International Journal of Safety and Security Engineering
Vol. 10, No. 6, December, 2020, pp. 739-746
Journal homepage: http://iieta.org/journals/ijsse

Network Security and Its Implications on Program Management

Bongs Lainjo

Cybermatic International, Montreal QC H2Y 1T6, Canada

Corresponding Author Email: bsuiru@icloud.com

https://doi.org/10.18280/ijsse.100603

Received: 24 September 2020
Accepted: 10 December 2020

Keywords:
electronic hacking, cybercrime, healthcare and medical institutions, cloud computing, analytics

ABSTRACT

The Internet and related technologies have enabled companies to automate almost all of their operations resulting in enhanced efficiencies and cost-effectiveness. The technologies, however, have also introduced numerous security risks. Through security risks such as Electronic Hacking (EH), individuals and companies have lost a lot of valuable data and money. In this regard, there is a need to understand the extent of the threat of EH. A comprehensive thematic review and analysis of EH with a focus on developments, evolution, challenges, prognosis, and prevalence in select institutions was thus conducted. The research involved reviewing the literature on cybersecurity and its effect on organizations' operations. The result shows that cases of security breaches and associated costs continue to increase. Over five years, the healthcare and medical institutions were the most vulnerable. They were closely followed by corporations. The implications are that as institutions become more automated, their respective degrees of cybercrime vulnerability increase. The consequences of security breaches are normally dire for companies, as well as individuals. Millions, or possibly billions, of dollars worth of data, have been lost as a result of security breaches. This trend is expected to continue in the future, as computers and Internet technologies continue to advance. Through cybercrimes, numerous companies' operations have been sabotaged, and personal information from social media and email stolen. Long term, effective and sustainable strategies are therefore required. The paper is significant because it identifies the information security risks various organizations are exposed to and strategies that organizations can use to mitigate the risks.

1. INTRODUCTION

Cybersecurity is a major issue of concern in the current business and other user environments. Organizations in high-income countries such as the US have incurred significant losses as a result of cybercrimes. The common ways of executing cybercrime include hacking, malware, and distributed denial of service attacks. Sophisticated hacking tools and malware are readily available on the internet. It is thus easier for criminals to compromise the security of user networks. Despite enabling efficient and cost-effective communication, the internet has brought many security challenges including sabotage and theft [1]. Additionally, new forms of cybercrimes are emerging to exploit vulnerabilities in new technologies such as cloud computing and mobile computing.

Digitization or electronic transition is driven by convenience. It guarantees universal access to services by users regardless of their geographical location. Computerization facilitates competitiveness and the management of large amounts of data. It also improves productivity by ensuring that the execution of routine processes is optimized. Computerization can also expose an organization to numerous security risks such as the denial of service attacks, loss of intellectual property, legal liabilities, damage to reputation, and financial losses.

Since information systems are vital in the current business environment, an organization needs to formulate adequate strategies that can mitigate the identified risks. This will ensure those information systems are used in ways that add value and protect the confidentiality, integrity, and authenticity of information resources. The purpose is to analyze common information security threats in organizations including how they are executed, consequences and measures that can be taken to minimize the threats. Since information systems have become vital in many organizations, it is important to identify the security risks associated with the systems so that necessary measures can be taken to mitigate the risks. The paper thus contributes to the cybersecurity literature by identify common information security threats and effective strategies that can be implemented to reduce exposure to the risks.

2. METHODOLOGY

A comprehensive thematic review and analysis methodology is used in this paper. Thematic review involves organizing literature around topics or issues instead of progression of time. The approach was selected because it allows the researcher to critically examine the available reports and documents regarding cybersecurity. Literature on different topics such as the cyber threat landscape in the United States, costs associated with security breaches, and common tools used by cybercriminals were analyzed.

3. METHODS OF EXECUTING CYBERCRIME

Applegate [2] notes that currently there are three main ways in which cybercrime may be executed; through hacking, through malware, and through "distributed denial of service attacks." According to Morris [3], hacking gaining unauthorized access to private information. Cashell et al. [4] argue that not all hackers are criminals. Some of them are law-abiding people who gain access to systems to test their vulnerability. The ethical hackers are employed by organizations to help them in identifying security holes that can be exploited by criminals [5].

3.1 Hacking incidents

Several companies have suffered as a result of electronic hacking. For example, according to Walters [6], in 2014 South Korea alone reported that more than 140 million accounts stemming from retailers, gas stations, and e-commerce websites were compromised [6]. In the United States (US), according to Allen [7], in December 2013, Target (a departmental store based in Minneapolis) reported that information from more than 110 million credit and debit card payments by its customers were accessed illegally. The hackers stole personal identification numbers (PINs) from the cards, and as a result, Target lost more than $3.5 billion [8]. Hutchings [9] cited that Neiman Marcus (a Dallas based retail store) also reported that the information from 1.1 million credit and debit card payments was hacked in 2013. In 2008, data in more than 130 million credit and debit cards belonging to Heartland Payment Systems (a US-based payment processing and technology service provider) customers were breached by electronic hackers [10].

