

2017 Cyber Incident & Breach Response Guide

Enhancing data protection,
reducing the impact of an incident
and helping to protect users worldwide



ACKNOWLEDGEMENTS

The Guide is a collaborative multi-stakeholder effort reflecting input and data from industry leaders and government agencies. Contributing organizations include Act-On Software, ACT-The App Association, American Greetings Interactive, Bryan Case LLP, Center for Democracy & Technology, Consumer Federation of American, DigiCert, Hartford HSB, Guardian Life, Iconix, Identity Guard, Identity Theft Council, Internet Society, Intersections, LifeLock, Malwarebytes, Microsoft, nNovation LLP, Privacy Rights Clearing House, Risk Based Security, SecurityScorecard, SiteLock, Symantec, ThreatWave, Twitter, and Verisign. In addition, special thanks to the California Department of Justice, 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 for their input and collaboration.

Underwritten in Part by Grants and Donations From:

 IDENTITY GUARD® BUSINESS SOLUTIONS	Identity Guard is a proactive identity and credit monitoring service that delivers premium solutions to help busy families and individuals take control over their personal and private information. Our services help educate and empower individuals to protect themselves from the growing threat of identity theft with premier identity protection and credit monitoring solutions. Identity Guard is provided by Intersections Inc. (NASDAQ: INTX), which, since 1996, has protected more than 47 million consumers. www.identityguard.com
 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. www.lifelock.com
 Symantec™	Symantec is the leading cyber security company, helping organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure including device protection, and cyber insurance analytics, incorporating data from the insurance industry and Symantec's cyber intelligence network. www.symantec.com
 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. www.verisign.com

TABLE OF CONTENTS

Acknowledgements	2
Introduction	5
Executive Summary	6
Threats Beyond Data Loss	7
Benefits of Readiness	7
Prevention, Preparation & Vigilance	8
What Have We Learned?	10
Risk Assessment	11
Board/Executive Strategic Questions	11
Operational Risk Assessment	12
Third Party Risk Assessment	13
Security Best Practices	14
Data Stewardship	17
Data Governance	19
Cyber Insurance Considerations	22
Incident Response Fundamentals	24
Incident Response Teams	24
Creating Response Plans	25
Forensics, Intrusion Analysis & Auditing	26
Critical Logs	28
Notification Requirements	29
Communicating Effective Responses	30
Providing Assistance & Remedies	31
Training, Testing & Budgeting	32
Employee Awareness & Training	32
Funding and Budgeting	33
Post Incident Analysis	33
Regulatory Landscape	34
Conclusion	36

APPENDICES & ENDNOTES

Appendix A – Resources & Readings	37
Online Trust Alliance	37
Industry	37
U.S. Government & State Agencies	38
Canada	38
Non-Profits	38
Appendix B – Notification Templates	38
If Social Security Numbers Were Involved	40
If Financial Account Numbers Were Involved	41
If Driver's License or ID Numbers Were Involved	41
If Medical, Health or Insurance Information Were Involved	41
Appendix C – Cyber Insurance Considerations	42
Appendix D – Forensics Basics	43
Appendix E – Incident Reporting Template	44
Appendix F – Remediation Service Considerations	48
Appendix G – Internal Risk Assessment	49
Appendix H – Third Party Risk Assessment	50
Appendix I – Incident Readiness Checklist	51
Endnotes	52

INTRODUCTION

For nearly a decade the Online Trust Alliance (OTA) has published a Breach Readiness Guide to help organizations of all sizes enhance data protection and prepare for a breach incident. Reflecting the evolution of cybercrime beyond the traditional breach and extraction of data, the 2017 Guide has been broadened to include the wider impact of cyber incidents. Today's risks increasingly include business interruption from ransomware, stealing of funds via Business Email Compromise (BEC) attacks, denial of service attacks (DDoS) and takeover of critical infrastructure and physical systems. They all impact consumers as well as business operations and continuation of services, impacting revenue with a potential crippling impact. The Guide has been designed for a broad range of organizations and stakeholders, from executive decision makers to technical security and privacy professionals. The goal is provide readers the guidance and knowledge to enhance security and adopt responsible data privacy practices to help prevent, detect, mitigate and effectively respond to a cyber incident.

"There is no perfect security. All organizations need to recognize they will encounter an incident and they will be judged on how they respond."

While recognizing "one size does not fit all," the Guide is designed to help organizations understand and assess risk, implement security best practices and develop strong incident response plans to aid in prevention, detection and remediation. Adopting the Guide's principles not only will help prevent identity theft and business interruption, it can improve business economics through the ability to secure cyber insurance at efficient premiums while minimizing incident-related costs and business down-time.

While one cannot control the bad guys, one can control and manage the fall-out of an incident. Even the most cyber-savvy organizations have found themselves exposed and ill-prepared to manage the effects and costs of an incident. The best defense is a three-step strategy. First, implement a broad set of operational and technical best practices that help maximize the protection of customer and company data; second, be prepared with an incident response plan that allows a company to respond with immediacy while ensuring maximal business continuity and third, understand that human factors play a critical role in how strong or weak an organization's security defenses are, how they respond and most importantly, how their actions are judged. Organizations need to look beyond technology and internal processes/protocols to the employees themselves to help close security gaps.

Cyber Incidents - Unauthorized

1. access to a system or device and its data,
2. extraction, deletion or damage to any form of data,
3. disruption of availability and/or integrity of any business operation or service,
4. activities causing financial or reputational harm.

Data is among the most valuable assets a company has and its management and protection must be viewed as mission-critical stewardship rather than mere compliance. Effective preparation for and handling of an incident are a shared responsibility that includes every functional group within an organization and requires a strong guiding hand from senior

executives. While there is no perfect defense against a determined attacker, the best practices outlined in this Guide can help greatly reduce a company's attack surface and the impact of an incident.

Report updates, resources and worksheets may be downloaded at <https://otalliance.org/incident>.

EXECUTIVE SUMMARY

The cyber threat landscape has changed dramatically over the past twelve months, with the definition of incidents expanding significantly beyond reported data breaches. Organizations large and small have been the target of attacks that stole, published or manipulated sensitive, personal information. Confidential medical data and personal records of world-class athletes became public when the Olympic Anti-Doping Agency database was breached and the records published.¹ The scope of the Yahoo breach including some 1 billion records has redefined the landscape as well as opened up the debate on ethical breach reporting.² In the tumultuous months of the U.S. presidential election, the Democratic National Committee faced multiple attacks not focused on consumer data but on the political strategy of the organization.³ These headlines remind us that no organization or government entity is immune when targeted by skilled adversaries. Organizations must pivot from an outlook solely focused on prevention to one of readiness, working to limit the impact of any cyber incident.

Each year the stakes get higher. Larger and more costly cyber incidents coincide with annually increasing regulatory and liability pressures. On a global basis the number of breaches are estimated to be on par with prior years, but most concerning is the number of consumer records exposed is estimated to exceed 4.2 billion.⁴

The real story is not with these breach numbers but the total number of incidents including loss of corporate data, ransomware, incidents not involving covered information, and unreported breaches. Phishing emails have become a common occurrence. According to the FBI, losses from Business Email Compromises increased 1300% in 2016 with losses exceeding \$3.1 billion.⁵ At the same time ransomware device infections averaged 35,000 per month with the average ransom paid doubling to nearly \$700.⁶ The FBI estimates ransomware payments in 2016 are expected to hit a billion dollars, up from just \$24 million in 2015.⁷ Security firm Malwarebytes' survey of 500 companies found one-third have been impacted by a ransomware attack.⁸ Not only have DDoS attacks increased 58%, but most concerning is the peak attack size and intensity increasing 82%.⁹

Combined, OTA's analysis and tracking of threat intelligence data from multiple sources has revealed the true number of incidents is over twenty times that of consumer data breaches publically reported. Based on preliminary year-end data, on an annualized global basis this equates to over 82,000 incidents impacting more than 225 organizations daily.¹⁰ As the majority of incidents are never reported to executives, law enforcement or regulators, the actual number of incidents causing harm combining all vectors including DDoS attacks could exceed 250,000.

As society and world economies are increasingly reliant on the internet and data, we are facing a critical juncture. As reported by the Internet Society, online trust is at an all-time low with 59% of users reporting they would likely not do business with a company that had suffered a data breach.¹¹ While we have reaped the benefits of the exponential growth of the internet, the number, scale and scope of cyber incidents is reshaping the future as we know it. Compounded in part by abusive privacy practices, government surveillance, deceptive news and advertising, consumer trust has been significantly tarnished.

These metrics illustrate the need for all stakeholders, including industry, policy makers and governments, to take decisive action. The recurring incidents have an additive, long-term effect on society not unlike global warming and carbon emissions. We are facing the tragedy of the trust commons which, left unaddressed, can and will have significant impact to society and world economies.

Cyber Security Tenets

1. There is no perfect security and any organization is at risk; most organizations hold data of interest.
2. Organizations must make security a priority; those that fail to adopt sound practices will be held accountable.
3. Organizations need to look beyond the impact and cost of a "traditional data breach" to the life safety and physical impact of an incident, damage to an organization's reputation and risks to users.
4. Business incentives are needed to accelerate "security by design" along with the need for annual security assessments of sites, applications services and devices.
5. Signaling of commitment to security and privacy can become product and brand differentiators.
6. Employee training and awareness must be addressed to help close the security technology gaps.

THREATS BEYOND DATA LOSS

The reality is that measuring an incident by the number of records lost or exposed is only one indicator. Increasingly, the motivations may be to create disruption and damage the reputation and trust of the organizations. The recent DDoS attacks are case in-point, making several high visibility sites inaccessible for several hours. The impact could be significant lost revenues if the attack were timed for maximum disruption. Phishing is getting harder to distinguish from legitimate emails and sites reflecting criminal's increased skills and ability to a mimic organization. Other more focused financial and disruptive attacks have been spearphishing and malvertising, focused on credentials as a dominant threat vector.¹² More disruptive is the rise of extortion or "ransomware" targeting high net worth companies timed for maximum disruption and payouts targeting professional services and manufacturing sectors.¹³ As IoT devices are becoming commonplace in the home and office, we have witnessed a security "blind spot" where unauthenticated email security notifications are being spoofed driving unauthorized password resets and devices being botched as a result of users downloading malicious updates.^{14 15} (See Best Practice #7, page 15)

Regardless of type, cyber incidents lead to business interruption, unanticipated costs and threats to security and privacy. Raising the complexity and business risk is the increasingly intricate technology landscape. Due to the explosive proliferation of mobile and "Internet of Things" connected devices, the risk of an incident has been amplified. Further, the regulatory landscape is also changing. The Federal Communication Commission (FCC) recently enacted privacy rules which also include breach notification requirements for broadband providers and carriers.¹⁶ This rule making may have implications to others including edge-providers and commerce sites.

