2016
DATA PROTECTION AND BREACH READINESS GUIDE

Providing prescriptive advice to help businesses optimize privacy and security practices, reducing the risk and impact of data loss incidents

Updated May 16, 2016
Released January 26, 2016

ACKNOWLEDGEMENTS

The Guide is a collaborative effort reflecting input from industry leaders and government agencies. Contributing organizations include Act-On Software, American Greetings, AVG Technologies, Bryan Cave LLP, Dorsey & Whitney LLP, Epsilon, Holland & Knight LLP, The Goodman Law Firm, ICONIX, Identity Guard, Identity Theft Council, LifeLock, Microsoft, New Zealand Internet Task Force, nNovation LLP, Privacy Rights Clearing House, Publishers Clearing House, PwC, SiteLock, Symantec, Threatwave, TrustSphere, TRUSTe, Twitter, Yesmail and Verisign. In addition, special thanks to the Federal Bureau of Investigation, Federal Communications Commission, Federal Trade Commission, the U.S. Department of Commerce, the U.S. Department of Homeland Security and the U.S. Secret Service.

Underwritten in Part by Grants and Donations From:

IDENTITY GUARD.	Intersections Inc. provides innovative based solutions that help consumers manage risks and make better informed life decisions. Under its IDENTITY GUARD® brand the company helps consumers monitor, manage and protect against the risks associated with their identities and personal information.
LifeLock®	LifeLock, Inc. is a leading provider of proactive identity theft protection services for consumers and consumer risk management services for enterprises. LifeLock's threat detection, proactive identity alerts, and comprehensive remediation services help provide peace of mind for consumers amid the growing threat of identity theft.
Symantec.	Symantec Corporation is the global leader in cybersecurity. Operating one of the world's largest cyber intelligence networks, we see more threats, and protect more customers from the next generation of attacks. We help companies, governments and individuals secure their most important data wherever it lives.
VERISIGN™	Verisign is a global leader in domain names and Internet security, enables Internet navigation for many of the world's most recognized domain names and provides protection for websites and enterprises around the world. Verisign ensures the security, stability and resiliency of key Internet infrastructure and services.

TABLE OF CONTENTS

INTRODUCTION

The 2016 Data Protection & Breach Readiness Guide (Guide) has been developed to help organizations of all sizes – from startups to large enterprises – enhance their data security, adopt responsible privacy practices and be prepared for a data breach incident. Published annually since 2009, the Guide includes content to help aid a broad range of stakeholders – from business and technical decision makers to privacy and security professionals to web and application developers.

The goal of the Guide is to help organizations assess risks, issues and solutions to accelerate the development of data breach readiness plans. While it is recognized "one size does not fit all," the adoption of the principles will aid in prevention, detection and remediation related to a data loss incident, while helping prevent identity theft and keeping the victim company from being victimized.

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 to implement a broad set of operational and technical best practices that help protect your company and your customers' personal data. The second step is to be 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 company's 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 against a determined attacker, the best practices advocated by OTA and outlined in this Guide can help greatly reduce a company's attack surface and the impact of a data loss incident.

The 2016 Guide has been updated to reflect industry best practices and the global regulatory framework, including the recent passage of the General Data Protection Regulation (GDPR) and introduction/debate of the EU-US Privacy Shield. The Guide has expanded discussions of risk assessment, cyber insurance, remedies and supply chain management, highlighting the expanded threats to business data. In addition, several appendices have been reformatted to provide worksheets to aid organizations in their assessments. They can be downloaded individually at https://otalliance.org/Breach.

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 Guide 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. To receive updates subscribe to the OTA newsletter at https://otalliance.org/subscribe and follow OTA on Twitter at @otalliance.

EXECUTIVE SUMMARY

The threat level has never been higher for any organization. As recent headlines attest, no company, organization or government agency is immune to targeted attacks by persistent, skilled adversaries. Their unprecedented success has led many to question the efficacy of solely prevention-focused countermeasures. Rather, there is recognition that a more modern approach includes a multi-layer strategy in which early detection, attack containment and recovery measures are considered together. Having processes in place to detect, mitigate, respond to and remediate the impact of such attacks is imperative for all organizations from startups to global enterprises.

For the past several years we have proclaimed the previous year as the "year of the breach," overtaking prior years in the numbers and impact of breaches. 2015 was no exception. With a 23% increase vs the prior year, 2015 broke the previous all-time record, set in 2012, for the number of reported data breaches.[1] In the first half of 2015 more than 245 million data records were stolen every day, equivalent to 16 records per second.[2] This trend is continuing with the Identity Theft Resource Center reporting 2016 year-to-date breaches are up nearly 24%.[3] Further, over the past ten years the type of data stolen and how it can be used indicates increasing sophistication – from 2007 theft of TJX Companies' credit card info; to 2011 breach of Sony business data; to 2014 attack on JP Morgan and other banking data which was used to manipulate stock prices; to the 2015 OPM breach which included fingerprint data.[4]

2015 made its mark not only in absolute numbers but, equally as troubling, in the expanded scope and impact of breaches and exploits. Victims included nearly every segment of the population including consumers, government employees, and children. Going beyond credit card data, recent breach targets have included insurance, medical, voter and political interest data. Few were spared and the collective impact of breaches will not be known for years to come.

The Office of Personnel Management (OPM) breach contained over 21 million records including security clearance applications with social security numbers, employment history and fingerprints, placing government employees and contractors at risk far beyond that of a typical credit card compromise. VTech, a multinational toy company experienced a breach impacting 6.3 million children, including their names, home addresses, passwords, and even selfies and chat logs.[5]

In the mobile sector, a T-Mobile breach exposed some 15 million customers, in another incident 70 million inmate phone calls were compromised, putting at risk attorney-client privilege, and the infamous

---

[1] Risk Based Security https://www.riskbasedsecurity.com/2015-data-breach-quickview/

[2] Gemalto http://www.gemalto.com/press/Pages/Gemalto-Releases-Findings-of-First-Half-2015-Breach-Level-Index.aspx

[3] Identity Theft Resource Center http://www.idtheftcenter.org/images/breach/ITRCBreachReport2016.pdf

[4] See Dark Reading http://www.darkreading.com/endpoint/10-biggest-mega-breaches-of-the-past-10-years/d/d-id/1325374?_mc=NL_DR_EDT_DR_daily_20160506&cid=NL_DR_EDT_DR_daily_20160506&elqTrackId=5a9462f4232942eb99e25ecc3139c124&elq=a0d4e980f13a42a28b6eeb8336e8e9c3&elqaid=69649&elqat=1&elqCampaignId=21003

[5] VTech https://motherboard.vice.com/read/hacked-toymaker-vtech-admits-breach-actually-hit-63-million-children

Ashley Madison breach impacted 37 million "socially active" adults.[6] [7] Topping the charts was the Anthem breach of 78.8 million records.[8]

The year ended with the disclosure of over 191 million American citizens' voter data including their political party affiliation and voting record. Combined, these paint a comprehensive picture of a user's interests, motivations, and personal views on a range of personal and sensitive subjects and are the path to identity theft and socially engineered exploits targeting both personal and business data.[9]

BEYOND CONSUMER DATA

What is not revealed in these and other headlines is the increased focus on (and success in) targeting businesses and their proprietary and confidential data. With increased precision through the use of micro-targeted spear phishing and malvertising, there is a growing ability to compromise higher net worth entities including professional services organizations and their respective C-suite. [10] According to the U.S. Federal Bureau of Investigation, since January 2015, Business Email Compromise (BEC) scams designed to socially engineer the employees of a business increased 270%[11]. Such malicious emails are sent from domains which closely resemble a known domain and/or forge the "from" address of a known sender and typically not covered by insurance companies.[12]

Virtually all industries are being targeted – from legal and accounting to architectural and engineering firms. Moving past credit cards, cybercriminals are increasingly obtaining proprietary business data and / or client records and deploying ransomware and cyber blackmail. Ransomware took the number two "crimeware" spot for 2015.[13] Criminals are holding data hostage, or alternatively threatening to expose data, attempting to extort millions of dollars from companies who wish to avoid the risk of public embarrassment, data destruction and loss of intellectual property.[14]

> *"Cyber-Blackmail of corporate data is becoming widespread, increasing the impact and costs for businesses and their employees worldwide"*

---

[6] 70 Million Inmate Calls http://www.slate.com/blogs/business_insider/2015/11/12/anonymous_hacker_released_70_million_jail_calls_indicating_routine_violation.html

[7] Ashley Madison breach http://www.forbes.com/sites/thomasbrewster/2015/07/20/ashley-madison-attack/

[8] Anthem breach http://www.computerworld.com/article/2888267/anthems-now-says-788m-were-affected-by-breach.html

[9] Voter Data http://www.forbes.com/sites/metabrown/2015/12/28/voter-data-whats-public-whats-private/

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

[11] FBI press release https://www.fbi.gov/cleveland/press-releases/2016/fbi-warns-of-rise-in-schemes-targeting-businesses-and-online-fraud-of-financial-officers-and-individuals

[12] BEC fraud http://krebsonsecurity.com/2016/01/firm-sues-cyber-insurer-over-480k-loss/

[13] Verizon Data Breach Investigation Report 2016 http://www.verizonenterprise.com/verizon-insights-lab/dbir/

[14] 2015 Ransomware trends http://www.darkreading.com/endpoint/2015-ransomware-wrap-up/d/d-id/1323424

With the increased rise in ransomware over the past six months targeting health care providers and professional services firms[15] it is clear that criminals are increasingly learning the value of the data and the impact to a business. Recent ransom demands have shifted from opportunistic extortion to one of market based extortion or "cyber-surge pricing." Leveraging users' data posted on social media including Facebook and LinkedIn, has increased the ability for hackers to successfully create socially engineered exploits targeting high net-worth business victims.

