Data Breaches:

Who is behind them, why they do it, and how to protect your data

David McDaniel

East Carolina University

Spring 2019

Abstract

In today's increasingly connected world, personal data on nearly every person is held by many organizations from financial institutions, educational institutions, government agencies, credit reporting firms, commercial establishments, and more. These large troves of information are often the target of attackers. As a result, data breaches have become a normal part of the modern news cycle. Rarely is there much of a lull between stories of these entities having data compromised by malicious actors. In this research paper, the author begins by exploring some of the largest data breaches to date. In the second part of the paper, the author explores the people, organizations, and nation states behind these breaches and strives to answer the question as to who they are and why they perform these malevolent acts. In the third and final part of the paper, the author provides general best practice recommendations in order to prevent an individual or organization from falling victim to these actors. It should be noted that this paper was not written to be a sole source of information on any one subject but should guide the reader in their additional research for more detailed information on these topics.

Introduction

In today's modern, connected world, it is becoming increasingly common for organizations to rely on cloud providers and centralized data repositories to house troves of potentially confidential information. These large compilations of data are very often a target of interest for malicious actors due to their high reward potential. In addition, disgruntled employees, negligent employees, and system misconfigurations can result in the improper disclosure of sensitive information. Whether the target of the breach is an intentional or an unintentional release, the results can be catastrophic for an organization, both financially and to its reputation. Virtually all industries in the public and private sector are vulnerable to data breaches to some extent.

Recent High-Profile Data Breaches

Although there have been countless data breaches prior and after the advent of the Internet, the breaches that seem to garner the most attention do so due to either their sheer size of disclosed records or the type of data that has been breached (e.g., medical information, financial information, etc.). A number of these breaches are listed and detailed below. These breaches are listed in descending order of number of breached records or accounts. As is evident by the information portrayed below, data breaches can be caused by a multitude of reasons, both technical and non-technical.

Yahoo!

Yahoo!, the e-mail and search giant, has suffered several high-profile data breaches in recent years with varying degrees of severity. In one of the incidence, during September of

2016, Yahoo! disclosed that they were the victims of the largest known data breach in history, with approximately 500 million user accounts being compromised (Armerding, 2018). To worsen the issue, in October of 2017, Yahoo! altered the estimate of impacted accounts to include all 3 billion user accounts that they maintained, saying they had all been included in the compromised data (Smith & Mulrain, 2017). After disclosing the breach, Yahoo! stated that they believed the hacker to have been state-sponsored, although they came short of accusing any particular entity of the attack. Following the disclosure, the United States Federal Bureau of Investigation (FBI) began investigating the attack and traced the attack back to two Russian spies (Williams, 2017). Using targeted spear-phishing campaigns, attackers targeted Yahoo! employees in order to gain access to an internal system, which allowed them to search the network for fruitful information such as the customer database (Yahoo breach indictments, 2017).

Information stolen in the attack included customers' actual names, usernames, dates of birth, email addresses (including recovery addresses), telephone numbers, hashed passwords, security questions, and the answers to the security questions were all included in the breached information (Armerding, 2018). Unfortunately, it was revealed that there were passwords listed that were hashed with an MD5 or weaker function, rather than the robust bcrypt function which includes a salt (Goodin, 2016). Rainbow tables are available online for values that would hash to over 99% of the possible hash results, meaning the passwords could be easily cracked (Brown, 2019). This means that even if a relatively small percentage of the passwords were hashed using an MD5 or weaker function, tens of millions or hundreds of millions of accounts could have been instantly compromised.

Adult Friend Finder

FriendFinder.com is a group of adult websites which includes Penthouse.com and is largely focused on casual sexual encounters and pornography (Anonymous, 2018). During October of 2016, the FriendFinder.com network was breached, with over 412 million user's information being compromised (Botha, Grobelr, & Eloff, 2017). The information included in the breach was contained within six databases published online and included usernames, email addresses, passwords (Ragan, 2016). Some of these passwords were stored within the database using plaintext, with the remainder stored using the SHA-1 hash function, Ragan (2016) continues. Unfortunately, the SHA-1 hash is known to suffer from vulnerabilities, similar to the MD5 hash function used by Yahoo!. This effectively meant that any published credentials could have been easily reverse engineered to gain working credentials for the applicable website(s).