A potential greater impact is the EU General Data Protection Regulation (GDPR) which includes comprehensive data protection regulations. While a company may not have a physical nexus in the EU, the directive could be enforced if a single EU citizen is directly impacted, with fines of up to 4 percent of a company's global revenue.¹⁷ (See Regulatory Landscape on page 34)

BENEFITS OF READINESS

The financial benefits of effective incident readiness are significant. As discussed in the Guide, effective planning requires anticipating decision-points. Evaluating scenarios in advance and running tabletop exercises help organizations optimize decision-making aligned to their (and their investors') strategic goals and objectives. Not only is there the benefit of lowering the risk of an incident, establishing a robust incident response plan can dramatically reduce the impact of an incident. Having demonstrable processes including internal and partner risk assessments and business continuity plans can potentially lower cyber insurance premiums.

According to the Ponemon Institute, the global average cost of a breach has risen almost 14% in the past two years to \$4 million in 2016. In the U.S. data losses have increased to \$7 million.¹⁸ While such data is helpful, it does not account for other externalities. In cases of business interruption such as ransomware freezing data assets and

demanding payment, the lost revenue from business down-time compounds the costs. Typical business ransom payouts are often in the tens of thousands of dollars, yet the real cost is the business down-time and long-term risk of compromised data integrity.¹⁹ Even as direct costs are rising, another externality – the costs to users – remains largely undefined from the business perspective, but clearly impacts brand reputation.

Penalties levied for incidents can be significant. For example, the FCC's enforcement action against AT&T resulted in a \$25 million fine.²⁰ Failure to perform risk analysis, failure to implement broadly accepted security practices such as encryption, ignoring third party vulnerabilities reports and failure to ensure third parties comply with security and privacy requirements are some of the top factors cited in lawsuits, and regulatory and enforcement actions.²¹

Together, these incidents underscore how risk assessment and preparation pay off. In addition to aiding in protection against an incident and reducing exposure to regulatory action, commitment to best practices allows faster discovery of attacks and shorter times to containment. An impact study on business continuity management programs found that having an incident response team, extensive use of encryption and employee training were the top three drivers of cost savings in breach incidents, together accounting for 24% savings.²²

Further mitigating risk, securing cyber insurance coverage can help buffer financial exposure and is on the rise. While cyber insurance is an evolving arena and exact comparisons are complex, companies armed with risk assessments (including third party providers), appropriate data stewardship practices, strong security and trained incident response teams are best poised to be able to secure cyber insurance at the most efficient rates possible.

PREVENTION, PREPARATION & VIGILANCE

No matter how good a company's security is, cyber incidents are unavoidable. There is no perfect security, yet there is also no excuse for failing to embrace fundamental security principles. With the growing networks of connected devices, every organization – from startups to global enterprises – must be prepared for the inevitable attack and loss of (or loss of access to) critical data. It is imperative that all organizations recognize the risks, optimize readiness and make data security and privacy part of every employee's responsibility from the boardroom to the mailroom.

2016 Incident Highlights

- 82,000+ total cyber incidents in 2016 (OTA)
- 90%+ of incidents could have been prevented (OTA)
- 4,149 confirmed breaches worldwide (RBS)
- \$75 billion financial impact of ransomware (TA)
- 78% increase in phishing sites through 3Q16 (APWG)
- 35% rise in business targeted ransomware (Symantec)
- 1300% increase in BEC losses (FBI)
- 58% increase in DDoS attacks (Verisign)

Sources: (OTA) Online Trust Alliance, (RBS) Risk Based Security, (PI) Ponemon Institute, (APWG) Anti-Phishing Working Group, (TA) The Atlantic

OTA's analysis of reported breaches through Q3 2016, revealed 91% were avoidable, consistent with previous year's research. Of the reported breaches, 13% were due to lack of internal controls resulting in employees' accidental or malicious events and 53% the result of actual hacks. Consistently for the past several years, more than 90% of incidents originate from a deceptive or malicious email. Similarly, analysis of data regarding enterprise ransomware incidents, which increased 35% in 2016, points to a lack of employee training and protection from spearphishing emails.²³ Business Email Compromise (BEC) attacks also are generally preventable since they rely on spearphishing and social engineered tactics. Unfortunately the complexity of business operations, lack of blocking unauthenticated email and the sophistication of social engineered exploits overwhelm all too many organizations.

Key avoidable incident causes:

- Not patching known / public vulnerabilities
- Failure to block unauthenticated email
- Misconfigured devices / servers
- Unencrypted data and/or disclosed keys
- Use of end of life devices, operating systems and applications
- Employee errors and accidental disclosures - lost data, files, drives, devices, computers, improper disposal
- Business Email Compromise & social exploits

While organizations may be aware of the threat, they are not necessarily equipped to respond effectively.

Businesses must acknowledge the chaos and disruption that can occur with any incident. Viewing breaches and incidents as a “technical issue” belonging to the IT department is a recipe for failure. Instead, organizations need to recognize that many departments play a part in readiness planning. Readiness starts with responsible data privacy and collection practices, and includes ongoing employee training and security assessment of vendors and connected devices. Those that prepare in advance will not only be postured to survive an incident, but also are more likely to retain a positive reputation with their customers.

A key learning from past high-profile incidents is that organizations all too often ignore warnings from third parties and researchers. Organizations must have a process to analyze vulnerabilities reported to them. Failure to have a process can lead to reputation damage and potential lawsuits as seen with Snapchat in early 2014. Having a mechanism to review and respond to vulnerability reports is an essential part of an organization’s security strategy.²⁴

Fundamentals

- Data stewardship, privacy and incident readiness are everyone’s responsibility
- Data management and privacy practices need continual review
- All businesses collect some form of PII (Personally Identifiable Information)
- Cyber incidents will occur
- Every organization needs to have a current and tested plan
- Ongoing employee training is a critical key to success

INCIDENT READINESS CHECKLIST

See Appendix I for expanded recommendations (pg 51)

- Complete risk assessments for executive review, operational process and third party vendors (pg 11)
- Review security best practices and validate adoption or reasoning for not adopting (pg 14)
- Audit data management and stewardship programs including data life-cycle management (pg 17)
- Complete an audit of insurance needs including exclusions and pre-approval of third party coverage (pg 22)
- Establish an end-to-end incident response plan including empowering 24/7 first-responders (pg 24)
- Establish/confirm relationships with law enforcement and incident service providers (pg 25)
- Review and establish forensic capabilities, procedures and resources (internal and third-party providers) (pg 26)
- Review notification processes and plans (pg 29)
- Develop communication strategies and tactics tailored by audience (pg 30)
- Review remediation programs, alternatives and service providers (pg 31)
- Implement employee training for incident response (pg 32)
- Establish employee data security awareness. Provide education on privacy, incident avoidance (password practices, how to recognize social engineering, etc.) and incident response (pg 32)
- Understand the regulatory requirements, including relevant international requirements (pg 34)

WHAT HAVE WE LEARNED?

The increasing number, precision and impact of incidents are wake-up calls for all organizations, whether they are non-profits, governmental agencies, or start-ups and Fortune 500 companies. While credit card theft and identity theft is on the rise, their impacts can pale in comparison to mass data breaches, ruthless ransomware and crippling DDoS attacks. Reviewing leading incidents for the past two years highlights several important lessons:

1. **Protection involves not only data loss, but also incidents which interrupt business** including ransomware attacks, network and system interruption and connected device takeover.
2. **Responsibility for incident protection and readiness is company-wide.** There needs to be a critical shift in attitudes regarding responsibilities of data stewardship security and responsible privacy practices.
3. **Data is often a company's most valuable asset.** Identify what you have, where you have it, how you use it and the potential risks should it be inappropriately accessed, held hostage, released or erased.
4. **The level of data security you apply must be commensurate with the data held** – the security in place should reflect the risk of damage to consumers and the company should that information be inappropriately accessed. Organizations should develop a data minimization strategy including a classification matrix that guides how various types of data should be protected, stored and discarded across an organization.
5. **Only collect and retain data that has a business purpose.** Protect it while it's held, and delete it when it's no longer needed. Criminals cannot steal or hold hostage data you don't have.
6. **Have an incident plan to reduce impacts of an attack.** It's dangerous to think you won't be a target. Consumer, employee and corporate data are valuable commodities. When combined or appended with other breached data, they increase in value. Alternatively, freezing these assets can paralyze a business.
7. **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.
8. **Security is beyond your desktops, networks and walls.** As more businesses rely on cloud services and third-party providers, companies must consider the expanded attack landscape. A risk assessment must be conducted prior to usage and on an ongoing annual basis. Supplier risk assessment must be done before a contract is signed and managed through the term of the contract. Management should require regular (weekly, monthly, quarterly or annual) reports from vendors specifying their internal data security processes, data removal methods, tools and technology implementation and documentation.
9. **Being prepared is not just for Boy Scouts.** An incident plan needs to incorporate 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 trust and the vitality of the Internet, while helping to ensure business continuity. Developing key relationships ahead of time with attorneys, public relations, forensics, and identity protection firms is essential to maximizing the response effectiveness.
10. **Connected devices introduce new risk levels.** The rapid adoption of connected devices from Smart TVs in the boardroom to coffee makers in the breakroom dramatically increase the threat landscape. Ongoing risk assessment of all IoT devices and the development of an employee policy for connecting devices to the corporate network is critical since a single connected device can introduce threats network wide.²⁵
11. **Build trust through transparency.** Whether communicating with customers or board members, keeping important stakeholders informed early with regular updates is a critical part of maintaining trust.

RISK ASSESSMENT

Risk assessments are critical for every organization. Increasingly, organizations and their executives are being held accountable and facing lawsuits for the failure to uphold fiduciary duties as they apply to data security and governance.

While there is no absolute guarantee of protection from an incident or data loss event, Boards and management committees need to evaluate the legal and compliance risks, ranging from accounting and financial practices to personnel policies to data security. The following lists serve as a baseline for assessments. Organizations are encouraged to build from these and add other questions as they apply to their industry and business sector. Such risk assessments should be conducted regularly to aid in the identification of potential vulnerabilities, evolving business operations and business practices. A complete and objective review of these audits serves as the foundation for developing an effective data security and response strategy. (See Appendices G and H for sample risk assessment forms.) In addition, organizations are encouraged to review the OTA IoT Trust Framework to assess the risks of connected devices and to evaluate future device acquisitions.²⁶

BOARD/EXECUTIVE STRATEGIC QUESTIONS

1. What makes our company or service an appealing target for hackers, hacktivists and/or cyber criminals; what organizations or industry sectors similar to ours have been targets?
2. What is the worst-case scenario; what are our major assets and “crown jewels” that could be compromised? Could an incident have a material impact on an IPO, merger or acquisition? Is there a seasonality of our businesses cycles that could be most appealing to a cybercriminal or hacktivist?
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? Is there a seasonality in our business that would have a material impact?
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? To what extent are our third-party partners covered and how does their coverage relate to or impact ours? Are we prepared for regulatory enforcement and/or lawsuits? Are our existing outside counsel, forensics and breach response vendors approved from the insurance company panel(s) (See Attachment C, Cyber Insurance)
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? Have we prioritized our benchmark assessments by level of risk? Do we have the right bandwidth for risk mitigation?
12. Do we have a documented external vulnerability reporting mechanism for third-party submissions?
13. What recent incidents and exploits have been reported? Do they expose new vulnerabilities or attack vectors which haven't been considered?