Raising the complexity and business risk are the far reaching changes in the legal and regulatory framework. October brought the end of 15 year Safe Harbor agreements with the EU, bringing forward the proposed replacement EU-US Privacy Shield.[16] In December the European Union passed a far reaching EU General Data Protection Regulation. This directive unifies the legal framework across the 28-member European Union, bolstering European's privacy rights including strict data collection regulations and fines of up to 4 percent of a company's global revenue.[17]

Currently the U.S. Federal Communications Commission has proposed new reporting requirements including reporting to itself as the regulatory authority, to law enforcement and to consumers. While focused on ISPs and mobile carriers, this proposal may accelerate the development of national breach laws. (See Regulatory Landscape on page 38)

Consumers are increasingly concerned. According to a 2015 survey from the Pew Research Center, 93% of adults say that being in control of who can get information about them is important. Further, 90% say that controlling what information is collected about them is important; 88% say it is important that they not have someone watch or listen to them without their permission. Most troubling is that only 9% say they are "very confident" their credit card data will stay private and secure. Combined, these are key reference points for all organizations to consider when amassing consumer data.[18]

Since OTA's first report in 2009, we have learned that no organization is immune. As larger quantities of diversified data are amassed and the reliance on third party service providers increases, every business must be prepared for an inevitable loss of data. The facts highlight the need for startup and global enterprises to shift attitudes and make data security and privacy part of every employee's responsibility.

2015 Breach Highlights & Impact

23% increase in reported/disclosed incidents (RBS)

93% could have been prevented – OTA

15% due to employees – OTA

$3.8 MM Average cost per breach (PI)

$154 Cost per record (PI)

Sources: OTA – Online Trust Alliance, (PI) Ponemon Institute
RBS – Risk Based Security- Data Breach Report

[15] Hollywood Presbyterian Medical Center in California in February and MediStar health network in Maryland in March 2016.

[16] Data regulators reject Privacy Shield https://www.theguardian.com/technology/2016/apr/14/data-regulators-reject-eu-us-privacy-shield-safe-harbour-deal

[17] EU Data Protection Directive http://www.nytimes.com/2015/12/16/technology/eu-data-privacy.html

[18] Pew Research Center - Americans' Attitudes About Privacy, Security & Surveillance http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/

OTA's analysis of publically reported breaches for 2015 revealed 93% were avoidable. 15% were due to lack of internal controls resulting in employees' accidental or malicious events and 65% the result of actual hacks. The balance of incidents were primarily attributed to lost or stolen devices (4%) and fraud (5%). Lost, stolen, or misplaced documents accounted for 4% of all incidents.

Key avoidable causes of data loss incidents include:

- Not patching known / public vulnerabilities.
- Misconfigured devices / servers.
- Unencrypted data and/or disclosed keys.
- Use of end of life devices, operating systems and applications.
- Employee errors - lost data, files, drives, devices, computers, improper disposal.
- Accidental disclosure via email, posting on public sites.
- Business Email Compromise & social exploits.

THE IMPACT OF A BREACH

The impact and resulting costs can be staggering to a business and its ability to remain solvent. According to the Ponemon Institute's 2015 global breach survey, on a global basis the average cost of a breach was $3.8 million, with a cost of $154 per individual record lost or compromised.[19] The post breach impact on a company's customers can also be significant, ranging from the legal and regulatory costs to damaged brand reputation with resulting consumer abandonment and lost sales.

Small and large companies alike run the risk of a data breach, and the implications of a breach to the organization can be grave. The business shock 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 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 and security 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.

While businesses may be aware of the threat, they are not necessarily equipped to respond effectively. Businesses must acknowledge that company-wide panic and disruption can occur. Viewing breaches as a "technical issue" belonging to the IT department is a recipe for failure. Instead, businesses need to

[19] 2015 Ponemon Institute Global Cost of Breach Report – sponsored by IBM http://www-03.ibm.com/security/data-breach/. Note data for U.S. only breaches (62 incidents) was $217 per record and an average cost of $6.5 million. http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=SEW03055USEN&attachment=SEW03055USEN.PDF

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 systems as well as those of its vendors. 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.

Not only must companies be prepared for a breach, but they must also 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 damaged their reputation and opened them up for potential lawsuits and regulatory scrutiny. Having a mechanism to review and respond to vulnerability reports is now considered an essential part of an organization's security strategy.[20]

These trends suggest a need for increased adoption of responsible privacy and voluntary security best practices, 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 Fundamentals

- Data stewardship and privacy is everyone's responsibility
- Data collection and privacy policies need continual review
- Many businesses collect some form of PII (personally identifiable information)
- Data breaches or losses will occur
- Every organization needs to have a current and tested breach plan

OTA advocates that every organization handling data, ranging from email addresses to more sensitive 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 or exceed the expectations of consumers. Consumers very often expect security even if they don't explicitly ask for it, and are surprised when breaches occur and their security expectations are not met.[21]

[20] NTIA http://www.ntia.doc.gov/other-publication/2015/multistakeholder-process-cybersecurity-vulnerabilities

[21] Developing Secure Software http://www.cnet.com/news/gary-mcgraw-on-developing-secure-software-q-a/#!

WHAT HAVE WE LEARNED?

Breach incidents are a wake-up call for all organizations, whether they are non-profits, governmental agencies, or companies with proprietary and employee data. While a compromised credit card amounts to an inconvenience, the consequences of other breaches can be much more significant. Looking ahead, we anticipate data analytics will play an increasing role in helping identify and raise the alarm in discovering a threat. Such tools can provide visibility into what a threat is doing, where it's leaving the network and what data is being removed or modified. There are several key lessons to keep in mind.

1. There needs to be a critical shift in attitude regarding roles and responsibilities of data stewardship and security. The emphasis is moving from an IT focus to a company-wide issue.
2. Data is often a company's most valuable asset and, as a result, requires the appropriate level of protection and care.
3. The level of data security you apply must be commensurate with the data held. In other words, the level of security in place should reflect the potential risk and damage to consumers and to the company should that information be inappropriately accessed.
4. Only collect and retain data that has a business purpose. Protect it while it's held, and then delete it when it's no longer needed. Criminals cannot steal or hold hostage data you don't have.
5. All businesses need to think about the consequences of a data breach and what could happen. It's dangerous to think you aren't going to be a target. Consumer, employee and corporate data is a valuable commodity. When combined or appended with other breached data, it increases in value.

> *"There will never be perfect security. That said, a prudent company should be paranoid recognizing that a breach or accidental loss will occur.*

6. Security and privacy are not absolutes and must evolve. Organizations need to regularly review how they store, manage and secure their data. A plan needs to include prevention, detection, notification, remediation and recovery processes and operations.
7. Security is beyond your walls. As more businesses rely on cloud services and third-party providers, a risk assessment must be conducted prior to usage and on an ongoing annual basis. Supplier risk management isn't a one-time event. It needs to be done repeatedly before a contract is signed, and regularly after the contract is signed. Management teams should ask for regular (weekly, monthly, quarterly or annual) reports from vendors specifying their internal data security processes, data removal methods, tools and technology implementation and documentation.
8. Being prepared is not just for Boy Scouts. An incident plan needs to incorporate both disaster planning and training to help prevent, detect, mitigate and respond. Just like first responders, employees must be trained, equipped and empowered to deal with a data loss incident. Planning is the key to maintaining online trust and the vitality of the Internet, while helping to ensure the continuity of business.

RISK ASSESSMENT

Risk assessments are critical for every organization including the Board and C-suite. Increasingly, organizations and their executives are being held accountable and facing lawsuits for the failure to uphold fiduciary duties. To help address this risk the Department of Justice has provided guidelines for cybersecurity awareness for board members.[22]

While there is no absolute guarantee of protection from a data loss event, Boards and management should evaluate associated legal and compliance risks, ranging from accounting and financial practices to personnel policies to data security. The following lists serve as a baseline for such assessments, including internal systems and, increasingly of importance, third-party vendors and service providers. While organizations may also consider other key questions, these lists have been developed to help organizations complete a basic risk assessment of their infrastructure and privacy practices as they apply to their business sector(s) and operating geographies. Such risk assessments need to be conducted regularly to aid in the identification of potential vulnerabilities. A complete and objective review of these audits serves as the foundation for developing an effective data security and response strategy. (See Appendix H for sample risk assessment forms.)

BOARD, OFFICER & INVESTOR QUESTIONS

1. What makes our company or service an appealing target for hackers and cyber criminals?
2. What is the worst-case scenario; what are our major assets and "crown jewels" that could be compromised?
3. What will be the impact if we are targeted and (a) the breach is made public; (b) data is held for ransom; and/or (c) our corporate or consumer data is destroyed?
4. What are the risks *to* our infrastructure, business partners, vendors and third-party service providers?
5. What are the known risks *from* our infrastructure, business partners, vendors and third-party service providers?
6. Have we completed an audit / risk assessment for all potential acquisitions? Do our current privacy policy and data practices reflect our business practices?
7. Do we have a valid business purpose for all of the data we have and continue to collect?
8. What are our data minimization and destruction policies and procedures?
9. Is our cyber insurance coverage adequate? Have we completed a coverage gap analysis and do we fully understand the exclusions? Are we prepared for regulatory enforcement and/or lawsuits?
10. How current, complete and tested is our data breach incident plan?
11. Are we using industry best practices and do we adhere to a cybersecurity framework reflecting our current countries of operation and types of business operations?

[22] Board Cyber Risks https://www.sec.gov/News/Speech/Detail/Speech/1370542057946

OPERATIONAL RISK ASSESSMENT

1. Do we understand the international regulatory requirements and privacy directives related not only to where our business physically operates but where our data and customers reside?
2. Do we know all specific data attributes we maintain for all customers? How and where is this data stored, maintained, flowed and archived (including data our vendors and third-party/cloud service providers store or process)?
3. Is the original business purpose for collecting our data still valid and relevant? Can we identify points of vulnerability and risk?
4. Are our encryption, de-identification and destruction processes in alignment with industry accepted best practices and regulatory requirements?
5. Do we have a 24/7 incident response team and response plan in place? Do employees have reporting and escalation processes?
6. Are we prepared to communicate to employees, customers, stockholders, government regulators and the media during a data loss incident?
7. Do we follow generally accepted security and privacy best practices? If not, are we prepared to explain why? Do we have an audit trail of access to sensitive data, where it is being stored and how it is being used?
8. Does our privacy policy reflect our data collection and sharing practices, including use of third parties? Have we audited our site to confirm we are in compliance?
9. Do we know whom to contact in the event of a breach? Are we prepared to work with our local state and national law enforcement authorities such as the FBI, U.S. Secret Service and State Attorney Generals? Or will we have to resort to making these contacts in the "heat of the battle" on an ad hoc basis?
10. Are we (and our Board) willing to sign off on our breach response plan and be accountable that we have adopted best practices to help prevent a breach?
11. Do we understand the security, privacy and notification practices of our third-party vendors and service providers?
12. Do we 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?

