Data Theft

By

Cameron Meyer

Submitted to the Department of Technology Systems

In partial fulfillment of the requirements for the degree of

Master of Science

At

EAST CAROLINA UNIVERSITY

May 2017

This page intentionally left blank

Abstract

Data theft is an ever present and continually growing issue in today's networked world. Data theft is not simply an issue for individual computer users; it plagues large corporations and governments as well. With this in mind, individual's privacy and financial standing are at risk in these attacks. Corporations are primarily affected monetarily and when governments are attacked, it can bring on national security issues. Individuals targeted for data theft are at risk of having their identities stolen and potentially suffering personal monetary damages. Corporate data theft has now become one of the most significant concerns for companies of every size and cybersecurity teams are essential to companies in order for companies to be successful. Without proper protection from data theft companies stand to suffer large monetary losses or loss of industry/company secrets. Governments especially must take every precaution to protect against data theft due to the highly sensitive and classified nature of data. This data can range from confidential (if lost this information is slightly damaging to national security) to top secret (if lost this information is extremely damaging to national security). Staying ahead of the curve has been a difficult task for experts within the cybersecurity field as data theft has become a much more prevalent issue in recent years. The best way to ensure protection is to have a security policy and stance that is all encompassing. Every security measure available must be taken in order to safeguard against data theft from antivirus software to physical security to training employees.

Introduction

Today's world is dominated by computer networks. Almost everything is handled online digitally whether it be government information, military planning, business/financial transactions, social networking, etc. With the ever expanding Internet, this data is increasingly vulnerable as more and more people and devices are constantly gaining access to the Internet. When this digital data is compromised or stolen the act is called data theft or breach. "According to 38 USCS Â§ 5727(4) [Title 38. Veterans' Benefits; Part IV. General Administrative Provisions; Chapter 57. Records and Investigations; Subchapter III. Information Security] the term "data breach" means the loss, theft, or other unauthorized access, other than those incidental to the scope of employment, to data containing sensitive personal information, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data (US Legal Inc)".

The act of data theft is not limited to the targeting of one of these domains or even individual persons. While individual persons may be targeted for reasons such as stealing sensitive personal information to include: social security numbers or bank account information, the larger issue is when governments and businesses are the targets of data theft. Governments in particular need to safeguard their information as some of the data is rated as top secret or even higher in classification and can pose serious threats to national security. For example, The United States government has three official classification levels of information. The lowest is confidential, "which reasonably could be expected to cause damage to the national security" (Executive Order 13526, pg. 299) The classification level of secret is the middle tier classification, “which reasonably could be expected to cause serious damage to the national security” (Executive Order 13526, pg. 299). The highest level of official classification is top secret “which reasonably could be expected to cause exceptionally grave damage to the national security” (Executive Order 13526, pg. 298). According to the Government Accountability Office in a report from 2016, cyberattacks on the U.S. government rose 1,300% from 2006-2015 (Bhattacharyya, 2016). Businesses are also a large target or attackers to attempt to steal data as these can be very lucrative for hackers if they are successful in stealing data. For example, a spam e-mailing company named “A Whole Lot of Nothing LLC” targeted over 60 million individuals personal information and resulted in $2 million in illegal profits for the company (Walters, 2016). When government and business information systems are targeted, individuals are often secondary targets as these organizations typically maintain large databases with personal information of clients and employees. In December 2015, Alliance Health was targeted and hackers gained access to and released personal information of more than 1.5 million users (Walters, 2016).

With the threat of data theft constantly growing, organizations and individuals must have a more rigorous posture in protecting against data theft. It starts at the individual and user level with educating on the risks associated with operating on the Internet and expands all the way to physical security and more intricate network security designs and capabilities for large organizations. The more valuable and important the information, the more rigorously it must be protected.

