Cybersecurity Attacks

Dhanushga Lionel
Ontario Tech University
Ontario, Canada
dhanushga.lionel@ontariotechu.net

Abstract— **Many state-of-the-art technologies have been integrated into most businesses operations since the past decade. Automation, efficiency and convenience, are the main driving factors for businesses to adopt such technologies. Some classic examples would be digitalising sensitive information that were once stored and written on paper into computers and hard disc servers. However, in order for these systems to work properly, there needs to be a secure system set in place to protect such sensitive information. This is especially so when information are shared and distributed easily over an insecure network such as the internet. As long as one has the relevant skills, it is possible for one to retrieve such information from the internet. The internet has become a crucial part for the government sectors, private companies and millions of users worldwide. Being the main backbone of many activities, crippling the network would disrupt many severely. Thus, cybersecurity has since become a hot topic as there are always discussions on improving the current methods. This is especially so for the government sector worldwide as it concerns national security issues. There have been examples on conflicts occuring due to cybersecurity attacks, for example the WannaCry incident. Also, organisations such as WikiLeaks have supporters that exploit sensitive information in government sectors of different countries. Such information leaks could potentially strain the relationship between countries.**

This paper will touch on the main threats in cybersecurity, categorise these threats accordingly, analyse how the threats were carried and resolved using notable case studies.

Keywords-component; formatting; style; styling; insert (key words)

I. Introduction

The world has accepted cyber security as the act of defending networking systems, software applications and hardware systems from any form of digital attacks[1]-[3]. A digital attack is generally defined by the public as a deliberate attempt to intrude and gain access to software, computer systems, technology-dependent businesses, government agencies through the use of computers or network. Once they succeed in gaining access, take over admin access privileges,[2] they could steal information such as identity theft or alter software code.[3] Such attacks could potentially defame individuals, disrupt the lives of others and businesses. [4] Hence, its is a challenging task to design a secure cyber security measure and there are more electronic devices than users in the world. Also, there will always be a loophole in any measure and attackers are always innovating and capitalising on such loophole.[1]

CyberSecurity attacks did not just appear in the 21st century. Its history goes all the way back to 1988, where the first worm was created that gave birth to an attack that we would commonly know it as Distributed Denial of Service (DDoS) attack. In [5] the author elaborated that the first worm was created by a Cornell University graduate student, Robert Tappan Morris. As stated by the author, the initial purpose of the worm was determine the size of the internet by crawling the web, duplicate a copy of itself on other computers and compute the number of duplicate copies it made. The computed sum would then represent the number of computers that are connected to the internet. However, Morris had issues with ensuring its accuracy as the worm was forced to make a copy of itself on a for every one out of seven times. This duplication would still occur even if the computer tells the program that it has a copy of the worm. With an increasing number of worms present on a specific computer, the computer will be debilitated and crash in the end, which eventually lead to an unintentional DDoS attack [5].

From [5], the worm program that Morris created. resulted in damages for an estimated 6,000 computers, which accounts for 10% of the entire internet in 1988. The approximated cost for fixing the effects of what the worm did ranges from $100,000 to $ 1 million USD. Morris was eventually **charged** with the Computer Fraud and Abuse Act.

This eventually gave birth to various cybersecurity attacks subsequently.

II. Related Work

In [8], the author provides detailed insights on the various social engineering cyber attacks such as phishing, pretexting, baiting, quid pro quo and tailgating. The author explains how such attacks manipulate and deceive users and steal their information. The authors explains the motives between social attacks, the types of users that fall prey to social engineering attacks and preventive measures available. [9] mentions how costly and time consuming it takes to eradicate and prevent against viruses and worms. [9] investigates the minimal level of protection needed to ensure a healthy network exist and source for measures to infections such as SQL Slammer worm, instead of containing and removing it. Solutions towards tackling such attacks requires the cooperation of individuals. In [10] , the author based its research on Ecuador and emphasis on the importance of educating the public on cyber security attacks. Although businesses in Ecuador has some knowledge on cyber security, there are still room for improvement. Another notable point that the author in [10] has pointed out would be, the importance of nurturing the next generation of cyber security experts. In another literature review in [11] the author suggested a way to understand the vulnerabilities and classify attacks based on taxonomies. Taxonomy is defined by collin Dictionary, the science of classification. In the literature [11], many different kinds of tax monies were adopted by from different sources. The taxonomy that the author adopted was classification scheme, classification attribute description, objective and comments.