THIRD PARTY RISK ASSESSMENT

As businesses innovate, look add efficiencies and be more agile, employees are increasingly relying upon cloud providers and third-party vendors to outsource key functions, often involving some of their most sensitive data. Assessments and audits of third-party capabilities need to continue after a vendor is on-boarded to help monitor for potential lapses in security and privacy practices as well as ascertain the adoption of new technologies and standards. Companies should consider penetration testing, scan vendor sites, and review vendor privacy policies regularly for vulnerabilities and insecure configurations.

According to a survey of 200 Chief Information Security Officers, on average it takes nearly 18 days to evaluate the security of a cloud provider. Top causes for rejecting a vendor include lack of adequate encryption (46%) and lack of data loss prevention (43.9%).[23] These statistics underscore the importance of having an inventory of a vendor's policies, practices and notification obligations.

Asking vendors the following questions/items will help you assess vendors' practices and your risk factors:

1. Given our data includes [describe what types of data will be stored], what integration offerings are available and will our organization's data be commingled with other customer's data?
2. Describe the physical security of your data centers.
3. Do you use any third parties (e.g., for development, QA, help-desk, integration services, etc.) that would impact the servicing of our account and do they have access to our organization's data?
4. How is staff who have access to client data managed; how are privileged actions monitored and controlled? Outline your process for background checks on your employees. Include a description of the password policy management and account lockout policies.
5. Describe the organizational structure for security operations at your company.
6. Do you have a comprehensive security program that adheres to a recognized framework and is periodically reviewed by a third-party, including vulnerability scans and periodic penetration tests?
7. How are you protected from DDoS attacks?
8. List all 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. (See Appendix I for Acronyms)
9. Do you have security audit reports such as SAS70/SSAE16 that can be reviewed?
10. 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.
11. Provide an overview of your backup practices including where and how long you maintain backups. Are backups encrypted? Have you tested recovering data from a backup?
12. Describe your security incident process and testing. How do you define an incident? Please list all incidents which required reporting to affected individuals or regulators in the past two years.

[23] Survey of Cloud Providers Risks https://www.skyhighnetworks.com/csa-report/

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. Helping to address these threats, through a multi-stakeholder process, OTA developed a list of recommended best practices. By design these are easy to implement and manage across all industry sectors. In addition to these practices, 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.[24]

OTA recommends that all organizations implement the following best practices.

1. Encryption of data at rest / in storage and in transit is a fundamental security requirement and the respective failure is frequently cited as the cause for regulatory action and lawsuits. If an organization properly encrypts its data with strong, industry-standard cryptography (e.g., at a minimum AES-128, ideally AES-256 bit encryption) and properly manages cryptographic keys used, it can effectively contain the effects of an attack. Even in the event of an intrusion where encrypted data (but not the corresponding cryptographic keys) are stolen, the data would be useless to the attacker. Encryption of data breaches may preempt the requirement of consumer notifications as specified by individual State breach regulations. It is essential that companies carefully consider not only the strength of encryption, but also the proper management of cryptographic keys. See Appendix F for more information.
2. **Enforce effective password management policies**. Attacks against user credentials, including spear phishing, 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.[25] Best practices include:
    a) Use multi-factor authentication (e.g. smartcard and PINs in addition to a password) for access to administratively privileged accounts. Administrative privileges should be unique accounts monitored for anomalous activity and should be used only for administrative activities[26];
    b) Consider requiring employees to use a password manager to generate and store passwords. Such tools can help require a unique password for each external vendor systems and refrain from reusing the same password for internal systems and personal website logins;

[24] NIST's Security Controls for Federal Systems and Organizations (Publication 800-53 Rev. 4, April 2013).
[25] National Strategy for Trusted Identities in Cyberspace http://www.nist.gov/nstic/
[26] Multi-factor authentication adds a layer of security to username/password authentication by requiring an additional verification method See http://azure.microsoft.com/en-us/documentation/articles/multi-factor-authentication/.

c) Deploy a log-in abuse detection system to monitor connections, login counts, cookies, machine IDs, and other related data;

d) Avoid storing passwords unless the passwords (and files) are hashed and salted or are otherwise encrypted.[27] A password manager, as suggested above, can help;

e) Remove or disable all default accounts from all devices and conduct regular audits to ensure that inactive accounts can no longer access your infrastructure;

f) Remove access immediately for any terminated employees and any third parties or vendors that no longer require access to your infrastructure.

3. **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.

4. **Conduct regular security design and code reviews including penetration tests** and vulnerability scans to identify and mitigate vulnerabilities. Regularly scan your cloud providers' sites and services for potential vulnerability points and risk of data loss or theft. Deploy solutions to detect anomalous flows of data which will help detect attackers staging data for exfiltration.

5. **Secure 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. In addition, another best practice to consider is to implement app control technology (such as Applocker or Device Guard) to better protect against the types of malware. [28, 29]

6. **Require email authentication on all inbound and outbound mail** servers to help detect malicious email including spear phishing and spoofed email.[30] All organizations should:

   a) Authenticate outbound mail with SPF and DKIM, including parked and sub-domains;

   b) Implement inbound email authentication to check for SPF, DKIM, and DMARC;

   c) Recommend business partners to authenticate all email sent to your organization to help minimize the risk of receiving spear phishing and spoofed email;

---

[27] Hashing http://www.webopedia.com/TERM/H/hashing.html

[28] Microsoft AppLocker https://www.microsoft.com/en-us/download/details.aspx?id=40330

[29] Microsoft Device Guard https://technet.microsoft.com/en-us/library/dn986865(v=vs.85).aspx

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

d) 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.

7. **Implement a mobile device management program** requiring authentication to unlock a device, locking out a device after a determined number of failed attempts, using encrypted data communications/storage, and enable remote wiping of devices if a mobile device is lost or stolen.
8. **Continuously monitor in real-time the security** of your organization's infrastructure including collecting and analyzing all network traffic 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.
9. **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).[31] If relying on third-party hosting services, require deployment of firewalls.
10. **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.
11. **Implement Always On Secure Socket Layer (AOSSL)** for all servers requiring log on authentication and data collection. AOSSL helps prevent sniffing of data being transmitted between client devices, wireless access points and intermediaries.[32]
12. **Review server certificates for vulnerabilities** to assess the risk of your domains being hijacked. Attackers have targeted "Domain Validated" (DV) SSL certificates to impersonate websites and defraud consumers. Sites are recommended to upgrade from DV certificates to "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, providing assurance that the site owner is who they purport to be by presenting the user a green trust indicator.[33]

[31] See OWASP www.owasp.org

[32] Always On SSL https://otalliance.org/AOSSL

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

13. **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. After every incident conduct a post-mortem and make improvements to your plan. Conduct regular tabletop exercises testing your plan and personnel.

14. **Establish and manage a vulnerability / threat intelligence reporting program.** The majority of breaches and vulnerabilities are discovered by external sources, and the ability to respond to and manage reports of threats is key to mitigating the impact of an incident. Failure can amplify the public relations and reputational damage along with damages to impacted parties. To help encourage such reporting, many organizations are establishing "bug bounty" programs.[34]

DATA LIFECYCLE & STEWARDSHIP

A well-designed, actionable data management program is an essential first step in not only meeting compliance and regulatory obligations, but perhaps more importantly, to demonstrate to consumers and business partners that an organization has taken reasonable steps to protect data from abuse and loss. Developing a program can help minimize risk to consumers, business partners and shareholders, while increasing the value of the brand and the long-term viability of a business. Shifting from a compliance mindset to one of stewardship is key to an organization's ability to maximize protection of their data and corporate reputation. As outlined in Figure 1, data stewardship requires a comprehensive view of a range of issues from the business, regulatory and consumer perspectives.

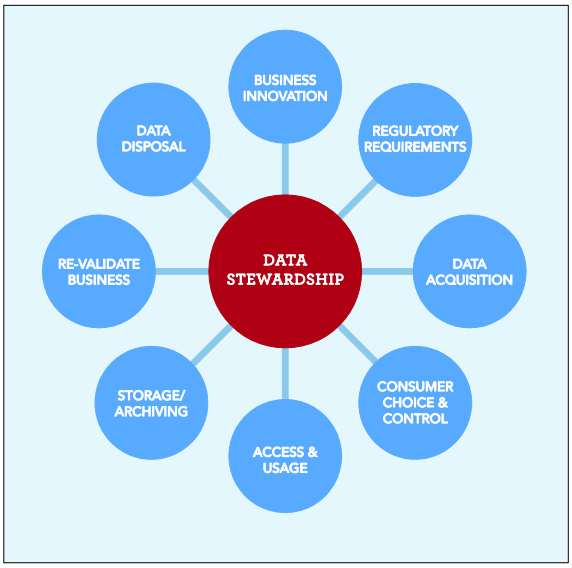

Figure 1 - Data Stewardship

At a minimum, data management programs need to focus on several key fundamentals. First, privacy policies and practices evolve. Just as business is dynamic, so too privacy policies require ongoing review and updating. Second, every organization should assume that they collect one or more forms of covered data 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, as outlined in Figure 2, ensures the confidentiality, integrity and availability of data collected, used or stored by an organization through the life of the data, including the ultimate

[34] Bug Bounty Programs Overview https://en.wikipedia.org/wiki/Bug_bounty_program

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 primary data lifecycle stages include: collection, storage, usage, sharing, archiving and destruction.

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 revalidate the business purpose of any data collected. Ask questions – is the data required, relevant and does it need to be retained? Whether 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 U.S. and abroad. Applying yesterday's rules may no longer be applicable in today's data driven economy.

