issues you have experienced? How do you define a security incident? Please list all data loss incidents which required reporting to regulatory authorities in the past twenty-four months.
11. Who would perform forensic analysis of a breach if one were to occur in your environment?
12. Please provide a description of the password policy for accounts on your service, including account lockout policies?

INCIDENT RESPONSE

Organizations must be prepared to react on several fronts when confronted with a potential data loss incident or breach. It is critical to have an orchestrated response plan in place, including relationships with key vendors and law enforcement. A well-documented response 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 and law enforcement officials), communicate timely, accurate information and consider offering remedies to those affected.

Creating An Incident Response Team

Data breaches are interdisciplinary events that require coordinated strategies and responses. Every functional group within an organization needs to be represented.[26]

As a first step, organizations should appoint an executive with defined responsibilities and decision-making authority regarding a data breach response. This role should be assigned to a corporate officer or high-level executive with decision making authority and ability to provide Board briefings. Equipped with a response 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 ambiguous responsibilities is essential.

Plan Fundamentals

- Create and Empower a Team
- Designate First Responders
- Develop LE Relationships
- Create and Document a Plan
- Create a Notification "Tree"
- Create Communication Templates
- Team Training
- Regulatory and Legal Review
- Budgeting and Funding
- Testing Critique and Refinement

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 an understanding of operations and security.
- In-house legal counsel.
- 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 hours phone numbers including outside legal counsel, PR agency and law enforcement.

[26] 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.

Establishing 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, organizations should consider domain monitoring and take-down services to help reduce the exposure from malicious and phishing sites, and auditing outbound email for compliance to the latest email authentication protocols.[27] 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 in the event of a significant breach.

Vendor selection considerations:

- Subject matter expertise in the relevant industry
- Bonding, indemnification and 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
- Ability to assist 24/7

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 response costs, as well as responsibility for notifications.

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

Prior to a data loss incident, reach out to regulators and law enforcement such as state Attorneys General, FBI, U.S. Secret Service and local U.S. Attorney's Offices. In addition, in many locations there are regional task forces for high technology crimes compromised of a number of federal, state and local law enforcement and business security experts. Become active in the local chapter of InfraGard, an information sharing and analysis partnership between the FBI and the private sector, as well as the Electronic Crimes Task Force sponsored by the U.S. Secret Service; this can help build relationships with both law enforcement and data breach experts.[28]

Creating Response Plans

A comprehensive data breach response plan includes a time-line 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 response plan must have the ability to be "activated" 24/7, including holidays and weekends, as attackers often strike on holidays, weekends and during high volume business times, when staff may be limited. As observed in the case of the Target breach in late 2013, the sheer volume of holiday transactions help to masked attackers' activity and was a "perfect storm."

Your response plan should address the following key questions:

1. What is the overall impact?
2. What are the regulatory obligations and should law enforcement be notified?
3. How will the breach be communicated?

[27] Email Authentication Resources https://otalliance.org/eauth.

[28] To find a local InfraGard Chapter visit https://www.infragard.org.

4. Who needs to be informed and what are the notification requirements (internally and externally)?
5. What data do you or your partners hold and how have you protected it?
6. What changes need to be made to your internal processes and systems to help prevent a similar breach from reoccurring?
7. How damaging will the loss of confidential data be to your customers or partners?
8. How damaging will it be to your business and employees?
9. 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.
10. Are the above answers the same for all of your customer segments?

Forensics, Intrusion Analysis and Auditing

The actual incident response (IR) has several phases. These phases are preparation, detection and analysis, containment and eradication, recovery and post-incident analysis.[29]

An essential element of the analysis phase of a breach response is conducting a forensic examination to help determine the source (root cause) and magnitude (scope) of a breach. A forensic examination is best left to experts, as it is easy to render forensic evidence inadmissible in court by accidentally modifying the evidence or disrupting the chain of custody. It is imperative to have an unaltered original of any data collected, including images of impacted systems, network logs and other data, have it stored in a secure location, with limited access for forensic experts or law enforcement to analyze.