After much consideration, the following taxonomy will be adopted for this paper: type of attacks, incident categories, target sector, consequences of attack.

.

III. Proposed Taxonomy

After much consideration, the following taxonomy will be adopted for this paper: **type of attacks, incident categories, target sector, consequences of attack.**

A. *Types of Attacks*

Trojans: A type of malware that appears to be a legitimate software, or its embedded in a legitimate software that has been tampered. The malware would act on its own and open backdoors to allow other malicious malware to enter[12]-[14]

Virus: Malware that attaches to clean files and subsequently, infect other clean files. As the virus grows, it will corrupt, delete files or destabilise the core's functionality. [12]-[14]

Worm: A kind of malware that crawls through network interface to infect multiple devices that are connected to the network. the malware in turn uses the infected devices to further infect others.[12]-[14]

Spyware: A type of malware whose purpose is to spy on the user. It stays hidden in the background and steals personal information when the user does enter confidential information such as passwords. [12]-[14]

Ransomware: Ransomware is a type of malicious software used in cyberattacks that threatens to publish the victim's data or blocks access to it unless a ransom is paid. These attacks come in varying complexity where simple ransomware may lock the system in a way that a knowledgeable person is able to reverse or gain access to the data to more sophisticated attacks which encrypts the victim's data preventing access to it. The later uses a technique called cryptoviral extortion which when properly implemented is near impossible to regain access to data. The attackers use untraceable currencies such as cryptocurrencies for ransom payments making it difficult and in most cases impossible to trace and prosecute the perpetrators. Often the ransom must be paid within a time frame before the data will be lost forever to the victim. Depending on the target of the attack the ransom can range from a few hundred dollars for an attack on personal computers to thousands of dollars for an attack on businesses. [12]-[14]

Mitigation of Ransomware Attacks:

In order to protect against ransomware attacks users should have antivirus software installed and also keep offline backups of all data. Security software may not detect ransomware until the files have already been encrypted in which case it is too late. But in cases that the ransomware is detected early, it is relatively easy to quarantine and remove the malicious software since it takes some time for the encryption process to begin and complete. Other measures that users should take include exercising good "cyber hygiene". This includes exercising caution when opening email attachments and links.[28] Files from unknown senders should not be opened unless scanned with an updated antivirus software. It is also important to check the extension of the file to ensure that the file is the intended file type as attackers often disguise executable files with other file types. Network segmentation involved breaking up the network into smaller subnetworks. This can help mitigate the spread of an infection from reaching the entire network as infected subnetworks can be quarantined. Also, critical computers should be isolated from the rest of the network. In addition to this, in order to mitigate the spread of ransomware, infection control can be applied. This includes disconnecting infected machines from all networks.[28]

File system defenses against ransomware

There are various file systems that keep a snapshot of the data on a system, which can help to recover in the case of a ransomware attack.

-Volume shadow copy (VSS) is used on windows to store backups of data. In order to protect against the ransomware targeting the snapshots that VSS takes, users should disable user access to the user tool VSSadmin.exe"

-on windows 10, users can add backups and other important directories to Controlled Folder Access in Windows defender. This will proceed them from ransomware.

-ZFS is a software designed by Sun Microsystems which is a combined file system and logical volume manager. File servers running ZFS are almost universally immune to ransomware. This is because it is able to snapshot even large file systems many times an hour. These snapshots are read only so they cannot be modified and they cannot be deleted other than by an administrator.[28]

File decryption and recovery

In the case that a user's files have successfully been encrypted by ransomware, there are a number of tools that can possibly decrypt these files, although this may not always be possible. If a file has been encrypted and there exists a copy of this same file that has not been encrypted the tool can use these two files to figure out what key has been used to encrypt the file. Once this key has been found it can be used to decrypt the file. This process can take up to a couple days.