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. Annually conduct an audit to identify all data types and attributes collected and stored. 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 plan in place? Are employees trained on a reporting and escalation processes?
6. Do we have an incident communication strategy and plan segmented for employees, customers, stockholders, regulators and the media?
7. Do we follow generally accepted security and privacy 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 actual practices, including use of third parties collection, use and sharing? Have we audited our site, devices, applications and cloud services to confirm we are in compliance and the business purpose for such data collection and sharing is valid and required?
9. Do we know whom to contact in the event of a breach or incident? Are we prepared to work with our local state and national law enforcement authorities such as the FTC, FCC, FBI, U.S. Secret Service and/or State Attorneys General?
10. Are we (and our Board) willing to sign off on our incident 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 and are these specified as contractual obligations?
12. Do we have an incident response vendor that can have experts on call to assist with determining the root-cause of a breach, identifying the scope of an incident and collect threat intelligence data? Did the incident response vendor validate that the company has collected all the relevant data needed for an incident response engagement?"
13. Has an inventory of all connected devices been completed (including IoT, smart devices and personal employee devices connecting to company networks)? This inventory should include review for known vulnerability and patching capabilities.

"Data security is a major issue for both consumers and businesses, yet companies are not doing everything in their power to prevent cyber incidents. The status-quo is not acceptable.

THIRD PARTY RISK ASSESSMENT

As businesses innovate, look to add efficiencies and be more agile, they are increasingly relying upon cloud providers and third-party vendors to outsource key functions, which may be handling some of their most sensitive data. Assessment of third parties' security and privacy practices should be part of the vendor selection process and requires a commitment of both time and resources. Companies are recommended to plan to allocate 30 days or more to complete an audit and review the findings.

Assessments and audits of third-party capabilities need to continue after a vendor is on-boarded to help identify 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.

Asking vendors the following questions will help you assess their practices and 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 do you manage and restrict staff who have access to client data; 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. Please provide an overview of your use of encryption technologies and practices.
6. Describe the organizational structure for security operations team.
7. 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?
8. How are you protected from DDoS attacks? Have you ever experienced incidents taking your service offline? If so please explain the impact and how you mitigated and responded to the incident.
9. List all third party certifications or attestations, such as FedRamp, FIPS 140 -2, FISMA and DIACAP, HIPAA, ISO 27001, PCI DSS, or SOC 1/SSAE 16/ISAE 3402 or other relevant certifications. (See Appendix H for acronyms)
10. Do you have current security audit reports such as SOC70/SSAE16 or similar audits which can be reviewed?
11. 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.
12. 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?
13. 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.

SECURITY BEST PRACTICES

Data loss and identity theft occur from an ever-increasing level of deceptive practices and cyber incidents. In addition to physical security measures (building security, locking drawers/cabinets/offices, etc.), protection of digital data includes additional technology measures. Threats such as social engineering, forged email, malvertising, phishing, and fraudulent acquisition of internet domains are on the rise and can lead to system infiltration. Helping to address these threats, through a multi-stakeholder process, OTA developed a list of recommended best practices which are easy to implement and manage across all industry sectors. These practices apply to all connected and “smart devices” including printers, copiers, TVs, and personal mobile devices. Beyond the list provided, organizations are encouraged to review other controls including the Critical Security Controls for Effective Cyber Defense, published by the Council on Cyber Security and the Department of Homeland Security Strategic Principles for Securing IoT Devices.²⁷ Combined with OTA’s IoT Trust Framework, these controls are a baseline set of recommendations to help prevent, detect and contain today’s most pervasive threats.²⁸

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 incident. It is essential that companies carefully consider not only the strength of encryption, but also the proper management of cryptographic keys. Companies must consider all devices including desktop PCs, tablets, servers and smart phones. It is critical to review each platform’s respective encryption controls as part of an overall product acquisition strategy. Encryption of data breaches may preempt the requirement of consumer notifications as specified by individual State breach regulations.
2. **Implement 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.²⁹
3. **Enforce effective password management policies.** Attacks against user credentials, including spearphishing, brute force, sniffing, host-based access and theft of password databases, remain attack vectors warranting the use of effective password management controls. Businesses should review the National Strategy for Trusted Identities in Cyberspace (NSTIC) as an alternative for password management.³⁰ Best practices include:
 - a) 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 system and refrain from reusing the same password for internal systems and personal website logins;
 - b) Deploy a log-in abuse detection system to monitor connections, login counts, cookies, machine IDs, and other related data;
 - c) Avoid storing passwords unless the passwords (and files) are hashed and salted or are otherwise encrypted.³¹ A password manager, as suggested above, can help;
 - d) Remove or disable all default accounts from all devices and conduct regular audits to ensure that inactive accounts can no longer access your infrastructure;
 - e) Remove access immediately for any terminated employees and any third parties or vendors that no longer require access to your infrastructure;
 - f) Prevent password re-use or recycling.

4. **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.
5. **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.
6. **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.).
7. **Maximize security and privacy of email** by requiring email authentication on all inbound and outbound mail servers. This helps prevent business email compromise (BEC) and detect malicious email including spearphishing and spoofed email.³² Unauthenticated email can be a “blind spot” in an organization’s security including IoT devices where security notifications can be spoofed resulting in unauthorized password resets , devices being botched and other/or being disabled from users downloading malicious updates. All organizations should:
 - a) Authenticate outbound mail with both 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 spearphishing and spoofed email;
 - 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;
 - e) As possible, implement TLS for email to maximize the privacy and security of email in transit.³³
8. **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.
9. **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.
10. **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).³⁴ If relying on third-party hosting services, require deployment of firewalls.

11. **Permit only authorized wireless devices** to connect to your network (including any IoT devices). Encrypt communications with devices such as routers, printers, point of sale terminals and credit card devices. Keep “guest” network access on separate servers and access devices with strong encryption. If using Network Address Translation technology make sure that guest devices receive a different NAT address at the boundary of your network.
12. **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.³⁵
13. **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.³⁶
14. **Ensure all updates and patches verified/signed** coming from a trusted source. This includes enterprise-wide implementations, connected devices and individual user updates and mobile devices.
15. **Back up key data to offline storage.** Being prepared for data corruption and ransomware data encryption is critical. Even after paying ransom and receiving keys to unlock files, it is not uncommon for some data to become corrupted.
16. **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.
17. **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.³⁷
18. **Complete an inventory** of all IoT devices including personal employee devices that connect to company networks. This inventory should be ongoing and reviewed for known vulnerabilities and product vendors’ life-cycle security policies.
19. **Benchmark your company’s security posture with third-party assessments.** Continual evaluation of your security program can help identify strengths and areas of improvement. It can also be a useful communication tool for important stakeholders.
20. **Bake DDoS protection into your business incident response plan.** You need to include procedures for DDoS mitigation in your plan. This will help to minimize any delay in responding to an attack and help assure that your company executives will commit the necessary resources for prevention and mitigation. If you don’t have a DDoS protection solution in place, then at least know who to contact immediately if you suspect your company is under attack. DDoS attacks are on the rise. Every good security plan has to include mitigation in order to minimize the effects of a service outage.³⁸

DATA STEWARDSHIP

A well-designed data management program is an essential first step in not only meeting compliance and regulatory obligations, but more importantly, demonstrating to consumers and business partners that an organization has taken reasonable steps to protect data and an organization from abuse and loss. A fundamental element is embracing the concept of data minimization; the collection and holding only the minimum amount of personal data needed to fulfil a business purpose. Developing a program can help minimize risk to consumers, business partners and shareholders, while increasing the value of the brand and the long-term business value. 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.

At a minimum, data management programs need to focus on several key fundamentals. First, privacy policies and practices must evolve. Just as business is dynamic, so too are privacy policies which require ongoing review and updates. Second, organizations should recognize that they collect one or more forms of covered data / PII or have intellectual property of value to cybercriminals or hacktivists. This can range from employee payroll data to consumer birthdays, phone numbers and home addresses to executives' personal and confidential emails. Third, business leaders need to realize that while there is no perfect security, there is also no excuse for not adhering to industry standards and norms. An incident, 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 security defenses, data lifecycle strategy and to develop an effective incident response plan.

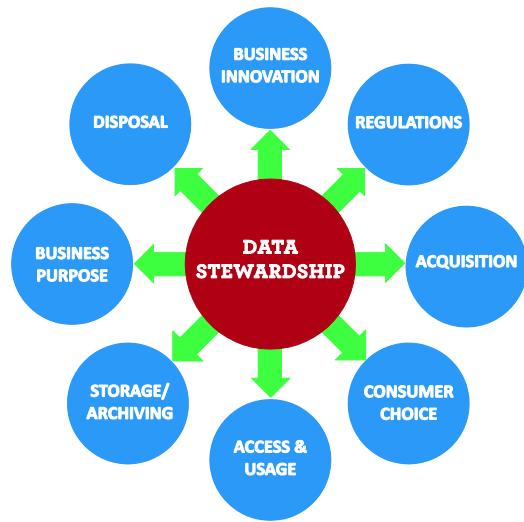


Figure 1 - Data Stewardship

Active management of the data lifecycle (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 disposal at the end of its business purpose. The primary data lifecycle stages include: collection, storage, use, sharing, archiving and destruction. The objective of a data minimizations strategy and data lifecycle management is to prevent unauthorized disclosure, modification, removal or destruction of data.



Figure 2- Data Lifecycle

Beyond simply managing the lifecycle, you must be a good steward of your data. The first step is to identify what data you gather and revalidate its business purpose. As observed in the Sony and recent DNC breaches of executives' emails, the reputational impact due to breaches of email services can be significant. Organizations should include a review of your email retention, archiving and storage practices. 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. Business leaders must continually review their notification, collection and use practices when new products, services, and

marketing partnerships are developed. The definition of “privacy” and the composition of PII continues to evolve, both in the U.S. and abroad. Applying yesterday’s rules may no longer be applicable in today’s data driven economy.

This Guide has been written to help identify 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 program are outlined in Figure 3.

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 retail point of sale systems, in-store mailing lists, event registrations and ecommerce shopping carts. Major challenges include not only evolving legal definitions of “covered” or “sensitive” data, but also widening awareness of the importance and sensitivity of other types of business information such as emails.

It is important for organizations to continually inventory their information, compare it to changing definitions of covered information as well as understand its business sensitivity. 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 information 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, data minimization strategies and implement BYOD and device management policies. With the advent of IoT connected and smart devices in the workplace, organizations need to survey and establish policies to help prevent the devices from becoming a back door to an organization’s network.