A majority of the accounts that were compromised used Hotmail, Gmail, and Yahoo! email addresses; however, over 5,000 accounts were registered to accounts with .gov addresses and over 78,000 accounts were registered to accounts with .mil addresses (BBC, 2016). This fact could prove to be embarrassing to many individuals, similar to the Ashley Madison data breach which occurred the previous year (Lord, 2017). One of the more shocking revelations of the breach was that it included over 15 million accounts that users had "deleted" from the website, showing that the organization was not purging data per customers' wishes (Whittaker, 2016).

Prior to the attack, security researcher 1x0123 (also known as "Revolver") alerted Adult Friend Finder that their website was susceptible to a local file inclusion (LFI) vulnerability (Ragan, 2016). Local file inclusion is a vulnerability that is most often seen on Web servers and allows an attacker to arbitrarily redirect a web server to execute a locally-stored file of his/her

choosing by modifying an attacker-controlled variable (Alnabulsi, Islam, & Talukder, 2018). Shortly after the alert by 1x0123, FriendFinder Networks stated that they had resolved an injection flaw, but it was not clear if they addressed the particular LFI vulnerability, which may have led to the breach (Kirk, 2016)

Target

As a leading retailer in the United States, Target has a high load of traffic that comes through their stores, especially during the holiday season between Thanksgiving and Christmas. From the end of November until December of 2013, Target security personnel received alerts from their malware systems indicating that some potentially malicious activity had been discovered within the network (Xiaokui Shu, Ciambrone, & Yao, 2017). However, it was not until the Department of Justice contacted Target to warn of the potential issue that they began investigating (Plachkinova & Maurer, 2018). Had Target began investigating the alerts when first generated (November 30, 2013), the effects of the breach may have been minimized or eliminated completely (Xiaokui Shu, Ciambrone, & Yao, 2017) as the data exfiltration had been proceeding for more than 12 days when the Department of Justice notified Target.

In the aftermath of the breach, the attackers were able to exfiltrate approximately 40 million credit and debit card numbers and over 70 million customer records which included addresses, telephone numbers, and email addresses (Kashmiri, Nicol, & Hsu, 2017). Initially, Target announced that even though the credit card and debit card numbers were stolen, there was no theft of the PIN numbers. However, several days later, it was confirmed that the PIN information was contained in the stolen data, but the information was encrypted with Triple Data Encryption Standard (Triple DES) encryption and should be secure (Goldman, 2013).

The hackers in the Target breach allegedly performed a significant amount of reconnaissance, determining the weak points in the Target information security system. Approximately two months prior to the start of the breach, the attackers sent a malicious email message to a Fazio Mechanical Services, a supplier of refrigeration devices (Radichel, 2014). Contrary to what has been widely circulated, Fazio did not "perform remote monitoring of or control of heating, cooling and refrigeration systems for Target," but they did provide electronic billing, contract submission, and project management services via remote connections (Krebs, 2014). The malicious email that was sent to Fazio was then used to capture login credentials to Target's payment system (Vijayan, 2014). From the infected systems, the attackers were then able to infiltrate point of sale terminals, installing malware that would perform memory scraping functions to collect unencrypted cardholder information when cards were swiped at the terminals (Plachkinova & Maurer, 2018). Once the data was collected, the malware used specially crafted ICMP packets sent to the hackers to inform the hackers that the data was ready to be uploaded to remote FTP servers and then sold on the dark web (Kassner, 2015).

Sony Pictures

In 2014, Sony Pictures Entertainment, Inc. was preparing to release the film *The Interview*, a comedy which is based on a plot to assassinate North Korean leader Kim Jong Un. On June 11, 2014, the North Korean government sent a letter to the United Nations Secretary General Ban Ki-moon, and threatened retaliation if the United States allowed the movie to be released (Sullivan, 2016). When Sony employees arrived to work on November 24, 2014, they were greeted with an image on their screen of a skeleton and the words "Hacked by #GOP" which represents the first instance that Sony knew that they had been compromised (Seal, 2015).