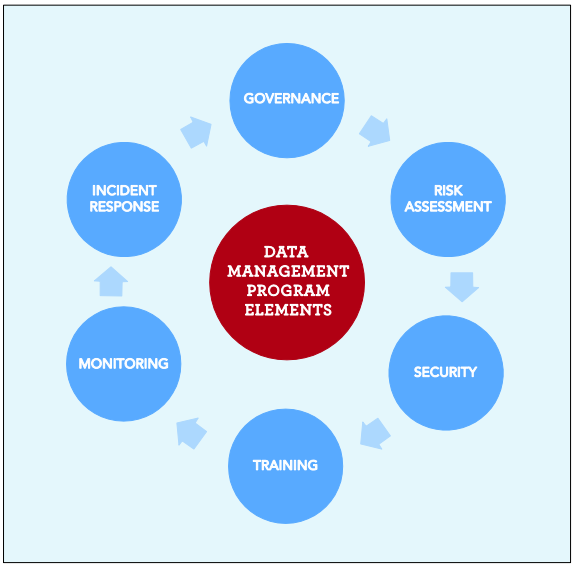

Figure 3 - Data Management Program Elements

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. Key components of a data lifecycle and stewardship program are outlined in Figure 3.

An essential part of creating a data lifecycle and stewardship program is designating a data protection officer and creation of cross-functional response teams. Such teams typically include privacy professionals, security specialists, legal and operational managers, and are becoming commonplace in the U.S. and other geographies. Such roles are no longer optional and in the recent EU General Data Protection Regulation passed in late December 2015, organizations must designate Data Protection Officers by 2017. [35]

As illustrated in Figure 4, data may be collected, used, transmitted, and shared in multiple dimensions. Information is gathered from multiple devices and platforms, both online and offline. Examples include

[35] EU Data Protection Directive Summary http://europa.eu/rapid/press-release_IP-15-6321_en.htm

retail point of sale systems, in-store mailing lists, event registrations and ecommerce shopping carts. A major challenge is the evolving legal definitions of "covered" or "sensitive" information.

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

As a best practice, companies need to adopt leading security and privacy practices, including implementing policies for BYOD and device management. With the advent of IoT connected and smart devices in the workplace, organizations need to survey and establish restrictions to help prevent the devices from becoming a back door to an organization's network.

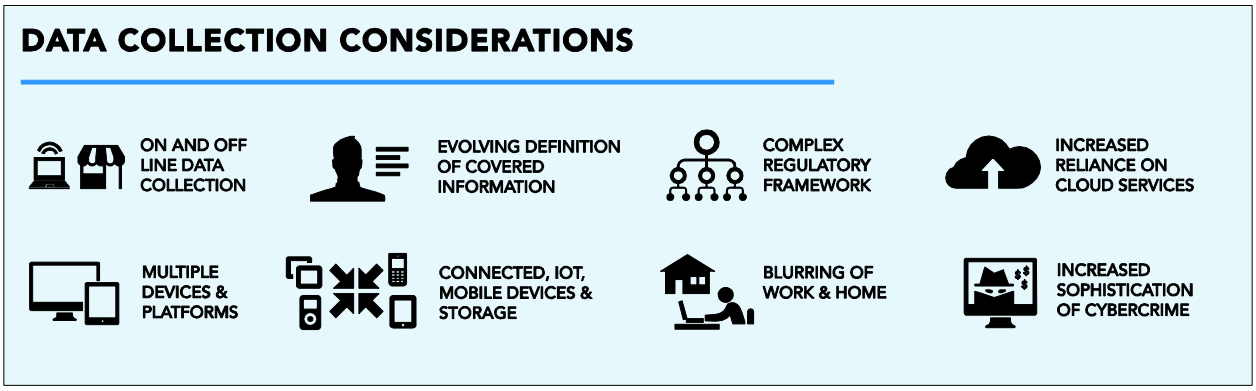

Figure 4 – Data Collection Considerations

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 minimize the risk and mitigate the 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 data 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.[36] The scheme your organization chooses is less important than 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 client devices, 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 which is at rest or in use even if not stored on mobile devices is also at risk of being compromised. Steps to encrypt and sandbox data in use 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. An example of a breach incident this past year included privately branded digital photo processing service used by some of the largest retailers included Costco, placed family photos and digital memories at risk due to an attack on their shared supplier.[37]

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.[38] 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.

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

---

[36] 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 systems: http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf

[37] Initial report of PNI breach http://www.imaging-resource.com/news/2015/07/20/costco-rite-aid-and-tesco-also-affected-by-pni-digital-media-security-breac; confirmation of breach http://www.databreaches.net/cvs-confirms-customer-data-stolen-in-pni-digital-media-attack/

[38] 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.

- 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
- Data sharing and collaboration sites

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 (DLP));
- Digital Rights Management (DRM), to control and limit access of proprietary or copyrighted data (if applicable);
- Auditing or confirming that cloud storage services 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 AWS, 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;
- 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, IoT 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 both inside and outside of their organizations. In addition to protecting regulated data, many organizations are also looking to help protect intellectual property and other sensitive business data within the organization that may pose a threat to their enterprise but where protection of such data may not be regulated.

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

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

DLP Fundamentals

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

It should be noted that DLP solutions can also raise data privacy concerns – particularly for solutions that may automatically read emails of employees that may be personal in nature. Organizations that consider deploying such solutions need to be aware of global employee privacy policies.

DLP solutions work in conjunction with existing security and anti-virus tools in environments such as:

- Data at rest – Data stored within the network perimeter.
- Data in motion – Data transmitted over the internet through multiple protocols (HTTP, SMTP, FTP, etc.) to locations outside the enterprise.
- Data in use – Typically defined as data being created and modified.[39]

[39] 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.[40] 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 in several instances researchers have been able to re-identify individuals with supposedly de-identified data.[41] It should be noted that de-identification standards may differ among different industries.

DATA DESTRUCTION POLICIES

A common mistake is not purging unneeded data. Organizations need to identify reasonable and lawful disposal methods based on the sensitivity of the data. 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, 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, Comcast agreed to pay more than $25 million for disposal of documents with customer's names, addresses and phone numbers.[42] 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.[43]

---

[40] Data aggregation is any of a number of processes in which information is gathered and expressed, for a variety of purposes.

[41] De-Identification & Re-Identification https://www.cippguide.org/2010/09/21/de-identification-re-identification/

[42] Comcast $25M Settlement http://fox40.com/2015/12/15/comcast-prosecutors-reach-25m-waste-disposal-settlement/

[43] 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/

INCIDENT RESPONSE FUNDAMENTALS

Being prepared for the inevitable breach or data loss incident is a requirement for every organization. No different than being prepared for an on-the-job injury, potential fire or earthquake, companies must develop, maintain and continually test and update their response plans.

Organizations must be prepared to react on several fronts when confronted with a report of a potential data loss incident. All reports must be taken seriously and fully evaluated. It is critical to have an orchestrated response plan in place, including relationships with vendors and law enforcement.

A well-documented response plan is only as good as the training and readiness of the incident team. While the size and details of a plan's fundamentals may vary, at a minimum organizations need to consider the fundamentals as outlined below.

Plan Fundamentals

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

INCIDENT RESPONSE TEAMS

Data breaches are interdisciplinary events that require coordinated strategies and responses. Every functional group within an organization needs to be represented.[44] 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 able 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.

TEAM SELECTION CRITERIA:

- An executive with decision-making authority, reporting to the Board.
- 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, policy, marketing and communications team).
- Staff with access and authority to key systems for analysis and back-up.

[44] This includes, but not limited to 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.

- A single individual (and a delegate) with the authority and access to management for decisions.
- A summary of internal and external contacts with after-hours phone numbers including outside legal counsel, PR agency, insurance, law enforcement and identity theft prevention and mitigation services.

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 to audit outbound email for compliance to the latest email authentication protocols.[45] 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
- On-call executives and/or key management

Agreements should include risk management language and an assessment of your data. (See Appendix I). 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.

Prior to a data loss incident, reach out and make introductions to local regulators and law enforcement such as your state Attorneys General's office, FBI, U.S. Secret Service and local U.S. Attorney's Offices. The U.S. Secret Service has established the Electronic Crimes Task Force with regional offices. [46] In addition, there are regional task forces for high technology crimes comprised of a number of federal, state and local law enforcement and business security experts including InfraGard, an information sharing and analysis partnership between the FBI Cyber Task Force and the private sector.[47] Appendix E includes a form to collect information commonly requested by law enforcement when investigating a breach incident.

---

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

[46] To locate your local U.S. Secret Service Electronic Crimes Task Force visit http://www.secretservice.gov/investigation/ and scroll to the bottom of the page and enter your zip code.

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

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. Mock drills should be conducted on a quarterly basis to effectively learn from and hone response skills.

Your response plan should at a minimum address the following key questions:

1. What is the overall impact of the breach (number of consumers, types of data….)?
2. What are the regulatory obligations and should law enforcement be notified?
3. How will the breach notification be communicated?
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 PII and/or 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

An incident response has several phases. These phases are preparation, detection and analysis, containment and eradication, recovery and post-incident analysis.[48]

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, and 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 in advance of an incident as well as when one occurs. Having your attorney retain a forensics company should be considered since their reports may be "attorney client privileged" (deemed confidential) and 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 preserve the confidentially of any findings.

Upon learning of a possible breach or intrusion, one of the first things to determine is if the attackers still have access to your system. This is critical because it impacts an organization's response significantly. In general, if the criminals are gone one can proceed with forensic analysis to determine both the scope of the attack and assess endpoint vulnerabilities. If, however, the hackers are still in your system, these long-term questions need to be balanced with quarantine and containment — turning your top priority to ensuring that attackers are unable to cause any more harm or steal any more data.

The typical first response is to try to protect your network by shutting down systems and hoping that attackers move on. Unfortunately, this often destroys valuable cached data or limits the ability to determine the root cause of your breach while also allowing the attackers to observe your remediation tactics.

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.

[48] 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

- 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 needs 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 servers back online (as directed by forensics experts).
- 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.