3.2 Reasons for hacking

According to Snail [11], criminal hackers do not hack systems for pleasure, fun, or sport. They search the Internet for vulnerable systems to steal information they deem they can benefit from financially. Such types of information may include Social Security numbers; insurance identification numbers; passport numbers; bank credit and debit card numbers; usernames, personal identification number (PINs), and passwords; driver's license numbers; utility bill account numbers; student and employee identification numbers [12]. McGuire & Dowling [13] noted that hackers tend to use this information to commit fraud. They may use credit and debit card numbers to make purchases or sell the information to third parties. Moore [14] observed that a single credit card number might be sold for ten dollars ($10). Moore [14] further notes that elite cards with no limit may be sold for hundreds of dollars. This means that a hacker who successfully accesses such information from a big company and steals thousands or even millions of such information may make huge sums of money.

3.3 Implications of cybercrime on Program Operation Management

The aim of every company, regardless of it being non-profit oriented, profit-oriented, government-owned, or privately owned, is to ensure that its operations such as supply chain, contracts, production processes, and management are running smoothly. Any interference to such operations may have dire consequences. With computerizations and the advent of the Internet, management of such operations has not only become easy but efficient. However, the adoption of computers and the Internet in the program operation management has also exposed companies to electronic hacking.

Iovan, S. and Iovan, A.A [15] reported that in 2014, several supply chains of companies located in the US and Europe were attacked by cybercriminals. Since these hackers were unable to attack the main companies directly, they targeted their contractors who were located in Japan, China, and South Korea [15]. One such group of attackers was known as "Icefog." According to Iovan, S. and Iovan, A.A [15], these attackers were so focused, that after getting the information they wanted from the supply chain agent, they would disappear within a very short period. The hackers used specialized electronic hacking programs to track online banking operations and either sabotage the system or steal money from the banks - or even both. Hackers are also capable of compromising company websites and redirect visitors to other sites to damage the company's reputation or interfere with its supply chain [15].

3.4 Prognosis of hacking

It is certain that as the internet and personal computer technologies become more sophisticated, new forms of electronic hacking will emerge to exploit the vulnerabilities and opportunities that these new technologies will offer [16]. This means that in the future, hacking will be high tech and even harder to combat. For example, as the automobile and aviation industries continue to take advantage of computer technology to develop technologically advanced cars and airplanes, new threats that target these technologies are coming up. An example of this would be the case in which two professional hackers gained access to the Toyota Prius' computer system and were able to accelerate the car, stop the car, and jam its steering wheel. They were able to do all these activities remotely [7].

Even though the advent of the Internet and computers has come with a lot of advantages, such as improved efficiency and automation, they also come with serious threats of electronic hacking. Both companies and individuals are vulnerable concerning their personal information in cyberspace. Electronic hackers have sabotaged operations in many companies, including stealing people's personal information from social media, and email. Companies have also lost billions of dollars as a result of electronic hacking. The future still does not look good in terms of these types of threats because as technologies in the Internet and computer become more sophisticated, new forms of electronic hacking techniques emerge to exploit the vulnerabilities and opportunities offered by the new technologies.

3.5 Malware

These are software downloaded and installed into the target's computer or computer network system [17]. The software may launch itself by exploiting the vulnerabilities in the target's computer operating system or compel the owner to install it by enticing them with some kind of false information. After successful installation, the malware can then do anything on the host computer or network, from stealing sensitive information or data to encrypting the data and demanding a ransom. A ransom is usually demanded the victim to be able

to regain access to the encrypted data [18]. A good example of software that can download and launch itself into the victim's computer is Trojan. This malware is capable of tracking victims' operations such as online banking activities, shopping activities, etc., to steal information or sabotage systems. Another example of this malware is ransomware. As explained earlier, this malware encrypts victims' data and demands ransom in exchange for re-access.

Many types of malware exist, including spyware, crimeware, computer virus, scareware, and adware. To spread this malware, hackers may create malicious websites and lure victims to them. They may also exploit vulnerabilities in software applications used on a website or the vulnerability of a web server.

