Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

EDDY ODHOMI

The Operative Level Perception of Cybercrime

Threats and prevention in a logistic company

INDUSTRIAL MANAGEMENT ENGINEERING

2021

Author(s)
Odhomi, Eddy

Type of Publication:
Bachelor's thesis

Date:
May 2021

Number of pages:
68

Language of publication:
English

Title of publication:
The Operative level Perception of Cybercrime (Threats & Prevention) in a logistic Company

Degree Program: Industrial Management Engineering

Abstract

The Thesis work has explored the effects of cybercrime and their motives behind the actions of the hackers for taking such an act, in disrupting companies services, networks, and most obviously, the financial consequences that can lead to millions of euros.

Other areas that were covered were the types of cybercrime and their differences. The main objective of the thesis is to reveal the operative level of cybercrime in the logistic industry and the potential risk, threats, that when not properly handled could result in huge detrimental effects to the company. The responsibility of the company, in taking the initiative for prioritizing of their security major, on their internal security- for the protection of corporate data, and taking the responsibility on the cloud customer, staff, or employee rather than the cloud security provider would be discussed.

The research style used was the quantitative approach, in the gathering of data through the newsletter, from the company's webpages (DHL). Some other sources consulted were the internet and books for the theoretical background, in giving a conceptional understanding of what cybercrime is and its potential threats.

The findings were intriguing, because, they revealed that, cybercrime is becoming soon, the most prevailing threat to companies, as well as society, since technology usage is becoming, the norm in handling information. With the current COVID 19 pandemics, making technological usage tripled, also brings alongside the unavoidable consequences of the cyber threat that most companies are not prepared for.

Conclusively, cybercrime is a modern-day issue that should be dealt with, proactively rather than reactively, if the consequence is to be minimized or prevented.

Keywords
Cybercrime, Hacking, Malware, Cybercrime

Acknowledgment

I am very grateful for the encouragement and support which my wife has given me, during the entire process of my study and as well as the writing of this thesis report. She has made my entire effort fruitful in making things possible, because of her contribution both in words and suggestions. I am so thankful and feel blessed to have her by my side in both good, bad, and tough times.

Dr. Leonard Raphael, Ph.D. a friend, brother has made a great contribution to my life in assisting me in starting this study in 2018. His advice and experiences have made this study a dream come through. May God Almighty bless him richly.

Senior lecturer Juha Aromaa, my thesis advisor, has been of great assistance to this thesis work, through his encouragement, support, and advice. His countless pieces of information and suggestions were of valuable contribution in making the thesis work easy to complete. I am grateful for his relentless contributions.

CONTENTS

1 FOUNDATION OF THE STUDY

The current times which we are living in is the era of online processing, and maximum information usage, with this information, are prone to cyber-attacks or threats.

It is also identified that as the number of cyber threats are increasing, and the difficulty in understanding their behavior as well as the restriction for discovering these attacks, in their early phase are challenging (Saini, Rao & Panda,2012,202).

Cybercrimes are daily experiences that affect companies, public parastatals, and private individuals around the world.

As cybercrime is becoming a widespread issue, in the modern-day world of increasing technological usage, is the need for considerable attention in dealing with the effects, which has already affected around 96 percent of all German both small and medium-sized (SMEs) as well as large companies that have experienced various IT security incidences. (BMBF,2020).

IT security, which is becoming a major concern in the logistics and transport sector, with a wide geographically reaching and diverse supply chain connectivity, has exposed companies to a significant increase of attacks.

The need for managing the threats and using protective means will be important but must be ‘first’ by identifying the causes of the risk and the potential threat that could affect business, leading to financial losses and the imminent risk to customer identity theft, breaches of security as well as the reputational risk that maybe involve for the companies. (Callon,2018).

Observing, the operative level of cybercrime in the logistic Company and what can be done, in curbing the further spread and the involvement of the government through joint policies would be considered.

1.1 Background of the problem

In creating a safe environment: where a business would be negotiated, as well as the generation of finances in a highly secured modern technological and cyber informative world, is the need to understand the problems and threats that could lead to high risk in both financial, intellectual risk and the possible losses.

According to LogMeIn, about 91% of business around the world including companies in Germany, which understood the risk of password reuse, has admitted the non-changing of password in more than a year, has thereby increased the security risk as well as the financial risk that is growing exponentially, as logistical supply chains are growing bigger and more complex. (Callon, 2018).

1.2 Problem's statement

According to the Federal Criminal Police Office, confirmed in 2012 that computer crime increased to about 3.4 percent with 87,871 cases amounting to a 4.2 billion euros per year loss to the German industry (BMBF,2020).

Brockett, Golden &Wolman (2012) stated that "Cybercrime and the risk are ever-growing with the threat on the public establishment, government, companies' reputational risk, with the risk of customers, stakeholder confidence that is lost. Other proliferation of information technology with the increase of the frequency, severity over time, changing nature that is needed to be dealt with, as well as the disruption of network servers and facilities are also consequences."

Cybercrime is a unique topic, because of the operational enterprise risk that is involved, due to the mobile location and the scope of the threat, and the extent of the high-profile impact. Keeping in mind, that of the financial losses due to liabilities from the cyber events, which affect product and services, identity theft, threat and the breaches of information leading to reputational risk. (Brockett, Golden & Wolman,2012).

1.3 The need for the thesis work

The purpose of the thesis work is to research logistic companies and investigate the threat and protective major that are in place, for curbing or fighting against cybercrime and its presence in the logistical world. Taking into consideration one of the human's basic requirements, which is security, is needed to be focused on.

Observing the current unavoidable application of information technology in our lives, as well as in businesses, has made it easy for a country like Germany to be competitive while generating revenue for societal good.