Companies may want to consider retaining outside legal counsel and/or third parties to help conduct a forensic analysis. Having your attorney retain a forensics company should be considered since their reports may be "attorney client privileged" deemed confidential and likely not discoverable in case of a civil lawsuit. If an internal forensic examination is conducted, consider having in-house counsel involved in the investigation to also preserve the confidentially of any findings.

Suggestions on what you should do:

- Secure and protect the physical integrity of any data collected 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 collected data and store an unaltered original of any collected data in a secure location with limited access.
- 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 network and local OS log files in a secure location, including web client and server operating systems, application, mail, firewall, IDS, VPN, DLP and network flows. Due to rotation schedules and possible overwriting, the saving of critical logs need to happen as soon as possible. Review archived logs and collect any that may contain data relevant to the incident.
- Contact your Incident Response executive and in-house counsel prior to performing any forensics on suspected systems. 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.
- Memory and disk image capture/evidence preservation should strongly be considered before placing machines back online.
- Review internal remediation plans and policies, considering any data loss events.
- Document everything that has been done on the impacted systems since the incident was detected.

[29] For more information, see Computer Security Incident Handling Guide, NIST (Special Publication 800-61) http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf.

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, leave them off.
- Do not shut down or unplug any server or device.
- Do not try to image the impacted systems or make copies of data.
- Do not attempt to run programs, including anti-virus 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 any forensic analysis in order to determine the root cause, scope and impact of an incident, including whether any PII, regulated or other sensitive data was impacted or compromised. Businesses may have a number of log types, including transaction, server access, application server, firewall and client operating system. Attackers understand the value of logs, so it is important to protect the logs from attack and routinely back them up.

A best practice is to examine in advance the events, records and data elements being captured by various logs and your log retention policy (both stored locally and archived), in order to ensure appropriate data is being captured to meet your business and regulatory requirements. This best practice applies equally to any logs of vendors, third parties, or cloud service providers where you have an agreement providing log access. A security event manager (SEM) is highly recommended. A SEM is a tool used 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 a data loss incident. In addition, all servers and logs should have times and zones synchronized, to facilitate data analysis throughout an organization's global infrastructure.

Critical Logs

- Firewall
- Transaction
- Database Server
- Application Server
- Point of Sale Systems
- Operating System
- Net Flow / VPN

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 on any potentially impacted systems, 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 staging of data for exfiltration.

If you identify that any data was compromised, speak with your attorney or Chief Privacy Officer to understand your reporting obligations. Ultimately, it is critical to enable appropriate logging (including archiving) 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 critical logs, including stated provisions outlining access as well as to 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 a separate or centralized logging systems with good audit trails for access. Also specify the minimum retention period required for vendors maintain the logs. See Appendix E, Computer Forensics Basics, for further information.

NOTIFICATION REQUIREMENTS

Business decision makers must be familiar with the regulations that govern their industry concerning data breach notification requirements. This includes not only digital data, but also the loss of paper documents or other items containing regulated data. The failure to timely notify the appropriate government agency and affected individuals can result in further governmental inquiries and substantial fines. It is equally important to review your contracts with customers and partners; they may have notification requirements that differ from government regulations and may vary based on customer size and jurisdictions.

Breaches are not "invitation only" events - any regulator can play. This has been underscored by recent actions of the Federal Communication Commission including the levying of a $7.4 million fine against Verizon for privacy violations.[30] Whether or not a regulator has official jurisdiction, businesses need to consider neighboring state requirements in addition to 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 and government regulators. 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 and New York State recently announced a call for revamping laws to map to California's standards.[31] [32]

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.