Next, the hackers began to move laterally through the network and delete all of the data from each workstation and server that it could get to before Sony's staff could prevent the spread (Verhoeven & Hod, 2015) Ultimately, 3,262 of Sony's 6,797 computers and 837 of its 1,555 servers were completely erased, including corrupting startup software, effectively rendering the systems completely useless (Elkind, 2015).

The release of data from the breach began shortly after with the release of several Sony Pictures films, some of which had not been released in theaters yet, including *Annie* and *Fury*, the latter of which had been downloaded over 1.2 million times in the course of just a few days (Bora, 2014). Other released data contains sensitive employee information such as social security numbers, health information, family information, corporate bank account information, passports and visas of cast and crew members, and corporate and personal communications, including those of Sony executives (Sullivan, 2016). The type and scope of the release information resulted in the resignation of several top Sony executives, including Amy Pascal, the co-chairman of the studio (Roman, 2015).

To execute the attack, the hackers utilized a Server Message Block (SMB) worm tool which includes five components: a listening implant, lightweight backdoor, proxy tool, destructive hard drive tool, and destructive target cleaning tool (Lennon, 2014). Since the worm utilizes SMB to propagate between systems, the tool is highly destructive if it can gain a foothold into an organization's network (US-CERT, 2014). The method of initial infiltration into the network is still unknown, but it is thought that the attack originated using a phishing email to an employee within the organization (Zetter, 2014).

Equifax

Equifax, along with Transunion and Experian, performs credit research and monitoring for organizations and individuals. Given the scope of their business, Equifax maintains a trove of personal information for numerous individuals in both the United States and abroad. When organizations such as Equifax are breached by malevolent actors, the results can prove to be disastrous due to both the size of the release and the type of material contained within the release.

On Thursday, September 7, 2017, Equifax announced that that very thing had occurred. The troubling initial reports reported that approximately half of the population of the United States could have had their data exposed during the breach (Ng & Musil, 2017). With the initial count at 143 million people, Equifax gradually increased these reports to 147 million individuals included in the compromised data (Fung, 2018). Although the announcement was made in September, it later became apparent that Equifax had spent the prior 6 months determining the scope of the breach and patching their systems before alerting customers and shareholders (Tsukayama, 2017). The complete breakdown of the stolen information in the Equifax breach is shown in Table 1 below.

Information Type	Quantity
Birthdays	146.6 million
Social Security Numbers	145.5 million
Addresses	99 million
Gender Identifications	27.3 million
Phone Numbers	20.3 million
Drivers License Numbers	17.6 million
Email Addresses	1.8 million
Credit Card Numbers and Expiration Dates	200,000

Table 1. Types and quantities of records exposed during the Equifax data breach (Woodall, Candy, 2018)

Approximately two months prior to the incident, Equifax admittedly knew of a vulnerability in the Apache Struts tool which is used to build web applications (Wattles & Larson, 2017). The timeframe that the attackers had to find consumer information once the network was breached is unknown, making it difficult to know how long the attack was in progress and when it concluded (Newman, 2017). However, it is known that there were several other information security vulnerabilities located in Equifax systems around the same time as the data breach. For instance, Brian Krebs (2017) reported that a consumer dispute portal was hosted on a server that was open to the Internet and accepted login credentials of "admin" as both the username and password. This portal allowed users who authenticated with the "admin" account to add, modify, and delete additional users in the system and to access employee credentials (including plaintext passwords in the HTML source code) along with consumer dispute information (Dellinger, 2017).

The Actors Behind the Breaches

Data breaches are incidents which occur in a multitude of ways. Likewise, the actors behind these breaches can be from varying backgrounds, professions, cultures, and have a number of motives for performing the act. According to a report by Verizon (2018), an overwhelming majority (76% in 2018) of data breaches come from actors with a financial interest in obtaining the data. Individuals or groups with this goal are hoping to sell the information that they gained on the black market or to extort money from the victim (Calyptix, 2017).