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 approved in April 2016, organizations must designate Data Protection Officers by 2018.³⁹



Figure 3 - Data Management Program Elements

DATA COLLECTION CONSIDERATIONS



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 approach includes:

- What data and attributes do you collect?
- Is the business purpose for this data collection still valid?
- What data do you care about protecting and why?
- Do you have an inventory of where is the data (and emails) are stored and archived?
- 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.⁴⁰ 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. 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 or isolate 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.

As the definition of PII and covered information is rapidly evolving, organizations need to take a broader view of the sensitivity of the data they retain. Historically in the US, 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, car license plates, etc.⁴¹ 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
- 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. 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 providers;
- Scanning of outbound email for protected content (Data Loss Prevention (DLP) solutions);
- 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 and recovering/securing all appropriate physical media or devices upon employee transfer, 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, and connected devices as well as their respective encryption requirements. 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 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 including malvertising. 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.

DATA LOSS PREVENTION TECHNOLOGIES

Data Loss Prevention (DLP) solutions enable enforcement of data protection policies and provide data discovery, data encryption, event monitoring and quarantine of sensitive data. Usage can help identify vulnerabilities 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 of unauthorized employee access. While such actions may appear benign they can help identify lapses of adherence to company policies and help identify the need for employee training and the implementation of added controls. 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 are recommended to communicate such policies in employee handbooks. 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 externally
- Data in use – Typically defined as data being created and modified.⁴²

DATA MINIMIZATION, DE-IDENTIFICATION & DESTRUCTION

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.⁴³ 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.⁴⁴ It should be noted that de-identification standards may differ among different industries.

A common mistake is not purging unneeded data including but not limited to email archives. 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. Legal requirements for data retention and destruction must be considered and addressed. Requirements differ by industry and type of information (email retention, transaction data, PII, etc.) and vary by country. To reduce risk of unauthorized access while meeting retention requirements offline storage and/or online archiving may be considered.

Any data no longer required 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.⁴⁵

CYBER INSURANCE CONSIDERATIONS

The sophistication and severity of cyber incidents have highlighted the need for all organizations to complete an assessment of their insurance coverage including cyber insurance, general liability and business continuity coverage. Cyber insurance is rapidly evolving in all areas from underwriting review and risk assessment to coverage and exclusions. Annual premiums are projected to grow tenfold from \$2 billion today to over \$20 billion by 2025, underscoring the demand for coverage for organizations of all sizes.⁴⁶

Compared to other insurance products, the cyber market is somewhat immature, facing rapidly shifting risk exposure and limited actuarial data. While loss experience grows and policies become more standardized, simple comparisons can be difficult. Business customers should be alert to potential policy deficiencies. For example, in Target's breach in 2013, they only had coverage for 38% of reported losses.⁴⁷ At one time it may have been safe to assume that costs of a breach would be covered under a commercial liability policy, but many newer policies explicitly exclude direct and third party costs associated with breach.

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. Adoption of best practices for risk assessment, data stewardship, security and encryption, incident response planning and enterprise-wide training not only can improve a company's ability to secure cyber insurance, it can help lower premiums. The process of obtaining data breach insurance varies depending on the size of the insured and the amount and type(s) of coverage sought. For larger policies, as part of the underwriting process, carriers increasingly demanding qualitative assessments of their policyholders' cyber security defenses, as opposed to strictly quantitative assessments historically used to underwrite property and casualty risks. The prospective insurer may require an information technology security 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 to guide such assessments.⁴⁸

When selecting cyber insurance policies, it is imperative to consult with an insurance broker who can provide expertise in navigating coverage options and alert businesses to important coverage exclusions. Policies may exclude such things as physical damage which might result from an external cyber incident targeting internal infrastructure, costs associated with breaches caused by third parties, and costs associated with business interruption and/or third party liability. All of these costs can be covered by a policy or an add-on endorsement, but they may not be. It is critically important to anticipate the coverage your business may require, communicate these needs to a broker and review any proposed coverage. In addition, a review of current coverage should be conducted to assess what cyber risks current policies cover. Look for possible cyber coverage in Crime, Directors & Officers, Professional Liability and Property policies. These lines may also respond to cyber events or contain important exclusions. It is difficult to make direct comparisons of the price per million dollars of coverage without getting into a detailed policy analysis. On the one hand, the purchase of 'fit for purpose' cyber insurance has been successfully used to offset financial impacts of some of the largest cyber incidents in recent years, including high profile breaches in the retail and healthcare sectors. On the other hand, companies have been surprised by limited coverage and broad exclusions resulting in denial of claims.

Cyber risk is complex and constantly changing, and the lack of historical data can make it difficult to evaluate exposure and 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 case, insurers refused to pay on the grounds that the event was the result of an indirect incident.⁴⁹⁵⁰ Others such as PF Chang's found their coverage reimbursed their credit card processor but did not cover fees charged to them by the merchant bank even though they were a direct cost the third party incurred as a result of the breach.

In review of these high-profile examples cited there are two recurring lessons.⁵¹ First, it is imperative that you and your legal team thoroughly review the scope of any cybersecurity coverage you select, paying particular attention to the express exclusions. Second, if your business contracts with third-party facilitators to process credit card transactions, you and your legal team must scrutinize those contracts (and likely others) to assess whether they potentially create uninsured losses. Such information not only might dramatically impact service contract negotiations with your vendors, but might educate you on what to look for when securing a cybersecurity policy.

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, its appetite to hold that risk, the retentions / deductibles the company can sustain and appropriate coverage limits. Increasingly, third-party contracts require "cyber" coverage. If entering such a contract, be certain to define "cyber" such that correct coverage is secured in order to avoid possible future disputes or lapses in coverage. In its 2016 annual report, the Federal Insurance Office encouraged insurers to hold their business partners, suppliers and customers to the risk management principles in the 2014 National Institute of Standards and Technology Cybersecurity Framework.⁵²

For cyber insurance considerations, see Appendix C. Common cyber insurance coverages include:

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

For all areas of coverage, it is important to carefully understand specific policy elements, including:

- Whether sub-limits on coverage match the corresponding risk
- Presence of sub-retentions (sub-deductibles) that are attainable vs unlikely to be reached
- Exclusions which prevent payment for key risks (e.g., charges following a credit card breach, common theories alleged in class actions, etc.)
- Ability to select legal counsel vs being restricted to a pre-defined panel
- Retroactive date/prior acts coverage for liability coverages
- Additional loss prevention/mitigation services available to the policyholder

INCIDENT RESPONSE FUNDAMENTALS

Being prepared for the inevitable cyber incident is a requirement for every organization. No different than being prepared for an on-the-job injury, potential fire or earthquake, all organizations large and small in both the public and private sector 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 and observed vulnerability. 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 in the Guide.

INCIDENT RESPONSE TEAMS

Cyber incidents are interdisciplinary events that require coordinated strategies and responses. Every functional group within an organization needs to be represented.⁵³ 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.

Plan Fundamentals

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

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.
- Legal counsel (both in-house and external).
- 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.
- 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, forensics and identity theft prevention and mitigation services.

ESTABLISHING VENDOR AND LAW ENFORCEMENT RELATIONSHIPS

Service providers should be considered for supporting critical functions including public relations, notification activities, and forensics. Recognizing that in the midst of an incident you will have relatively little leverage to negotiate preferable terms of a service agreement, given the importance and criticality and need to ramp up quickly, organizations are best suited to negotiate services prior to an incident. 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.⁵⁴ Other third parties to consider are PR and reputation management, credit monitoring \volumes in the event of a significant breach. Vendor selection considerations are:

- 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
- Pre-approved by your insurance carrier

Agreements should include risk management language and an assessment of your data. Audit validation processes and performance benchmarks are essential parts of any agreement. In addition, include terms that address responsibility in the event of an incident. These provisions should include the allocation of costs, such as response costs, as well as responsibility for notifications.

Prior to a cyber incident, organizations are encouraged to develop relationships with local regulators and law enforcement such as the state Attorneys General's office, regional FTC staff, the FBI, U.S. Secret Service and local U.S. Attorney's Offices. Knowing who to contact and their regional processes can pay significant dividends in the middle of an incident. The U.S. Secret Service has established the Electronic Crimes Task Force with regional offices.⁵⁵ 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. Organizations are encourage to join InfraGard, an information sharing and analysis partnership between the FBI Cyber Task Force and the private sector.⁵⁶ Appendix E includes a form to collect information commonly requested by law enforcement when investigating a cyber incident.

CREATING RESPONSE PLANS

A comprehensive cyber incident response plan includes a time-line and process flow. This is a critical tool for managing the pressing demands resulting from an incident. 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 issues and manage the expectations of each group. 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.

Response plans should address the following key questions:

1. What is the overall impact of the incident (number of consumers, types of data, business continuity, etc.)?
2. What are the regulatory obligations and should law enforcement be notified?
3. How will the incident 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 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 the incident 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 and business partners?

FORENSICS, INTRUSION ANALYSIS & AUDITING

Effective incident response has several phases including preparation, detection and analysis, containment and eradication, recovery and post-incident analysis.⁵⁷ When an incident is first discovered the initial actions taken can have important ramifications for regulatory compliance, legal actions, insurance coverage and business continuity. Ideally, before an incident occurs companies will have prequalified potential forensics vendors in concert with their insurance coverage. Many insurers have pre-approved panels of legal counsel and forensics vendors with pre-negotiated rates which are covered. Failure to use an approved vendor can lead to significant costs which may not be fully recovered.

The forensic examination is an essential element of the analysis phase of a cyber incident response to help determine the source (root cause) and magnitude (scope) of an incident. Because it is easy to render forensic evidence inadmissible in court by accidentally modifying the evidence or disrupting the chain of custody, forensic examination is best left to experts. 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 forensic analysis in advance of an incident. 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 confidentiality of any findings. In all cases, be sure to consult with your insurance provider to understand what services and which providers would be covered.

Upon learning of a possible incident, 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.

Recommended Forensics First Steps:

- Prior to an incident contact your cyber insurance provider(s) and legal staff for guidance on actions and covered (“in network”) forensics providers.⁵⁸
- 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.
- Secure and protect the physical integrity of any data collected and ensure that any systems impacted are only accessible to internal or hired investigators and law enforcement. Make sure you track the chain of custody of all collected data and store an unaltered original of any collected data in a secure location with limited access.
- Isolate suspected servers and client workstations from the network, unplugging network cables or disconnecting the workstations from wireless access points as appropriate.
- Preserve and store all critical network and local OS log files in a secure location, including web client and server operating systems, application, mail, firewall, IDS, VPN, DLP and network flows. Due to rotation schedules and possible overwriting, saving of critical logs must happen as soon as possible. Review archived logs and collect any that may contain data relevant to the incident.
- 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 if possible) and if they are off, leave them off.
- Do not shut down or unplug any server or device unless required to do so.
- 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. Organizations may have a number of log types, including but not limited to transaction, server access, application server, firewall and operating systems. In addition endpoint security controls (e.g. AV, IDS, DLP and APT and others), can provide invaluable insights and telemetry and should be reviewed on an ongoing basis. As attackers understand the value of logs and often attempt to delete them to “cover their tracks”, it is important to help protect logs by isolating and archiving them.