3.6 Phishing

Phishing involves sending potential victims fake emails that appear to have come from reputable and legitimate companies, such as a person's credit union or bank [19]. These fake emails have a Uniform Resource Locator (URL) that redirects the victim to a malicious web page where they will be asked to enter private information such as credit card numbers, bank account information, passwords, etc. [19]. The hackers may then use this information to commit fraud. The phishing sites are normally hosted on legitimate websites, which have been attacked as a result of poor internet security [20].

There are different types of phishing, including clone phishing, spear phishing, and whale phishing. Whale phishing normally targets high-profile business people, such as executives [19]. Spear phishing is aimed at specific departments or people. It collects personal information about its victims [19]. Clone phishing, on the other hand, duplicates a legitimate email that someone has sent and resends it [19]. However, it replaces the original email attachments or links with malicious ones.

3.7 SQL injection

Structured Query Language (SQL) injection is a code that takes advantage of security vulnerabilities that exist in the database of a software application [21]. Generally, it targets software and applications that require user input information, such as a username and password, to access the system or database. This method has been used to gain access to several financial institution systems, global payment processor systems, and retail enterprise systems. Applications such as ModSecurity may help prevent these types of attacks [22].

3.8 Denial of service

A denial of service (DoS) attack works differently compared to how other cyberattack techniques work. While other types of electronic hacking are looking for ways of gaining access into the victim's website, network, database, or computer, the denial of service technique allows hackers to sabotage a computer network system, or a computer itself, without actually gaining internal access [23]. The attackers overload the system's routers with large quantities of fake traffic until they fail. It is usually very difficult to prevent these types of attacks. An attempt at reducing the consequences of such attacks employs services or software that can differentiate between malicious traffic and legitimate traffic.

3.9 The threat of electronic hacking

Many individuals and organizations have become either vulnerable to, or the victims of cybercrime. According to Iovan, S. and Iovan, A.A [15], a big proportion of organizations throughout the world have experienced some form of electronic hacking. Of the companies that have experienced these cybercrimes, a good proportion of them has either lost important data or money. These attacks are often carefully planned to successfully access the network infrastructure of a target company. The current ubiquity of electronic hacking is a result of the widespread use of digital technologies businesses use to enhance operations. This has also made it relatively easy for cyber-espionage malware to steal company data.

It is important to note that cybercrime (through computer fraud) is not necessarily carried out online. Some of these computer frauds may also be carried out offline [22]. However, an online platform provides a perfect environment for a wide variety of cybercrime: stealing of debit and credit card information, identity fraud, phishing, advance fee fraud, internet auction fraud, etc. [15]. These types of cybercrime may be conducted via several media, such as social networking sites, emails, online shopping sites, company websites, etc. This means that companies whose operations have gone digital (online) are highly vulnerable to electronic hacking. Company operations that may be carried out online may include submission of tender and contract documents, supply information, monitoring of employee performance, monitoring of the manufacturing or production process, carrying out online payments, conducting job interviews and employee selections, etc. [17]. Once these operations are online, a company becomes vulnerable to electronic hacking since the information tied to these activities can then be accessed [13]. Therefore, proper actions should be taken to prevent illegal access to the company's network infrastructure. Any successful access to the company's system may have both legal and financial consequences.

4. CURRENT DYNAMICS IN CYBERCRIME

Cyberattacks have become a reality since the advent of the Internet and computer technologies. In an attempt to deal with this threat posed to companies and individuals, computer and Internet technologies have become highly sophisticated. However, this sophistication also helps to create highly sophisticated cyber threats, as hackers also upgrade their systems to exploit vulnerabilities in these new systems. Therefore, it is harder to fight electronic hackers today compared to many years back. For example, it is estimated that in 2017 alone, electronic hackers caused more than $5 billion in damages in the US [24]. This is a more than 15 times increase in damages compared to the two years previous to that. The estimates for losses that resulted from cybercrime are shown in Figure 3. At this rate, it is estimated that within the next three years, spending on cybersecurity could exceed $1 trillion [24]. It is also estimated that, given current trends, by the year 2022, damages inflicted by cyberattacks could exceed $6 trillion per year [24]. This is because even more complicated and sophisticated threats will emerge in the future.

Recently, a new crop of cyber threats has emerged. These attacks, which are harder to fight and highly sophisticated,

include Wanacry, Ethereum attack, NotPetya, Yahoo (revised), and Equifax attack.

4.1 Wanacry

This was a ransomware cyberattack that occurred and spread around May 2017 [25]. It infected the victims' computers and encrypted the contents in their hard drives. It then demanded payments in Bitcoin to decrypt the files [25]. One of the biggest victims of Wanacry was NHS (National Health Service), the national healthcare system in the United Kingdom [25]. The malware (Wanacry), infected computers at NHS facilities by taking advantage of a weakness in Microsoft Windows using an algorithm that was developed by the United States National Security Agency (NSA) [25]. This code was developed secretly and without the knowledge of Microsoft. The code (algorithm), called "EternalBlue," was stolen from the United States National Security Agency's systems by a group of hackers who call themselves "Shadow Brokers" [25]. This is just one glimpse of what modern-day cybercrime is capable of.