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 unless directed by forensics experts (internal or external).
- 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 help determine the root cause, and impact, including whether any PII or other sensitive data was impacted or compromised. Businesses may have a number of log types, including transaction, server access, application server, firewall and operating systems. Attackers understand the value of logs, so it is important to protect them from attack.

Critical Logs

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

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). Doing so will help ensure appropriate data is being captured to meet your business and regulatory requirements. This best practice applies equally to logs of vendors, third parties, or cloud service providers where you have an agreement providing log access. A security incident and 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 that 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.

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 copy 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 that your contracts with third-party data providers and vendors provide businesses access to critical logs, including stated provisions outlining access, as well as to logs of other related servers and historical data. Consider including a contract provision 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. In addition, specify the minimum retention period required for vendors to maintain the logs. See Appendix D, Forensics Basics, for further information.

CYBER INSURANCE CONSIDERATIONS

The sophistication and severity of breaches in 2015 has contributed to an increase in demand among enterprises for cyber insurance policies. Cyber insurance is a relatively new product with over seventy-five carriers offering stand-alone insurance products. Unfortunately there is a lack of actuary data and little uniformity in the policies and terms being offered making simple comparisons difficult. Annual premiums are projected to grow tenfold from $2 billion today to $20 billion by 2025, underscoring the demand for coverage for organizations of all sizes.[49] While there is exponential growth in policies, significant coverage deficiencies exist. In Target's breach in 2013, they only had coverage for 38% of their losses underscoring costs to major corporations.[50] Further, it can be unclear whether data breach is covered under legacy commercial general liability policies. Newer policies tend to explicitly exclude data breach liability and older policies without such exclusions are still being addressed in the courts.[51]

The cost of cyber insurance coverage can vary significantly, and the premium is typically dependent upon a company's security practices, past history and business sector. As part of the underwriting process, carriers are increasingly demanding qualitative assessments of their policyholders' cyber security defenses (as opposed to quantitative assessments historically used to underwrite property and casualty risks), this can extend the time for coverage and resources required to complete applications. Carriers often now require an audit and risk assessment including not merely the security infrastructure, but also review of the data types collected and retained, and whether a disaster response plan is in place with controls that will help prevent, detect and mitigate the impact of a data loss incident. The NIST Cybersecurity Framework and best practices outlined in this guide are frequently used for such assessments.[52]

When selecting cyber insurance policies, it is imperative to use an insurance broker that has expertise advising clients on the purchase of cyber insurance. In addition, look for experience with other insurance areas including Crime, D&O, Professional Liability and Property. These lines may also respond to cyber events or have exclusions and it is important to be able to identify, evaluate and address any gaps. Given the lack of standardization in coverage between insurance carriers, it is difficult to make comparisons of the price per million dollars of coverage without a detailed understanding of a specific carrier's cyber insurance policy. On the one hand, the purchase of 'fit for purpose' cyber insurance has been successfully used to offset financial impacts of some of the biggest cyber security breaches in recent years, including high profile breaches in the retail and healthcare sectors. On the other hand, companies have been

[49] Cyber Insurance Projections http://www.propertycasualty360.com/2016/01/01/cyber-insurance-2015-inside-a-robust-and-rapidly-c?slreturn=1452796687

[50] Target Coverage http://www.businessinsurance.com/article/20140806/NEWS07/140809889

[51] Portal Healthcare and Travelers Insurance http://www.ibamag.com/news/data-breach-covered-under-commercial-general-liability-policy-court-rules-30373.aspx

[52] NIST Cybersecurity Framework http://www.nist.gov/cyberframework/index.cfm

surprised by limited coverage and broadly worded exclusions resulting in denied claims. An experienced broker with expertise in cyber insurance will help companies navigate these pitfalls.

Cyber risk is complex and constantly changing, which makes it very difficult to evaluate exposure, particularly when combined with the lack of historical data to properly underwrite and price policies. Broadly worded exclusions should be clarified as these have resulted in disputes and litigation with carriers asserting companies have failed to comply with the coverage conditions. Recent cases have cited the failure to follow minimum required practices concerning file transfer protocol settings on internet servers, maintaining security patches, assessing information security exposure, and detecting network intrusions. Another case resulted from socially engineered exploits. In at least one incident, insurers have refused to pay on the grounds that the event was the result of an indirect incident.[53] [54] Such exclusions should be thoroughly understood and negotiated.

The purchase of cyber insurance will often involve the CFO, General Counsel, Chief Risk Officer and/or the Board, who may be unfamiliar with cyber security practices. It is important to understand a company's aggregate financial exposure to a cyber-attack, the company's appetite to hold that risk, the retentions / deductibles that the company can sustain and the coverage limits that are appropriate. Increasingly 3rd party contracts require "cyber" coverage. If entering into a contract requiring you to carry such insurance, be certain to define "cyber" such that the correct coverage is secured in order to avoid possible disputes in the future. In its 2015 annual report, the Federal Insurance Office encouraged insurers to hold their business partners, suppliers and customers to the risk management principles outlined in the 2014 National Institute of Standards and Technology Cybersecurity Framework.[55]

For large companies, multiple insurance carriers are often needed to "build a tower" sufficient to cover the company's exposure, and in some cases there may be insufficient capacity available from insurers to reach the limits desired by a company. For cyber insurance considerations, see Appendix C.

Common cyber insurance coverages include:

- Liability (defense costs, settlements, judgments)
- Incident response (including forensics, public relations, breach notification, credit monitoring)
- Loss/replacement of electronic data
- Expenses for cyber extortion
- Regulatory fines
- Business interruption, including lost revenue

---

[53] MBIC Insurance http://www.networkworld.com/article/2984989/security/cyber-insurance-rejects-claim-after-bitpay-lost-1-8-million-in-phishing-attack.html

[54] Company sues insurance company for $480,000 http://krebsonsecurity.com/2016/01/firm-sues-cyber-insurer-over-480k-loss/

[55] Annual Report on the Insurance Industry by the U.S. Department of the Treasury https://www.treasury.gov/initiatives/fio/reports-and-notices/Documents/2015%20FIO%20Annual%20Report_Final.pdf

NOTIFICATION REQUIREMENTS

Business decision makers must be familiar with the regulations that govern data breach notification requirements. This includes not only digital data, but also can include loss of paper documents or other items containing regulated data. The failure to notify the appropriate government agency and affected individuals among others in a timely manner can result in governmental enforcement, litigation and brand damaging publicity. It is very 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, (FCC) levying a $25 million fine against ATT for privacy violations.[56] In April 2016, the FCC published a Public Notice of Proposed Rule Making; specifying breach reporting requirements. If adopted they could become the national standard for all organizations.[57] Whether or not a regulator has official jurisdiction, businesses need to consider state, federal and foreign requirements in addition to jurisdictions with a high number of customers. Since many state, federal and foreign regulations specify time requirements for notification, it is important to be prepared in advance 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. [58] [59] In 2015, other states made revisions including Washington which expanded its breach notification bill and Connecticut which passed legislation regarding data security.[60] [61]

Knowing these requirements in advance will significantly improve your organization's ability to mitigate consumer angst and increase compliance, while reducing the risk of 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

---

[56] ATT Privacy Breach https://apps.fcc.gov/edocs_public/attachmatch/DOC-332911A1.pdf

[57] FCC NPRM http://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db0401/FCC-16-39A1.pdf

[58] State of California data security breach reporting http://oag.ca.gov/ecrime/databreach/reporting. Effective January 1, 2014, California amended its definition of "Personal Information" to include "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.

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

[60] Washington State Data Breach Notification Bill http://www.atg.wa.gov/news/news-releases/attorney-general-s-data-breach-notification-bill-approved-house

[61] Connecticut https://www.cga.ct.gov/2015/ACT/PA/2015PA-00142-R00SB-00949-PA.htm

breached, may have an expectation to be provided remediation and credit monitoring services free of charge.

As of January 2016, there are 47 states, plus Washington, D.C., Guam, Puerto Rico, and the Virgin Islands with laws that govern data breach notifications.[62] Additionally, an organization may have data breach notification obligations in the EU and Canada as well as other countries. Regulations and contract 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 information for relevant data protection authorities for all jurisdictions in which your organization conducts business.[63] Recently, the Federal Trade Commission (FTC) issued guidance concerning data protection and security from over fifty cases alleging that a failure to have "reasonable" data security constitutes an unfair or deceptive trade practice.[64]

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 that customers update their user and contact information. This helps to develop customized notices based on where the user resides.

Tips on writing an effective breach notification communication:

- Take responsibility, be humble and apologize if possible.
- 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.
- Be confident that your information is accurate. Avoid making assumptions or speculation about facts that you may not know.
- Write at a sixth grade reading level, so that any impacted person can easily understand. Many consumers may not be computer literate and may not understand technical terminology or 'legalese' resulting in increased frustration and anxiety. Consider language options or offer bilingual support.
- Explain options to impacted persons 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 you are taking to help make sure this type of incident will not happen again.
- Lastly, apologize again and mean it.

The Guide provides sample breach notification letters 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,

---

[62] Summary of Breach Legislation http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

[63] World Law Group data breach guide http://www.theworldlawgroup.com/wlg/global_data_breach_guide_home.asp

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

these 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 regulatory enforcement or litigation. 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.[65] Readers are encouraged to work with a law firm specializing in data breaches. In addition, a firm's cyber insurance policy should be reviewed for coverage. See Appendix C for cyber insurance considerations.

Figure 5 – Critical Audiences

COMMUNICATING APPROPRIATE AND EFFECTIVE RESPONSES

A well-executed communications plan not only minimizes harm and potential legal liability, but 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 the messaging and order of communications may vary.

Communication plans typically need to address six critical audiences:

1. Internal teams including Board, employees and investors,
2. Key partners and customers,
3. Regulators and credit 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 pages, templates and phone scripts 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.

[65] Different types of data events may require different responses. In most scenarios, the reporting messaging should include how the incident occurred, the scope, what steps are being taken to help individuals from becoming victims of identity theft and what is being done to prevent a potential re-occurrence.

