Cyber Incident & Breach Trends Report

Review and analysis of 2017 cyber incidents, trends and key issues to address

OTA
Online Trust Alliance
an Internet Society initiative

Released January 25, 2018

BACKGROUND & INTRODUCTION

This year marks the Online Trust Alliance's tenth annual publication related to cyber incidents and breach readiness. Now an initiative of the Internet Society, OTA reviews cyber incident and breach events to extract key learnings and provide guidance to help organizations of all sizes around the world raise the bar on trust through enhanced data protection and increased defense against evolving threats. This Cyber Incident & Breach Trends Report builds on last year's expanded recognition of threats beyond just data breaches to include ransomware, business email compromise (BEC), distributed denial-of-service (DDoS) attacks and connected device vulnerability.

These increasing threats challenge all manner of organizations – businesses, health and education institutions, governments – and also impact their clients, customers and citizens. This report is a precursor to the Cyber Incident & Breach Readiness Guide to be published in the first quarter of 2018. The Guide will provide knowledge, guidance and resources to help a broad range of stakeholders – from executive decision-makers to technical security experts to privacy professionals – prevent, detect, mitigate and effectively respond to a cyber incident.

Cyber Incidents Defined

They are 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,
4. activities causing financial or reputational harm.

The past year has brought high-profile data exposures including Equifax, Uber, Verizon, Ai.Type (Israel), DU Caller (China), Taringa! (Argentina) and Zomato (India), demonstrating that even organizations with substantial resources and expertise in data and technology can find themselves inappropriately defended and unprepared. All organizations must adopt an attitude of expectation – breach attacks will happen – and develop the dual view of defense:

1. Implement strong data stewardship (including security, privacy and risk reduction) through all phases of the data lifecycle, recognizing the global regulatory landscape and its impact on breach readiness (e.g., GDPR enforcement beginning in May 2018)
2. Prepare strong, well-practiced incident response measures (including a well-designed plan, appropriate team, predetermined action steps, regular training and testing)

The exponential growth in data and its value make data assets mission-critical to all organizations. Its appropriate use and protection is not just a question of compliance to be handled by a specific department or expert team. Data protection and readiness for all manner of cyber incidents must become part of the shared responsibility of all employees across all organizational functions. While there is no perfect defense against a determined attacker, the best practices outlined here and detailed in the complete Cyber Incident & Breach Readiness Guide at https://otalliance.org/incident can help greatly reduce a company's attack surface and the impact of an incident.

2017 – A YEAR OF THREAT

Surprising no one, 2017 marked another "worst year ever" in personal data breaches and cyber incidents around the world. Attacks involving data theft, ransomware takeovers, business email compromise (BEC) for financial or credential theft and infiltration of Internet of Things (IoT) connected devices hit organizations both large and small.

In terms of data breaches, Equifax's headline-making incident exposing personal financial/credit data on 145 million people across several countries not only underscores the breadth of the problem and its cause (lack of basic security update actions), but highlights how rigor may be lacking even in organizations we view as expert. In addition, Equifax's response was a playbook of how not to handle a breach: slow disclosure; a poorly designed external breach response site; mistakenly Tweeting an incorrect, similar-sounding URL; confusing public messaging; conflicting actions surrounding potential class action suits; and unseemly executive stock trades.[1] Every facet of the Equifax breach undercut trust and amplified the company's lack of readiness. Data breach expenses for Equifax already approach $90 million, even before government actions or consumer litigation.[2]

2017 Incident Highlights

159,700 total cyber incidents in 2017 (OTA)

93% of breaches could have been prevented (OTA)

18.2% increase in reported breach incidents (RBS)

7 billion records exposed in first 3 quarters (RBS)

$5 billion financial impact of ransomware (CV)

90% rise in business targeted ransomware (Symantec)

$5.3 billion in global BEC losses (FBI)

Worldwide estimates. Sources: (OTA) Online Trust Alliance, (RBS) Risk Based Security, Cybersecurity Ventures (CV)

Another recent high-profile breach incident involved Uber. In 2017 it came to light that data from 57 million riders and drivers was stolen in 2016.[3] Verizon faced exposure of data from 14 million customers via an unsecured Amazon cloud server controlled by one of Verizon's service providers.[4] Meanwhile, at Yahoo!, which was recently acquired by Verizon, officials reported new information: that all 3 billion user accounts were compromised in the breach of 2013.[5] Overall, Risk Based Security reported 7 billion records exposed in the first three quarters of 2017, about four times the number from the same period in 2016.[6]

