signetique

MANAGED SERVERS EXPERTS

WEB SECURITY THREATS

to Watch For in 2018

ABSTRACT

In the recent world of sophisticated technologies, more threats to cybersecurity have been reported than ever before. As the experts advance in outwitting the criminals, their opponents are still up to the task and have therefore devised more dangerous attack methods. Cyber-attacks form one of the most dangerous nightmares to the system administrators. These hackers compromise the most vital systems stealing critical information, they can as well lock files which are sensitive and may leak information to the outside world.

It has been estimated that it is really hard for companies to recover from such threats especially for the Small to Medium Enterprises (SMEs) this challenge not only affects the SMEs but also the well-established large businesses. For example, Equifax Company was data breached in 2017 and turned out to be one of the most expensive costs in history as it cost the company a whopping cost of $275 million. This is really a large amount of money and if the company does not strategize well, it ends up making losses.

Cyber-attacks have also a huge effect to the customer base. After a cyber-attack, most customers may quit the affected company and this has significant effects on the whole progress of the company. The sales decline, loss of customer base and an overall decline in popularity of a company due to criticism. Therefore, cyber-attacks are the most dangerous threats to the overall well-being of private organizations, public institutions, businesses, and various websites. The web security trends in 2018 and the previous decades will be discussed in detail.

TABLE OF CONTENTS

Abstract	**1**
Web security trend in 2018	**3**
Introduction	**3**
Statistics of cyber attacks in 2018	**3**
Types of cyber attacks in 2018	**5**
Five most common cyber attacks in 2018	**6**
Cloud services infected with ransomware	**6**
Cryptojacking	**7**
Socially engineered malware	**7**
Artificial intelligence weaponization.	**8**
How many Cyber Attacks happened in the past decades?	**9**
Adobe systems (2013)	**10**
Target (2013)	**10**
eBay (2014)	**11**
Sonny (2014)	**11**
Anthem (2015)	**12**
How frequently does Cyber Attack happen?	**12**
How do Cyber Attacks ruin a business or website?	**13**
The TalkTalk case study	**15**
Summary and conclusion	**16**
References	**17**

INTRODUCTION

Web security is one of the major concerns today with most companies, private organizations as well as public institutions investing heavily in cyber security. This is because most of hacks and cyber-attacks have been directed to the major institutions with a view of stealing institutional and personal information from the systems. Cyber-attacks can be defined as those attacks which are socially or politically motivated and are executed through the internet. They are executed through unauthorized web access, the spread of viruses or malicious programs and any other means which is intended at stealing personal or organizational information. These cyber-attacks can be geared towards particular organizations or institutions, individuals or services with an aim of obtaining technical, private, intellectual assets and institutional assets for the purpose of monetary gains or vandalism.