Spokesperson(s) must be prepared to respond to media inquiries. The plan should anticipate the need to provide access to service and information that helps impacted individuals; this includes emails, written correspondences and website postings.[66] Companies should monitor the use of social networking sites such as Facebook, Twitter and blogs to track consumer sentiment during a breach incident.

Organizations may 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 key at-risk segments such as the elderly, the disabled, minors, and others.

Recommended components and facts to include in external communications:

- Incident description including what, how and when the incident occurred
- What types of data were lost or compromised?
- Who was impacted, including an estimate of the number and affected customers?
- What actions are the business taking to assist affected persons or organizations?
- What steps are being put in place to help assure it will not happen again?
- What is being done to minimize the impact of identity theft for affected customers?
- Where can affected customers go for information (include contact info and toll free number)?
- How will the organization keep affected customers informed?

PROVIDING ASSISTANCE AND REMEDIES

Offers to affected parties may 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, driver license and Social Security numbers; however, these offers are increasingly being provided for a broader range of data loss scenarios, including actual or anticipated identity theft. Affected individuals expect companies to take responsibility and protect them from potential consequences that go beyond fraudulent credit card charges, such as opening a new financial account or taking out a loan in their name, which can be challenging to resolve. 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.

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 the services your company will offer affected customers. Remedies can help offset user inconvenience and thus mitigate damage to an organization's brand. A pre-negotiated plan can also save the company money through discounted rates. Organizations without pre-negotiated plans may pay premium prices for expedient emergency solutions. 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. As companies are increasingly responding to class-action law suits, data defense

[66] 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 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

metrics should be tracked such as whether or not the breach is increasing the risk of consumers' exposure to fraud relative to the general population.

As impacted consumers may be anxious and concerned, live operator assistance should be a required part of the service plan with call centers ideally based in the same country as the victims and with multi-lingual capabilities and options.[67] Because identity protection coverage typically expires within 12-24 months, companies should consider the business practices of the firms they select as service providers. Some service firms may attempt to retain consumers and solicit them to sign up for related products and services. Such business practices could reflect back on consumer's perception of the company that recommended them. [68, 69]

In addition to offering identity theft and credit monitoring services, organizations may want to considering offering credit counseling and making donations to 501(c)(3) charitable organizations that work to help prevent breaches, support consumer privacy and/or provide consumer counseling. Such donations can be leveraged in the media as well as in settlement proposals with regulatory authorities. Companies should consider offering the collection of customer-facing services detailed in Appendix G.

TRAINING, TESTING & 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 and/or 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 coordinating with external public relations and communication vendors.

[67] Support options should be provided for hearing impaired.

[68] Note when social security numbers are involved it is recommended 24 months of monitoring be provided.

[69] Consumer Federation of America, ID Theft Best Practices, http://consumerfed.org/pdfs/CFA-Best-Practices-Id-Theft-Services.pdf

EMPLOYEE AWARENESS AND READINESS TRAINING

Do not wait for an incident to occur to consider training. Once an initial plan is developed, providing baseline privacy training is an important step in preparing employees for a breach. Feedback from the training and desktop exercises should be incorporated into plans. 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. Training should not only include responding to a breach, but educating employees on the risk and implications from a loss as well as how to avoid falling for phishing and related socially engineered exploits.

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. 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 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.[70]

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, 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 & Monitoring Services
- Forensic Specialists
- Employee Training
- PR & Crisis Management
- Legal/Compliance
- Capital Costs/Equipment
- Cyber Insurance
- Goodwill and Contingency

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

POST INCIDENT ANALYSIS

Carefully analyze past events to improve future plans and minimize the possibility of future recurrences. Conducting penetration testing of systems, scans, 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), critique them to identify and remediate any deficiencies. Such evaluations 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?

REGULATORY LANDSCAPE

The regulatory landscape has changed dramatically in the past 18 months. On April 1, 2016, the U.S. Federal Communications Commission released a Notice of Proposed Rule Making, outlining specific privacy protections and data breach requirements for ISPs and carriers.[71] If adopted they have far reaching implications to both those organizations under their regulatory oversight as well as edge providers. Separately Congress' efforts in the United Stated to develop a unified regulatory breach notification framework combining the 47 separate state laws have stalled; the EU, Canada, Australia and other counties have moved forward on both data breach and privacy legislation. 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.

EUROPEAN UNION

The view of data privacy in the European Union (EU) has impacted businesses worldwide as represented by the European Court of Justice's decision in October 2015 to overturn the 15 year old decision which had approved that the U.S.-EU Safe Harbor agreement provided an adequate level of protection for the data of EU citizens. Among other things, the court cited concerns that the data may be subject to U.S. government surveillance calling for the limits and safeguards regarding access by national-security services to Europeans' data.[72] Until this recent ruling, the Safe Harbor allowed over 4,500 U.S. based companies the ability to store personal data about Europeans on U.S.-based computer servers without running afoul of Europe's strict privacy rules. To address the confusion and business challenges created by the loss of Safe Harbor, the European Commission and US Department of Commerce announced the EU-US Privacy Shield in February 2016[73]. The Privacy Shield proposal, however, has been rejected by the pan-European data regulatory group Article 29 and its future remains unclear.

EU Considerations

- Opt-In vs 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

[71] FCC Proposed Rules to Protect Broadband Consumer Privacy https://www.fcc.gov/document/fcc-releases-proposed-rules-protect-broadband-consumer-privacy

[72] Safe Harbor Advisory http://export.gov/safeharbor/

[73] European Commission press release http://europa.eu/rapid/press-release_IP-16-216_en.htm

More far-reaching will be the impact of the EU's General Data Protection Regulation (GDPR). After years of discussion the final draft of the GDPR was agreed to in December 2015 (and fully passed by the EU Parliament in April 2016) with the overall goal of putting people in control of their data and making businesses more accountable for their data practices. The GDPR includes the following strategic objectives:[74]

- Strengthen individuals' 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.

Companies that are active in the EU, offer services to EU citizens and/or handle their personal data are subject to GDPR which will enable people to better control their personal data and aid businesses which benefit from reduced red tape and a single legal framework. For many organizations the GDPR will be a game changer and likely have a global impact. The GDPR will facilitate cross-border cooperation of police or prosecutors to combat crime and terrorism more effectively across Europe. The GDPR will supplant the current patchwork of national laws in Europe which can be complicated and inconsistent.

Scheduled to go into effect in January 2018, the GDPR has a key provision of EU-wide reporting requirements for breach notification. The EU regulation directs member countries to impose penalties of up to 4% of global revenues for failing to adopt reasonable security measures and/or failure to notify regulators.

In parallel, several countries have enacted legislation independent of the EU. Germany has strengthened the ability of consumer groups to enforce data protection rights. In December, 2015, Germany's lower house of Parliament passed a bill extending the rights of consumer protection organizations and certain other associations to take actions in court to prevent violations of consumer data protection regulations. The objective of the law is to further improve consumer protection as well as to protect compliant businesses from unfair competition. It is set to go into effect on October 1, 2016, and considering the strong position of consumer and privacy protection attitudes in Germany, a rise in enforcement actions is expected.[75]

On January 1, 2016, a Dutch law became effective that includes a general obligation for data controllers to notify the Data Protection Authority (DPA) of a breach. This Act authorizes the DPA to impose direct fines for violations of up to €820,000, including failure to report data breaches. [76] [77]

---

[74] European Parliament News Data Protection Reform http://www.europarl.europa.eu/news/en/news-room/20160407IPR21776/Data-protection-reform-Parliament-approves-new-rules-fit-for-the-digital-era

[75] German Updated Consumer Data Protection Bill http://dip21.bundestag.de/dip21/btd/18/046/1804631.pdf

[76] Dutch Data Breach Bill https://www.huntonprivacyblog.com/files/2015/06/gewijzigd_voorstel_van_wet.pdf

[77] Dutch Data Protection Web Site (English) https://autoriteitpersoonsgegevens.nl/en

In May 2014, the Court of Justice for the European Union issued a landmark ruling on the "Right to be Forgotten". The Court ruled that search engines must remove links to sites from search results for a person, where the information linked is inaccurate, inadequate, irrelevant or excessive.[78] 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 personal information where the data is no longer necessary for the purpose for which it was collected, the subject withdraws consent, the storage period has expired or processing the data does not comply with other regulations. And, in December, 2014, the Article 29 Group representing the 28 EU Data Protection Agencies issued a set of guidelines on implementing the Right to be Forgotten.[79]

[78] 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".

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

AUSTRALIA

At present, Australian Privacy Principle (APP) 11 in the Privacy Act 1988 requires government agencies and businesses subject to the Act to take reasonable steps to secure personally identifiable information, but does not mandate notification with the exception of unauthorized access to eHealth information under the My Health Records Act 2012. Broader data breach notification legislation is pending and not anticipated to pass until 2017. Notwithstanding the pending legislation, organizations are voluntarily notifying regulators. The Office of the Australian Information Commissioner (OAIC), the chief enforcer of the Privacy Act, received 110 voluntary data breach notifications in 2014-15, up from 67 notifications in 2013-14 and 61 in 2012-13.

The OAIC's inquiries into voluntary data breach notifications focus on the nature of a breach (such as the kind of personal information involved, and how the breach occurred), and the steps taken to contain the breach, mitigate harm to affected individuals, and improve security practices going forward.