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 (SIEM) is highly recommended. A SIEM 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.

Critical Logs

- Firewall
- Transaction
- Database Server
- Application Server
- Point of Sale Systems
- Operating System
- Net Flow / VPN
- Web Servers
- Endpoint Security Devices

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, Data Protection Officer and/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 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 additional information.

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 or “covered data”. Failure to notify the appropriate government agency(s) 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 and, as recently observed, multiple regulators may have jurisdiction. In October 2016, the FCC adopted rules for Internet Service Providers which address privacy and include specific breach reporting requirements. This recent rule making could set the stage for a national standard for all organizations.⁵⁹ 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.^{60 61} In 2016, other states made revisions including New York, Washington, Nebraska and Illinois, each updating requirements and many expanding their definition of personal data among other covered data revisions.⁶² In early 2017 California updated its data breach reporting requirements including instances where encrypted data and a key may have been exposed.⁶³

Knowing 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 may include: the number of individuals impacted; the specific data elements exposed; the risk to the affected constituents from such exposure; regulatory requirements; and law enforcement jurisdiction. Speed and accuracy are equally important. Consumers expect timely and clear notification delivered in a manner appropriate to their needs, and depending on the data that was breached, may have an expectation of remediation and credit monitoring services free of charge.

As of January 2017, there are 47 states, plus Washington, D.C., Guam, Puerto Rico, and the Virgin Islands with laws that govern data breach notifications. 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.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 including at a minimum their address and primary email address. This helps to develop customized notices based on where the user resides.

COMMUNICATING EFFECTIVE RESPONSES

A well-executed communications plan not only minimizes harm and potential legal liability, but can also enhance a company's brand reputation. Ineffective 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. Being ready to communicate during a cyber incident crisis requires much more preparation than a basic crisis plan and generic messaging.

Missteps can generate cascading negative effects.

Understanding these common errors can help stricken companies avoid adding insult to injury when a crisis strikes.

Communication plans typically need to address six audiences:

1. Internal teams including 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.

Appendix B includes sample breach notification letters in to assist in writing data breach notification letters for affected individuals. Regularly check that the contact information provided in the sample letter is up to date for federal and state agencies as well as the national consumer reporting. Remember, these letters must be tailored to reflect your company's particular circumstances and to address all specific legal requirements.

Organizations found to be in violation of breach notification laws or industry regulations could face regulatory fines or settlements. 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. Organizations are encouraged to work with data privacy experts and/or legal counsel specializing in data breaches. In addition, a firm's cyber insurance policy should be reviewed for coverage. See Appendix C for cyber insurance considerations.

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.

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 SMS/text alerts, emails, written correspondences, in-mobile app messaging and website postings. 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 customized messages and methods of delivery for the company's most important relationships, such as its highest-value customers or senior employees.

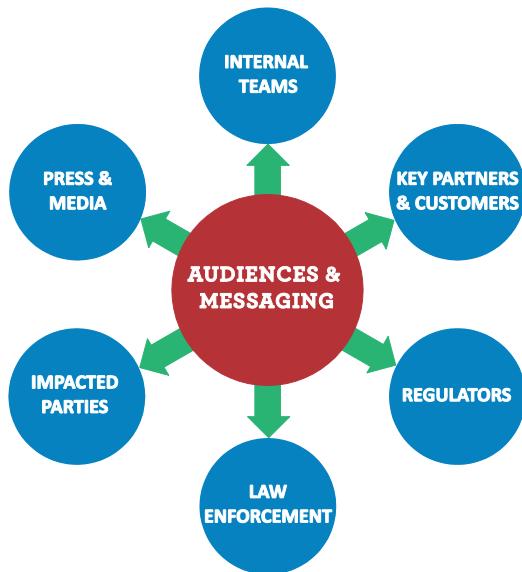


Figure 5 – Critical Audiences

Tips on writing an effective breach notification communications:

- Take responsibility, be humble and apologize if possible. Be clear and unassuming. Explain what happened, be transparent and honest.
- Provide a clear description including what, how and when the incident occurred using language and terms comprehensible by the intended audience. Avoid technical terminology or ‘legalese’ which may result in increased frustration and anxiety. Consider multiple language options or offer bilingual support.
- Outline what types of data were lost or compromised and the scope of the incident.
- Communicate the actions you are taking to assist affected persons or organizations. Outline remedies such as credit monitoring and identity theft protection services.
- 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? Provide a phone number and online resources for additional information.
- How will the organization keep affected customers informed?
- Lastly, apologize again and mean it, signing the letter by an executive or officer of the organization.

PROVIDING ASSISTANCE & REMEDIES

Offers to affected parties may range from credit report monitoring and identity theft protection to credit counseling. In addition, commerce sites may wish to offer promotion offers and gift certificates to gain back disgruntled customers. It is important to note there are significant differences between credit monitoring and identity theft protection services. Fraud alerts show that fraud has occurred, usually well after the fact, frequently leaving customers frustrated and solving identity problems on their own. Identity theft protection often monitors an extended network of services, and can alert members to potential fraud much earlier than credit monitoring, covering a host of fraud types not covered by credit monitoring

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 incidents, 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. 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 cyber incident 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 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 for users who are hearing impaired. 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.⁶⁵

In addition to offering identity theft and credit monitoring services, organizations may want to consider 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 F.

TRAINING, TESTING & BUDGETING

A well-prepared incident response plan is at risk if employees are not adequately trained and prepared. Organizations must allocate staff time and budget to properly execute their plan, accounting for employee turnover and evolving regulatory requirements. 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 tabletop 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.

EMPLOYEE AWARENESS & 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 tabletop 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. In addition password management processes need to be enforced including but not limited to password strength, prevention of reuse of common words and forced reset parameters. Training should not only include responding to an incident, 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.

DLP services and software can help identify processes 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 included 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 compliance. In addition, the training session should discuss the importance of password management practices including not allowing re-use of passwords on multiple sites, safe computing practices. As BEC exploits are on the rise and spear phishing has become more precise, it is critical that employee training reviews how to help identify and potential phishing emails and social exploits and provide guidance on posting company information on social networking sites.⁶⁶

FUNDING AND BUDGETING

Responding to a cyber 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 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
- Physical & Life Safety Damages

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 incident should also include a postmortem analysis in which key team members analyze the circumstances pertaining to the incident 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?
- Was operational and system downtime acceptable?

REGULATORY LANDSCAPE

The global regulatory landscape has changed dramatically in the past 12 months. In the U.S., rules recently enacted by the U.S. Federal Communications Commission outline specific privacy protections and data breach requirements for ISPs and carriers.⁶⁷ In the last days of the Obama administration, the “Framework for Breach Response” was released to provide consistent breach response requirements cross US government agencies, replacing guidance released nearly a decade ago.⁶⁸ While the U.S. Congress’ efforts to develop national breach legislation have stalled, other countries are have moved forward including many in Europe, Latin America and the Asia Pacific.⁶⁹

European Union

The view of data privacy in the European Union (EU) impacts businesses worldwide as demonstrated in 2015 when the European Court of Justice overturned the 15 year old U.S.-EU Safe Harbor agreement with more stringent data security and privacy requirements. The replacement is the EU-U.S. Privacy Shield which was approved in July 2016, providing companies with a mechanism to comply with requirements when transferring personal data from the European Union to the United States in support of transatlantic commerce.⁷⁰

The European data protection requirements covered in Privacy Shield are those in the EU’s General Data Protection Regulation (GDPR). Passed by the EU Parliament in April 2016, with the goal of enabling users to control their data while making businesses more accountable, the GDPR includes the following strategic objectives:⁷¹

- Strengthen individuals’ privacy rights.
- Harmonize rules and enforcement throughout the EU.
- Promote high standards of data protection in a technologically 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.

For many organizations the GDPR will be a game changer. The GDPR supplants the prior patchwork of national laws in Europe. Companies that are in EU member countries, offer services to EU citizens and/or handle EU citizens’ personal data are subject to GDPR. These regulations have been designed to help enable people to better control their personal data and aid businesses which benefit from reduced red tape and a single legal framework. The GDPR is scheduled to apply beginning May 25, 2018. It contains key provisions including breach notification and data security requirements. The EU regulations direct 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.⁷² In December 2016, the Article 29 Working Group announced implementation guidelines providing added clarification.⁷³

Concurrently the EU has published proposed updates of the e-Privacy Directive creating a harmonized set of requirements including specifying the requirement to support browser based privacy settings.⁷⁴ In parallel, several countries have enacted related legislation independent of the EU. In January 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.^{75 76} In October 2016, Germany strengthened the ability of consumer groups to enforce data protection rights and others to take actions to prevent

EU Considerations

- Opt-In vs Opt-Out
- Honoring “Do-Not-Track”
- Privacy Shield Provisions
- Reasonable Security
- Adequate Notice
- “Right to be Forgotten”
- Data Server Locations
- Definition of PII
- Penalties up to 4% of revenue

violations of consumer data protection regulations.⁷⁷ Similarly, in November France adopted a law creating specific class action rights for violations of the data protection law.⁷⁸

Australia / New Zealand

The Australian Privacy Act of 1988 (updated in 2014) regulates organizations' handling of personal information through the application of the Australian Privacy Principles (APP). The Act generally only applies to entities with an annual turnover of over AUD\$3 million. Updates to the Act includes a maximum fine to AUD\$1.7 million per incident and a modified definition of the scope of personal information to include any information which is reasonably identifiable. This change expands the Act to include information about an individual which, when combined with other information an entity has access to (e.g. through a related organization), could enable that individual to be identified. The Act requires an organization subject to the Act which discloses personal information to an international entity to take reasonable steps to ensure the recipient does not breach the APPs.⁷⁹

The APP requires government agencies and businesses to take reasonable steps to secure personally identifiable information, but does not mandate notification, with the exception of unauthorized access to eHealth information. Broader legislation including a draft bill on serious data breach notification, is pending amid concerns around limited disclosure to avoid "breach notification fatigue."⁸⁰ Notwithstanding pending legislation, organizations are voluntarily notifying regulators when they determine a reasonable person would conclude that there is a likely risk of serious harm to as a result of the unauthorized access or unauthorized disclosure (assuming, in the case of loss of information, that the access or disclosure occurred).⁸¹

Organizations conducting business and collecting personal information in New Zealand should be aware of the pending legislation. Key provisions of the privacy act, including 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.⁸²

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

The Digital Privacy Act approved in 2015 made 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. 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 The Department of Innovation, Science and Economic Development is required to develop regulations, which appears likely to occur sometime in 2017⁸⁶ with breach notification requirements likely coming in to effect in 2018.

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

CONCLUSION

Organizations and businesses around the globe are faced with mounting complexity, severity and precision in cyber-criminal activities, abuse and hacktivism. Compounded in part by abusive privacy practices, government surveillance, deceptive news and advertising, consumer trust has been significantly tarnished. The recurring incidents have an additive, long-term effect on society not unlike global warming and carbon emissions. Their collective impact to the environment, while first dismissed, have now created what many believe are non-reversible environmental damages. The current disregard for core security and responsible privacy practices are now leading the internet down a similar path. Combined with the explosive growth of big data, IoT devices and the reliance on cloud providers, it is vital to recognize that data stewardship should become a priority for every organization. Failure to do so risks placing consumers in harm's way, adding to the call for regulatory oversight and internet governance which run the risk of inhibiting innovation.