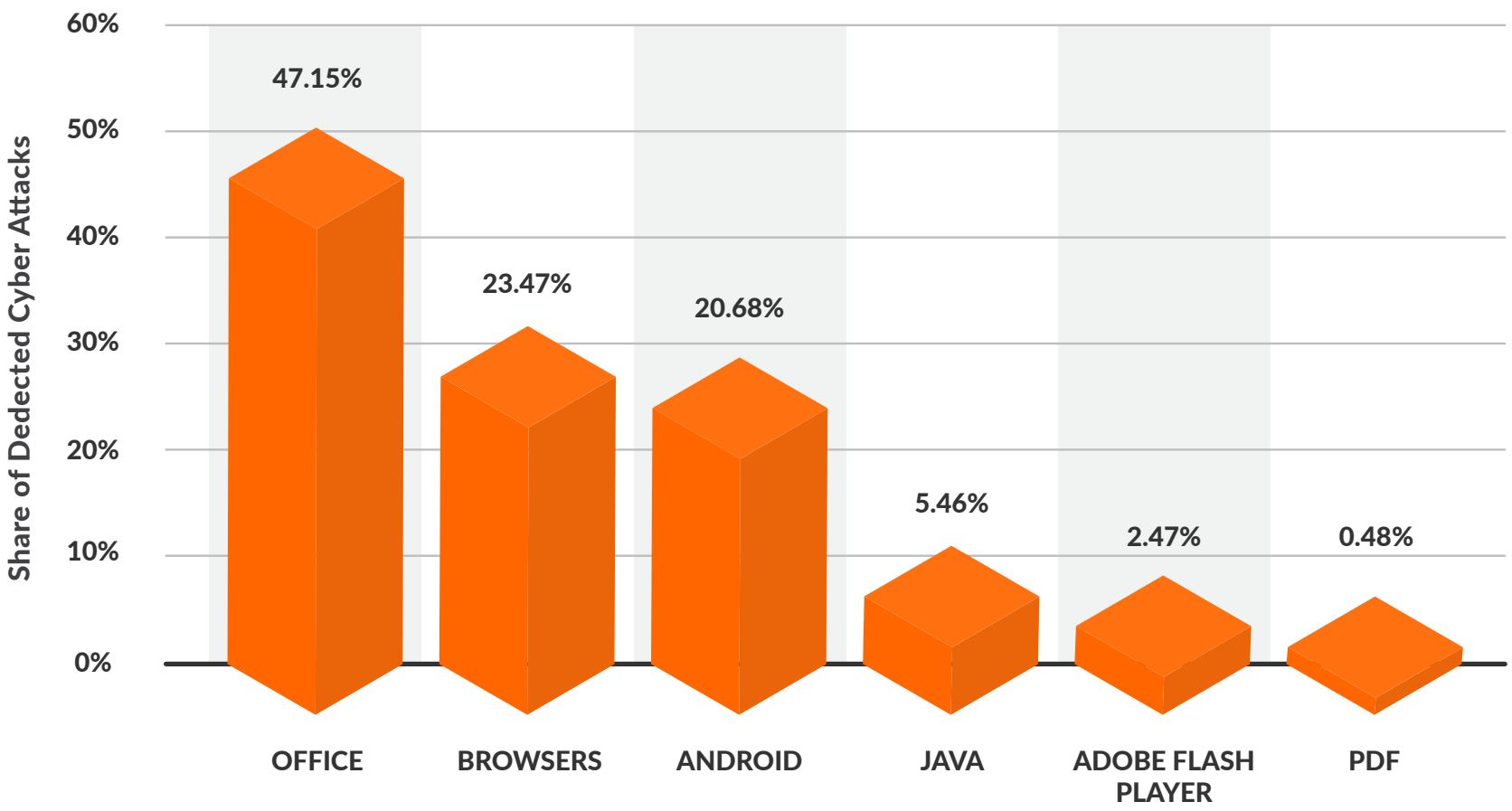
STATISTICS OF CYBER-ATTACKS IN 2018

Cyber-attacks have been happening in every day and its surprising that as experts try to devise different methods of overcoming them, the hackers still outwit them with more sophisticated ways. In 2018, an account belonging to Under Armor 'My Fitness Pal' was hacked. It affected 150million users. According to Symantec, around 24,000 mobile apps are affected by malicious software every day. Attacks involving cryptojacking also increased in 2017 by 8,500 percent, blocked attacks from WannaCry virus rose to 5.4 billion in the same year; according to Symantec. The number of recorded breaches since January 1, 2015, and April 18, 2018, is 8,854 according to Theft resource center. Cybersecurity costs are increasing dramatically every New Year. The costs are crippling especially to those companies who have not considered cybersecurity in their budget. For instance, according to Accenture, cybercrime costs significantly increased whereby most organizations spent approximately 23% more in 2017 as compared to 2016. It has been estimated that the average cost of malware crime is about $2.4 million and the average time cost is about 50days according to Accenture. In terms of percentage, there was an increase in 22.7% from 2016 to 2017 in cybersecurity costs. It is estimated that by the year 2021, the damage associated with cybercrime might shoot up to $6 trillion annually. These high costs have a very significant effect on small to medium enterprises (SMEs). This might be the reason why most SMEs are closed after a malware attack.

Ransom ware attack detections have been very high in countries with a high population connected to the internet. For example, the United States ranks the highest with an 18% reported cases of malware attack according to Symantec. A report by Cisco indicates that in 2017, Trojan horse virus Ramnit accounted for 53% and affected mostly financial records. Also, 60% of all malicious domains were linked to spam campaigns according to Cisco. It is evident that new threats are emerging every new day and for companies with unsecured files, the risk is very high indeed. It has been reported by Varonis that approximately 21% of are never protected. Moreover, around 41% of all companies in the world have sensitive files over 1,000 which include both health records and credit card numbers unprotected (Sobers, 2018).

The chart in the next page shows some of the areas which have been affected by cyberattacks in 2018 so far with offices being the most vulnerable.