Another way users can recover files is by using a tool to recover old copies of files that have previously been deleted. [28]

Notable examples of Ransomware Attacks:

Reveton

Reveton was a ransomware Trojan that began to spread in 2012. It was based on the Citadel Trojan which targets credentials stored in password managers such as Keepass, Password Safe and nexus Personal Security Client. The Reveton would display a warning on the screen of the victim's computer designed to look like a message coming from law enforcement or the FBI. This message claimed that the computer had been used for illegal activities such as downloading pirated media/software or for viewing child porn and that a fine had to be paid in order to unlock their system. This ransom was to be paid using an anonymous prepaid cash service such as Ukash or paysafecard. It would also display the users IP address on the screen and sometimes displayed footage from the victim's webcam to give the illusion that the user was being recorded.[19]-[22]

CryptoLocker

CryptoLocker was an encrypting ransomware that appeared in September 2013. It generated a 2048-bit RAS key pair which was uploaded to a command-and control server which was used to encrypt files. To obtain the key, the user would have to pay a ransom in Bitcoin within three days before the key would be deleted. The extremely large key size made it extremely difficult for analysts to repair. After the deadline, the user could still obtain the key using an online tool but the user would have to pay a much larger ransom which was around $2300 in bitcoin.[27]

CryptoLocker.F and TorrentLocker

CryptoLocker and CryptoWall (different from the original) were Trojan ransomware that spread starting in September 2014. These Trojans spread via fraudulent emails which claimed to be failed parcel delivery notices from Australia Post which allowed them to evade detection by automatic email scanners. They required users to visit a webpage and enter a CAPTCHA code before the software was automatically downloaded. A notable victim of this ransomware was the Australian Broadcasting Corporation whose live programming was disrupted for half an hour.[27]

Distributed denial of attack:

DoS:

A denial of service attack is a type of cyber-attack where an attacker disrupts services of a host. This is usually done by flooding a targeted machine or resource with requests which will overload the system and prevent legitimate requests from being fulfilled. Blocking requests from the source of the attack is usually enough to stop the attack.[25]

DDoS:

In a distributed denial of service attack, the flood of requests comes from a vast network of 'bots' called a 'bot net'. In this case, since there is no single source, but rather the requests are coming from a network of bots, it is effectively impossible to stop the attack. To be classified as a DDoS attack, the attack must involve more than around 3-5 nodes on different networks, fewer would be classified as a DoS attack.

DDoS attacks come in various forms:

Application layer attacks:

In an application layer attack, application layer processes are targeted. The application layer is where common internet requests such as HTTP GET and POST occur. Attacks on the application layer are effective due to their consumption of server resources in addition to network resources. The effectiveness of application layer attacks is attributed to the disparity between the amounts of resources it takes to launch an attack versus the amount of resources the attack is disrupting or hogging on the victims end.[25] This attack takes advantage of the fact that a client making a request to a server takes very little resources compared to the server responding to that request. For example, the resources used when a user makes a request to log into a user account such as a Gmail account is minimal compared to the amount of resources required to respond to that request which involves checking login credentials, loading relevant user data from a database, and sending back a response containing the requested web page. [26]

Advanced persistent DoS:

This form of attack is one where the attack duration can range from days to weeks. It is a persistent attack in that it is of extended duration and often is hard to detect and mitigate. The longest attack of this form noted has lasted 38 days and involved approximately 50,000+ terabits of malicious traffic. In order to evade defensive DDoS countermeasures and to remain undetected, attackers may switch between several targets in order to create a diversion.[25] The characteristics of an APDoS attack are: advanced reconnaissance involving pre attack data collection of the target victim, tactical execution where there are secondary victims making it harder to find the source of the attack, an explicit motivation behind the attack, large computing capacity, simultaneous multi-threaded OSI layer attacks, and persistence over extended periods. [26]

A coordinated attack that overload a server's resources to process and service any request[26] One of the most common ways DDoS operate would be through a Transmission Control Protocol SYN attack, where the hacktivists uses the server's buffer space during a TCP session initialisation handshake. Thereafter it floods the system small in queue with connection requests but does not reply when those requested are being answered. Hence the system will crash or when the queue is full.[13].

Phishing: Phishing is a form of attack that sends emails to users that seemed to be trustworthy at first glance. However, it is used by the hacktivists to redirect the users to download malware unknowingly.[13] Classic examples would be to trick the user to hand over information such as banking credentials.

B. Incident Categories

In [6][7], the authors mentioned that the motives behind every cybersecurity attack can be analysed from 4 main perspectives, mainly information theft, espionage, warfare and sabotage.