As of January 2015, there are 47 states, plus D.C., Puerto Rico, and the Virgin Islands with laws that govern data breach notifications.[33] Additionally, an organization may have data breach notification obligations in the EU as well as other countries. Regulations and requirements may vary not only by state, but also by country, industry sector and type of breach, requiring businesses to be familiar with a broad set of regulations. Be up to date on relevant laws, data breach reporting requirements, and contact info for relevant data protection authorities for all jurisdictions in which your organization conducts business.[34] The regulatory landscape is rapidly expanding with renewed calls for Federal breach legislation recently announced by President Obama.[35] See Appendix C for regulations that may affect your business in the event of a breach. Recently, the Federal Trade Commission (FTC) has also exercised its authority concerning data protection and security. The Commission has settled nearly fifty cases alleging that a failure to have "reasonable" data security constitutes an unfair or deceptive trade practice.[36]

---

[30] http://www.fcc.gov/document/verizon-pay-74m-settle-privacy-investigation-0.

[31] 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.

[32] http://www.ag.ny.gov/press-release/ag-schneiderman-proposes-bill-strengthen-data-security-laws-protect-consumers-growing.

[33] See, Intersections Consumer Notification Guide (May 2014).
http://www.intersections.com/library/Consumer_Notification_Guide_May%202014_Final.pdf.

[34] http://www.theworldlawgroup.com/wlg/global_data_breach_guide_home.asp.

[35] White House Fact Sheet: Safeguarding American Consumers & Families,
http://www.whitehouse.gov/the-press-office/2015/01/12/fact-sheet-safeguarding-american-consumers-families.

[36] See http://www.ftc.gov/tips-advice/business-center/legal-resources?type=case&field_consumer_protection_topics_tid=249.

One strategy is to draft a single template letter that meets the requirements of most states; then add one or more additional template letters to address relevant states that have conflicting or more restrictive requirements. A best practice is to periodically request customers to update their user profiles. This aids marketing as well as in any potential compliance efforts related to data breach notifications.

Tips on writing effective an breach notification letter include:

- Take responsibility and apologize.
- 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.
- Write at a sixth grade level, so that any impacted person can easily understand. Older generations or demographics who are not computer literate may not understand terminology or legalese, resulting in increased frustration and anxiety. Consider language options or offer bilingual support.
- Explain to impacted persons 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, likely without the wealth of knowledge a security or privacy professional may have.
- Explain steps your company is taking to help make sure this type of incident will not happen again.
- Lastly, apologize again and mean it.

The Guide provides a sample breach notification letter in Appendix B to assist in preparing data breach notice letters for affected individuals. 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.

Organizations found to be in violation of breach notification laws or industry regulations 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.[37] *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 for insurance policy considerations.

[37] 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 re-occurrence.

Communicating Appropriate and Effective Responses

A well-executed communications plan not only minimizes harm and potential legal liability, but it can also enhance a company's overall reputation. Effective communications 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.

Figure 6 - Critical Audiences

Communication plans needs to typically address six critical audiences:

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

The communications plan should have a set of pre-approved web page and templates and phone script prepared along with frequently asked questions drafted. Staff needs to anticipate call volumes, take steps to minimize hold times and consider the need for multi-lingual support.

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 websites postings.[38] Companies should monitor the use of social networking sites such as Facebook, Twitter and blogs to track consumer sentiment during a breach incident.

Most organizations realize too late or in the heat of the incident that there are subsets of 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.

Recommended components and 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 an estimate of the number and type of customers?
- What action is the business taking to assist the 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 (include 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)?

[38] 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.

Providing Assistance and Remedies

Typical offers to affected parties 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.[39] A data response plan 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. Quickly delivered remedies can provide the opportunity to turn a bad situation into a positive brand experience.

Training, Testing and Budgeting

A well-prepared data breach response plan is at risk if employees charged with its administration are not adequately trained and prepared. Organizations must allocate staff time and budget to properly execute their plan. In order for a data lifecycle and stewardship program to be successful, it is critical that the response plan be reviewed by key stakeholders, fully tested, and updated regularly (consider a quarterly review) to address changes in the company, business models, services or in the threat landscape. A best practice includes running quarterly desktop 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 and Readiness Training

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

As discussed, DLP 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 investigate, report findings and 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.[40]

---

[39] 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.").