MOST COMMONLY EXPLOITED APPLICATIONS WORLDWIDE AS OF 1ST QUARTER 2018



Source: Kapersky lab @ statistic 2018

This chart above shows the percentage of cyberattacks experienced in offices, bowsers, android, java, adobe flash player and PDF in the first quarter of 2018

TYPES OF CYBER-ATTACKS IN 2018

There are several types of cyber-attacks happening today. With the outbreak of malicious programs such as Notpetya, ransomware which targets encrypting of files and then demanding for ransom payment in order to restore them, was one of the most discussed issues of malware attack in 2017. At that time, the rates of malware attach began to shoot up around the middle of the year, by December 2017, it accounted for around 10% of the attacks. In the first few months of 2018, research shows that 90% of attacks executed by remote code were linked with cryptomining.

Malware attacks have been discovered to be delivered by email. According to Verizon's breach report in 2018, email accounted for 92% of all malware attack. Phishing attacks are one of the methods commonly used by email malware attack. According to a survey conducted on 1300 IT security decision makers for CyberArk Global Advanced Threat Landscape report, a large proportion of 56% indicated that phishing attacks were one of the major top security issues they faced. In earlier days, these malware attacks were expressed in the form of .exe files which were attached to those emails where the antivirus programs easily assessed and blocked them before a serious security issue had occurred.

In recent days, another form of malware attack has cropped up. Fileless malware is becoming more notorious since it attacks and exploits the software which is already installed in someone's computer and do not attempt to download the large executables; for instance, this fileless malware may choose to execute as macros for Microsoft office, they may also execute in a browser plug-in or inject the malicious executable codes after exploiting the vulnerabilities found in the server programs. This was the case experienced by the Equifax breach. According to a report, "state of endpoint security risk" by Ponemon Institute in 2017, 77% of all the compromised attacks were fileless.

This attack on the company will largely affect the company's balance sheet and will definitely prompt employee idleness because the computes were dysfunctional coupled with wrecked networks and therefore, there will be no means of doing the work. It is very costly to successfully recover the whole operation. Ponemon estimates that a single attack costs about $5 million. However, a quarter of the total amount, $1.25 is attributed to the system's downtime, another 30% which is about $1.5 is attributed to end-user productivity loss and IT.

It is really hard to halt all the attacks in a company's infrastructure at a go. It is therefore advisable to identify and repair the breaches which have already occurred immediately. In relation to this initiative, things seem to be improving. According to Ponemon's 2017 study on the cost of data breach, it indicated that in 2016, organizations identified data breaches on an average of 201 days but of late, organizations take about 191 days although it seems like a shocking number, there is an indication of a progressive improvement (Fruhling, 2018).

FIVE MOST COMMON CYBER ATTACKS IN 2018

There are five most common types of cyber attacks in 2018. Security experts have continued to fight cyber threats which have compromised both company and individual data. However, as much as they struggle to shut down one threat, another one emerges. Hackers and all other related web security criminals seem to have improved their tactics in order to outdo the experts. It is therefore helpful to engage in educating the users on potential attacks that they may face. The most common cyber attacks in 2018 have been discussed below.

Cloud services infected with ransomware

Cloud-soft infected with ransomware is one of the major cyber attacks in 2018. It seems like criminals have realized a goldmine of data and they can, therefore, hold for a ransom on cloud services. Users have assumed a higher level of security and hence let their guard down, therefore, thieves easily succeed in attacking cloud services by attaching their attacks. It has been realized that in 2016. The criminals launched their attack on cloud services by using Dropbox to spread Petya, one of the favorite strains of ransomware.

Without prior knowledge, users clicked on the resume stored on a Dropbox and unfortunately, the virus began to install. When their machines locked up, they realized that something was wrong. However, it was too late because the hard drives were already overwritten and the data in them destroyed. Although cloud services may still be there, it is more advantageous to have a data backup which can be stored locally or can be in an offsite location.

Cryptojacking

Cryptojacking is another cyber attack which has affected various websites. For instance, criminals realized that Tesla was not password protected and attacked and took control over it. Later on, an expert realized that the console was being used by the criminals to crypto mine AWS. Cryptojacking became popular in the period when the prices of Ethereum, Bitcoin and other related crypto-currencies rose to the stratosphere. Since those days have subsided, it is now hard to predict when the prices might rise again. As at today, Bitcoin is trading at $6000 from $19000 in last December. This sudden rise in prices gives the thieves a chance to steal the computing time. There is a possibility that cryptojacking may fade in and lose its popularity in the next years. However, this might not be the case because much money will be made and it's a low-risk venture for the criminals since in most cases the crime usually goes unnoticed.