Just as the amount of data exposed has increased, so has the financial impact. The Ponemon Institute estimates the 2017 average cost of a data breach incident worldwide was $3.62 million, up 10% from 2016, though due to economic variations some countries' average costs are much higher.[7] For example, the average cost in the US was $7.35 million per breach incident, up 5% from the prior year.[8] Even these estimates likely underestimate the true cost of breach incidents since they do not include costs related to loss of proprietary data. The country facing the highest volume of records breached in the first nine months of 2017 was China at 3.8 billion, with the US in second place.[9] Overall, the breach trend continues a relentless march upward in all categories – numbers of breaches, numbers of records exposed and breadth of countries/organizations impacted.

While breached records increased by four times in 2017, ransomware had already increased four-fold between 2015 and 2016 with the FBI's most recent estimate at 4,000 ransomware attacks per day.[10] Symantec research estimates business-targeted ransomware infections in 2017 at nearly double the prior year.[11] Malwarebytes research finds that ransomware represents roughly 60% of all malware attacks in Q1 2017, far outpacing all other types.[12] Kaspersky reported that 65% of businesses hit with ransomware lost access to a "significant amount or all" of their data and 1 in 6 of those *paying* the ransom never recovered their data.[13] WannaCry, one of the most widespread and devastating attacks in history, hit an estimated 300,000 computers across 150 countries, crippling organizations such as healthcare networks, manufacturers, transportation services and government agencies.

Similarly, NotPetya infected hundreds of thousands of computers in over 100 countries in days, costing large companies such as Merck over $300 million in Q3 alone.[14] Europol's 2017 crime assessment states that ransomware has eclipsed most other cyber-threats[15] and Cybersecurity Ventures estimates 2017 ransomware damages in excess of $5 billion.[16]

Mid-2017 also saw a spike in another ransom-related attack – the ransom denial-of-service (RDoS). In this attack, criminals send an email to domain owners threatening a distributed denial-of-service (DDoS) attack unless a ransom (usually via Bitcoin) is paid.[17] Though many of these turn out to be empty threats, the success of a small percentage of the attacks encourages criminals to continue the practice.

The spread of ransom-based attacks is one of the goals of malicious email, which is also on the rise. According to Proofpoint, in 2017 malicious email volume rose 85% in Q3 vs Q2 and ransomware appeared in 64% of the malicious messages.[18] Email continues to be an important vector for malware, but it also provides opportunity for other abusive practices. Business email compromise (BEC) continues to plague organizations and increasing sophistication in targeting and social engineering means even well-trained employees can fall victim to malicious phishing attacks.[19] Though the FBI only began tracking BEC as a unique cyber crime in 2017, it estimates that BEC may be responsible for up to $1.6 billion in US losses since 2015 and $5.3 billion globally.[20]

Beyond increases in breaches and ransomware, and the emergence of BEC as a recognized threat, 2017 made the reality of IoT risk more vivid than ever. Some of this risk showed up in the form of IoT botnets poised to initiate Mirai-level DDoS attacks,[21] while some showed up as infiltrations – in the past year UK teddy bears were breached, resulting in compromise of 800,000 customers' details; a US casino fish tank was used to infiltrate the casino's network resulting in theft of 10 Gb of data; and a European hotel's smart cardkey/room lock system was taken over by hackers.[22] While innovation in connected devices brings exciting and useful advances, privacy and security protections lag behind, putting users and organizations at risk.

By combining all of these incidents from threat intelligence data – breaches, ransomware, BEC and DDoS – OTA analysis has found that the true number of incidents is more than 30 times the number of reported breaches. Though this analysis is based on data through the third quarter of 2017, on an annualized basis it equates to nearly 160,000 incidents, almost double the number seen in 2016.[23] This increase is primarily due to the significant growth in ransomware infections during 2017. Unfortunately, even this estimate likely significantly understates the real number. Since most incidents are not reported to executives, law enforcement, regulators or the public, the actual number of harmful incidents could easily exceed 350,000.

PREPARATION AND DILIGENCE ARE KEY

Regardless of an organization's security posture, there is no perfect security. On the other hand, there is no excuse not to implement fundamental security best practices. All organizations, regardless of size, must plan for inevitable attacks and loss of (or loss of access to) critical data. By recognizing risks, planning ahead and instilling a culture of security and privacy in the entire organization, losses and their impact can be minimized.