[40] See Department of Homeland Security Stop Think Connect Campaign http://www.dhs.gov/stopthinkconnect.

Funding and 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, third party forensic costs and higher merchant card processing fees. The heat of a crisis is not the best time to make vendor selections. Also consider pre-contracting services for affected individuals, including 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. Annually review your coverage to ensure it is keeping pace with regulatory requirements. (see Appendix C for a partial list of cyber-insurance considerations).

Budgeting Considerations

- Physical Security
- Security and Monitoring Services
- Forensic Specialists
- Employee Training
- PR and Crisis Mgt.
- Legal/Compliance
- Capital Costs/Equipment
- Cyber Insurance
- Goodwill and Contingency

Post Incident 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 with desktop exercises during the year (including weekends); critiquing them to identify and remediate any deficiencies. Such evaluation should look to confirm and remedy the root cause of a breach, including any back doors that may exist for future exploits.

Any breach should also include a postmortem 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.

Key questions to ask and document after a breach incident:

- 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?
- How were we treated by the press? Was the reporting accurate?
- How did our spokesperson(s) perform?
- What lessons have we learned?
- What internal policies and procedures need to change?
- What was the impact to employee morale and operations?
- What can we do better next time?

INTERNATIONAL CONSIDERATIONS

Businesses need to be aware of the breach notification laws and guidelines for all of the countries in which their customers reside and where their data may be located.[41] 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).

The proposal includes the following strategic objectives:[42] [43]

- Strengthen individual's rights.
- Harmonize rules and enforcement throughout the EU.
- 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.

Considerations

- Opt-In verses Opt Out
- Honoring "Do-Not-Track"
- Safe Harbor Provisions
- Reasonable Security
- Adequate Notice
- "Right to be Forgotten"
- Data Server Locations
- Definition of PII
- Government Access

Companies that are active in the EU, offer services to EU citizens and handle personal data 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 to their published privacy policy and in developing new products and services, as the deadline for implementation is early 2015.[44]

In May 2014, the Court of Justice for the European Union issued a landmark ruling on the right to be forgotten. In this case, the Court ruled that search engines must remove links to sites from search results for a person, where the information linked to is inaccurate, inadequate, irrelevant or excessive.[45] The EU Commission proposed in 2012 to expand the Right to be Forgotten rules to require data controllers (e.g. a company that offers services to European consumers) who make personal data public to delete

[41] See supra, note 34.

[42] European Data Protection Supervisor (EDPS) http://bit.ly/1jtVR00.

[43] http://www.computerweekly.com/guides/Essential-guide-What-the-EU-Data-Protection-Regulation-changes-mean-to-you.

[44] Data Protection Reforms http://bit.ly/1hISa5X.

[45] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (PDF), European Commission, 2012, Article 17 "Right to be forgotten and to erasure".

personal information where the data is no longer necessary for the purpose it was collected for, the subject withdraws consent, the storage period has expired or processing the data does not comply with other regulations. And, in December of 2014, the Article 29 Group representing the 28 EU Data Protection Agencies issued a set of guidelines on implementing the right to be forgotten.[46]

In addition to the EU, the following countries have recently revised regulations that may impact global organizations. Readers are encouraged to review regulations in every company they operate in.

Australia

Organizations collecting personal information in Australia need to be aware of three pieces of legislation. These are the The Do Not Call Register Act 2006, which prevents organizations (other than certain exempt public interest organizations and those with an existing relationship with an individual) from engaging in telemarketing activities in relation to phone numbers on the register. The Spam Act 2003 prevents the sending of unsolicited commercial electronic messages, and strictly requires an opt-in for email and SMS marketing. It is well enforced by the Australian Communications and Media Authority (ACMA). The Privacy Act 1988 regulates the handling of personal information by organizations through the application of a single set of Australian Privacy Principles (APPs).