4.2 NotPetya

Another recent cyberattack was NotPetya. This is also another form of ransomware, which started spreading in 2016 as phishing spam [24]. It encrypted "master boot record" (files in a computer operating system responsible for booting up the computer) of the victims' computers, making it difficult to gain computer access. In 2017, a more dangerous and sophisticated version of the malware popped up and started spreading quickly, causing close to $850 in damages [24]. This version also spread via EternalBlue, just like the Wanacry attack.

4.3 Ethereum attack

This attack occurred in 2017, and huge amounts of money were stolen by an unknown hacker in the form of Ether, a cryptocurrency similar to Bitcoin [26]. The hacker took advantage of a weakness that existed within the "Parity multi-signature wallet" on Ethereum (the cryptocurrency's platform) [25]. The attacker first stole $7.4 million from the platform [25]. Two weeks later, the system was hacked again, and the hacker managed to steal more than $31 million within a few minutes before they were stopped [25]. Given they had more time, it is estimated that more than $180 million could have been stolen [25]. Since the stolen money could not be recovered, and the system could not be protected, a group of computer security specialists drained all the funds before the attackers could do any more damage. The estimate for the total amount of money that has been lost by cybercrime victims in the last four years as a result of electronic hacking is shown in Table A.

4.4 Equifax attack

In 2017, Equifax, a credit rating agency, reported that cybercriminals exploited the vulnerability of their US website and accessed several files. These files contained personal information of close to 150 million people [27]. The scale of this single attack is proof of just how successful modern hackers can be [27].

4.5 Yahoo attack

Technology giants like Yahoo are not spared when it comes to these high-tech criminals. Although Yahoo systems were hacked in 2013, the potential severity of this type of attack was not realized until 2017, when more than 3 billion Yahoo email addresses were hacked [28]. The hackers stole backup email addresses, encrypted data (data encrypted through outdated techniques), and passwords [29]. This attack proved the secrecy of anything stored online can never be guaranteed.

5. EVOLUTION OF CYBERCRIME

It is understood that cyber-related crimes were committed even before the arrival of the Internet [30]. The internet, computers and related technologies were invented mainly to create, store, and distribute information. That information may be personal, corporate information or government information. The desire to access this information for personal gain has bred cybercrime.

Generally, the evolution and history of cybercrime coincide with the evolution of the World Wide Web (the Internet). Initially, cybercrimes didn't even require the Internet to be executed [30]. They involved stealing information from a local computer network. With the invention and advancements of Internet technology, cybercrime also became advanced. While cybercrime has been in existence for a long time, major cybercrimes started to occur in the 1980s, with the invention and spread of the use of emails [30]. In these early hackings, the hacker would create malware or/and scams and send them to the victim's mailbox. A good example of this kind of scam was "Nigerian Prince," where an email was sent to someone's mailbox by someone pretending to be a prince from Nigerian [30]. The email purported that the prince wanted to send millions of dollars out of their country but could not do so for one reason or another [30].

The second wave of cybercrime came in the latter part of the 20th century, with the invention and advancement of web browsers. It is understood that most web browsers that were in use during the 90s were vulnerable to viruses [30]. The virus would be delivered to people's computers whenever they visited malicious websites. Some of these viruses made computers operate slowly, others would create some pop-up advertisements that tended to crowd the victim's computer screen, and some would redirect the victim to websites such as pornography sites [30].

Cybercrime started becoming a more serious threat in the early 2000s (21st Century) when social networks were invented [30]. This was propagated by the desire to put personal information on social networks. This effectively created a database of personal and identifying information. This availability of personal information gave rise to cybercriminals, who then targeted this identifying information for theft. This information was used for number purposes, namely: to set up credit cards, access victims' bank accounts, etc.

The latest cybercrimes involve highly sophisticated electronic hackers who target anything on the Internet that they may deem beneficial to them. Cybercrime is a global industry, responsible for damages worth trillions of dollars annually [30].