Other attackers may be motivated by espionage reasons. Perpetrators of attacks with an espionage purpose are looking to cause harm or to gain an advantage over a competing company

or a foreign government and are therefore often nation-state actors participating in these attacks (Carbon Black, n.d.). A vast majority of the attackers who do not have a financial or espionage goal are categorized into a group known as fun, ideology, or grudge (FIG) assailants (Radware, 2018). Generally, these individuals have a personal vendetta against their victim, or they simply enjoy causing the harm to the individuals and companies which are being attacked (Calyptix, 2017).

Verizon's 2018 report (Verizon, 2018) also reported that 73% of all cyber attacks (including data breaches) were performed by entities external to the organization that was attacked. This means that approximately a fourth of all cyber attacks and data breaches originate with internal staff. This demonstrates that efforts to thwart attacks need to focus both on external and internal vectors. Also, it should be noted that all internal threats are not intentional or malicious. Data breaches can be caused by negligent behavior as well. For instance, the healthcare industry is often plagued with workers accessing patient records through curiosity or for fun when they do not have a valid reason to be accessing the patients' information (Leyden, 2018). This unauthorized access of data would constitute a data breach since protected health information would have been presented to an unauthorized individual.

Other industries and sectors other than healthcare also have their own unique challenges and areas of concern: Financial and insurance services are more at risk for payment card skimmers and ATM attacks and educational institutions and public sector organizations are more susceptible to espionage attacks attempting to steal research material and state or military secrets (Leyden, 2018). However, even though each type of organization has its own challenges, all organizations are in some way vulnerable to nearly every category of attack. A particular concern to all organizations is the threat of social engineering. Verizon (2018) found that ninety

percent of all data breaches that were examined contained some aspect of phishing or social engineering. Regardless of the particular vector chosen by the attacker, it is clear that all of these attacks are a means to achieve some goal that benefits the attacker in some way, but to the detriment of the victim.

Best Practices for Preventing a Data Breach

Each organization will be at varying levels of risk to a particular attack vector depending on countless variables including public Internet presence, internal technology, and network devices and configurations, staff education, political affiliations, and more. The aim of this section will not be to provide any detailed information as to how to accomplish risk remediation for any individual vulnerability but to provide a basis on which further research can be built in order to design a plan to address some of the weaknesses that the reader's organization may currently have.

Risk Assessment

In order to do any vulnerability remediation, a proper risk assessment must be performed for the organization. Potentially the most important part of the risk assessment is the thorough identification of all information assets. The assets identified should include all data that is deemed as important to an organization by means of its operation or to provide it with an advantage over their competitors (Rees & Allen, 2008). Also included should be all physical hardware devices, software packages, and any communication system(s) used by the organization (Shameli-Sendi & Aghababaei-Barzegar, 2016).

After an inventory has been completed, an organization should determine what vulnerabilities exist to each asset. These vulnerabilities can be technical in nature (e.g., a security vulnerability in a software package) or non-technical in nature (e.g., a network close that does not contain a door lock to prevent entry). These vulnerabilities should then be analyzed and assigned a priority along with potential remediation steps that could be undertaken to mitigate the threat. Once the risk assessment has been completed, the organization must determine what risks they are willing to accept, known as the risk appetite (Miyamoto, Holzer, & Sarkani, 2017). It is then up to the organization how to proceed in the remediation of risks that they decide to not accept.

Security Policy

All organizations should develop and maintain a comprehensive information security policy for their staff. An organization's information security policy should include even the most rudimentary of topics such as logging off or locking a computer when stepping away or not sharing usernames and passwords with other staff (Brown E. , 2017). Additional points that should be incorporated into the policy are change control processes, password complexity requirements, and system acceptable use policies which dictate for what purposes the organization's computer and communication systems can be used (Bayuk, 2009).