The Privacy Act generally only applies to entities with an annual turnover of over AUD$3 million, subject to some limited exceptions. The Privacy Act was amended in March 2014 including an increase of the maximum fine to AUD$1.7 million per incident. Some key changes include a modified definition of the scope of personal information to include any information or opinion about an identified individual, or an individual who is reasonably identifiable. This change expands the ambit of the Privacy Act to include information about an individual which, when combined with other information that an entity has access to (e.g. through a related organization), could enable that individual to be identified. The Act also contains new provisions regarding cross-border disclosures of personal information which require that an organization subject to the Privacy Act which discloses personal information to an international entity first takes reasonable steps to ensure the overseas recipient does not breach the Australian Privacy Principles. The regulating authority provides additional guidelines.[47]

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.[48] However, the requirements for breach notification vary. In May 2010, the Alberta Personal Information Protection Act (PIPA) became the first private sector privacy law to require breach notification. PIPA requires organizations to notify the 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."[49] 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, (CND).[50]

Although the federal Personal Information Protection and Electronic Documents Act (PIPEDA) does not contain breach notification requirements, the general requirements for accountability and safeguarding personal information can be interpreted to require some form of notification. The Office of the Privacy

[46] http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/index_en.htm.

[47] http://www.adma.com.au/ http://www.oaic.gov.au/privacy-policy-summary.

[48] The Federal Personal Information Protection and Electronic Documents Act applies to commercial activity across Canada except for the following provinces, 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.

[49] PIPA Section 34.1.

[50] PIPA Section 59(1)(e.1) and (2).

Commissioner of Canada has published voluntary guidelines for responding to breaches.[51] A draft bill would amend PIPEDA to require organizations to notify the Commissioner as well as affected individuals of any "breach of security safeguards" involving personal information if it is reasonable to believe that the breach creates a real risk of significant harm to the individual. Canada's Anti-spam Legislation (CASL) became 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.[52]

New Zealand

New Zealand has recently updated national legislation regarding privacy.[53] It may be worth noting that parts of the privacy act, including the aspects relating to breach notification are currently being reviewed and will likely be further enhanced. Further, New Zealand Government agencies must also comply with the official information act.[54] New Zealand also has 'anti-spam' legislation covering all forms of unsolicited electronic messaging.[55]

[51] http://www.priv.gc.ca/information/guide/2007/gl_070801_02_e.asp.

[52] http://www.crtc.gc.ca/eng/casl-lcap.htm.

[53] http://www.legislation.govt.nz/act/public/1993/0028/latest/DLM296639.html and https://www.privacy.org.nz.

[54] http://www.legislation.govt.nz/act/public/1982/0156/latest/DLM64785.html and http://www.ombudsman.parliament.nz/resourc.

[55] http://www.legislation.govt.nz/act/public/2007/0007/latest/DLM405134.html and http://www.dia.govt.nz/services-anti-spam-index.

SUMMARY

Worldwide we are a data-driven society, which benefits consumers and businesses alike. Unfortunately, attackers and deceptive businesses have also recognized the value of data and ease of targeting unsuspecting companies and consumers. Compounded by the blended attacks from State sponsored actors and hactivists and exploits with increased precision, the need for every business to take a holistic view of data security and privacy protection practices is a business necessity.

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 the reliance on 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, academia 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 an attacker. 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; and
- 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 a data lifecycle and stewardship program and breach response plan to help protect your 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 businesses be 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 of their documents and photos. They need to take steps to protect their data and devices. This includes: ensuring they are using current browsers, automatically patching and updating their software and applications to having users think before they indiscriminately click on links, open email attachments 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.