6. REVIEW OF CYBERSECURITY DATA BREACH IN THE USA

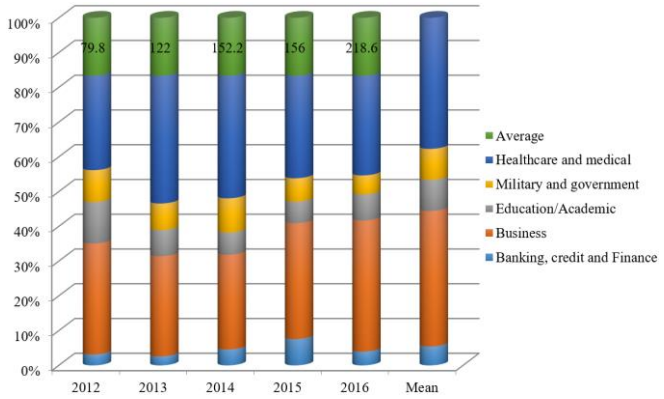

Figure 1. Reported annual thematic cybersecurity breaches in the US [31-35]

6.1 Figure 1 analysis

Between 2012 and 2016, there was an increasing trend in banking and finance, business, and health care institutions. The trend in education/academic and combined military and government was mixed. The business had the greatest number of cases reported in 2012, 2015 and 2016. The health care and medical institutions took the lead in 2013, 2014 and 2016. The banking finance and credit institutions had the least number of cases reported between 2012 and 2016.

On average during this period, business institutions had the greatest number of cases closely followed by health and medical establishments. Banking, credit, and finance were at the bottom with military and government with education and academic setups in between with an equal number of cases.

Concerning the annual performance, there is an increasing trend among these select institutions between 2012 and 2016; with the highest mean reported in 2016 and the least in 2012.

In summary, the thematic of reported electronic hacking cases maintained an upward trend between 2012 and 2016.

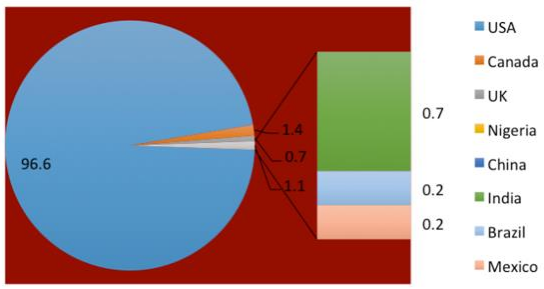

Figure 2. Percentage of annual regional EH reported cases in select countries [36-39]

6.2 Figure 2 analysis

The results do not include 2015 because of incomplete data. Hence the period under consideration was from 2012 to 2014 and 2016. The select count from N America, S America, Europe, and Asia. The highest proportion of reported cases was from the US with 96.6% or 298728 cases. China and Nigeria had the least percentages, which were both not significant. The UK and India had 0.7% each while Brazil and Mexico came up 0.7% each. Periodically, the number of reported cases peaked in 2016 and bottomed in 2013 with 38498 and 34025 respectively.

7. IMPACT OF CYBERCRIME ON POM

Given the current trends and the escalating negative impact of electronic hacking, one is led to believe that the service providers and users will develop different ways of defeating this potentially ubiquitous crime. The burden will, however, be more daunting on the latter. They will need to be more polyvalent in addressing these dynamic and complex landscapes. Mindsets will change (hopefully for the better); more effective and inclusive strategies will be developed and enhanced; the level of resilience will be strengthened; more enabling environments and effective mechanisms will be developed, established and implemented; and level of awareness will be significantly improved.

7.1 Loss in sales

Over the past five years, a new crop of cybercriminals called cyberactivity has emerged. These electronic hackers target a company's online operation programs. Their main intention is to shut down the operations and steal information regarding a company's business practices, which they give or sell to third parties [40]. Examples of companies that have been attacked in this way are MasterCard and PayPal.

In 2010, PayPal's website was hacked by a group claiming to be part of "Anonymous" (responsible for many cyberattacks) [41]. The hackers tried to access a “denial of service” system, which PayPal had imposed on WikiLeaks. The motive of the attack was revenge on PayPal against its decision to shut down services provided to WikiLeaks [41]. Several hackers were arrested and charged. Even though PayPal was not entirely shut down by this attack, many companies were not as lucky [41]. As a result of the "denial of service" attack, customers were not able to access online stores for several companies. If such a denial continues for a long time, the victim company may lose some of its customers, and consequently, company revenues go down.

7.2 Changing modes of doing business

As a result of cybercrimes, companies normally think of new ways of collecting and storing data to ensure these data are not vulnerable to electronic hacking [15]. Due to the vulnerability of online platforms, many companies no longer store their customers' personal and financial information such as birth dates, Social Security numbers, and credit card numbers on their platforms [15]. Other companies have completely shut down online operations they cannot adequately secure. These changes in operations may cost businesses a lot of money since they will not enjoy the competitive advantage that comes through the use of digital technology.