As in previous years, OTA analyzed reported breaches through Q3 2017 and found that 93% were avoidable, which is consistent with previous years' findings. Of the reported breaches, 52% were the result of actual hacks, while 11% were due to lack of internal controls resulting in employees' accidental or malicious events. Regular patching and paying close attention to vulnerability reports has always been a best practice and neglecting them is a known cause of most breaches,[24] but this category received special attention this year in light of the Equifax breach.

The vast majority of other types of attacks – ransomware and BEC – are initiated by deceptive or malicious emails. Analysis reveals that these too are avoidable, by blocking fake messages and training users to recognize spearphishing attacks. In addition to better processing of email, there are several other steps that can prevent or limit the impact of ransomware, which include updated system and security software as well as regular data backups.[25] Since BEC attacks rely almost entirely on “social engineering” deception and rarely include any malicious links or attachments, better processing of email can generally stop these attacks in their tracks. Unfortunately, the day-to-day urgency of business often prevents organizations from appropriately defending against these email-based attacks.

Key avoidable causes for incidents:

- Lack of a complete risk assessment, including internal, third-party and cloud-based systems and services
- Not promptly patching known / public vulnerabilities, and not having a way to process vulnerability reports
- Misconfigured devices / servers
- Unencrypted data and/or poor encryption key management and safeguarding
- Use of end of life (and thereby unsupported) devices, operating systems and applications
- Employee errors and accidental disclosures - lost data, files, drives, devices, computers, improper disposal
- Failure to block malicious email
- Users succumbing to Business Email Compromise & social exploits

ECONOMIC VALUE OF READINESS

The complete cost of a cyber incident to an organization encompasses far more than merely the business downtime and interruption caused by data held for ransom or the lost IP of a data theft. Regulatory penalties for failure to take basic protective steps have increased in recent years and are on a steep incline in 2018. Organizations that do not prioritize data protection may find themselves victimized by criminals, then also penalized by regulators and consumers in fines and lawsuits. Additionally, in the business-to-business segment, having a readiness plan is becoming a mandatory business requirement so failure to have one can have a significant financial impact.

A critical regulatory framework that organizations now need to consider is the EU’s General Data Protection Regulation (GDPR)[26] which goes into full enforcement on 25 May 2018 and addresses not only consumer data but employee and job applicant data. Because the GDPR establishes laws that impact every organization handling EU resident and citizen data, even for organizations located outside the EU, its importance cannot be overstated. The GDPR outlines detailed requirements for data stewardship, data minimization, transparency and security practices such as encryption, in addition to detailed rules for breach notification, both to regulators and to impacted parties. GDPR imposes stiff penalties of up to 4% of global revenues for “negligence” in security, failure to follow best practices in data protection and/or failure to notify regulators within specified time-frames for data breaches.[27] The EU is not alone – many countries have been rapidly advancing data security and breach related legislation.

Even prior to the GDPR coming into effect, the Italian Data Protection Authority issued a record sanction of €11 million[28] in 2017 and the settlement of the Anthem class-action suit in the US for $115 million represented the largest data breach settlement to date.[29] The total sum of regulatory fines and class action suits against Equifax is not yet known, and is sure to break records, but litigation is moving beyond data breaches. In 2017, Ukraine saw the beginning of the first known ransomware class action suit stemming from the NotPetya malware infection. It was tied to Intellect Service, LLC servers, creators of the M.E.Doc software that was used to spread the malware. [30] In addition, a law firm filed suit to recover $700,000 in lost billing time due to a ransomware shut-down.[31]

As if the wide array of business costs (e.g., downtime, interruption, lost business, fines and litigation) were not enough, further costs include specific damages to consumers from their exposed data and wider losses from tarnished consumer trust. Accenture valued today’s lack of consumer trust in the billions of dollars.[32] Prevention of, and preparation for, cyber incidents – whether breach, ransomware, BEC or IoT infiltration – provides direct benefits in reduced risk and faster mitigation, but also strengthens an organization’s brand, reputation and position with regard to consumers, regulators and business partners.

TOP TRENDS TO ADDRESS

Though most best practice guidance stays relatively constant over time, several trends developed in 2017 that deserve special attention and focus due to their frequency or impact. These trends, and ways to address them, are listed below.