Combined, the “environmental cyber threat landscape” underscores the need for every organization, small and large, to recognize their responsibility along with the urgency to take a holistic view of data security and privacy protection practices. Left unaddressed, we risk a significant impact to society and commerce.

Putting in place technologies, processes and procedures to help prevent, detect, mitigate and respond to all incidents is essential. Developing an end-to-end readiness plan recognizing one size does not fit all is the only way to control and manage the fall-out of an incident. As outlined in this Guide, the best defense is a three-step strategy. First, implement a broad set of operational and technical best practices that help maximize the protection of customer and company data; second, be prepared with an incident response plan that allows a company to respond with immediacy while ensuring maximal business continuity and third, understand that human factors play a critical role in how strong or weak an organization’s security defenses are, how they respond and most importantly how their actions are judged. Following the guidance in this document will help minimize the impact from any incident.

Key Principles:

- Every organization is at risk, and those that fail to demonstrate they have adopted and implemented sound practices will ultimately be held accountable,
- Every organization holds data of interest to criminals, hacktivists or state sponsored actors,
- Organizations and policy makers need to look beyond the impact and cost of a “traditional data breach” to the life safety and physical impact of an incident and damage to an organization’s reputation,
- Incentives and possible regulations are needed to accelerate “security by design” along with annual security assessments of sites, applications services and devices,
- Assessment of all vendors and cloud providers must be ongoing,
- Have an updated response plan involving cyber first responders and ongoing “table top exercises,”
- Develop and continually update communications plans with messages tuned for all audiences,
- Review the regulatory landscape quarterly for potential changes and implication of business operations.

OTA encourages all businesses, non-profits, app developers, and government organizations to make a renewed commitment to cyber security and privacy. Being prepared for a cyber incident is good for your business, your brand and most importantly your customers.

APPENDIX A – RESOURCES & READINGS

ONLINE TRUST ALLIANCE

- Cyber Incident & Breach Response Resource Center - <https://otalliance.org/incident>
- Email Security & Authentication (SPF, DKIM & DMARC) – <https://otalliance.org/eauth>
- Internet of Things Trust Framework & Checklists – <https://otalliance.org/IoT>
- Online Trust Audit & Honor Roll – <https://otalliance.org/TrustAudit>
- Security & Privacy Enhancing Best Practices - <https://otalliance.org/resources/security-privacy-best-practices>
- Visions for Online Trust - <https://otalliance.org/Vision>

INDUSTRY

Identity Guard / Intersections Inc.

- Consumer ID Theft Resources - <http://www.identityguard.com/news-insights/category/tools/>
- Breach Readiness –http://www.intersections.com/library/7stepstodatabreach_040611%20FINAL.pdf
- Learnings- <https://www.identityguardbusiness.com/resource-center/learning-from-a-recent-data-breach-case/>
- Breach Response Solutions <https://www.identityguardbusiness.com/breach-services>
- Identity Guard - <http://www.identityguardbusiness.com/>

LifeLock

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

Symantec

- Symantec Cyber Insurance - <https://www.symantec.com/solutions/insurance>
- Security Internet Security Threat Report - <https://www.symantec.com/security-center/threat-report>
- Symantec Encryption Solutions - <http://www.symantec.com/encryption>
- Symantec File Share Encryption - <http://www.symantec.com/file-share-encryption/>
- Symantec Website Security - <https://www.symantec.com/website-security/>

Verisign

- DDoS Mitigation Support - https://www.verisign.com/en_US/forms/underattackrequestform.xhtml
- Featured Reports - https://www.verisign.com/en_US/internet-technology-news/published-reports/index.xhtml
- Verisign Blog - <https://blog.verisign.com/>
- DDoS Reports - https://www.verisign.com/en_US/security-services/ddos-protection/ddos-report/index.xhtml

U.S. GOVERNMENT & STATE AGENCIES

Federal Trade Commission

Responding Breaches - <https://www.ftc.gov/news-events/blogs/business-blog/2016/10/responding-data-breach>

Complying with the FTC's Health Breach Notification Rule <https://www.ftc.gov/healthbreachnotificationrule>

Dept. of Education, Breach Response Kit - <http://ptac.ed.gov/document/data-breach-response-training-kit>

Dept. of Homeland Security, Cybersecurity - <https://www.dhs.gov/topic/cybersecurity>

Federal Bureau of Investigation (FBI) Cyber Resources - <https://www.fbi.gov/investigate/cyber>

Secret Service Electronic Crimes Task Force - <http://www.secretservice.gov/investigation/>

Department of Commerce Privacy Shield resources: <https://www.commerce.gov/page/eu-us-privacy-shield>

NIST Cybersecurity Framework - <https://www.nist.gov/cyberframework>

State of California

Breach reporting <https://oag.ca.gov/ecrime/databreach/reporting>

Privacy <https://oag.ca.gov/privacy>

Breach Reports <https://oag.ca.gov/privacy/privacy-reports>

State of Massachusetts - <http://www.mass.gov/ocabr/data-privacy-and-security/data/>

State of New York - <https://its.ny.gov/eiso/breach-notification>

State of Ohio - <http://infosec.ohio.gov/Business/DataBreachNotificationandResponse.aspx>

State of Rhode Island - <http://webserver.rilin.state.ri.us/BillText15/SenateText15/S0134B.pdf>

State of Washington - <http://www.atg.wa.gov/data-breach-notifications>

CANADA

Personal Information Protection and Electronic Documents Act (PIPEDA) - <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/>

Privacy Toolkit - https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/guide_org/

Office of the Privacy Commissioner of Canada - <https://priv.gc.ca/en/>

NON-PROFITS

Anti-Phishing Working Group (APWG)

Research & Whitepapers <http://apwg.org/resources/apwg-reports/whitepapers>

Educating Your Consumers <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 - www.bbb.org/cybersecurity

Data Security Guide - <http://www.bbb.org/data-security>

Identity Theft Council - <https://www.identitytheftcouncil.org/>

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

Internet Society, Global Internet Report 2016 - <https://internetsociety.org/globalinternetreport/2016/>

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

OWASP Incident Response - https://www.owasp.org/index.php/OWASP_Incident_Response_Project

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 endnotes 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.

[Name of Company/Logo] Date: [Insert Date]

NOTICE OF DATA BREACH

Dear [Insert Name]: We are contacting you about a data breach that has occurred at [insert Company Name].

What Happened? [Describe how the data breach happened, the date of the breach, and how the stolen information has been misused (if you know)].⁸⁸

What Information Was Involved? This incident involved your [describe the type of personal information that may have been exposed due to the breach].⁸⁹

What We Are Doing [Describe how you are responding to the data breach, including: what actions you've taken to remedy the situation; what steps you are taking to protect individuals whose information has been breached; and what services you are offering (like credit monitoring or identity theft restoration services).]

What You Can Do We recommend that you place a fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Call any one of the three major credit bureaus. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. The initial fraud alert stays on your credit report for 90 days. You can renew it after 90 days.

Equifax: equifax.com or 1-800-525-6285

Experian: experian.com or 1-888-397-3742

TransUnion: transunion.com or 1-800-680-7289

Request that all three credit reports be sent to you, free of charge, for your review. Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Thieves may hold stolen information to use at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, file a police report and call [insert contact information for law enforcement if authorized to do so]. Get a copy of the police report; you may need it to clear up the fraudulent debts.

If your personal information has been misused, visit the FTC's site at IdentityTheft.gov to get recovery steps and to file an identity theft complaint. Your complaint will be added to the FTC's Consumer Sentinel Network, where it will be accessible to law enforcers for their investigations.

You also may want to consider contacting the major credit bureaus at the telephone numbers above to place a credit freeze on your credit file. A credit freeze means potential creditors cannot get your credit report. That makes it less likely that an identity thief can open new accounts in your name. The cost to place and lift a freeze depends on state law. Find your state Attorney General's office at naag.org to learn more.

We have enclosed a copy of Identity Theft: A Recovery Plan, a comprehensive guide from the FTC to help you guard against and deal with identity theft. We've also attached information from IdentityTheft.gov about steps you can take to help protect yourself from identity theft, depending on the type of information exposed.

Other Important Information [Insert other important information here.]

For More Information Call [telephone number] or go to [Internet website]. [State how additional information or updates will be shared/or where they will be posted.]

[Insert Closing] [Your Name]

IF SOCIAL SECURITY NUMBERS WERE INVOLVED

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

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

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

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

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

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 individuals can take to protect against misuse of their 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 WERE 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.

Sincerely, [Name] [Title] / [Contact Information]

Note: Notices should, and in some states must, include contact information who can assist and provide information to affected individuals and be signed by an executive demonstrating concern and commitment.

APPENDIX C – CYBER INSURANCE CONSIDERATIONS

PROTECTIONS	
<input type="checkbox"/>	Coverage for loss resulting from administrative or operational mistakes – extends to acts of the employee, business process outsourcing (BPO) or outsourced IT provider.
<input type="checkbox"/>	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.
<input type="checkbox"/>	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 separate media liability policy.)
<input type="checkbox"/>	Coverage for socially engineered exploits including account credential disclosures, ACH transfers and other related losses arising from such exploits (may be available via endorsement or crime policy).
<input type="checkbox"/>	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.
<input type="checkbox"/>	Broad coverage for damages to third parties caused by a breach of network security.
<input type="checkbox"/>	Breach of privacy coverage includes damages resulting from alleged violations of HIPAA, state and federal privacy protection laws and regulations.
<input type="checkbox"/>	Regulatory expense coverage to comply with an alleged breach notice order (both Federal and State).
<input type="checkbox"/>	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 (CCRAA) and the EU Data Protection Act.
<input type="checkbox"/>	Public relations expenses to repair your reputation as a result of a data breach.
<input type="checkbox"/>	Breach notice coverage (via sub-limit) – reimburses for costs to notify and remediation costs including but not limited to credit monitoring. <i>Consider voluntary notifications.</i>
<input type="checkbox"/>	Coverage for rogue employee(s) causing intentional damage to the insured's network.
<input type="checkbox"/>	Expenses including forensics, legal, remediation (credit monitoring expenses, postage and advertising) and other costs. Coverage for contractual liabilities including PCI-DSS costs.
<input type="checkbox"/>	Breach definition extends to acts of the Insured and acts of a Service Provider(s).
<input type="checkbox"/>	Punitive and exemplary damages coverage provided on a most favorable venue basis.
<input type="checkbox"/>	Business interruption coverage, including lost revenue as a result of a cyber incident.
<input type="checkbox"/>	Physical and bodily injury damages resulting from a cyber incident.
POLICY ELEMENTS	
<input type="checkbox"/>	Sub-limits on coverages match corresponding risks and sub-retentions (sub-deductibles) are attainable.
<input type="checkbox"/>	Knowledge provision includes Board of Directors, President, Executive Officer, Chairman, Chief Information Officer, Chief Technology Officer, Risk Manager or General Counsel.
<input type="checkbox"/>	Includes the ability to select legal counsel and third-party forensics services vs being restricted to a pre-defined panel.
<input type="checkbox"/>	Retroactive date/prior acts coverage for liability coverages.