7.3 Protection cost

Because electronic hacking can have dire consequences, companies normally protect their systems against such threats. However, this protection does not come cheap. The costs involved in detecting threats, buying cybersecurity hardware and software, and developing safer operation processes are

usually high [41]. Regardless of the high cost, businesses that are highly complex or store sensitive information, or whose operations are controlled digitally, often hire cybersecurity consultants to develop a system that is safe and customized to suit their needs [41]. But this also does not come cheap. The upfront fees normally paid to these consultants are usually very high [41]. Besides, the developed systems must be continuously monitored and tested to ensure that they still function effectively [41].

8. PROGNOSIS

Without a doubt, computer and Internet technologies are here to say, and will not be going obsolete anytime soon [16]. These technologies will become more advanced as time goes by [16]. It is also a fact that more and more companies will adopt these technologies in their operations. As a result, more operations and systems will be exposed or vulnerable to electronic hacking [16]. The consequences of electronic hacking are normally dire to companies, as well as individuals. Millions or possibly billions of dollars worth of data have already been lost in the past as a result of electronic hacking. The trend is expected to continue in the future as computer and Internet technologies continue to advance [16]. From Figure 3, it is observed that as the years pass, the number of cases of electronic hacking continues to rise. It is also observed that the cost of cybercrime has also been on the rise, year after year. What this means is that, in the future, cybercriminals will become more advanced and they will be able to inflict more damage [16]. As a result, government agencies, as well as companies, will spend more money trying to defend their systems against any cyber attack [16].

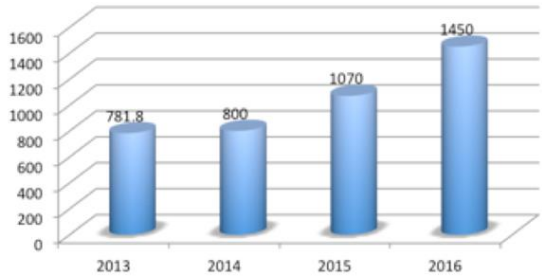

Figure 3. Annual cybercrime costs (million $) in the US [42]

9. FINDINGS

Figure 3 illustrates a cybercrime positive rate increase from 2013 to 2016, inclusive. The annual rate increase between 2013 and 2014 was about 2.3 percent. Between 2014 and 2015, there was a positive increase rate of 3.4%. This positive trend continued with an increased rate of about 3.6% between 2015 and 2016.

From Figure 3, it is observed that there is a positive trend in the number of successful cybersecurity breaches in the US in almost all industries from 2013 to 2016. There was an exception for the education sector and military and government agencies, which recorded staggering trends in the same period. Regardless of this, there is a generally positive trend in the total number of successful cybersecurity breaches per year for the same period (2013–2016). The successful breaches were as follows: 614, 761, 760, and 1,093 for the years 2013, 2014, 2015, and 2016 respectively. It is also observed that the most vulnerable sectors are businesses, and healthcare and medicine. These two sectors account for more than 70% of the total data breaches in all the years considered. In 2012, they accounted for 79.7% of the total breaches. In the years 2013, 2014, 2015, and 2016, they accounted for 70.9%, 78.2%, 75.3%, and 75.4%, respectively, of the total data breaches as a result of electronic hacking.

From Figure 2, it is observed that the US accounts for a larger number of reported cases of electronic hacking. In all the years, it accounted for more than 90% of the total reported cases – except for the year 2015, where it accounted for 80.2% of the cases. The US was followed by Canada, which accounted for less than 3% for the years considered. Recorded countries in other regions such as Nigeria (Africa), China (Asia), Brazil (South America), etc., accounted for less than 1% of the reported cases.

10. DISCUSSION

The results show that there is a general increase in almost every aspect of electronic hacking. The cost of cybercrime in the US is on the rise, and the number of successful cybercrime breaches is also on the rise. There is a cause for serious concern when one looks at these positive trends. These results are just a glimpse of the actual figures, as many businesses do not report cases of cybercrime for fear of negative outcomes, such as losing credibility, client confidence, and potential revenues.

The results also show that the most vulnerable sectors to cybercrime are businesses and healthcare institutions. This means that program operations in these sectors are at high risk of being attacked by cybercriminals. Therefore, every company, NGO, government, and other institution (especially the ones under the above sectors) need to stay on alert and seriously consider the possible ramifications if this trend were to continue. In that case, the future remains bleak and enigmatic. But the advancement of technology such as blockchain technology offers some hope in the future. According to experts, a system that is developed using blockchain technology cannot be hacked (at least for now). This is currently being tested by several companies. However, it is important to remember that as technology continues to advance, the knowledge and skills of electronic hackers will also continue to advance. It is, therefore, hard to predict the effectiveness of future cybersecurity technologies, like blockchain.