RISE IN RANSOM-BASED ATTACKS

As previously mentioned, ransomware attacks doubled in 2017 and were the primary driver for an overall doubling in total incidents. Ransom-based attacks came in various forms – via malware-laced phishing attacks, malvertising, and drive-by malware that encrypt data and block access to systems, as well as via RDoS, threats to attack a site via a denial-of-service attack if ransom is not paid.

Defending against such attacks involves well-known best practices such as use of email authentication checks to block malicious messages, adding browser-based scanning for malware, increasing employee awareness of such attacks, limiting administrative access by employees to contain the spread of an infection and use of DDoS protection services to limit the impact of an attack. Another best practice is regular offline backups so that data can be restored and is not permanently lost.

However, since some organizations may determine that paying a ransom is the necessary course of action for a given incident, and Bitcoin is the most common form of payment request, it is recommended that organizations set up a Bitcoin wallet in advance. This type of proactive planning is not unlike establishing relationships in advance with crisis management firms, forensics specialists and law enforcement – it is easier to make logical, informed decisions during the calm than it is during the storm. There are several sites that compare wallets and approaches as well as the security considerations related to cryptocurrency wallets.[33] [34] Since many ransom situations have tight deadlines, setting up a digital wallet in advance (and holding some cryptocurrency there) allows an organization to respond quickly. Note that while most states do not require notification of ransomware exploits, some industry sectors such as healthcare may require reporting and the FBI has encouraged reporting of incidents.[35] [36]

PATCHING PACE IS CRITICAL

Though Equifax is a prime example of unnecessary exposure due to lack of patching, many other incidents such as WannaCry and Petya also spread quickly due to inadequately patched systems. Verizon's 2017 DBIR analysis showed that only 61% of organizations complete their patching process and patches not completed after 12 weeks tended to go unpatched.[37] With the revelation of the KRACK Wi-Fi and BlueBorne vulnerabilities in late 2017 and the Spectre and Meltdown chipset vulnerabilities in January of 2018, the need to patch has reached a fever pitch. Regular patching has long been a best practice, but due to this "perfect storm" it deserves extra attention this year.

Addressing this trend requires diligence and discipline to keep up with available patches from a wide variety of sources, promptly test them for impact and interaction with other systems and software, and deploy them in a timely manner. The goal is to shut the vulnerability window as quickly as possible with the least system disruption, which can be a challenging balance to strike.

CLOSELY MONITOR CLOUD CONVERSION

The trend toward increased reliance on third-party cloud-based services continues for organizations of all sizes, and underscores the need to assess and continually monitor all systems which hold an organization's data. Cloud-based spending is predicted to be more than half of IT spending by 2022.[38] Many large and public breaches in 2017 involved data stored in cloud-based services, which have their own set of vulnerabilities often outside direct control of the contracting organization.

Addressing cloud-based issues involves basic best practices such as thorough auditing of a cloud provider's processes and security practices, and contracts should be specific about security-related expectations and commitments. However, some security elements are often left to the contracting organization, as seen in the wave of unsecured Amazon Web Services S3 containers (most of which were configured for public access) leading to breaches in 2017.[39] [40] This unfortunate trend calls for increased vigilance and understanding of all aspects of cloud-based services to properly secure data stored there.

USER-ENABLED ATTACKS

As in previous years, many cyber incidents were enabled via users who accidentally provide credentials or whose systems are infected when they click on links or attachments. As the workforce shifts to be more mobile and flexible, and use of personal devices increases, the ability to keep a tight rein on security becomes more difficult.[41]

Addressing this trend can take many forms. Traditional best practices such as blocking malicious email, heightening the security awareness of users and invoking the principle of least privilege (i.e., users are only given access levels to systems appropriate with their role) are foundational, but in today's environment, an extra boost is needed. This can be provided by enabling multi-factor authentication on key systems (since most attacks start with credential theft) and monitoring access to key systems to look for anomalies.

INCREASE IN IOT DEVICES

Adoption of IoT devices and services within enterprises is expected to triple in the next several years,[42] and many consumer-grade IoT devices are finding their way into the enterprise (e.g., smart TVs in conference rooms). Many of these IoT devices have vulnerabilities, ranging from default passwords to unencrypted data to insecure software stacks, and can become an entry point for data monitoring or network intrusions (e.g., the previously mentioned casino fish tank attack).