Information theft: This occurs when attackers are interested in to acquire data that are stored in the target's network servers. The data could include business critical information, or customers' database. In [7], the author quotes that 25% of all data breaches since 2005 have occurred due to targeted attacks. Banks are one of the most common targets as cyber attackers found ways to extract any forms of monetary transactions [6]. RSA data breach is a classic example of an information theft, where information related to their SecurID technology were stolen. This was done through spear phishing mail, which basically carried malware to infiltrate the network and retrieve the data [7].

Espionage attack: Hacktivists observes and steals highly confidential data that could bring risk to national security. Hacking organisations such as Rocket Kitten are usually the mastermind behind an espionage attack [6][7].

Cyberwarfare: Government agencies could also be behind an attack, Government agencies would infiltrate private businesses for competitive gains or national interest [6].

Sabotage: Sabotage are attacks that are done by hacking organisations in order to get their message across. A sabotage cyber attack would be a DDoS attack.

C. Target Sector

Healthcare: Healthcare sectors includes hospitals, clinics, quarantine centres and healthcare research centres. This sector contains database records of patients' health records.[16]-[17]

Manufacturing: This sector consists of areas such as automotive, electronics, pharmaceutical sectors. These areas are very vulnerable to such attacks as there are financial benefits involved for attackers. [16]-[17]

Financial: Areas such as banks, stock exchange. This sector process many private information of customers and handles large amount of money. Thus, this sector is often targeted by attackers in the past, with 2014 being the year that it had been attacked the most. [16]-[17]

Government agencies: Includes building, emergency services that provides benefits to the public. Any breach in the government cyber security environment could exposed private information of government employees. It could expose military and trade secrets, which could lead to worldwide state issues.[16]-[17]

D. Consequence of attack

Defamment: Cybercrime reduces the confidence that customers have in companies significantly. This can lead to a snowball effect where employees leave the company or investors withdraw their investments.[18]

Information theft: The loss in data information pertaining to the customers. Such information can be login credentials, information of different membership account holders.[18]

Financial loss: A cybersecurity breach could result in huge amount of financial loss. Breaches in contracts, expenses to engage security experts to curb the security breaches could easily amount to millions of dollars[18]

Disruption: Any cyber attack would cause a delay in the usual operations of any organisations.

IV. Case Studies - Notable Examples of Cyber Attacks

WannaCry

Wannacry was a worldwide ransomware attack that occurred in may 2017 which targeted computers running Microsoft windows. It was considered a network worm because it includes a "transport" mechanism to automatically spread itself to other networks. It spread by use of EternalBlue which was an exploit developed by the NSA which was later leaked by the Shadow Brokers hacker group. EternalBlue exploited a vulnerability in Microsoft's implementation of the server message block protocol. The vulnerability exists because the SMB version 1 server in various versions of Microsoft windows mishandles specially crafted packets from remote attackers. This allowed them to execute arbitrary code on the target computer.[19]-[22]

Defensive Response:

WannaCry patch:

Microsoft had released patches to close the EternalBlue exploit before the WannaCry attack even began, however much of WannaCrys spread was from organizations that had not applied the patches or were using older windows systems that were past their end-of-life. Once WannaCry had infected a system that had not previously had the patch applied, there was little that could be done to recover the system.[19]-[22]

Discovery of a killswitch:

A British computer security researcher named Marcus Hutchkins discovered a kill switch that was hardcoded into the Wannacry malware. He discovered that once launched, the malware would try to access a hard-coded URL. It would attempt to access this URL and if could not be accessed, it would proceed to search for files of certain formats and begin to encrypt them. With the discovery of this important "kill-switch" Marcus registered the domain to a DNS sinkhole. With the domain now being registered, the attempt to access[21] would be serviced causing WannaCry to shut itself down. This stopped the spread of WannaCry as worm. The reason for the existence of this "kill switch" in the malware is a topic of debate. Some researchers believe that it was a way for attackers to stop the attack if they for whatever reason wanted to. In this case, the attackers would simply register the hard-coded domain which would cause WannaCry to stop. Marcus Hutchkins believed that it was implemented to make the code harder to analyze. A method that researchers use to analyse malware is to run it in a virtual sandbox environment. In this environment, any URL or IP address that the malware attempts to reach will appear reachable. In this case WannaCry would stop execution in this environment as it would only continue if the hard-coded URL was unreachable. This would make it difficult for researchers to further analyze.[21]