11. CONCLUSION

Computer and Internet technological advancements have enabled companies, government institutions, NGOs, etc., to carry out their daily program operations efficiently through automation. In many companies, almost every aspect is automated. However, the enjoyment of the full potential of these technologies is being hampered by cybercrime. The more a company digitizes its operation through online platforms, the more vulnerable it is to electronic hacking. Companies and individuals have lost billions of dollars worth of data due to electronic hacking. In recent times, companies, as well as individuals have faced very complicated cyber threats such as Wanacry, Ransomware, Notpetya, etc. These

threats can sabotage operations of a company, such as preventing its customers from accessing the company's website or redirecting customers to malware websites, or even stopping a company's production machine remotely.

The trend of increasing cyberattacks is expected to continue as the Internet and computer technologies become more advanced. This is because as technologies in the Internet and computer become more sophisticated, new forms of electronic hacking techniques emerge to exploit the vulnerabilities and opportunities offered by the new technologies. The levels of vulnerability are global and inclusive with very high thematic risks of large-scale negative effects on productivity. Long term, effective and sustainable strategies are urgently required. These need to include more innovative national laws and policies. The current levels of vulnerabilities are as expected skewed towards big data, cloud computing and analytics service providers: primarily from industrialized and high-income countries with the US significantly most affected. The result shows that companies are susceptible to many forms of cybercrimes that can lead to significant losses. To reduce exposure, there is need to implement effective security management programs.

REFERENCES

[1] Bossler, A.M., Burruss, G.W. (2011). The general theory of crime and computer hacking: Low self-control hackers? Corporate Hacking and Technology-driven Crime: Social Dynamics and Implications, Thomas Holt and Bernadette Schell (Ed.): 38-67 Hershey, PA: IGI Global. https://digitalcommons.georgiasouthern.edu/crimjust-criminology-facpubs/247.

[2] Applegate, S. (2015). Cyber conflict: Disruption and exploitation in the digital age. In: Lemieux F. (eds) Current and Emerging Trends in Cyber Operations. Palgrave Macmillan's Studies in Cybercrime and Cybersecurity. Palgrave Macmillan, London. https://doi.org/10.1057/9781137455550_2

[3] Morris, R.G. (2011). Computer Hacking and the Techniques of Neutralization: An Empirical Assessment. Corporate hacking and Technology-Driven Crime: Social Dynamics and Implications, 1-17. https://doi.org/10.4018/978-1-61692-805-6.ch001

[4] Cashell, B., Jackson, W., Jickling, M., Webel, B. (2004). The economic impact of cyber-attacks. Congressional Research Service Documents, CRS RL32331 (Washington DC).

[5] Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q., Laplante, P. (2011). Dimensions of cyber-attacks: Cultural, social, economic, and political. IEEE Technology and Society Magazine, 30(1): 28-38. https://doi.org/10.1109/MTS.2011.940293

[6] Walters, R. (2015). Cyber attacks on US companies since November 2014. The Heritage Foundation, (4487).

[7] Allen, J. (2015). Online Privacy and Hacking. Referencepoint Press.

[8] Jarvis, L., Macdonald, S., Nouri, L. (2014). The cyberterrorism threat: Findings from a survey of researchers. Studies in Conflict & Terrorism, 37(1): 68-90. https://doi.org/10.1080/1057610X.2014.853603

[9] Hutchings, A. (2014). Crime from the keyboard: organised cybercrime, co-offending, initiation and knowledge transmission. Crime, Law and Social Change, 62(1): 1-20. https://doi.org/10.1007/s10611-014-9520-z

[10] Poulsen, K., Summerer, E. (2015). Kingpin: How One Hacker Took over the Billion-Dollar Cybercrime Underground. Crown; Reprint edition (Feb. 7 2012).

[11] Snail, S. (2009). Cyber crime in South Africa-hacking, cracking, and other unlawful online activities. Journal of Information, Law and Technology, 1: 2009-1.

[12] Orr, T. (2008). Privacy and hacking. New York: Rosen Central.

[13] McGuire, M., Dowling, S. (2013). Cybercrime: A review of the evidence–Summary of key findings and implications. Home Office Research Report 75. http://www.gov.uk/, accessed on 11 November 2020.

[14] Moore, R. (2010). Cybercrime: Investigating High-Technology Computer Crime. Routledge.

[15] Iovan, S., Iovan, A.A. (2016). From cyber threats to cyber-crime. Journal of Information Systems & Operations Management, 10(2): 425-434.

[16] Robert, E., Eric, J.E., John, L. (2013). Digital Crime and Digital Terrorism. Pearson Publishing.