Socially engineered malware

This is a type of cyber attack malware which happens when a user is lured towards opening a file or website or install a software from a trustworthy sender. This attack is executed in different forms. Most people know that it is not advisable to click attachments from unknown people. However, these criminals are so much sophisticated such that they know people are more likely to click or open a file from people they know. Other attacks have also been used. Websites have been used which inject a code to the browser. This code is then used to collect private data from the victims without being noticed. This attack is responsible for the successful hundreds of millions of hacks each year. Companies have tried to overcome this type of attack by encouraging users to browse using accounts which do not have higher levels of elevated security clearance. An example of these companies is Microsoft. In order to prevent or reduce the occurrence of this malware attacks, one should install prevention programs and also educate their users in order to recognize these attacks before they are attacked.

Social media threats

Most people today spend much of their time on social media such as Twitter, LinkedIn and Facebook managing their business connections and end up overlooking threats related to these services. The attacks associated with these social media platforms are very much disturbing because the normally take advantage of the bonds we have with our colleagues.

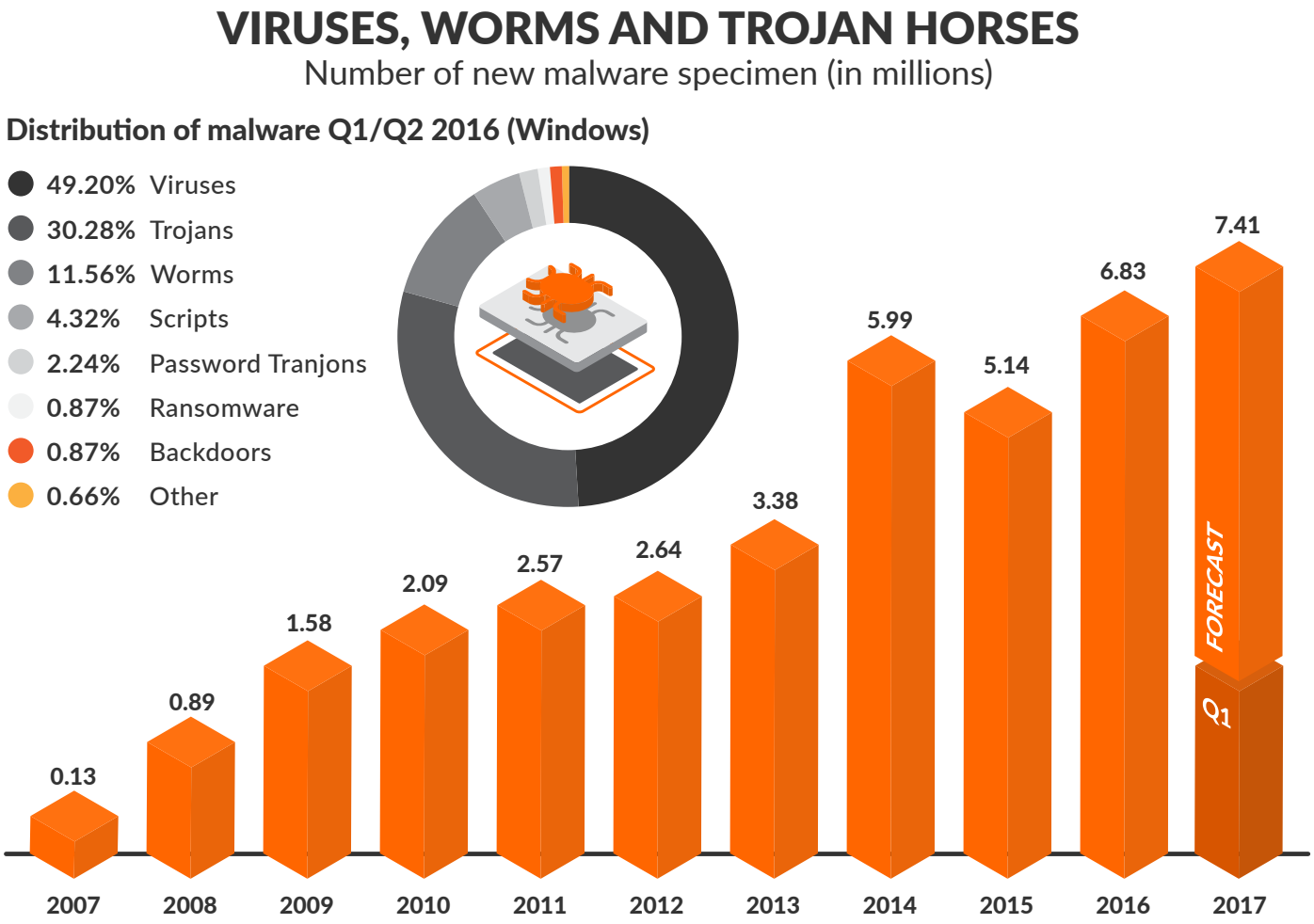
These attacks may be launched in different forms. A friend request may be sent to a person which includes a link to more information. Before you view the profile, you may be asked to install a program. Although everything may seem fine at this stage, you have actually given more information than you intended. In most cases, few of these cases may be reported by the media unless the case is more embarrassing. For instance, in last year, HBO's social media accounts were taken over including their most popular Twitter account for the game of thrones. These attacks are normally used to confuse and embarrass many companies and it takes a long time to recover the hacked accounts.