High-Profile Data Theft Cases and Cyberattacks Against Governments

In recent years there have been many noteworthy cyberattacks against government organizations that have taken place, many of which have garnered national and even world news coverage. In 2005, the United States government was targeted in a series of large scale attacks against military and government sites alike. The British and German governments were also targeted and these attacks are believed to have originated from the People's Liberation Army of China and the attacks are believed to have been ongoing for approximately four years (Jones, 2016). This large scale ongoing attack was the largest attack against government organizations in history and the intelligence gathering effort on behalf of China came to be known as Titan Rain (Jones, 2016). In 2016, it was believed that Russia played a large role in influencing the Presidential election. The United States government has publicly blamed Russia for stealing emails from the Democratic National Committee and playing a role in influencing the outcome of the 2016 Presidential election. U.S. intelligence communities have stated that the methods and motivations directly tie into those used by Russian hackings in recent years and that they were directed in the attacks by the Russian government (Renaud & Tankard, 2016). It is also believed that the attempts to breach voter registration systems in over 20 states can be linked back to Russian hackings (Renaud and Tankard, 2016). This is not the only high profile case that has been attributed to Russian hackings in recent years. The Russian government has also been accused of hacking other governments and the World Anti-Doping Agency and publishing the information from these hackings on to sites such as Wikileaks and DCLeaks (Renaud and Tankard, 2016).

Although not necessarily a case of data theft, one of the largest and most devastating cyberattacks against a government targeted Estonia. The attacks were political in nature as the attacks were attributed to Russia. In 2007 Estonia experienced denial-of-service attacks believed to be perpetrated by the Russian government. According to the Elliott School of International Affairs at George Washington University the "attacks targeted prominent government websites along with the websites of banks, universities and newspapers" and the attacks lasted around three weeks. The Elliott School goes on to say that this is the first documented case of an act of cyber warfare levied upon a nation. The attacks managed to kick the Parliamentary sites as well as political party sites of the Estonian government offline within the first week. The second week of the attacks shifted the focus from political targets to the country's newspapers and effectively cut Estonia off from the rest of the world as they "could not inform the rest of the world of what was happening in their country" (Elliott School, 2015). The last week of the attacks saw another shift in its focus as the banking industry of the country became the target. This was crippling as the country "conducted ninety-seven percent of its banking transactions online" (Elliot School). The Estonian government and economy were crippled during this time due to the importance of the Internet in conducting everyday matters.

Another large scale cyberattack against a government worth noting occurred in 2009-2010 and targeted the country of Iran. The attack took place in the form of a computer worm virus that was programmed to take over specific industrial control systems and cause those systems to malfunction. However, while causing the systems to malfunction the worm also fed false information to monitoring systems that the equipment was running as it was supposed to be. Computer security experts that analyzed the Stuxnet worm found that it was designed to target specific systems manufactured by Siemens AG that. These systems were used in power plants and other places in order to control specific machinery. The following excerpt from the Encyclopedia Britannica:

> the worm targeted only Siemens SCADA systems that were used in conjunction with frequency-converter drives, devices that control the speed of industrial motors, and even then only drives that were made by certain manufacturers in Finland and Iran and were programmed to run motors at very specific high speeds. This combination indicated to analysts that the likely target of Stuxnet was nuclear installations in Iran—either a uranium-enrichment plant at Naṭanz or a nuclear reactor at Būshehr or both—a conclusion supported by data showing that, of the approximately 100,000 computers infected by Stuxnet by the end of 2010, more than 60 percent were located in Iran.
>
> The worm was found to have been circulating since at least mid-2009, and indeed in the latter part of that year at the Naṭanz plant an unusually large number of centrifuges (machines that concentrate uranium by spinning at very high speeds) were taken out of operation and replaced. The Iranian nuclear program, which most foreign governments believed was working to produce nuclear weapons, continued to suffer technical difficulties even after discovery of the worm."

Stuxnet is revered as one of "the most sophisticated pieces of malware ever written" (Encyclopedia Britannica). This highlights the severity a cyberattack can have and the level of damage that can be levied upon a country's government. It was believed that the Stuxnet worm originated from either the United States or Israeli governments. Cyber security experts speculated that the damage done to the Iranian nuclear program was a serious setback (Encyclopedia Britannica).