The Australian Parliament is in the process of examining a draft data breach notification bill. Key open issues and debate center on what constitutes a 'serious breach' creating a real risk of serious harm, as this is the expressed threshold trigger for a data breach notification. The agency is soliciting public comments through March 2016 including the assessment of real risk of harm.[80] [81]

The Do Not Call Register Act 2006 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.[82]

---

[80] Breach Notification https://www.ag.gov.au/Consultations/Pages/serious-data-breach-notification.aspx

[81] http://www.corrs.com.au/publications/corrs-in-brief/mandatory-data-breach-notification-is-coming-to-australia/?utm_source=Mondaq&utm_medium=syndication&utm_campaign=View-Original

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

CANADA

Organizations which operate and/or have customers in Canadian are subject to federal and provincial privacy laws that establish rules for the collection, use and disclosure of personal information in the course of commercial activity.[83] 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."[84]

Most recently in June, 2015, the Digital Privacy Act was approved which makes a number of amendments to the federal Personal Information Protection and Electronic Documents Act (PIPEDA), including new breach notification requirements. Once the breach notification comes into effect, the Act will require organizations to notify the Privacy Commissioner as well as affected individuals of any breach of security safeguards involving personal information under its control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the individual. Although not yet in effect, it is expected that breach notification requirements, along with obligations to report breaches to the Office of the Privacy Commissioner and possibly other organizations are coming. Organizations will also be required to keep records of data breaches and be able to produce these records on request. Failure to notify, report, or maintain records can result in a fine of up to $100,000.[85] Industry Canada is required to develop regulations, which appears likely to occur sometime in late 2016 or early 2017.[86]

Combined with directives of the Office of the Privacy Commissioner and evolving regulations, businesses should review the data protection responsibilities, including data which may be stored and processed by Canadian service providers and vendors.[87]

NEW ZEALAND

Organizations conducting business and collecting personal information in New Zealand should be aware of the national legislation regarding privacy. 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. New Zealand also has 'anti-spam' legislation covering all forms of unsolicited electronic messaging. Further, New Zealand Government agencies must also comply with the official information act.[88, 89, 90]

---

[83] The Act applies to commercial activity across Canada except for 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.

[84] PIPA Section 34.1.

[85] TRUSTe Client Advisory http://www.truste.com/blog/2016/04/28/preparing-new-breach-notification-requirements-canada/

[86] Digital Privacy Act http://nnovation.com/wp-content/uploads/2015/08/nNovation_LLP_-_Digital_Privacy_Act.pdf

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

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

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

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

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, hacktivists 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, IoT 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 places consumers in harm's way, adding to the regulatory and legal framework that can inhibit growth and innovation.

Data loss incidents can occur in organizations of all sizes, including non-profits, academia and government agencies. 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, IoT start-up 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 and contractual provisions;
- Acknowledge the data they collect contains one or more forms of PII or sensitive data;
- Know that a data incident can result in significant damage to a business's brand reputation; and
- Recognize that being unprepared can significantly add to direct and indirect costs.

Data security and privacy must become part of an organization's culture. Being prepared will help protect your data, detect a loss and quickly mitigate the impact. The responsibility cannot be assigned to a single individual or group; it is everyone's responsibility. Following the guidance in this document will help businesses minimize damage to their customers and brand.

Equally as important is completing an audit of all business practices, products and services. This includes assessment of third-party vendors and validation of 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, users (consumers as well as employees) have a responsibility to understand that they may be exchanging their online data when they use advertising-supported services such as free content, news and email, or hosting and storage for 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 and really thinking 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

Internet of Things Trust Working Group – https://otalliance.org/IoT

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

U.S. GOVERNMENT AGENCIES

Federal Trade Commission Start with Security Program www.ftc.gov/startwithsecurity

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

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

Federal Trade Commission; https://www.ftc.gov/tips-advice/business-center/guidance/careful-connections-building-security-internet-things

Federal Trade Commission; 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

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

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

Federal Trade Commission Big Data Report January 2016 -
https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf

U.S. Secret Service Electronic Crimes Task Force http://www.secretservice.gov/investigation/

CANADA

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: http://www.priv.gc.ca/information/ar/201213/201213_pa_e.pdf

Amendment to the Personal Information Protection and Electronic Documents Act (December 2015)
http://www.parl.gc.ca/HousePublications/Publication.aspx?Language=E&Mode=1&DocId=8057593

INDUSTRY & NON-PROFITS

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

Consumer Federation of America - http://consumerfed.org/issues/privacy/id-theft/ and www.IDTheftInfo.org.

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
- Identity Guard - http://www.identityguard.com/

InfraGard - https://www.infragard.org/

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

LifeLock - https://www.lifelock.com/education/

- Online Risk Calculator - https://www.lifelock.com/risk-calculator/
- Breach Solutions - https://www.lifelockbusinesssolutions.com/industries/lifelock-breach-solutions/

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

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

OWASP 10 Considerations Incident Response https://www.owasp.org/images/9/92/Top10ConsiderationsForIncidentResponse.pdf

Risk Based Security - https://www.riskbasedsecurity.com

SiteLock

- Security Breaches – It's Not If, It's When - http://blog.sitelock.com/2015/12/its-not-if-its-when/
- Five Easy Ways to Avoid Being Hacked This Holiday Season - http://blog.sitelock.com/2015/10/five-easy-ways-to-avoid-being-hacked-this-holiday-season/
- How to Survive a Data Breach - http://blog.sitelock.com/2015/05/how-to-survive-a-data-breach/

Symantec

- Security Threat Report http://www.symantec.com/security_response/publications/threatreport.jsp
- Endpoint Encryption: http://www.symantec.com/encryption
- Symantec – http://www.symantec.com/file-share-encryption/?fid=encryption

TRUSTe

- How Good Privacy Practices Can Help Prepare for a Data Breach - https://download.truste.com/dload.php/?f=IZC8I93X-553 (August 15, 2015 Webinar)
- Protecting Customer Information http://www.truste.com/resources/privacy-best-practices

APPENDIX B – NOTIFICATION TEMPLATES

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. Note as many states are in the midst of revising reporting requirements one should check for updates.

Take into account the footnotes throughout the Guide and in the Appendices 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).[91]

[91] 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.

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].[92]

[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].[93]

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

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.

---

[92] 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.

[93] 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.

For more information on identity theft, we suggest that you visit the web site of [insert link to State Attorney General website].

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 DRIVER'S LICENSE OR ID 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 MEDICAL, HEALTH OR INSURANCE INFORMATION IS 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.[94]

Sincerely, [Name] [Title][95]

[Contact Information]

[94] 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.

[95] 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 – CYBER INSURANCE

The following criteria are suggested considerations. For specific needs contact your advisors

Protections and Policies	
☐	Coverage for loss resulting from administrative or operational mistakes – extends to acts of the employee, business process outsourcing (BPO) or outsourced IT provider.
☐	Cyber extortion reimbursement costs including a credible threat to introduce malicious code; pharm and phish customer systems; or to corrupt, damage or destroy systems. May include costs to investigate threat or pay the ransom as well as costs for hiring a negotiator.
☐	Electronic media peril broadly defined to include infringement of domain name, copyright, trade names, logo, and service mark on internet or intranet site. (May be found in a separate media liability policy as well.)
☐	Coverage for socially engineered exploits including account credential disclosures, ACH transfers and other related losses arising from such exploits
☐	Interruption expenses include costs associated with rented/leased equipment, use of third party services, staff expenses or labor costs directly resulting from a covered loss.
☐	Knowledge provision includes Board of Directors, President, Executive Officer, Chairman, Chief Information Officer, Chief Technology Officer, Risk Manager or General Counsel.
☐	Broad coverage for damages to third parties caused by a breach of network security.
☐	Breach of privacy coverage includes damages resulting from alleged violations of HIPAA, state and federal privacy protection laws and regulations.
☐	Regulatory expense coverage to comply with an alleged breach notice order issued by a regulatory agency, (include both Federal and State).
☐	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.
☐	Public relations expenses to repair your reputation as a result of a data breach.
☐	Breach notice coverage (via sub-limit) – reimburses for costs to notify and remediation costs including but not limited to credit monitoring. *Consider voluntary notifications*
☐	Coverage for rogue employee(s) causing intentional damage to the insured's network.
☐	Expenses including forensics, legal, remediation (credit monitoring expenses, postage and advertising) and other costs. Coverage for contractual liabilities including PCI-DSS costs.
☐	Breach definition extends to acts of the Insured and acts of a Service Provider(s).
☐	Punitive and exemplary damages coverage provided on a most favorable venue basis.
☐	Business interruption coverage, including lost revenue as a result of a cyber breach.

APPENDIX D – FORENSICS BASICS

The most common goal of forensics is to gain a better understanding of an event 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 to identify perpetrator(s). The following is intended to help provide an understanding of the basics. In general, the process comprises the following phases: [96]

Collection: Identifying, labeling, recording, and acquiring data from the possible relevant sources (computer workstations, external storage devices, network servers, logs, etc.), while following procedures that preserve the integrity of the data.

Examination: 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.

Processes include:

- Performing regular backups of systems and logs, and maintaining 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.

[96] 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 E – INCIDENT REPORTING TEMPLATE

1. Organization Information	
Organization Name:	
Organization Address:	
Name of Person Reporting:	
Name of Network Administrator:	
Name of CISO:	
Name of CIO/Executive Level Decision Maker:	
Date of Report:	

2. What type of network compromise has occurred? (please select all that apply)			
☐ Reconnaissance	☐ Malware	☐ Data Exfiltration	☐ Other (please describe)

3. What equipment and/or systems have been impacted?	
Type:	
Manufacturer:	
Model Number:	
Serial Number:	

4. What operating system(s) was (were) installed on the equipment at the time of the intrusion?					
OS:		OS:		OS:	
Version:		Version:		Version:	
Time Zone:		Time Zone:		Time Zone:	

5. Are/Were software patches regularly installed?		
☐ Yes	☐ No	☐ Unknown
6. Does your network utilize any virtual machines, cloud services or third party service providers?		
☐ Yes – If so, please list?	☐ No	☐ Unknown
7. Is remote connectivity enabled on your network?		
☐ Yes – Please select all that apply	☐ No	☐ Unknown
☐ SSH – Please provide which version:		
☐ Telnet – Please provide which version:		
☐ RDP – Please provide which version:		
☐ VPN – Please provide which version:		
☐ Other – Please provide type and version:		
8. Does your organization use any web or cloud services?		
☐ Yes – Please list all services in use	☐ No	
9. Please list all domain names associated with your network.		
10. Please provide your server's DHCP address.		
11. Does your organization maintain DCHP logs?		
☐ Yes – If so, where?	☐ No	☐ Unknown

12. Does your organization maintain web and application server logs?

☐ Yes – If so, where?	☐ No	☐ Unknown
13. Please provide your organization's network DNS address. Is it internal or external to your organization?		
☐ Internal	☐ External	☐ Unknown
14. Please list the range of your organization's IP addresses. Of these, how many does your organization own and/or use?		
15. How does your organization maintain any data backups? (internal and external)		
☐ Yes – If so, where?	☐ No	☐ Unknown
16. Is your data encrypted? If so provide an overview including how keys are managed.		
17. What terminal services are/were running on the impacted equipment?		
18. What ports are/were enabled on the impacted equipment?		
19. Does your organization own or operate any Wi-Fi access points?		
☐ Yes	☐ No	☐ Unknown
If so, are they active or passive?		
☐ Active	☐ Passive	
20. Do you suspect the unauthorized intrusion on your network to be the result of a current or former employee or vendor?		
☐ Yes	☐ No	
21. Are your employees informed of the limits of their acceptable use and privileges on your network?		