Addressing this trend includes best practices such as thoroughly vetting IoT products before purchase to understand their security capabilities, monitoring use of "non-IT" devices such as smart TVs to make sure they are handled properly and putting IoT devices on a separate, compartmentalized network (similar to the way guest networks are handled) to limit their interaction with core corporate networks.

REGULATORY SHIFTS

There are many regulatory shifts underway worldwide, led by the EU's General Data Protection Regulation (GDPR) which takes effect in May 2018. Several other countries have (or are) updating their data protection and privacy laws and regulations in line with GDPR (a thorough roundup will be provided in the upcoming 2018 Cyber Incident & Breach Readiness Guide). In general, these tighten requirements on data handling, consumer notice/transparency and data breach notifications.

In the US, largely due to heightened sensitivity in the wake of the Equifax breach, new data breach legislation has been introduced. This includes the "Data Breach Prevention and Compensation Act," which is focused on credit reporting agencies and gives the FTC the power to assess significant fines, and the "Data Security and Breach Notification Act," which creates a national breach notification law (vs today's 48 individual state laws) requiring breach notification within 30 days.[43] [44] Though it is unclear if this legislation will pass, there is certainly a move toward tightening data breach laws.

Addressing this trend requires a sharp focus on regulatory changes worldwide as well as a thorough understanding of the laws and regulations themselves as they are implemented. Many of these shifts will require changes to data collection and handling, reporting and breach notification processes. These changes need to be communicated and implemented throughout the organization, including in the cyber incident and breach readiness plan itself.

READINESS GUIDANCE

All organizations collect and use sensitive, mission-critical data and data is valuable. Therefore, all organizations must recognize that they are targets; incidents can and will happen to organizations of all types and sizes. Preparation includes an overall culture of data stewardship through all phases of the data lifecycle – from collection, to storage, to use, to transmission, to destruction/archive. This culture must embed security protections, that also address individuals' privacy rights and expectations, from a perspective of data protection and transparency.

Organizations must recognize that incident readiness is not a one-and-done task limited to a few IT experts – it is everyone's responsibility and requires teamwork, planning, testing and ongoing training. Risk reduction begins with risk assessment, appropriate security, and protections such as cyber insurance. Further, preparedness requires a tested and practiced response plan that can be implemented quickly and includes best forensic practices, clear communication and a thorough understanding of breach response regulations/requirements.

Fundamentals

- All businesses collect some form of sensitive, valuable information
- Cyber incidents will occur
- Data stewardship, privacy and incident readiness are everyone's responsibility
- Data management and privacy practices need continual review
- Every organization needs to have a current, tested response plan
- Ongoing employee training is a critical key to success

CORE READINESS PRINCIPLES

As cyber incidents increase and evolve in sophistication, the cost and damage grow. Through the years, the leading incidents (and how they were handled) have taught important lessons:

1. **Responsibility for incident protection and readiness is organization-wide.** Data stewardship, security and associated privacy practices are the responsibility of the board, executives, all employees and all departments (not just IT).
2. **Data is an organization's most valuable asset.** Identify what you have, where it is, why and how you use it and the potential risks should it be inappropriately accessed, held hostage, released or erased.
3. **Only collect and retain data that has a business purpose for as long as it is needed**. Secure it while it's held; delete it when it's no longer needed. Criminals cannot steal or hold hostage data you don't have, and such minimization may be a regulatory requirement for your organization.
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. **Protection involves not only the specific incident (data loss, ransom paid), but also the costs of business interruption** including locked data, network and system interruption and connected device takeover.
6. **Have plan to reduce the impact of an attack**. An incident plan needs to incorporate training to help prevent, detect, mitigate and respond. Just like first responders, employees must be regularly trained, equipped and empowered to deal with a data loss incident. Planning is the key to maintaining trust and business vitality

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.