User Education

As noted by Verizon (2018), ninety percent of data breaches included an aspect of phishing and/or other social engineering in the attack. The end users at an organization are often seen as the first line of defense against incidents such as phishing and social engineering as they

are often the individuals who come in contact with these attacks (Sharma, 2017). As important as this aspect of information security is, it is more often than not either neglected or still seen as sufficient for organizations. More than seventy percent of organizations state that a major vulnerability in their organization is a lack of security awareness for employees and forty percent don't provide any security education to their employees (Bhadane & Mane, 2017).

In addition to phishing and social engineering attacks, employee negligence is another large vulnerability for many organizations. A lot of these instances can be mitigated by user training. Symantec found that 62 percent of employees have a misconception that transferring data to an external location using either a personal device or a cloud service is acceptable (Hamilton, 2013). In situations such as this, routine user education to ensure that the users know what is and is not acceptable and to keep the topics fresh in their mind is imperative.

Defense-in-Depth

Defense-in-depth is a method of information security that has been around for years. Also known as the Castle Approach, this concept is simply a layering of security protections in order to best protect an information security asset (Forcepoint, n.d.). These layered approaches begin at the outer perimeter and include intrusion prevention systems, firewalls, proxy servers, etc. (Zhang, Kodituwakku, & HInes, 2019). If an attacker is successful in breaching the perimeter, additional layers of security would await, such as protections on the platform (for example antivirus software and operating system patches), application (such as secure coding), and data (e.g., encryption) layers (TCS, 2018). Simply implementing these layers is not enough. Care must be taken to ensure that all layers are properly configured (e.g., proper firewall rules) to prevent intruders. In addition, routine evaluations of the network up to and including penetration

tests should be performed with the attempt to find weaknesses in the security before they are found by the attackers. Properly employing a defense-in-depth strategy can drastically increase the security of an organization's network and decrease the likelihood of a successful attack and/or data breach.

Encryption

Encryption is the changing of plaintext information (clearly readable) into ciphertext which can only be read by the authorized party using the correct decryption keys and methods. Encryption can be implemented in a number of ways including on traffic being sent over a wired or wireless network, on a file-by-file basis (e.g., when emailing a file to a colleague), or as full-disk encryption methods on laptops and mobile devices. When using proper encryption ciphers, even if data is sent to an unauthorized individual or a laptop containing confidential information is stolen from a vehicle, the information lost will be of no use to the outside party (Yahnke, n.d.). The use of encryption will not prevent other attacks (such as ransomware), it can help to ensure that certain attack vectors are rendered useless to malicious actors.

Audit

Auditing in the sense used in this paper has a two-fold meaning. First is the auditing of the information security strategy that is currently put in place. Even the best security strategy eventually needs routine updating or improvement. Periodic evaluations and vulnerability assessments should be completed to ensure that no adjustments need to be made to the organization's current information security implementation(Yahnke, n.d.). If any new vulnerabilities are found, proper procedures set forth in the company's policy should be followed

to implement a strategy for mitigation (unless the organization is willing to accept the risk). Likewise, if a vulnerability or information asset was found previously but is no longer valid (e.g., a decommissioned server), system documentation should be updated, and any needed adjustments should be made to system configurations.

The second meaning for auditing is to audit the network for security violations. Implementations of intrusion detection and prevention systems (IDPS) and firewalls can largely automate this process. However, routine assessments of the systems' operation should be conducted to ensure network traffic is being properly monitored, classified, blocked, or allowed. Additional auditing can be put in place in the way of specialized software to monitor users on the network (e.g., what systems and data a user is accessing) and possible exfiltration of data from the network (using data loss prevention (DLP) solutions).

Summary

Today's computer systems operate in a highly connected environment. This increasingly connected world increases the likelihood of a cyber attack at any time. Often, these attacks come in the form of data breaches that often make national headlines. Breaches of Yahoo, Adult Friend Finder, Target, Sony, and Equifax, among others, have resulted in the release of billions of people's personal information. In some cases, this release was of just contact information such as email addresses. Other releases included more personal information such as social security numbers, passwords, credit card numbers and more.