☐ Yes	☐ No	☐ Unknown
22. Are employees given any instructions related to the cessation of their network use and privileges when they leave employment or are terminated?		
☐ Yes	☐ No	☐ Unknown
23. Has your organization taken any steps to mitigate the impact of the intrusion?		
☐ Yes – if so, please describe	☐ No	☐ Unknown
24. Do you believe the breach was the result of a socially engineered exploit (spear phishing, malvertising, other) targeting employees or vendors?		
☐ Yes – if so, please describe	☐ No	☐ Unknown
25. Who has been notified (internally and externally)?		

26. To the best of your ability, please quantify your estimated financial loss as a result of this incident.*	
Equipment Loss:	
Equipment Repairs:	
New Equipment:	
New Software:	
Employee Overtime:	
External costs? (Legal, PR, Forensics, Consultants)	
Reputation Degradation:	
Customer/Business Loss:	
Other Costs	
Total	

27. Include any other comments or information which be of assistance.

APPENDIX F – ENCRYPTION OVERVIEW

Encryption is considered a best practice to help contain the effects of a breach, not only for sensitive files and data stores, but also for laptop and mobile devices, which often contain sensitive data. As encryption standards continually evolve, readers should check the web site of their device and operating system provider and third party tools.

Encryption is only as strong as the cryptographic key or password which decrypts the file or disk, and can only be effective if the keys themselves are protected from theft. As such, cryptographic keys need to be protected with strong countermeasures in addition to the encrypted data that they protect. Like all security measures, encryption is subject to the "weakest link" principle, which may be the user's password in cases where a password is used to derive a cryptographic key, or the key management system that is used to protect cryptographic keys. 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. It should be noted file encryption does not fully protected since temp and, page files are not protected.

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. It helps prevent tampering of the operating systems files and configuration helping to ensure customer or sensitive data on a lost or stolen system cannot be accessed by others.

Microsoft offers BitLocker in Windows 8 (Enterprise and Professional) and Windows 10. Additionally, Windows 8.1 or greater also offers automatic device encryption, which is based on BitLocker technology, to provide 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).

When encrypting databases, there are layers of encryption to be considered, including both table-layer encryption and application-layer encryption. If an attacker steals a hard drive out of a data center where the database uses table-level encryption, the data on the disk would be useless to the attacker due to the database-table level encryption, but if someone were able to query the database (e.g., by a database administrator or other employee that has been given database access, or due to a vulnerability on a web site that is connected to the database), the attacker would be able to access unencrypted data. As such, table-layer encryption and application-layer encryption protect against different threats and can be used together. When application-layer encryption is used, the cryptographic key used to encrypt data at the application layer can be stored such that it is inaccessible to database administrators. In particular, cryptographic keys for application-layer encryption should not be stored in the database itself, but rather in a device such as a hardware security module (HSM).

APPENDIX G – REMEDIATION CONSIDERATIONS

ID Theft Recovery	
☐	Credit Monitoring Alerts – alerts to potential fraud appearing on credit reports. Typically, consumers sign up for 90 days or can pay for extended service.
☐	Additional Fraud Detection – alerts to potential fraud that may not appear on credit reports. Typically this type of alerting uses an expanded network for fraud detection.
☐	Fraud Specialist – access to fraud specialists to help manage fraud case on behalf of consumers.
☐	Identity Theft Insurance – Reimbursement of costs related to restoring consumer's identity, including, lawyers, investigators, consultants and others. Recommended $1 million policy.
☐	Lost Wallet Protection – assistance with canceling and replacing lost debit/credit cards.
☐	Resolution assistance in closing fraudulent accounts and removing from consumer's credit history.
Information Protection	
☐	Identity fraud protection should provide help for the unauthorized use of the following information to open bank accounts, take out loans in your name, including but not limited to ❑ Name ❑ Address and Phone Numbers ❑ Social Security Number ❑ Public Records ❑ Loans and Bank Accounts ❑ Credit / Debit Card Applications
Additional Protection & Services	
☐	Child ID Protection – helps protect against any unauthorized use of children's PII.
☐	Credit Monitoring – monitors your credit reports for any suspicious activity.
☐	Credit Reports – provides access to credit reports (ideally from the top 3 credit agencies).
☐	Credit Scores – provides credit scores.
☐	Early Warning Alerts – provides early warning alerts following suspicious behavior.
☐	Mailing List Removal – removal from mailing lists to help protect consumer personal information.
☐	Medical ID Theft Protection – monitors medical benefits for any suspicious activity.
☐	Security Freeze – ability to place a lock on access to credit reports if identity theft is suspected.
☐	Educational materials and detection tools optimized for both PC and mobile device viewing.
☐	Scanning of logs and forums used by cybercriminals for listing of users and their data.
Support	
☐	Operator assistance ideally in the same country as the victim with multi-lingual options.
☐	Support for hearing impaired consumers including but not limited to TTD/TTY support.
☐	Multi-lingual content including web site, phone scripts and related self-help documents
☐	Case management or tickets system to track and archive all consumer interactions, with client access for aggregated reports and data.
☐	24/7 Support. Does the provider provide support through the following: ☐ Phone ☐ Email ☐ Chat ☐ Social Media ☐ Other

These following risk assessment worksheets are intended to help organizations survey and identify possible risks and serves as the foundation and starting point. Based on an organization's size, business sector and geographic locations they are operating in, other questions may be appropriate for a business to consider.

APPENDIX H – INTERNAL RISK ASSESSMENT

Operational Risk Assessment	
☐	Do we understand the international regulatory requirements and privacy directives related not only to where our business physically operates but where our data and customers reside?
☐	Do we know all specific data attributes we maintain for all customers? How and where is this data stored, maintained, flowed and archived (including data our vendors and third-party/cloud service providers store or process)?
☐	Is the original business purpose for collecting our data still valid and relevant? Can we identify points of vulnerability and risk?
☐	Are our encryption, de-identification and destruction processes in alignment with industry accepted best practices and regulatory requirements?
☐	Do we have a 24/7 incident response team and response plan in place? Do employees have reporting and escalation processes?
☐	Are we prepared to communicate to employees, customers, stockholders, government regulators and the media during a data loss incident?
☐	Do we follow generally accepted security and privacy best practices? If not, are we prepared to explain why? Do we have an audit trail of access to sensitive data, where it is being stored and how it is being used?
☐	Does our privacy policy reflect our data collection and sharing practices, including use of third parties? Have we audited our site to confirm we are in compliance?
☐	Do we know whom to contact in the event of a breach? Are we prepared to work with our local state and national law enforcement authorities such as the FBI, U.S. Secret Service and State Attorney Generals? Or will we have to resort to making these contacts in the "heat of the battle" on an ad hoc basis?
☐	Are we (and our Board) willing to sign off on our breach response plan and be accountable that we have adopted best practices to help prevent a breach?
☐	Do we understand the security, privacy and notification practices of our third-party vendors?
☐	Do we 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?

APPENDIX I – THIRD PARTY RISK ASSESSMENT

Third Party Risk Assessment	
☐	Given our data includes [describe what types of data will be stored], what integration offerings are available and will our organization's data be commingled with other customer's data?
☐	Describe the physical security of your data centers.
☐	Do you use any third parties (e.g., for development, QA, help-desk, integration services, etc.) that would impact the servicing of our account and do they have access to our organization's data?
☐	How is staff with access to client data managed; how are privileged actions monitored and controlled? Outline your process for background checks on your employees. Include a description of the password policy management, and account lockout policies.
☐	Describe the organizational structure for security operations at your company.
☐	Do you have a comprehensive security program that adheres to a recognized framework and is periodically reviewed by a third party including vulnerability scans and periodic penetration tests?
☐	How are you protected from DDoS attacks?
☐	List all 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.
☐	Do you have security audit reports such as SAS70/SSAE16 that can be reviewed?
☐	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.
☐	Provide an overview of your backup practices including where and how long you maintain backups. Are backups encrypted? Have you tested recovering data from a backup?
☐	Describe your security incident process and testing. How do you define an incident? Please list all incidents which required reporting to affected individuals or regulators in the past two years.

Certification Acronyms - FedRamp – Federal Risk and Authorization Management Program; FIPS 140-2 – Federal Information Processing Standard Publication 140-2; FISMA – Federal Information Security Management Act; DIACAP – Department of Defense (DoD) Information Assurance Certification and Accreditation Process; HIPAA – Health Insurance Portability and Accountability Act; ISO 27001 – International Organization for Standardization; PCI DSS – Payment Card Industry Data Security Standard; SOC 1 – Service Organization Controls 1 Report; SSAE 16 – Statement on Standards for Attestation Engagements No. 16; ISAE 3402 – International Standard on Assurance Engagements No. 3402; SAS 70 – Statement on Auditing Standards No. 70

ABOUT THE ONLINE TRUST ALLIANCE (OTA)

The Online Trust Alliance (OTA) is a non-profit with the mission to enhance online trust and user empowerment while promoting innovation and the vitality of the Internet. Its 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, and meaningful self-regulation and data stewardship. Its members and supporters include leaders spanning public policy, technology, e-commerce, social networking, mobile, email and interactive marketing, financial, service provider, government agency and industry organization sectors.

OTA is a 501c (3) tax exempt global non-profit focused on enhancing online trust with a view of the entire ecosystem. OTA is supported by donations and support across multiple industries, representing the private and public sectors. To support OTA visit https://otalliance.org/donate.

Revised May 16, 2016