7. **Security and privacy are not absolutes and must evolve**. Organizations need to regularly review their procedures for collection, storage, management and security of all data (along with review of changing technologies, best practices and regulations).
8. **Security is beyond the organization's desktops, networks and walls**. Cloud services, third-party processors and external business partners expand the attack landscape. Conduct a risk assessment prior to partnerships or service agreements and periodically re-assess. Require regular (weekly, monthly, quarterly or annual) reports from vendors specifying their internal data security processes, data removal methods, tools and technology implementations and documentation.
9. **Connected devices introduce new risk levels.** The rapid adoption of connected devices from Smart TVs in the boardroom to coffee makers in the breakroom to employees' personal mobile devices and wearables connected to the office Wi-Fi dramatically increase the threat landscape. Ongoing risk assessment of all IoT devices and the development and enforcement of an employee policy for connecting devices to the corporate network is critical since a single connected device can introduce threats network wide.[45]
10. **Build trust through transparency**. In the event of an incident, keep communication clear. Whether communicating with customers or board members, keeping important stakeholders informed early with regular updates is a critical part of maintaining trust.

TOP-LEVEL INCIDENT READINESS CHECKLIST

- □ Complete risk assessments for executive review, operational process and third-party vendors
- □ Review security best practices and validate your organization's adoption or reasoning for not adopting
- □ Audit your data and review your data stewardship practices including data lifecycle management
- □ Complete a review of insurance needs including exclusions and pre-approval of coverage for any third-party services (such as cyber forensics, remediation provider, PR firm, etc.)
- □ Establish and regularly test an end-to-end incident response plan including empowering 24/7 first-responders
- □ Establish/confirm relationships with data protection authorities, law enforcement and incident service providers
- □ Review and establish forensic capabilities, procedures and resources (internal and third-party providers)
- □ Develop communication strategies and tactics tailored by audience (e.g., messages to employees vs messaging to media vs notifications to customers)
- □ Review remediation programs, alternatives and service providers
- □ Implement ongoing employee training for incident response
- □ Establish employee data security awareness and ongoing education on privacy, incident avoidance (password practices, how to recognize social engineering, etc.) and incident response
- □ Understand the regulatory requirements, including relevant international requirements

For more detailed information and definitions, along with additional checklists and links to resources, look for the 2018 OTA Cyber Incident & Breach Readiness Guide in the coming months. Additional resources can be found at: https://otalliance.org/incident.