High-Profile Data Theft Cases and Cyberattacks Against Companies

Companies have also been the target of some of the largest data breaches in history. One of the biggest online data breaches in U.S. history and the largest ever from a single site occurred in 2016 with Yahoo being the target. The attack resulted in over 500 million user accounts from the company (Fahey and Wells, 2016). Yahoo reported that no sensitive financial information was stolen during the breach but other valuable information on the individual users was stolen. This information included personal names, email addresses, telephone numbers, dates of birth, passwords and some answers to security questions (Fahey and Wells, 2016). The attack is believed to have occurred in 2014 with the information that the attack occurred not being brought forth until 2016. This delay in notification of the general public caused controversy and caught the attention of U.S. Senator Richard Blumenthal who began campaigning for tougher legislation on cyber security and companies reporting breaches that impact users and their sensitive information (Fahey and Wells, 2016).

What is known as the largest data theft case in history, targeted not just a single company but many companies. Hold Security firm discovered that over 1.2 billion accounts had been stolen by a Russian cyber gang (named CyberVor by Hold Security) that took breached over 420 thousand web and File Transfer Protocol (FTP) sites (Fahey and Wells, 2016). In order to perpetrate the attacks on these sites, the gang acquired large databases of stolen credentials on the black market. Once the gang had these credentials, they used the credentials to attack email providers, social media and other websites as carriers to distribute spam to its victims which then installed malware on systems (Hold Security Firm, 2014). The other tactic that was used by the cyber gang was the use of large botnets. These botnets tracked websites that its victims frequently visited and then queried those sites in order to identify SQL vulnerabilities. Hold Security Firm called these SQL queries of over 420,000 sites the largest security audit ever (Hold Security Firm, 2014). Once the SQL vulnerabilities were identified, the gang now had access and was able to steal databases from the sites in question where the gang then focused on stealing credentials and personal information. With this, the gang amassed a collection of 4.5 billion credentials in total with 1.2 billion of these being unique pairs of email addresses with their accompanying passwords (Hold Security Firm, 2014).

Myspace was the victim of a large scale attack in 2013 where 360 million accounts and their information were stolen by a hacker from Russia (Fahey and Wells, 2016). Once again, the information on the attack did not come to light immediately. Instead the information came in 2016, three years after the breach occurred. The information that was stolen from the social media site included personal names, email addresses and passwords. The affected users included not only current Myspace users but also past Myspace users even if the accounts had been inactive for a long period of time (Fahey and Wells, 2016). The attack has been attributed to an individual Russian hacker that goes by the codename “Peace” as this person was identified attempting to sell the stolen information from these 360 million accounts on the black market (Fahey and Wells, 2016).

The same Russian hacker (Peace) that stole the information of 360 million user accounts from Myspace also successfully stole the information of 167 million Linkedin accounts in 2012 (Fahey and Wells, 2016). Again, the hacker was identified as posting the stolen information in an attempt to sell it on the black market. Linkedin identified the breach as being extensive as there were over 433 million registered accounts at the time of the breach with 167 million of them being compromised (Constantin, 2016). The information that was stolen includes user identities, email addresses and the accompanying password hashes.

eBay has been the victim of a large attack as well wherein the company had 145 million user accounts compromised (Fahey and Wells, 2016). The attack against eBay was verified to be comprehensive affecting all of its 145 million users registered with the website according to Business Insider (Finkle & Seetharaman, 2014). In this case, the breach was made possible by hackers obtaining the credentials of three corporate level eBay employees in order to access databases that contained user account information. In this case, since eBay conducts financial transactions on its site, there were no signs that user’s financial data was stolen or compromised in any way (Finkle and Seetharaman, 2014). The breach is believed to have occurred in February or March of 2014 and was detected in early May and the information regarding the breach was made public that same month.

One of the most notable and financially damaging attacks targeted Heartland credit card processing company where the data from 130 million credit cards was stolen. The information from these credit cards, including full credit card numbers were sold on the black market and then used to make unauthorized purchases and even to withdraw money from banking institutions (Stone, 2009). The company had to pay $140 million in fines and penalties, in addition one of the hackers responsible for the attack was sentenced to 20 years in prison (Fahey and Wells, 2016) although 2 Russian conspirators involved in the attack were never apprehended (Stone, 2009). The attacker arrested, Albert Gonzalez, was also involved in a data theft case against Dave and Buster's restaurant chain as well as stealing debit and credit card information from T.J. Maxx stores (Stone, 2009). In order to facilitate these attacks, the hacker "took advantage of flaws in the SQL programming language" in order to gain access to database information. In addition, the hacker also used sniffer programs on corporate networks that intercepted data transmitted during credit card transactions (Stone, 2009).