Origin of WannaCry

There are a number of theories on the origin of WannaCry. Symantec, a cyber-security company, reported that the WannaCry attacks had strong links to Lazarus group which is a cybercrime group which possibly have links to North Korea. Lazarus group is noted for their attacks on Sony Pictures, and a theft of $81 million from the Bangladesh Central bank. Symantec came to this conclusion after analyzing a number of attacks that occurred months before the WannaCry attacks. They found that there were substantial commonalities in the tools, techniques and infrastructure used in both these attacks and in other attacks by the Lazarus Group.[22]

Summary of Links to Lazarus Group:

-During the initial WannaCry attacks, three pieces of malware were found on a victims network which are linked to Lazarus attacks: Trojan.Volgmer and two variants of Bacldoor.Destover, which is the same disk-wiping tool used in the Sony Pictures attacks
-Trojan.Apphanc was used to spread the WannaCry malware, which is a modified version of Backdoor.Duuzer, which has been linked to Lazarus
-Trojan.Bravonc used the same IP addresses as did Backdoor.Duuzer and Backdoor.Destover, both of which have been linked to Lazarus
-Backdoor.Bravonc was found to obduscate code similar to WannaCry and Infostealer.Fakepude, which has been linked to Lazarus[22]
-There is shared code between WannaCry and Backdoor.Contopee which has previously been linked to Lazarus

Wannacry was estimated to have affected 200,000 computers across 150 countries with total damages from hundreds of millions to billions of dollars.

GitHub DDoS Attack

On February 28, 2018, the largest known DDoS attack was made on GitHub, the world's leading software development platform. The attack that took GitHub offline for fewer than 10 minutes, hit GitHub with 1.35 terabits of traffic per second all at once. [23]

The attack was a Memcached Major Amplification attack. In Memcached DDoS attacks, attackers are able to spoof the IP address of their victim and send small queries to multiple memcached servers. These queries take a minimal amount of resources to send and elicit a response that requires much more resources. This is aptly named an amplification attack. Memcached server attacks do not require a malware-driven botnet.[24]

Defense Against the Attack

The attack was mitigated using the DDoS mitigation service Akamai Prolexic. Prolexic was able to take over the network traffic as an intermediary, and routed all traffic coming into and out of GitHub. This data was sent through its scrubbing centers which was able to weed out and block malicious packets. Josh Shaul, the vice president of Akamai reported that they modeled their capacity on five times the biggest attack that had ever taken place. This ensured that the 1.3Tbps could be absorbed by their system.[23]

Prolexic had recently implemented specific mitigations for DDoS attacks coming from "Memcached servers". Memcached servers work to speed networks and websites but are not meant to be exposed on the public internet. Because about 100,000 memcached servers are currently on the internet with no authentication protection, attackers are able to access them and send a special command packet that the server will respond to with a much larger reply[23]

Motivation behind the attack:

It is believed that the attack was made because GitHub is a high-profile service which would be impressive to take down. Another possibility is that the attackers hoped to extract a ransom in return for stopping the attack.[23]

V. Conclusion

To conclude, we feel that the various of cyberattacks that the paper has touched on would be here to stay for at least the next decade. Hence, it is crucial to empower the public and businesses with the knowledge of protecting themselves against cybersecurity attacks. Also, it is crucial to build and train the next generation of cyber security engineers. Hacktivists are only always improving their methods of phishing data, hence it is crucial for cybersecurity analyst to innovate and come up with new ways to defend against such attacks. Some of the current new methods would involve quantum cryptography.