APPENDIX A - RESOURCES

Online Trust Alliance

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

Data Breach Resource Center - https://otalliance.org/breach

Email Authentication - https://otalliance.org/eauth

Extended Validation SSL Certificates - https://otalliance.org/EVSSL

Mobile App Privacy & Security - https://otalliance.org/mobileBP

Security & Privacy Enhancing Best Practices - https://otalliance.org/2015BestPractices

Security & Privacy Risk Assessment - https://otalliance.org/Risks

Federal Trade Commission

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

Peer-to-Peer File Sharing: A Guide for Business
http://www.ftc.gov/tips-advice/business-center/peer-peer-file-sharing-guide-business

Mobile App Developers: Start with Security
http://www.ftc.gov/tips-advice/business-center/mobile-app-developers-start-security

Marketing Your Mobile App: Get It Right from the Start
http://www.ftc.gov/tips-advice/business-center/marketing-your-mobile-app-get-it-right-start

Video: Mobile Apps http://www.ftc.gov/news-events/audio-video/video/mobile-apps

California

Data Security Breach Reporting http://oag.ca.gov/ecrime/databreach/reporting

Privacy Enforcement and Protection http://oag.ca.gov/privacy

Identity Theft http://oag.ca.gov/idtheft

New York State

Information Exposed: Historical Examination of Data Breaches in New York State
http://www.ag.ny.gov/pdfs/data_breach_report071414.pdf

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

Privacy & Identity Theft http://www.ag.ny.gov/internet/privacy-and-identity-theft

Washington State

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

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

Industry & Non-Profits

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 Council - https://www.identitytheftcouncil.org/

Identity Guard / Intersections Inc.

- 7 Steps to Breach Readiness
  http://www.intersections.com/library/7stepstodatabreach_040611%20FINAL.pdf
- Data Breach Consumer Notification Guide
  http://www.intersections.com/library/Consumer_Notification_Guide_May%202014_Final.pdf
- Identity Protection http://www.intersections.com/IDProtection.html

InfraGard - California – Bay Area Chapter http://bit.ly/1KYxK8q

InfraGard - New York City Metro Chapter
https://www.infragard.org/RI0TmLh7O2Dt20vmk5kbMgchE68pns5EuN4QDsWBWDc%2525253D!

InfraGard National Capital Region Members Alliance http://bit.ly/1yBCgTM

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

Privacy Rights Clearing House www.privacyrights.org/data-breach

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

RiskBased Security https://www.riskbasedsecurity.com

SiteLock 10 Ways To Keep Hackers Away From Your Data
http://blog.sitelock.com/2014/08/25/10-ways-to-keep-hackers-away-from-your-data/

Symantec

- 2014 Internet Security Threat Report
  http://www.symantec.com/security_response/publications/threatreport.jsp
- Data Breach Calculator https://databreachcalculator.com/

TRUSTe

- Privacy Research http://www.truste.com/resources/#/Privacy_Research
- Protecting Customer Information http://www.truste.com/resources/privacy-best-practices

US Department of Education: Breach Response Checklist
http://ptac.ed.gov/sites/default/files/checklist_data_breach_response_092012.pdf

U.S. Federal Communication Commission http://www.fcc.gov/cyberforsmallbiz

APPENDIX B - NOTIFICATION TEMPLATE

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]

The data accessed may have 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].[57]

[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].[58]

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] 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.

[58] 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.

If Social Security Numbers Were Involved

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 impostor 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. 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 Numbers Were 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].

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.

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/.

If Drivers License or Identification Numbers Were 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 Medial, Health or Insurance Information Number 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.[59]

Sincerely, [Name] [Title][60]

[Contact Information]

[59] 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.

[60] 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.