In rare cases, attacks on companies have been state sponsored. That is to say that the government of a nation directs the cyber attack on a company. Such was the case in 2014 when it is believed that the North Korean government launched an attack on U.S. company Sony Pictures (Peterson, 2014). It is believed that the North Korean government perpetrated the attack in response to a movie being released by Sony Pictures titled "The Interview" which was a comedy portraying the North Korean dictator in an unflattering light and details a comedic assassination plot against him. The attackers stole confidential documents from Sony and then released the documents online to the public at a later date which exposed personal information of employees in the company as well as details of films being produced by the company (Peterson, 2014). In addition, when employees logged in to their computers at work following the attack, they were greeted with screens depicting "a graphic of a neon red skeleton featuring the words '#Hacked by #GOP' and a threat to release data later that night" (Peterson, 2014). The attack also threatened violence against movie theatres and movie goers where the movie would still be shown. In response to this threat of physical violence, Sony Pictures stopped the showings for the movie for a brief time and then released it to theatres to be shown at that theatres own risk (Peterson, 2014). This was not Sony's first issue with cybersecurity though as the Playstation network was taken offline by hackers for several weeks. The hackers that took down the Playstation network stole the personal information from an undisclosed number of gamers that belong to the network described as being in the millions (Peterson, 2014). The hackers also gained access to sensitive personal information of the employees of Sony to include medical data, social security numbers, emails and individual performance evaluations (Peterson, 2014).

Cyber Security Best Practices

With the ever present threat of cyberattacks and data breaches, an all-encompassing cyber security policy is more important than ever. Ken Hess compiled a list of 10 best security practices for organizations to follow that can eliminate the vast majority of cyber attacks and data loss. These practices are: "educate your users, maintain security patches, network-based security hardware and software, use a comprehensive endpoint security solution, use a spam filter on email servers, secure websites against man in the middle and malware infections, implement a removable media policy, implement data loss prevention and auditing, use digital certificates to sign all of your sites and encrypt your data" (Hess, 2013).

One of the most basic ways to safeguard an organization and one of the most effective ways is education. If the employees and individuals working in an organization are informed, understand the risks and are cautious in operating information systems and computers within the organization then a lot of vulnerabilities and risks can be mitigated. For example, the United States Marine Corps requires each and every Marine as well as civilian employee to pass several online classes each year regarding cyber security as well as operational security. These classes detail how to protect computer systems from malware that can be delivered via email or things such as physical deliveries of discs/hard drives, etc. Employees are also taught the importance of physical security of computer systems by locking doors, logging off computers and physically protecting Common Access Cards (used to login to computer systems as well as gain access to base) from threats such as theft or tampering. Training employees on how to spot and what to do in cases of social engineering where persons attempt to gain access to physical spaces where computers and information systems are present. The Marine Corps also implements another one of Hess' practices which is a policy that governs the use of removable media. Removable media can pose a security threat for insider attacks where employees write data onto a removable media and take it outside of the organization or employees bring infected removable media into the organization and infect a computer with malware. The Marine Corps does not allow thumb drives or other storage devices with flash memory. The Marine Corps allows external hard disk drives as long as they are scanned and approved first. The Marine Corps has a looser policy governing DVDs and CDs where they are allowed and need not be scanned prior to use.

Hess points to the importance of host based endpoint security as an important solution in network security. These hosts need to have up to date antivirus software installed on the devices. Also, personal software based firewalls on the device as an extra layer of defense against potentially malicious or suspicious traffic is useful. Host based intrusion detection can alert users and cyber security professionals to potential dangers on a single machine. This all adds up to what Hess refers to as a “comprehensive endpoint security solution” (Hess, 2013). It is extremely important to maintain relevant security patches to software and update antivirus software in order to protect against the latest malware and holes in security with regards to software. Scanning computers and information systems becomes obsolete if virus signatures are not updated. Antivirus software works to protect against known malware, with new forms of malware and new threats emerging everyday it is imperative to update antivirus software. This adds new and developing types of malware to be added to the database of known malware so that the software can properly handle detected malware.