Acknowledgment

[1] "What Is Cybersecurity?," *Cisco*, 26-Mar-2019. [Online]. Available: https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

[2] J. Fruhlinger, "What is a cyber attack? Recent examples show disturbing trends," *CSO Online*, 26-Nov-2018. [Online]. Available: https://www.csoonline.com/article/3237324/what-is-a-cyber-attack-recent-examples-show-disturbing-trends.html

[3] "What is a Cyberattack? - Definition from Techopedia," *Techopedia.com*. [Online]. Available: https://www.techopedia.com/definition/24748/cyberattack

[4] "What is cyber security? What you need to know," *Official Site*. [Online]. Available: https://us.norton.com/internetsecurity-malware-what-is-cybersecurity-what-you-need-to-know.html

[5] GoMindsight, "History of Cyber Attacks From The Morris Worm To Exactis," *Mindsight*, 21-Mar-2019. [Online]. Available: https://www.gomindsight.com/blog/history-of-cyber-attacks-2018/

[6] J. Hiner, "The 4 types of cybersecurity threats and a formula to fight them," *TechRepublic*. [Online]. Available: https://www.techrepublic.com/article/the-4-types-of-cybersecurity-threats-and-a-formula-to-fight-them/

[7] "Understanding Targeted Attacks: Goals and Motives," *Security News - Trend Micro USA*. [Online]. Available: https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/understanding-targeted-attacks-goals-and-motives

[8]
https://www.researchgate.net/profile/Nabie_Conteh/publi

cation/294421084_Cybersecurityrisks_vulnerabilities_and_countermeasures_to_prevent_social_engineering_attacks/links/56e2733408aebc9edb19eebc.pdf

[9]https://arxiv.org/pdf/cond-mat/0306002.pdf

[10] https://academic.oup.com/cybersecurity/article/5/1/tyz001/5382610?searchresult=1#132446702

[11] C. Joshi, “A Review on Taxonomies of Attacks and Vulnerability in Computer and Network System,” *Academia.edu*. [Online]. Available: https://www.academia.edu/26280657/A_Review_on_Taxonomies_of_Attacks_and_Vulnerability_in_Computer_and_Network_System

[12] “What is Malware? How Malware Works & How to Remove it,” *AVG*. [Online]. Available: https://www.avg.com/en/signal/what-is-malware

[13] “Top 10 Most Common Types of Cyber Attacks,” *Netwrix Blog Top 10 Most Common Types of Cyber Attacks Comments*. [Online]. Available: https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/#Malware attack/

[19]”What is WannaCry ransomware, how does it infect, and who was responsible?“ https://www.csoonline.com/article/3227906/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html

[20]“The WannaCry ransomware might have a link to North Korea“ https://www.csoonline.com/article/3196897/the-wannacry-ransomware-might-have-a-link-to-north-korea.html

[21]https://www.csoonline.com/article/3196685/a-kill-switch-is-slowing-the-spread-of-wannacry-ransomware.html

[22]*“5 MOST FAMOUS DDOS ATTACKS”* https://www.a10networks.com/resources/articles/5-most-famous-ddos-attacks

[23]“GITHUB SURVIVED THE BIGGEST DDOS ATTACK EVER RECORDED” https://www.wired.com/story/github-ddos-memcached/

[24]“February 28th DDoS Incident Report” https://github.blog/2018-03-01-ddos-incident-report/

[25]“What is a DDoS Attack?“https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/

[26]“What is a DDoS Attack?“https://www.digitalattackmap.com/understanding-ddos/

[27] "Cryptolocker victims to get files back for free". https://www.bbc.co.uk/news/technology-28661463BBC News. 6 August 2014. Retrieved 18 August 2014.

[28]”What is ransomware? How these attacks work and how to recover from them“https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html

[14] “Malware Attacks: What is Malware? Malware Protection Techniques,” *Rapid7*. [Online]. Available: https://www.rapid7.com/fundamentals/malware-attacks/

[15] R. Whitwam, “Ransomware Scammers Get Scammed Themselves By Tor Proxy Hack,” *ExtremeTech*, 31-Jan-2018. [Online]. Available: https://www.extremetech.com/internet/263151-ransomware-scammers-getting-scammed-tor-proxy-hack

[16] “Security Threats by Industry,” *Infosec Resources*. [Online]. Available: https://resources.infosecinstitute.com/category/enterprise/securityawareness/security-threats-by-industry/#gref

[17] S. Morgan, “Top 5 Industries At Risk Of Cyber-Attacks,” *Forbes*, 14-May-2016. [Online]. Available: https://www.forbes.com/sites/stevemorgan/2016/05/13/list-of-the-5-most-cyber-attacked-industries/#aba4075715e9

[18] “The Consequences of a Cyber Security Breach,” *Sungard AS*. [Online]. Available: https://www.sungardas.com/en/about/resources/articles/the-consequences-of-a-cyber-security-breach/