This paper explored these major data breaches at a high level, describing what information was breached, how many records were breached, and the vectors that the attackers took to compromise the data. Following, the author provided a broad overview of the actors

behind these breaches, including their purpose, whether it be for financial gain, political, or espionage reasons. All sectors are susceptible at some level to actors of all of the aforementioned actor types. However, these sectors, whether healthcare, financial, education, or government, each have a higher likelihood of an attack from one or more of these types.

This paper concluded with a brief explanation of several ways an organization can protect itself from a data breach. While there is no framework or strategy to guarantee an organization will not suffer an attack or a data breach, there are best practices that can be followed to decrease the likelihood of a data breach occurring or minimizing these impacts if a breach does occur. Methods such as ensuring a data security policy, user education, defense-in-depth, encryption, and auditing make it harder for an attacker to be successful in his or her attempts at gaining access to a system and exfiltrating the data for nefarious purposes.

The contents of this paper is not meant to be a sole source of information on any one of these areas. However, it is the author's hopes that the content can be used to guide the reader on further research to understand what data breaches are, why they happen, who conducts them, and how to best protect themselves.

References

Alnabulsi, H., Islam, R., & Talukder, M. (2018, November 30). GMS: Gathering Multiple Signatures Approach to Defend Against Code Injection Attacks. *IEEE Access*, 77829-77840.

Anonymous. (2018, March). Biggest breaches of personal data of 21st century. *Privacy Journal, 44*(5), 1-2.

Armerding, T. (2018, December 20). *The 18 biggest data breaches of the 21st century*. Retrieved from CSO Online: https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html

Bayuk, J. (2009, June 16). *How to write an information security policy*. Retrieved from CSO Online: https://www.csoonline.com/article/2124114/strategic-planning-erm-how-to-write-an-information-security-policy.html

BBC. (2016, November 14). *Up to 400 million accounts in Adult Friend Finder Breach*. Retrieved from BBC: https://www.bbc.com/news/technology-37974266

Bhadane, A., & Mane, S. B. (2017, December). State of Research on Phishing and Recent Trends of Attacks. *i-Manager's Journal on Computer Science, 5*(4).

Bora, K. (2014, December 1). *Sony Hack 2014: 'Fury,' 'Annie' Among Leaked Movies; Company Calls In FBI*. Retrieved from International Business Times: https://www.ibtimes.com/sony-hack-2014-fury-annie-among-leaked-movies-company-calls-fbi-1731055

Botha, J., Grobelr, M., & Eloff, M. (2017). Global Data Breaches Responsible for the Disclosure of Personal Information: 2015 and 2016. *European Conference on Cyber Warfare and Security*, (pp. 63-72).

Brown, E. (2017, December 22). *5 Best practices to prevent data leaks in 2018*. Retrieved from IT Pro Portal: https://www.itproportal.com/features/5-best-practices-to-prevent-data-leaks-in-2018/

Brown, K. (2019). *The Dangers of Weak Hashes.* SANS Institute.

Calyptix. (2017, June 29). *Top 3 Causes of Data Breach Are Expensive*. Retrieved from Calyptix Security: https://www.calyptix.com/top-threats/top-3-causes-data-breach-expensive/

Carbon Black. (n.d.). *What is Cyber Espionage?* Retrieved from Carbon Black: https://www.carbonblack.com/resources/definitions/what-is-cyber-espionage/

Dellinger, A. J. (2017, September 13). *Equifax Breach Worsens: Argentina Branch Used 'Admin' As Login and Password*. Retrieved from International Business Times: https://www.ibtimes.com/equifax-breach-worsens-argentina-branch-used-admin-login-password-2589657

Elkind, P. (2015, June 25). *Sony Pictures: Inside the Hack of the Century, Part 1*. Retrieved from Fortune: http://fortune.com/sony-hack-part-1/

Forcepoint. (n.d.). *What is Defense in Depth?* Retrieved from Forcepoint: https://www.forcepoint.com/cyber-edu/defense-depth

Fung, B. (2018, May 8). 145 million Social Security numbers, 99 million addresses and more: Every type of personal data Equifax lost to hackers, by the numbers. *The Washington Post*.