Artificial intelligence weaponization.

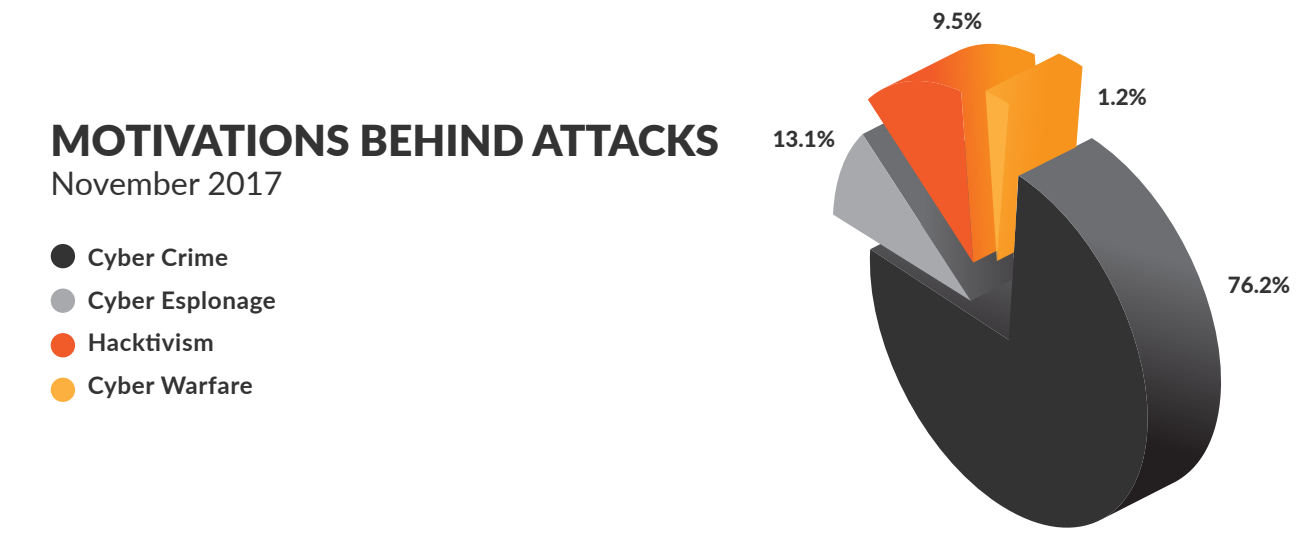
In the recent world, companies have engaged in the use of artificial intelligence, neural networks, and machine learning to predict the occurrence of cyber attacks. Amazon and Microsoft have used these techniques to predict when and where these attacks may be used. Visa and Mastercard have also used these techniques to intervene when they realize there is something out of ordinary going on. Criminals have also moved a step ahead in trying to cope with this advance in technology. They also use the same technology being used by these company to trick the users, for example, they can customize and send messages using machine learning to users which you are more likely to open. They achieve this by scanning any information about the target person from the social media, company websites and any other platform where your information is available. These attacks have been successful because each message can be easily tailored to the recipient. However, these attacks have been counteracted by the experts through the creation of tools which can recognize these attacks and "sandbox" them. These attacks may not be completely thwarted as some attack the emails and are more convincing such that they enter into the boxes of employees after successfully making it past the filters (Nordquist, 2018).

HOW MANY CYBER ATTACKS HAPPENED IN THE PAST DECADES?

Several cyberattacks have happened in the past decades. The discussed cyberattack below are the most famous ones which experienced major losses.



This bar chart represents the number of new malware attacks in millions from the year 2007 to 2017. The pie chart represents the various distribution of malware attacks Q1/Q2 in 2016



This pie chart shows the percentage of the various cyberattacks as at November 2017. It covers cybercrime, hacktivism, cyber warfare and cyber Espionage.