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 cyber incident, it is important to engage an expert in computer forensics. Your cyber insurance coverage may include a panel of approved forensics service providers from which to choose. The forensics expert 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:⁹⁰

Infrastructure/Architecture Audit: Review and mapping of all systems and critical controls in advance of an incident with the goal to identify risk and optimize prevention, notification and remediation practices.

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.

APPENDIX E – INCIDENT REPORTING TEMPLATE

1. Organization Information					
Organization Name:					
Organization Address:					
Name of Person Reporting:					
Name of Network Administrator:					
Name of CISO or CIO:					
Name of CIO/Executive Level Decision Maker:					
Location & Date of Incident:					
Contact Phone Numbers:					
2. What type of network compromise has occurred? (please select all that apply)					
<input type="checkbox"/> Reconnaissance		<input type="checkbox"/> Malware		<input type="checkbox"/> Data Exfiltration	
				<input type="checkbox"/> 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?					
<input type="checkbox"/> Yes—If so, please list (include dates & summary)			<input type="checkbox"/> No		<input type="checkbox"/> Unknown
6. Does your network utilize any virtual machines, cloud services or third party service providers?					
<input type="checkbox"/> Yes – If so, please list			<input type="checkbox"/> No		<input type="checkbox"/> Unknown

7. Is remote connectivity enabled on your network?

<input type="checkbox"/> Yes – Please select all that apply	<input type="checkbox"/> No	<input type="checkbox"/> 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?

<input type="checkbox"/> Yes – Please list all services in use	<input type="checkbox"/> No
--	-----------------------------

9. Please list all domain names associated with your network.

10. Please provide your server's DHCP address.

11. Does your organization maintain DHCP logs?

<input type="checkbox"/> Yes – If so, where?	<input type="checkbox"/> No	<input type="checkbox"/> Unknown
--	-----------------------------	----------------------------------

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

<input type="checkbox"/> Yes – If so, where?	<input type="checkbox"/> No	<input type="checkbox"/> Unknown
--	-----------------------------	----------------------------------

13. Please provide your organization's network DNS address. Is it internal or external to your organization?

<input type="checkbox"/> Internal	<input type="checkbox"/> External	<input type="checkbox"/> 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)

<input type="checkbox"/> Yes – If so, where?	<input type="checkbox"/> No	<input type="checkbox"/> 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?		
<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Unknown
If so, are they active or passive?		
<input type="checkbox"/> Active	<input type="checkbox"/> Passive	
20. Do you suspect the unauthorized intrusion on your network to be the result of a current or former employee or vendor?		
<input type="checkbox"/> Yes	<input type="checkbox"/> No	
21. Are your employees informed of the limits of their acceptable use and privileges on your network?		
<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Unknown
22. Are employees given any instructions related to the cessation of their network use and privileges when they leave employment or are terminated?		
<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Unknown
23. Has your organization taken any steps to mitigate the impact of the intrusion?		
<input type="checkbox"/> Yes – if so, please describe	<input type="checkbox"/> No	<input type="checkbox"/> Unknown
24. Do you believe the breach was the result of a socially engineered exploit (spearphishing, malvertising, other) targeting employees or vendors?		
<input type="checkbox"/> Yes – if so, please describe	<input type="checkbox"/> No	<input type="checkbox"/> 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:	
Physical Damages (non IT):	
Personal Injury:	
Other Costs	
Total	

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

--

APPENDIX F – REMEDIATION SERVICE CONSIDERATIONS

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

APPENDIX G – INTERNAL RISK ASSESSMENT

OPERATIONAL RISK ASSESSMENT	
<input type="checkbox"/>	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?
<input type="checkbox"/>	Do we know all data attributes we collect and store for all customers? Where is this data stored, maintained, flowed and archived (including data our vendors and third-party/cloud service providers store or process)?
<input type="checkbox"/>	Is the original business purpose for collecting our data still valid and relevant? Can we identify points of vulnerability and risk?
<input type="checkbox"/>	Are our encryption, de-identification and destruction processes in alignment with industry accepted best practices and regulatory requirements?
<input type="checkbox"/>	Do we have a 24/7 incident response team in place? Are employees trained on a reporting and escalation processes?
<input type="checkbox"/>	Do we have an incident communication strategy and plan segmented for employees, customers, stockholders, regulators and the media?
<input type="checkbox"/>	Do we follow generally accepted security and privacy 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?
<input type="checkbox"/>	Does our privacy policy reflect our actual practices, including use of third parties? Have we audited our site, devices, applications and cloud services to confirm we are in compliance?
<input type="checkbox"/>	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 Attorneys General?
<input type="checkbox"/>	Are we (and our Board) willing to sign off on our incident response plan and be publically accountable for the security practices adopted?
<input type="checkbox"/>	Do we understand the security, privacy and notification practices of our third-party vendors and service providers and are these specified as contractual obligations?
<input type="checkbox"/>	Do we have an incident response vendor that can have experts on call 24/7 to assist with determining the root-cause of a breach, identifying the scope of an incident and collecting threat intelligence?
<input type="checkbox"/>	Has an inventory of all IoT devices been completed (including personal employee devices connecting to company networks)? This inventory should include review for known vulnerability and patching capabilities. Is there a process in place for continued monitoring?

This worksheet is intended to help survey and identify possible risks. It serves as starting point and based on the business sector and locations, other questions may be appropriate for a business to consider. Consult with your security, risk management and/or legal advisors for updates reflecting your business sector and risk appetite.

APPENDIX H – THIRD PARTY RISK ASSESSMENT

THIRD PARTY RISK ASSESSMENT	
<input type="checkbox"/>	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?
<input type="checkbox"/>	Describe the physical security of your data centers.
<input type="checkbox"/>	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?
<input type="checkbox"/>	How are vendor 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.
<input type="checkbox"/>	Describe the organizational structure for security operations at your company.
<input type="checkbox"/>	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?
<input type="checkbox"/>	How are you protected from DDoS attacks?
<input type="checkbox"/>	List all third party certifications or attestations, such as FedRamp, FIPS 140 -2, FISMA and DIACAP, HIPAA, ISO 27001, PCI DSS, or SOC 1/SSAE 16/ISAE 3402 or other relevant certifications.
<input type="checkbox"/>	Do you have current security audit reports such as SAS70/SSAE16 or similar audits which can be reviewed?
<input type="checkbox"/>	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.
<input type="checkbox"/>	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?
<input type="checkbox"/>	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

This worksheet is intended to help survey and identify possible risks. It serves as starting point and based on the business sector and locations, other questions may be appropriate for a business to consider. Consult with your security, risk management and/or legal advisors for updates reflecting your business sector and risk appetite.

APPENDIX I – INCIDENT READINESS CHECKLIST

RISK, SECURITY & DATA STEWARDSHIP	
<input type="checkbox"/>	Complete risk assessments for executive review, operational process and third party vendors (pg 11)
<input type="checkbox"/>	Review security best practices and validate adoption or reasoning for not adopting (pg 14) <ul style="list-style-type: none"> <input type="checkbox"/> Encrypt data at rest and in transit <input type="checkbox"/> Implement multi-factor authentication <input type="checkbox"/> Enforce password management policies <input type="checkbox"/> Adopt Least Privileged User strategy <input type="checkbox"/> Conduct code reviews & pen testing <input type="checkbox"/> Deploy multi-layered firewall protection <input type="checkbox"/> Require email authentication <input type="checkbox"/> Implement mobile device management <input type="checkbox"/> Continuously monitor security in real time <input type="checkbox"/> Deploy web app firewalls <input type="checkbox"/> Permit <u>only</u> authorized wireless devices <input type="checkbox"/> Implement Always On SSL <input type="checkbox"/> Review server certificates for vulnerabilities <input type="checkbox"/> Ensure all updates/patches are verified/signed <input type="checkbox"/> Back up key data to offline storage <input type="checkbox"/> Develop, test, continuously refine data breach plan <input type="checkbox"/> Establish a vulnerability/threat reporting program <input type="checkbox"/> Inventory all devices connecting to company networks
<input type="checkbox"/>	Audit data management and stewardship program including data life-cycle management (pg 17) <ul style="list-style-type: none"> <input type="checkbox"/> Inventory data collected (what, where, business purpose) <input type="checkbox"/> Practice data minimization <input type="checkbox"/> Inventory system access and controls <input type="checkbox"/> Inventory employee (internal and third party) access and controls <input type="checkbox"/> Review data loss prevention technologies in use <input type="checkbox"/> Confirm/enact appropriate data archive and destruction policies
<input type="checkbox"/>	Complete audit of insurance needs including exclusions and pre-approval of third party coverage (pg 22)
INCIDENT RESPONSE	
<input type="checkbox"/>	Establish end-to-end incident response plan including empowering first-responders on-call 24/7 (pg 24)
<input type="checkbox"/>	Establish/confirm relationships with law enforcement and incident service providers (pg 25)
<input type="checkbox"/>	Review/establish forensic capabilities, procedures and resources (internal & third party providers) (pg 26)
<input type="checkbox"/>	Review notification processes and plans (pg 29)
<input type="checkbox"/>	Develop segmented communication strategies and tactics tailored by audience (pg 30)
<input type="checkbox"/>	Review remediation programs, alternatives and service providers (pg 31)
TRAINING & CONTINUOUS LEARNING	
<input type="checkbox"/>	Implement employee training for incident response (pg 32)
<input type="checkbox"/>	Establish culture of employee data security awareness – provide employee education on data stewardship (privacy, risks, etc.), incident avoidance (password practices, recognizing social engineering, etc.) and incident response (who to notify, forensic dos & don'ts, etc.) (pg 32)
<input type="checkbox"/>	Understand the regulatory requirements, including relevant international requirements (pg 34)
<input type="checkbox"/>	Conduct “desk top” exercises and critiques to help maximize prevention, detection and remediation capabilities. Consolidate learning into an update incident respond plan and update training as required.