Goldman, D. (2013, December 27). *Target confirms PIN data was stolen in breach*. Retrieved from CNN: https://money.cnn.com/2013/12/27/technology/target-pin/

Goodin, D. (2016, September 22). *Yahoo says half a billion accounts breached by nation-sponsored hackers*. Retrieved from Ars Technicahttps://arstechnica.com/information-

technology/2016/09/yahoo-says-half-a-billion-accounts-breached-by-nation-sponsored-hackers/: https://arstechnica.com/information-technology/2016/09/yahoo-says-half-a-billion-accounts-breached-by-nation-sponsored-hackers/

Hamilton, R. (2013, June 5). *Mistakes are costing companies millions from avoidable data breaches*. Retrieved from Symantec: https://www.symantec.com/connect/blogs/mistakes-are-costing-companies-millions-avoidable-data-breaches

Kashmiri, S., Nicol, C. D., & Hsu, L. (2017, March). Birds of a feather: intra-industry spillover of the Target customer data breach and the shielding role of IT, marketing and CSR. *Journal of the Academy of Marketing Science, 45*(2).

Kassner, M. (2015, February 2). *Anatomy of the Target data breach: Missed opportunities and lessons learned*. Retrieved from ZDNet: https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/

Kirk, J. (2016, November 14). *Alleged Adult Website Breach May Affect 412 Million Accounts*. Retrieved from Bank Info Security: https://www.bankinfosecurity.com/alleged-adult-website-breach-may-affect-412-million-accounts-a-9519

Krebs, B. (2014, February 5). *Target Hackers Broke in Via HVAC Company*. Retrieved from Krebs on Security: https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/comment-page-2/

Krebs, B. (2017, September 12). *Ayuda! (Help!) Equifax Has My Data!* Retrieved from Krebs on Security: https://krebsonsecurity.com/2017/09/ayuda-help-equifax-has-my-data/

Lennon, M. (2014, December 19). *Hackers Used Sophisticated SMB Worm Tool to Attack Sony*. Retrieved from Security Week: https://www.securityweek.com/hackers-used-sophisticated-smb-worm-tool-attack-sony

Leyden, J. (2018, April 10). *Company insiders behind 1 in 4 data breaches - study*. Retrieved from The Register: https://www.theregister.co.uk/2018/04/10/verizon_dbir/

Lord, N. (2017, July 27). *A Timeline of the Ashley Madison Hack*. Retrieved from Digital Guardian: https://digitalguardian.com/blog/timeline-ashley-madison-hack

Miyamoto, I., Holzer, T. H., & Sarkani, S. (2017, May). Why a counterfeit risk avoidance strategy fails. *Computers & Security, 66*, 81-96.

Newman, L. H. (2017, September 14). *Equifax Officially Has No Excuse*. Retrieved from Wired: https://www.wired.com/story/equifax-breach-no-excuse/

Ng, A., & Musil, S. (2017, September 7). *Equifax data breach may affect nearly half the US population*. Retrieved from CNET: https://www.cnet.com/news/equifax-data-leak-hits-nearly-half-of-the-us-population/

Plachkinova, M., & Maurer, C. (2018, Winter). Teaching Case Security Breach at Target. *Journal of Information Systems Education, 29*(1).

Radichel, T. (2014). *Case Study: Critical Controls that Could Have Prevented Target Breach.* SANS Institute.

Radware. (2018, January 3). *Why Hackers Hack: Motives Behind Cyberattacks*. Retrieved from Radware: https://www.radware.com/newsevents/mediacoverage/2018/why-hackers-hack-motives-behind-cyberattacks

Ragan, S. (2016, November 13). *412 million FriendFinder accounts exposed by hackers*. Retrieved from CSO Online: https://www.csoonline.com/article/3139311/412-million-friendfinder-accounts-exposed-by-hackers.html

Rees, J., & Allen, J. (2008, October 28). The State of Risk Assessment Practices in Information Security: An Exploratory Investigation. *Journal of Organizational Computing and Electronic Commerce, 18*(4), 255-277.