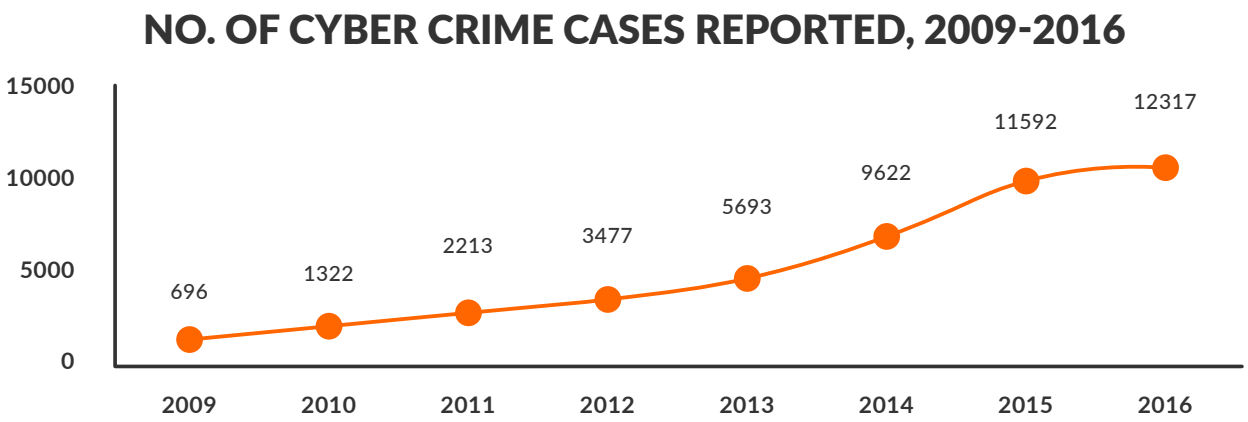
signetique
MANAGED SERVERS EXPERTS

Adobe systems (2013)

This is a software company most popular for the design of its products. The company announced a breach of a network in October whereby the hackers made away with the passwords and IDs of a larger number of its customers. This stolen information was found later on the dark web for sale. Moreover, the criminals also stole the source code which allowed them to scrutinize the Adobe software's confidential workings. Adobe provided an update on the number of accounts which were hacked. Although it claimed that only 2.9million were hacked, more details developed which indicated that around 38million accounts were interfered with. Consequently, Adobe was criticized more severely on how it secured its data from the hackers. It was easier for the hackers to guess the passwords correctly since the encrypted passwords looked more identical to the customer passwords. This instance, therefore, highlighted the need to provide double data encryption for better security.

Target (2013)

The retail chain Target became a victim of a major attack during the 2013 holiday. During this attack, the hack was not detected for a couple of weeks and this allowed the criminals to steal large amounts of credit card data. After this incidence, Target initially announced that the hackers stole credit and debit card numbers worth 40million. However, further investigation revealed that customer contact information was also stolen. The whole incidence is approximated to have affected 110million people. This tragedy affected the company's foot traffic in stores since they consequently slowed considerably. The immediate profits declined by 46% and ultimately, Target had to settle for a lawsuit brought by the shoppers which were estimated to be on the tune of $10 million. The hackers installed malicious software on the company's point of sale (POS) devices. However how they managed this remains a mystery up to date. For the short time, they managed to capture the card information from the POS memory. This incidence brought about the key importance of being informed of the current new methods of cyber attacks and hence the need to protect the computers accordingly.



signetique
MANAGED SERVERS EXPERTS

eBay (2014)

eBay is an online auction website. In May 2014, the company revealed to the public that the entire customer base private information was compromised. The hackers are said to have exposed the physical and email addresses, names, encrypted passwords and birthdays for the customers. It is overwhelming that the hackers accessed the system for 229days. This translated to a very enormous breach and affected 145million users although it is surprising that the company's profits were not affected, however, user activity on the website declined. This breach is said to have been facilitated by the fact that the hackers obtained the credentials of the employees. This occurrence served as a lesson to other companies on the importance of educating employees on the basic safety of a computer, for instance, not opening their emails from unknown addresses.

Sonny (2014)

This is a company which is associated with television, film and digital contents and was hacked in November 2014 by a group known as the "Guardians of peace" which was linked to North Korea. The attack is said to have been initiated as a response to the release of the film 'the interview' which was a comedy about the assassination of Kim Jong Un, a North Korean dictator. This group stole large amounts of data estimated to be about 100 terabytes which included passport information, contracts, films and film budgets, social security numbers, salary lists, and emails. This breach emptied many of the data centers containing the information.