Putting in place hardware and software in order to protect individual information systems and entire networks is essential. Incorporating network hardware such as firewalls, intrusion detection devices and honeypots although costly up front to buy will greatly improve network security for an organization (Hess, 2013). Firewalls in their most basic functionality can filter out harmful network traffic from entering or leaving a network and can restrict access to websites deemed dangerous or untrustworthy depending upon the rules configured on them. Intrusion detection devices can alert organizations to suspicious and dangerous activity taking place within the network. As evidenced by many of the large scale and high profile data theft cases and cyber attacks discussed earlier, breaches can go undetected by organizations for months or even years before they are detected and eventually stopped. This ties in with another of Hess’ best practices which is “implement data loss prevention and auditing” (Hess, 2013). It is crucial for organizations to constantly monitor their networks for suspicious activity and audit the traffic that is entering and leaving the network. When suspicious activity is detected on the network then in order to prevent the loss of data, traffic leaving the network needs to be halted.

One of the most common exploits that affected the databases of organizations were sites and servers that were unsecure, one of the exploits was SQL vulnerabilities. In the case Hold Security Firm detailed against Russian hackers they exploited SQL vulnerabilities in many of the attacks perpetrated against the over 420,000 sites that were attacked. Securing these sites against SQL injections can protect databases stored on sites and servers and help prevent malware infections. Hess approves using digital certificates to sign sites and saving these certificates on hardware devices rather than web servers can help to protect these credentials from becoming compromised or even stolen by hackers (Hess, 2013).

A common vehicle used in cyber attacks are spam emails. Spam emails were used to facilitate the attacks in the Hold Security Firm case against Russian hackers and also used in the case of the company “A Whole Lot of Nothing LLC”. Using a spam filter is beneficial in preventing spam emails from being delivered to users and employees inboxes. This is where educating employees also comes in hand, because the spam filter will not completely stop spam emails from being delivered to employees. Recognition of spam emails and the risks associated with them by employees will ensure that the spam emails that make it through the spam filter aren’t effective in delivering their malicious content.

The number one recommendation made by Hess as a best practice for cyber security is to encrypt data (Hess, 2013). When possible, encrypting data that is travelling across the network helps protect it even if it is intercepted in a scenario such as a man in the middle attack. When possible, the use of VPNs is highly encouraged. This is especially crucial if the data travelling across the network are financial transactions. Albert Gonzalez, the hacker in the Heartland credit card processing case used man in the middle to steal credit card numbers and also used the same tactic against TJ Maxx and Dave and Busters. Data that is stored on servers, file systems and computers should also be encrypted especially if the data being stored is sensitive in nature. Encrypting data stored on devices can also serve to protect sensitive data if equipment is lost or stolen. If data falls into the wrong hands it can still be protected depending on the level of encryption used.

One of the simplest ways to protect against cyber attacks and data breaches is physical security. This security measure ensures that would be attackers cannot gain physical access to network equipment. For example, the Marine corps constantly has an employee on duty 24 hours a day in order to keep a watchful eye over information systems that carry sensitive information. In addition to this, the Marine Corps also stores any equipment that has Secret level information or higher stored in locked vaults that are monitored 24 hours a day. When sensitive information systems cannot be monitored as rigorously as the Marine Corps does then it is best to cut off physical access as much as possible this includes keeping these systems locked up. Physical security also extends to wireless security, its important to measure how far wireless signals given off by routers and wireless access points reach. Strategically placing these pieces of network equipment so that the signal does not extend past the physical structure of the building can keep unwanted users from gaining access to the network.

Conclusions

With the growing dependence and high usage of the Internet today the prevalence of cyber attacks and data breaches are growing more and more. Often time governments and companies are the targets of these cyber attacks due to the high level of sensitive data that is stored on the network equipment of these organizations. Governments store highly classified information that can pose great threats to national security that must be protected from data loss as rigorously as possible. Companies store large amounts of data that are sensitive due to the financial nature of the data.