Roman, J. (2015, February 5). *Sony Exec Steps Down After Breach*. Retrieved from Data Breach Today: https://www.databreachtoday.com/sony-exec-steps-down-after-breach-a-7879

Seal, M. (2015, March). *An Exclusive Look at Sony's Hacking Saga*. Retrieved from Vanity Fair: https://www.vanityfair.com/hollywood/2015/02/sony-hacking-seth-rogen-evan-goldberg

Shameli-Sendi, A., & Aghababaei-Barzegar, R. (2016). Taxonomy of information security risk assessment (ISRA). *Computers & Security, 57*, 14-30.

Sharma, A. (2017, May 5). Dealing with Phishing and Ransomware the Right Way. *PCQuest*.

Smith, M., & Mulrain, G. (2017). Equi-Failure: The National Security Implications of the Equifax Hack and a Critical Proposal for Reform. *Journal of National Security Law & Policy, 9*(3), 1-54.

Sullivan, C. (2016). The 2014 Sony Hack and the Role of International Law. *Journal of National Security Law & Policy, 8*(3), 1-27.

TCS. (2018, August 10). Retrieved from Tata Consultancy Services: Cyber Security Community: https://securitycommunity.tcs.com/infosecsoapbox/articles/2018/08/09/defense-depth-%E2%80%93-what-strategy-follow

Tsukayama, H. (2017, September 8). Why It Can Take So Long for Companies to Reveal Their Data Breaches. *The Washington Post*.

US-CERT. (2014, December 19). *Alert (TA14-353A) - Targeted Destructive Malware*. Retrieved from US-CERT: https://www.us-cert.gov/ncas/alerts/TA14-353A

Verhoeven, B., & Hod, I. (2015, November 11). *Sony Hack Revisited: Next Hollywood Cyber Attack Is Question of 'Not If But When'*. Retrieved from The Wrap: https://www.thewrap.com/sony-hack-revisited-next-hollywood-cyber-attack-is-question-of-not-if-but-when/

Verizon. (2018). *2018 Data Breach Investigations Report.* Verizon.

Vijayan, J. (2014, February 7). *Target attack shows danger of remotely accesible HVAC systems*. Retrieved from ComputerWorld: https://www.computerworld.com/article/2487452/target-attack-shows-danger-of-remotely-accessible-hvac-systems.html

Wattles, J., & Larson, S. (2017, September 16). *How the Equifax data breach happened: What we know now*. Retrieved from CNN: https://money.cnn.com/2017/09/16/technology/equifax-breach-security-hole/index.html

Whittaker, Z. (2016, November 13). *AdultFriendFinder network hack exposes 412 million accounts*. Retrieved from ZDNet: https://www.zdnet.com/article/adultfriendfinder-network-hack-exposes-secrets-of-412-million-users/

Williams, M. (2017, October 4). *Inside the Russian hack of Yahoo: How they did it*. Retrieved from CSO Online: https://www.csoonline.com/article/3180762/inside-the-russian-hack-of-yahoo-how-they-did-it.html

Woodall, Candy. (2018, May 10). Equifax data breach worse than expected. *York Daily Record*.

Xiaokui Shu, K., Ciambrone, A., & Yao, D. (2017, January 18). Breaking the Target: An Analysis of Target Data Breach and Lessons Learned. *IEEE*.

Yahnke, K. (n.d.). *11 Expert Tips for Data Breach Prevention in 2019*. Retrieved from i-Sight: https://i-sight.com/resources/data-breach-prevention/#Use%20Encryption

Yahoo breach indictments may shed light on other hacks. (2017, March 16). Retrieved from Long Island Business News: http://link.galegroup.com/apps/doc/A487291055/ITBC?u=ncliveecu&sid=ITBC&xid=9e3d0242

Zetter, K. (2014, December 3). *Sony Got Hacked Hard: What We Know and Don't Know So Far*. Retrieved from Wired: https://www.wired.com/2014/12/sony-hack-what-we-know/

Zhang, F., Kodituwakku, H. A., & HInes, J. W. (2019, January). Multi-Layer Data-Driven Cyber-Attack Detection System for Industrial Control Systems Based on Network, System, and Process Data. *IEEE Transactions on Industrial Informatics*.