ENDNOTES

[1] https://www.wired.com/story/equifax-breach-response/
[2] https://www.nytimes.com/2017/11/09/business/equifax-data-breach.html
[3] https://www.scmagazine.com/uber-paid-florida-hacker-responsible-for-breach-100k-through-bug-bounty-program/article/712731/
[4] http://www.zdnet.com/pictures/biggest-hacks-leaks-and-data-breaches-2017/2/
[5] http://money.cnn.com/2017/10/03/technology/business/yahoo-breach-3-billion-accounts/index.html
[6] https://www.riskbasedsecurity.com/2017/11/2017-yet-another-worst-year-ever-for-data-breaches/
[7] Ponemon global study https://www.ibm.com/security/data-breach
[8] Ponemon US study https://www.ponemon.org/library/2017-cost-of-data-breach-study-united-states
[9] https://www.riskbasedsecurity.com/2017/11/2017-yet-another-worst-year-ever-for-data-breaches/
[10] https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view
[11] https://resource.elq.symantec.com/LP=4697?cid=70138000000zT9GAAU&inid=symc_symc-home-page_ghp_to_leadgen_form_LP-4697_ISTR22-ransomware-2017
[12] https://www.malwarebytes.com/pdf/labs/Cybercrime-Tactics-and-Techniques-Q1-2017.pdf
[13] https://cdn.securelist.com/files/2017/11/KSB_Story_of_the_Year_Ransomware_FINAL_eng.pdf
[14] https://www.techrepublic.com/article/the-top-10-worst-ransomware-attacks-of-2017-so-far/
[15] https://www.europol.europa.eu/newsroom/news/2017-year-when-cybercrime-hit-close-to-home
[16] https://cybersecurityventures.com/ransomware-damage-report-2017-5-billion/
[17] https://www.bleepingcomputer.com/news/security/online-extortion-campaigns-target-users-companies-security-researchers/
[18] https://www.techrepublic.com/article/report-malicious-email-attacks-jump-85-in-q3-ransomware-reigns-supreme/
[19] https://swimlane.com/cybersecurity-statistics-2017/
[20] https://securityledger.com/2017/05/fbi-business-email-compromise-is-a-5-billion-industry/
[21] http://fortune.com/2017/10/25/reaper-botnet-mirai-iot-ddos/
[22] https://www.ukfast.co.uk/blog/2017/09/13/the-5-most-unexpected-iot-hacks-of-2017/
[23] Includes data breach incidents from Risk-Based Security 3Q2017 report, BEC incidents from the FBI, ransomware incidents from the Symantec 2017 Ransomware report and data from the Verizon 2017 DBIR.
[24] Software patches could prevent most breaches, http://www.eweek.com/security/software-patches-could-prevent-most-breaches-study-finds
[25] How to Protect Yourself from Ransomware Attacks, https://www.nytimes.com/2017/05/15/technology/personaltech/heres-how-to-protect-yourself-from-ransomware-attacks.html
[26] EU GDPR portal site https://www.eugdpr.org
[27] IAPP Impacts of GDPR https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-1-data-security-and-breach-notification
[28] https://www.williamfry.com/newsandinsights/news-article/2017/03/16/companies-beware!-largest-ever-fine-for-breach-of-data-protection-laws-issued-by-the-italian-data-protection-authority
[29] https://www.reuters.com/article/us-anthem-cyber-settlement/anthem-to-pay-record-115-million-to-settle-u-s-lawsuits-over-data-breach-idUSKBN19E2ML
[30] https://themerkle.com/the-worlds-first-ransomware-class-action-law-suit-is-taking-shape/
[31] https://www.darkreading.com/attacks-breaches/law-firm-sues-insurer-over-income-loss-in-ransomware-attack/d/d-id/1328813
[32] https://www.marketingdive.com/news/accenture-lack-of-personalization-consumer-trust-cost-businesses-756b-la/512693/
[33] https://bitcoin.org/en/choose-your-wallet, https://99bitcoins.com/best-bitcoin-wallet-comparison-review/
[34] https://www.wired.com/story/how-to-keep-bitcoin-safe-and-secure/
[35] http://www.healthcareitnews.com/news/experts-there%E2%80%99s-no-gray-area-ransomware-breach-reporting
[36] https://www.ic3.gov/media/2016/160915.aspx
[37] https://www.ictsecuritymagazine.com/wp-content/uploads/2017-Data-Breach-Investigations-Report.pdf
[38] https://www.forbes.com/sites/louiscolumbus/2017/04/29/roundup-of-cloud-computing-forecasts-2017/#1414886231e8
[39] https://www.scmagazine.com/national-credit-federation-unsecured-aws-s3-bucket-leaks-credit-personal-data/article/710743/
[40] http://securityaffairs.co/wordpress/62752/data-breach/time-warner-cable-data-leak.html
[41] https://www.csoonline.com/article/3239848/security/could-the-security-industry-have-it-all-wrong.html
[42] https://www.forbes.com/sites/louiscolumbus/2017/12/10/2017-roundup-of-internet-of-things-forecasts/#6787dc8a1480
[43] https://www.cyberscoop.com/data-breach-bill-mark-warner-elizabeth-warren-equifax/
[44] https://www.cyberscoop.com/national-data-breach-notification-law-bill-nelson-uber-equifax-hack/
[45] See OTA IoT Trust Vision White Paper and IoT Trust Framework https://otalliance.org/Vision

ACKNOWLEDGEMENTS

The foundational principles of this report are a collaborative work product reflecting input and recommendations from industry leaders and government agencies worldwide. Special thanks to Jeff Wilbur of the Internet Society and Craig Spiezle of AgeLight LLC for strategic input and editing, and Madelon Smith for research, writing and editing of this report.

ABOUT THE ONLINE TRUST ALLIANCE (OTA)

The Online Trust Alliance is an initiative within the Internet Society. The initiative's mission is to enhance online trust, user empowerment and innovation through convening multi-stakeholder initiatives, developing and promoting best practices, ethical privacy practices and data stewardship.

The Internet Society is a non-profit organization dedicated to ensuring the open development, evolution and use of the Internet. Working through a global community of chapters and members, the Internet Society collaborates with a broad range of groups to promote the technologies that keep the Internet safe and secure, and advocates for policies that enable universal access. The Internet Society is also the organizational home of the Internet Engineering Task Force (IETF).

To learn more visit https://otalliance.org.

Material in this publication is for educational and informational purposes only. Neither the publisher, the Internet Society (ISOC), 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. ISOC 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 ISOC member companies or affiliated organizations.

ISOC MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT. For updates visit https://otalliance.org/Incident. No part of this publication may be reproduced or distributed in any form or by any means, or stored in a database, web site or retrieval without the written consent of ISOC.

Rev0125