This stolen information was also uploaded online for people to view. Thus, the hack prompted the cancellation of theatrical release for 'the interview'. This attack was attributed to a number of weaknesses. For example, Sony Pictures headquarters are said to have lacked basic protection on its campus and digitally. It was discovered that the administrative computers were logged in and remained unattended, guests walked anyhow without escort and also the computer systems did not have imported credentials such as encrypted data. This attack demonstrated the importance of staying attentive and vigilant to the world of evolving computer technologies.

Anthem (2015)

This is one of the largest insurance companies on health in the United States. This company was hacked in February 2015 and the attack was termed as one of the biggest breaches of data in the healthcare history. The information which was stolen were social security numbers, addresses, emails, names and employment information for both company employees and customers. This breach interfered with a huge number of records of up to 78.8 million records. Although the cost is still unknown, it is estimated to be beyond $100million. This attack was executed through spear phishing the administrative accounts. This attack, therefore, indicated the importance of ensuring limited data access even for the top officials in a company (Bernstein, 2017).

HOW FREQUENTLY DOES CYBER ATTACK HAPPEN?

Hackers attack after every 39 seconds. This is according to a research done by Clark School study at the University of Maryland. They quantified that on average, hackers attack the computers on average of 39seconds with the most vulnerable non-secure passwords and usernames which present a better chance of success to the attackers. This study was conducted by Michel Cukier and considered the behavior of hackers who attack computers using software-aided techniques. In the research, it was discovered which passwords and usernames are tried in most cases and what the hackers do once they gain access to the computer.

In Televisions and films, the hackers have been described as people who target specific institutions and try manually to break into the computers. On the study, Cukier claimed that the attacks happen all the time the computers are connected to the internet. On average, the computers may be attacked 2,244 times in a single day. On an experiment contacted on four computers with his fellow graduates, they set up weak security on the computers with internet access and observed on what happened when the computers were being attached.

They discovered that most attacks are from unsophisticated hackers who use ‘dictionary scripts’ which is a software that runs through passwords and usernames while trying to enter into a computer. The researchers also found that most guessing ploy used in passwords was trying to reenter username. In this research, 43% of guessing usernames reentered the username.

Once the hackers gain access to the computer, they act quickly to determine whether the computer could be of use to them. As the study reveals, the hackers have a common sequence of actions in which they operate. They normally check on the software of the computer accessed, the hardware, software configuration, change the password, download files, install a program and run it. Once the hackers achieve this, they set up undetected entrances into the computers they control commonly referred to as backdoors so that they can access and compromise as many programs as possible (Security magazine, 2017).

HOW DO CYBER ATTACKS RUIN A BUSINESS OR WEBSITE?

When a cyber attack successfully attacks a business, it causes severe damages. It affects the bottom line of the business, the business standing and the customers' trust. The impacts can be divided into financial, reputational and legal. In terms of finance, cyberattacks lead to substantial losses in finances which occur as a result of the loss of corporate information, theft of money, loss of financial information, disruption of trading for example to the companies which carry out online transactions and loss of contracts. Huge costs are also associated with the repairing o damages caused by the cyberattacks.

Most of the small businesses usually collapse as a result of an inability to finance the recovery. Reputational damage is another problem associated with the attack of businesses by cyber attacks. Trust is a very important element in business operations when relating with customers. This attacks can severely damage the business reputation as well as eroding the already built trust with your customers. This will consequently lead to customer loss, sales loss and overall profit reduction.

The last consequence is the legal effects of a cyber breach. It is required by the privacy and data protection laws that you regulate the security of any personal data held whether on customers or on your staff. If this data is compromised and the company responsible fails to employ the appropriate measures, one may face regulatory sanctions or being sued. However, there are methods of reducing cyber attacks. A security response plan can help one; reduce the impacts associated with the attack, one can also report the crime to the relevant authorities, clean all the infected systems and also, try to get the business up again and running in the shortest time possible (Nibusiness info.co.uk, 2018).

THE TALKTALK CASE STUDY

TalkTalk cybersecurity breach which occurred on October 22, is among the most common incidents which affected the company's reputation severely. In the manner in which it was executed has led to many commentators believing that breaching of data is inevitable. John Stewart CSO of Cisco argues that due to the many incidences of data breaching, it longer a unique experience. He believes that conversations related to data breaching are irrelevant as one will be definitely hit by these cyber attacks.