[17] McLaughlin, K.L. (2011). Cyberattack! is a counter-attack warranted. Information Security Journal, 20(1): 58-64. https://doi.org/10.1080/19393555.2010.544705

[18] Savage, K., Coogan, P., Lau, H. (2015). The Evolution of Ransomware. Security Response, p. 57.

[19] Chu, W., Zhu, B.B., Xue, F., Guan, X., Cai, Z. (2013). Protect sensitive sites from phishing attacks using features extractable from inaccessible phishing URLs. 2013 IEEE International Conference on Communications (ICC), Budapest, pp. 1990-1994. https://doi.org/10.1109/ICC.2013.6654816

[20] Alsharnouby, M., Alaca, F., Chiasson, S. (2015). Why phishing still works: User strategies for combating phishing attacks. International Journal of Human-Computer Studies, 82: 69-82. https://doi.org/10.1016/j.ijhcs.2015.05.005

[21] Loukas, G. (2015). Cyber-physical attack steps. Cyber-Physical Attacks, 145-179. https://doi.org/10.1016/B978-0-12-801290-1.00005-9

[22] Kim, A., Wampler, B., Goppert, J., Hwang, I., Aldridge, H. (2012). Cyber attack vulnerabilities analysis for unmanned aerial vehicles. Infotech@ Aerospace 2012. https://doi.org/10.2514/6.2012-2438

[23] Feng, S., Tesi, P. (2017). Resilient control under denial-of-service: Robust design. Automatica, 79: 42-51. https://doi.org/10.1016/j.automatica.2017.01.031

[24] Smyth, G. (2017). Using data virtualisation to detect an insider breach. Computer Fraud & Security, 2017(8): 5-7. https://doi.org/10.1016/S1361-3723(17)30068-4

[25] Fruhlinger, J. (2017) What is a cyber attack? Recent examples show disturbing trends. https://www.csoonline.com/, accessed on 11 November 2020.

[26] Karl, W., and Gervais, A. (2016) Ethereum Eclipse Attacks. https://doi.org/10.3929/ethz-a-010724205

[27] Perlroth, N. (2017). Equifax Says Cyberattack May Have Affected 143 Million Customers https://www.nytimes.com/, accessed on 11 November 2020.

[28] Goel, V. and Perlroth, N. (2016). Yahoo Says 1 Billion User Accounts Were Hacked. https://www.nytimes.com/, accessed on 11 November 2020.

[29] Thielman, S. (2016). Yahoo hack: 1bn accounts

compromised by biggest data breach in history. https://theguardian.com/, accessed on 11 November 2020.
[30] Le VPN (2017) Where Does Cyber Crime Come From? History of Cyber Crime. https://www.le-vpn.com/, accessed on 16 Jan. 2018.
[31] ITRC (2017) 2016 breach report, ITRC. https://www.idtheftcenter.org/, accessed on 11 November 2020.
[32] ITRC (2016) 2015 breach report, ITRC. https://www.idtheftcenter.org/, accessed on 11 November 2020.
[33] ITRC (2015) 2014 breach report, ITRC. www.idtheftcenter.org/, accessed on 11 November 2020.
[34] ITRC (2014) 2013 breach report, ITRC. www.idtheftcenter.org/, accessed on 11 November 2020.
[35] ITRC (2013) 2012 breach report, ITRC. www.idtheftcenter.org/, accessed on 11 November 2020.
[36] FBI-Internet Crime center (2016) 2015 Internet Crime Report, FBI. https://ic3.gov/, accessed on 11 November 2020.
[37] FBI-Internet Crime Center. (2014). 2013 Internet Crime Report, FBI. https://ic3.gov/, accessed on 11 November 2020.
[38] FBI-Internet Crime Center. (2013). 2014 Internet Crime Report, FBI. https://ic3.gov/, accessed on Nov 20 2020
[39] FBI-Internet Crime Center. (2012). 2013 Internet Crime Report, FBI. https://ic3.gov/, accessed on 11 November 2020.
[40] Cavusoglu, H., Mishra, B., Raghunathan, S. (2004). The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. International Journal of Electronic Commerce, 9(1): 70-104. https://doi.org/10.1080/10864415.2004.11044320
[41] Hintz, A. (2013). Dimensions of modern freedom of expression: In: Brevini B., Hintz A., McCurdy P. (eds) Beyond WikiLeaks. Palgrave Macmillan, London, 146-165. https://doi.org/10.1057/9781137275745_9
[42] FBI-Internet Crime Centre. (2017). 2016 Internet Crime Report, FBI. http://www.geoinform.ru/, accessed on 11 November 2020.