ENDNOTES

- ¹ Washington Post <https://www.washingtonpost.com/news/early-lead/wp/2016/09/13/world-anti-doping-agency-confirms-russian-hack-of-rio-olympic-drug-testing-database/>
- ² Yahoo Data Breach <http://searchsecurity.techtarget.com/news/450409941/Yahoo-breach-data-reveals-the-need-for-ethical-breach-reporting>
- ³ NYT http://www.nytimes.com/2016/08/11/us/politics/democratic-party-russia-hack-cyberattack.html?_r=0
- ⁴ Risk Based Security 2016 Year End Breach Report <https://pages.riskbasedsecurity.com/2016-ye-breach-quickview>
- ⁵ FBI BEC data <https://www.ic3.gov/media/2016/160614.aspx>
- ⁶ Symantec 2016 Ransomware Report
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ISTR2016_Ransomware_and_Businesses.pdf
- ⁷ NBC News Ransomware Growth <http://www.nbcnews.com/tech/security/ransomware-now-billion-dollar-year-crime-growing-n704646>
- ⁸ Malwarebytes ransomware rise <https://www.theguardian.com/technology/2016/aug/03/ransomware-threat-on-the-rise-as-40-of-businesses-attacked>
- ⁹ Verisign DDoS Trends Report <https://www.verisign.com/assets/report-ddos-trends-Q32016.pdf>
- ¹⁰ Includes data breach incidents from Risk-Based Security 3Q2016 report, BEC incidents from the FBI and ransomware incidents from the Symantec 2016 Ransomware report.
- ¹¹ ISOC <https://www.internetsociety.org/news/internet-trust-all-time-low-not-enough-being-done-protect-data-says-internet-society-report>
- ¹² Malvertising <https://otalliance.org/initiatives/malvertising>
- ¹³ Cybercrime targeting manufacturing <http://www.natlawreview.com/article/case-study-how-regional-manufacturing-firms-are-increasingly-targets-cybercrime>
- ¹⁴ Cisco / IronPort bogus security updates <https://tools.cisco.com/security/center/viewAlert.x?alertId=20315>
- ¹⁵ Fake Warnings <http://www.techrepublic.com/blog/it-security/fake-security-messages-more-believable-than-real-warnings-research-shows/>
- ¹⁶ FCC broadband privacy rules <https://www.fcc.gov/document/fcc-adopts-broadband-consumer-privacy-rules>
- ¹⁷ EU Data Protection Directive <http://www.nytimes.com/2015/12/16/technology/eu-data-privacy.html>
- ¹⁸ IBM-Ponemon Cost of a Breach 2016 <http://www-03.ibm.com/security/data-breach/>
- ¹⁹ The Atlantic <http://www.theatlantic.com/business/archive/2016/09/ransomware-us/498602>
- ²⁰ Reuters <http://www.reuters.com/article/us-at-t-settlement-dataprotection-idUSKBN0MZ1XX20150408>
- ²¹ CBS News <http://www.cnbc.com/2016/08/05/why-2016-could-be-banner-year-for-health-care-data-breach-fines.html>
- ²² 2016 Ponemon Business Continuity Impact <http://www-935.ibm.com/services/us/en/it-services/business-continuity/impact-of-business-continuity-management/>
- ²³ Enterprise focused ransomware <http://www.eweek.com/security/nine-ways-to-protect-an-enterprise-against-ransomware.html>
- ²⁴ NTIA Vulnerability Reporting Initiative <https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-cybersecurity-vulnerabilities>
- ²⁵ See OTA IoT Trust Vision White Paper and IoT Trust Framework <https://otalliance.org/Vision>
- ²⁶ OTA IoT Trust Framework <https://otalliance.org/IoT>
- ²⁷ DHS IoT Security Principles <https://www.dhs.gov/securintheIoT/>
- ²⁸ NIST's Security Controls for Federal Systems and Organizations (Publication 800-53 Rev. 4, April 2013).
- ²⁹ Multi-factor authentication <http://azure.microsoft.com/en-us/documentation/articles/multi-factor-authentication/>
- ³⁰ National Strategy for Trusted Identities in Cyberspace <http://www.nist.gov/nstic/>
- ³¹ Hashing <http://www.webopedia.com/TERM/H/hashing.html>
- ³² Email authentication standards and resources <https://otalliance.org/eauth>
- ³³ TLS resources <https://otalliance.org/tls>
- ³⁴ See OWASP www.owasp.org
- ³⁵ Always On SSL <https://otalliance.org/AOSSL>
- ³⁶ EV SSL Certificates <https://otalliance.org/EVSSL>
- ³⁷ Bug Bounty Programs Overview https://en.wikipedia.org/wiki/Bug_bounty_program
- ³⁸ Verisign DDoS Mitigation https://www.verisign.com/en_US/forms/ebookproactiveddosmitigation.xhtml?loc=en_US
- ³⁹ European Commission joint release http://europa.eu/rapid/press-release_STATEMENT-16-1403_en.htm; see also EU Data Protection Directive Summary http://europa.eu/rapid/press-release_IP-15-6321_en.htm
- ⁴⁰ 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>

-
- ⁴¹ Effective January 1, 2016, California amended its law to include data from Automated License Plate Recognition Systems. http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201520160SB34.
- ⁴² See Symantec DLP Overview <http://www.symantec.com/data-loss-prevention>
- ⁴³ Data aggregation is any of a number of processes in which information is gathered and expressed, for a variety of purposes.
- ⁴⁴ NIST De-Identification 2015 <http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8053.pdf>; see also De-Identification & Re-Identification <https://www.cippguide.org/2010/09/21/de-identification-re-identification/>
- ⁴⁵ These Critical Security Controls align with the NIST's Security Controls for Federal Information Organizations (Publication 800-53) <http://www.counciloncybersecurity.org/critical-controls/>
- ⁴⁶ Insurance Journal Growth in Cyber Coverage Expected <http://www.insurancejournal.com/magazines/features/2016/04/04/403439.htm>
- ⁴⁷ Target Coverage <http://www.businessinsurance.com/article/20140806/NEWS07/140809889>
- ⁴⁸ NIST Cybersecurity Framework <http://www.nist.gov/cyberframework/index.cfm>
- ⁴⁹ MBIC Insurance <http://www.networkworld.com/article/2984989/security/cyber-insurance-rejects-claim-after-bitpay-lost-1-8-million-in-phishing-attack.html>
- ⁵⁰ Company sues insurance company for \$480,000 <http://krebsonsecurity.com/2016/01/firm-sues-cyber-insurer-over-480k-loss/>
- ⁵¹ PF Chang <http://www.jdsupra.com/legalnews/know-your-cyber-insurance-gaps-before-a-82371/>
- ⁵² Annual Report on the Insurance Industry by the U.S. Department of the Treasury https://www.treasury.gov/initiatives/fio/reports-and-notices/Documents/2016_Annual_Report_FINAL.pdf
- ⁵³ Includes, but not limited to ding Risk Management, HR, Operations, Legal, PR, Marketing, Finance, and Customer Service.
- ⁵⁴ Email Authentication Resources <https://otalliance.org/eauth>
- ⁵⁵ To locate your local U.S. Secret Service Electronic Crimes Task Force visit <http://www.secretservice.gov/investigation/> .
- ⁵⁶ To find a local InfraGard Chapter visit <https://www.infragard.org>
- ⁵⁷ Incident Handling Guide, NIST (Special Publication 800-61) <http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf>
- ⁵⁸ Guidelines For Forensic Investigators <https://www.bryancave.com/en/thought-leadership/guidelines-for-retaining-a-forensic-investigator.html>
- ⁵⁹ FCC Release Broadband Privacy Rules <https://www.fcc.gov/document/fcc-releases-rules-protect-broadband-consumer-privacy>
- ⁶⁰ 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>.
- ⁶¹ NY State bill <http://www.ag.ny.gov/press-release/ag-schneiderman-proposes-bill-strengthen-data-security-laws-protect-consumers-growing>
- ⁶² JD Spura Business Advisor <http://www.jdsupra.com/legalnews/nebraska-and-illinois-update-breach-48552/>
- ⁶³ 2017 California Breach Law Updates <http://www.jdsupra.com/legalnews/california-amends-its-data-breach-24052/>
- ⁶⁴ World Law Group data breach guide http://www.theworldlawgroup.com/wlg/global_data_breach_guide_home.asp
- ⁶⁵ Consumer Federation of America, ID Theft Best Practices, <http://consumerfed.org/pdfs/CFA-Best-Practices-Id-Theft-Services.pdf>
- ⁶⁶ See Department of Homeland Security Stop Think Connect Campaign <http://www.dhs.gov/stopthinkconnect>
- ⁶⁷ FCC Adopts Rules to Protect Broadband Consumer Privacy <https://www.fcc.gov/document/fcc-adopts-broadband-consumer-privacy-rules>
- ⁶⁸ US White House breach response guidelines for USG <https://www.whitehouse.gov/sites/default/files/omb/memoranda/2017/m-17-12.pdf>
- ⁶⁹ Chile announce planned changes to privacy and data protection laws <https://www.bna.com/chilean-government-introduce-n17179918953/>
- ⁷⁰ U.S. Department of Commerce Privacy Shield resources: <https://www.commerce.gov/page/eu-us-privacy-shield>
- ⁷¹ EU 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>
- ⁷² IAPP Impacts of GDPR <https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-1-data-security-and-breach-notification/>
- ⁷³ GDPR Implementation Guidelines <https://www.huntonprivacyblog.com/2016/12/16/article-29-working-party-releases-gdpr-implementation-guidance-announces-privacy-shield-developments/>
- ⁷⁴ EU proposed updates to e-Privacy Directive <https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications>
- ⁷⁵ Dutch Data Breach Bill https://www.huntonprivacyblog.com/files/2015/06/gewijzigd_voorstel_van_wet.pdf
- ⁷⁶ Dutch Data Protection Web Site (English) <https://autoriteitpersoonsgegevens.nl/en>
- ⁷⁷ German Updated Consumer Data Protection Bill <http://dip21.bundestag.de/dip21/btd/18/046/1804631.pdf>
- ⁷⁸ Privacy Matters <http://blogs.dlapiper.com/privacymatters/france-new-law-introduces-class-actions-for-data-protection-violations/>
- ⁷⁹ OAIC <https://www.oaic.gov.au/privacy-law/determinations/>
- ⁸⁰ Draft bill <https://www.ag.gov.au/Consultations/Documents/data-breach-notification/Privacy-Amendment-Notification-of-Serious-Data-Breaches-Bill-2015-December-2015-exposure-draft.pdf>
- ⁸¹ Privacy Amendment Bill 2016 http://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r5747_ems_ed12b5bb-d3b3-4a6a-9536-53bb459a00df/upload_pdf/6000003.pdf?type=application%2Fpdf

⁸² Privacy Act of New Zealand <http://www.legislation.govt.nz/act/public/2007/0007/latest/DLM405134.html>

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 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 The language in this section must be tailored to the actual circumstances of the breach and legal requirements of the relevant states. Note that Massachusetts requires that the notice NOT include a description of the nature of the breach NOR the number of individuals affected.

⁸⁹ Several 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.

⁹⁰ NIST Guide to Forensic Techniques and Incident Response <http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf>

ABOUT THE ONLINE TRUST ALLIANCE (OTA)

The Online Trust Alliance (OTA) is a non-profit non-partisan think-tank 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. More at <https://otalliance.org/Vision>.

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 supported by donations, grants and annual dues. To support OTA visit <https://otalliance.org/membership>

© 2017 Online Trust Alliance. All rights reserved.

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

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