The Alva report analyzed the issues related to data breaching and covered 12-months data for Talk-Talk, Sony, Barclays and RSA, and Carphone Warehouse. Different hypotheses have been concluded on the impact of data breaches to the TalkTalk. Data breaches resulted in a significant decline in the TalkTalk's sediment score. Data breaches also produced a tenacious negativity in the lifecycle of Talk-Talk. This was realized as the company's sediment trend did not go back to its pre-breach starting point. Therefore, there was a big risk presented in the data for TalkTalk which indicated a great swing in the scores which are the main indicators of the shift in stakeholder and company relationship.

For the consumers, it was clearly visible due to the increase in criticism of the organization and also proactive discussions of provider switching. Nevertheless, social media score also plummeted after the occurrence of the incidence and was clearly expressed online by the switching behavior which suggested new business concerns and future retention. In regard to the investors, there was a drop in the company's share price which was a clear indication of the shift of the customer base and concern of the company's ability to prevent a future occurrence of the same attack (Alva group, 2015).

SUMMARY AND CONCLUSION

In summary, cyber attacks are more dangerous in the progress of a company. The costs associated with the recovery from these attacks are so huge such that most companies consider quitting. Malware is the most notorious form of cyberattack especially in populations with a good connection to the internet network. Once they attack and compromise the system, they can cause severe damage to the victims. Their recovery cost is very much expensive and therefore, there is a need to provide security measures in order to reduce the vulnerability to cyber attacks. This can be done through the installation of a firewall, SSL certification, and scanning. Firewall is a system designed to prevent unauthorized access from unknown sources or a private network. This firewalls can be implemented through a hardware or a software form or combining both of them. This will help prevent unauthorized users from accessing company data when connected to the internet, for example, intranets.

SSL certificates can also be used to help in security checks. They are small data files which digitally bind a cryptographic key to an organization's details. These SSL certificates can be installed on a web server. They help to activate the https protocol and padlock thus securing connections between the web server and a browser. Scanning for cyber attacks can also be achieved through installation of antiviruses. These are software that can secure a computer from virus or unknown networks. Some antiviruses instantly shut down the computer in case a threat occurs or notify the user when the need arises. Companies and organizations should constantly scan their devices in order to ensure security is maintained.

In conclusion, cyber attacks are increasing every new day and their severity and complexity cannot be questioned. Both the SMEs and large business should be aware of the threats posed by these criminals and hence they should seek to reduce their vulnerability. Based on the most recent studies, the attackers never attack as lone wolves but in groups. These groups use sophisticated methods and therefore, it requires a high level of cybersecurity in order to stay a bit a level ahead of the criminals.

Since most of the organizations are state-affiliated, this presents a very high risk to the customers as the hackers can gain access to their personal details. For example, it is expected that the attacks against pharmaceuticals and healthcare records may increase. This is because these records contain detailed personal information and the hackers may steal this information to commit fraud. Therefore, prevention is better than cure. Both the private sector and the public sector should invest in cybersecurity before they severely affected by these witty criminals.

REFERENCES

Alva group. (2015, october 31). *The reputational risk of cybersecurity attacks: TalkTalk case study | alva.* Retrieved from Alva: know where you stand: http://www.alva-group.com/en/the-reputational-risk-of-cyber-attacks-talktalk-case-study/

Bernstein, R. (2017, July 31). *5 Famous Cyberattacks in the Last 5 Years | PPU online.* Retrieved from Information technology: https://online.pointpark.edu/information-technology/famous-cyberattacks/

fruhlinger, J. (2018, October 10). *Top cybersecurity facts, figures and statistics for 2018 | CSO Online.* Retrieved from Cyber security business report: https://www.csoonline.com/article/3153707/security/top-cybersecurity-facts-figures-and-statistics.html

Nibusiness info.co.uk. (2018, Novermber 9). *Impact of cyber attack on your business | nibusinessinfo.co.uk.* Retrieved from Nibusiness info.co.uk: https://www.nibusinessinfo.co.uk/content/impact-cyber-attack-your-business

Nordquist, B. (2018, September 27). *The 5 Most Common Types of Cyberattacks in 2018.* Retrieved from Storage craft recovery zone: https://blog.storagecraft.com/common-types-cyberattacks-2018/

Security magazine. (2017, February 10). *Hackers Attack Every 39 Seconds | 2017-02-10 | Security Magazine.* Retrieved from Security:solutions for enabling and assuring business: https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds

Sobers, R. (2018, may 18). *60 Must-Know Cybersecurity Statistics for 2018.* Retrieved from Varons: https://www.varonis.com/blog/cybersecurity-statistics/