APPENDIX C - REGULATORY

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

- Individual state laws where a business has nexus or customers residing [61]
- Country laws if any of the lost data pertains to residents [62]
- Payment Card Industry Data Security Standards (PCI DSS) [63]
- Sarbanes-Oxley Act [64]
- Health Insurance Portability and Accountability Act (HIPAA),[65] including the HITECH Act of 2009, including the HITECH Breach Notification Rule [66]
- 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 [67]
- Federal Financial Institutions Examine Council (FFIEC) Guidelines [68]
- Fair Credit Reporting Act [69], including the Fair & Accurate Credit Transactions Act, Red Flags Rule [70]
- Federal Trade Commission Guidelines and Requirements [71]
- Children's Online Privacy Protection Act (COPPA), (updated) [72]
- International Standards Organization (ISO) security standards [73]

[61] See infra note 18.

[62] See infra note 20.

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

[64] 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.

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

[66] 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.

[67] 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.

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

[69] http://www.ftc.gov/enforcement/statutes/fair-credit-reporting-act.

[70] 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.

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

[72] A federal rule that applies to "operators of commercial web sites and online services directed to children under 13" http://www.ftc.gov/tips-advice/business-center/childrens-online-privacy-protection-rule-six-step-compliance-plan-your.

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

APPENDIX D - CYBER INSURANCE

CYBER SECURITY LIABILITY AND INSURANCE CONSIDERATIONS [74] [75]

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 a 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.

[74] K & L Gates Cyber Insurance http://bit.ly/LNE1d3.

[75] See http://www.dhs.gov/sites/default/files/publications/cybersecurity-insurance-read-out-report.pdf.

APPENDIX E - 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 help provide law enforcement the best opportunity at finding 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 the right processes have been put in place to preserve relevant data before a breach occurs. The types of processes include:

- Performing regular backups of systems and logs, and make sure to maintain 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 both successful and failed authentication attempts.
- Maintaining a database of file hashes for the files of common OS and application deployments, and using file integrity checking software on particularly important assets.
- Maintaining records (e.g., baselines) of network and system configurations.
- Establishing data retention policies that support performing historical reviews of system and network activity, complying with requests or requirements to preserve data relating to ongoing litigation and investigations, and destroying data that is no longer needed.

When performing forensics during incident response, 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.

If you have contacted law enforcement, be prepared to answer a series of questions. These will likely include the following: [76]

1. What evidence do you have that you were victimized?
2. What is the chronology of the event?
3. What is the 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 the 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 is your server environment (operating system, server software and 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.

[76] For a drill-down on computer forensics, see the NIST Guide to Integrating Forensic Techniques into Incident Response http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf.

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 laptop and mobile devices, which often contain sensitive data. As encryption standards continually evolve, readers are recommended to check the web site of their device and operating system provider and third party tools.

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 as outlined in this guide.

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) providing 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.

FileVault2 in Mac OS X Lion provides 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:

- PGP: http://www.symantec.com/business/whole-disk-encryption
- 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

File Encryption:

- Windows (XP through Windows 7), Encrypting File System (EFS): http://windows.microsoft.com/en-US/windows7/What-is-Encrypting-File-System-EFS
- 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://www.apple.com/iphone/business/it/security.html
- Android Encryption & Security https://support.google.com/a/answer/1408902?hl=en

ACKNOWLEDGMENTS

Support and contributions to the Guide reflect input from numerous organizations including the Identity Theft Council, Open Security Foundation 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. Additional support was provided by the 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 Washington DC.

Special thanks to the support from OTA members and report underwriters including Act-On Software, Agari, American Greetings Interactive, AVG, Bryan Cave LLP, DigiCert, Epsilon, Holland & Knight LLP, Listrak, IID, Intersections, Message Systems, Microsoft, Publishers Clearing House, Sailthru, SiteLock, Symantec, TRUSTe and Verisign. In addition, OTA Advisors including Mary Berk, Jennifer Fein, Barry Brailey, Shaun Brown, David Daniels, Mark Goldstein, Arun Raghu, Liz Shambaugh and Joe St Sauver provided strategic direction and technical edits and updates to this report.

ABOUT THE ONLINE TRUST ALLIANCE

https://otalliance.org | +1-425-455-7400 | 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.