There have been numerous attacks perpetrated against governments across the world with cyber attacks against U.S. government information systems rising over 1,300 percent from 2006 to 2015 alone (Bhattacharyya, 2016). The intent of these attacks may not always be data theft although that is the biggest concern due to the highly sensitive nature of the information, but simply taking systems offline in order to disrupt normal operations can also be the intent as evidenced in the attacks on Estonia and the use of Stuxnet against Iran. State sponsored attacks where governments target one another with cyber attacks have political intent such as the Russian attacks on the U.S. Democratic party reportedly influencing the 2016 U.S. Presidential election and attempting to hack voter registration systems.

Attacks on companies have been almost as prevalent as attacks on government organizations. The breaches have resulted in massive cases of lost data and compromised user accounts with personal information typically being the target of the attackers. This information was then sold on the black market in some cases. Financial gain being the main goal in attacking companies, the hack on Heartland credit card processing company still stands as one of the most costly data breaches in history.

The prevalence and ever growing threat of data breaches means that cyber security has never been more important. Cyber security must always try to stay one step ahead of potential attackers. It is important for organizations to take a rigorous stance in protecting their assets and network equipment, this means considering and assessing all aspects of cyber security from physical security to education and training to hardware and software solutions to employing data encryption techniques. However, each one of these domains can fail without the other. Hardware and software solutions must be maintained and updated or upgraded in order to stay current with the threats that are possible. Physical security can fail without the data stored on the devices being encrypted and without employees being educated and trained on the importance of protecting physical assets and being on the lookout for social engineering attacks. Email spam filters cannot completely stop all spam emails from getting delivered to users. Users must be educated on the risks of spam emails and how to properly handle these emails. The users are one of the most important links to protect an organization from data breaches.

References

"Data Breach Law and Legal Definition." *USLegal.com*. US Legal Inc, n.d. Web. 27 Mar. 2017.

The President of the United States. "Executive Order 13526." *Executive Order 13526 of December 29, 2009 Classified National Security Information* (n.d.): n. pag. *Authenticated U.S. Government Information*. 29 Dec. 2009. Web.

Bhattacharyya, Suman. "Cyberattacks Against the US Government Up 1,300% Since 2006." *The Fiscal Times*. The Fiscal Times, 22 June 2016. Web. 14 Mar. 2017.

Walters, Riley. "Cyber Attacks on U.S. Companies in 2016." *The Heritage Foundation*. The Heritage Foundation, 2 Dec. 2016. Web. 20 Mar. 2017.

Renaud, Karen, and Colin Tankard. "US Officially Accuses Russia of DNC Hack While Election Systems Come under Attack." *Network Security* 2016.10 (2016): 1-2. Web. 27 Mar. 2017.

Fahey, Mark, and Nick Wells. "Yahoo Data Breach Is among the Biggest in History." *CNBC*. CNBC, 22 Sept. 2016. Web. 27 Mar. 2017.

Jones, Andrew. "Industrial Espionage in a Hi-tech World." *Computer Fraud and Security* 2008.1 (2008): 7-13. Web. 27 Mar. 2017.

Elliott School of International Affairs at the University of George Washington.

Denial-of-Service: The Estonian Cyberwar and its Implications for U.S. National Security. Web. 25 Mar. 2015.

"Stuxnet." *Britannica Academic*. Encyclopedia Britannica, 22 Feb. 2011. Web. 28 Mar. 2017.

YOU HAVE BEEN HACKED! (2014, October 08). Retrieved March 30, 2017, from https://holdsecurity.com/news/cybervor-breach/

Constantin, L. (2016, May 18). A hacker is selling 167 million LinkedIn user records. Retrieved March 30, 2017, from http://www.csoonline.com/article/3072153/data-breach/a-hacker-is-selling-167-million-linkedin-user-records.html

Finkle, J., & Seetharaman, D. (2014, May 27). Cyber Thieves Took Data On 145 Million eBay Customers By Hacking 3 Corporate Employees. Retrieved March 30, 2017, from http://www.businessinsider.com/cyber-thieves-took-data-on-145-million-ebay-customers-by-hacking-3-corporate-employees-2014-5

Peterson, A. (2014, December 18). The Sony Pictures hack, explained. Retrieved March 30, 2017, from https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/?utm_term=.c670ace7e3da

Hess, K. (2015, December 04). 10 security best practice guidelines for businesses. Retrieved April 2, 2017, from http://www.zdnet.com/article/10-security-best-practice-guidelines-for-businesses/