According to the BMBF (Bundesministerium für Bildung and Forschung) also translated as the Federal Ministry of Education and Research located in Bonn, Germany, research findings are responsible for informational data security protection, theft in company security, and the avoidance of fraudulence act. (BMBF,2020).

1.4 The nature of the study or research approach

The research would be a quantitative approach style of obtaining information’s through data collection from websites and newsletters for further use in complementing the effect of cyber-attack, risk, and the possible protective major in place. The use of theoretical data from research material either through books or articles would be used as well as the collection of other research work that has been done before for further evaluation.

The data that would be obtained from this research would be analyzed for the identification of the causes and the possible means that would be needed for minimizing the effect of cybercrime.

The definition of the research would be about the investigation into the core of cybercrime and the potential threat that they have on the logistic company. literature data would be shown for confirmation with the impacts, on companies and other establishments for drawing attention and awareness to their hidden presence, even when it seems to elude the physical perception, would be analyzed.

1.5 Research question

Notably, as information technology is advancing, its presence in the commerce logistic and its effective usage for generating value for the entire supply chain as well as the optimal use of resources. They also have the potential risk that could hide the smooth flow of information, which could be both security breach of data and identity theft.

1.6 Research problems

The research question is as follow:

- The effect of cybercrime on productiveness in logistic company
- The cost of cybercrime and its effect
- Cybercrime and who losses in the process
- The need and the role of cyber technology in the logistic company.
- The principle of cybercrime
- Cyber technology advantage and disadvantages
- Types of cybercrime
- Hacking
- Virus horse and malware
- Phishing and spam through email
- Computer protective awareness and collaboration

1.7 Background story on the cybercrime

As the internet is becoming a normal way of life, it has made the world a smaller place, but it has also made ways to possibilities that did not exist before, as well as with so varying challenges. Therefore, as security is growing, so are the hackers growing faster with their attacks and crimes.

According to Joseph Aghatise (2006) “Crime and criminality have been associated with man since his fall. But one thing is certain, a nation with a high incidence of crime cannot grow or develop.

That is so because crime is the direct opposite of development. It leaves negative social and economic consequences."
"Cybercrime is defined as crimes committed on the internet using the computer as either a tool or a targeted victim." (1).

Cybercrime can also be defined as any harmful act committed from or against a computer or network, which is also defer according to McConnell International, as from terrestrial crimes which are easy to learn, how to commit, requiring few resources to the potential damage without being physically present and often not illegal.
(Osunada & Azeez. 2009,2).

The proliferation of digital technology and their convergence of communication devices has created a transformation in society and businesses. (Clough,2010,)
Cybercrime is a technological attack on computers, network devices. Some of the cybercrime is being carried out, for the generation of profits for a fraudulent purpose, and the spread of virus, malware, and the breach of identity theft. All these have also brought criminal activities, leading virtually, by affecting processes and disrupting daily businesses transaction.

Similarly, the availability of information and the ease of accessibility has led to fraudulent activities and eventually to breach of identity.

Taking note, electronic communication like e-mail and SMS can be used for harassing, stalking. The use of digital networks which is increasing rapidly has also exposed the business to the risk of disruption, damage of computer manipulation, sabotage of computers, and computer espionage. (Clough, 2010).

1.8 Literature review

Crimes occur in our society, which leads to the fact that cybercrime like a traditional crime, has different facet, that is occurring in a variety of environment and scenarios, is evolving experientially.

The cybercrime difference exists because of the varying perception of both the observer, protector, and the victim as well as the function of computer-related crimes. Therefore, “Cybercrime” is defined according to, The Council of Europe’s conversion Treaty as,
“Offenses which are ranging from fraud and forgery, copyright infringements, hacking the breach of security such as illegal data interception, child pornography and the compromising of data integrity and availability” (The Council of Europe, conversion).

Additionally, cybercrime as is defined by (Singe. P.W & Friedman A)” is the use of digital tools by criminals to steal or otherwise carry out illegal activities, as information technology grows more pervasive” (2014, 85).

The United Nations Office on drug and crime defines cybercrime as offenses, which clusters the following categories as content-related issues such as integrity and availability of computer data, systems, copyrights, related right infringement, and crime -types that are related to child sexual exploitation as well as abuse. (United Nation).

Cybercrime generates a lot of vulnerabilities for businesses and target various individuals through victimization and infringing on people's data (Humayun, Niazi, Jhanjhi, Alshayeb & Mahmood 2020).
Also stated, that the cybercrime consequences are difficult to estimate, impacting communities, Industries and their evidence of the negative impact are resulting in loss of brand images, and its costly Dilemna that over amounting the trafficking of marijuana, cocaine, and heroin, with at the cost of 288 billion dollars. (Urciuoli, Männisto, Hintsa & Khan ,2013, 52).

Cybercrime, which can be classified in several ways, according to Gordon and Ford, into two categories, namely Type I and Type II.
The Type I cybercrime which is not limited but includes the phishing attempt, theft or the manipulation of data and services through hacking and viruses, bank, and e-commerce fraud base on credential that are stolen as well as identity theft. (Gordon and Ford,2006).

1.9 Characteristic of the type 1 cybercrime

- It is discrete and singular from a victim's perspective.
- They are facilitated by crimeware programs been introduced such as keystroke loggers, viruses, rootkits, and Trojan horses into the system of users.
- The facilitation of vulnerabilities. (Gordon and Ford, 2006, 2).

The Type II cybercrime activities cover acts like cyberstalking as well as child predation, harassment, extortion, blackmail, stock market manipulation, complex corporate espionage, and the terrorist attack been carried online.
(Urciuoli, Männistö, Hintsa, & Khan, 2013,55).

The trend has been observed from the year 2009 to 2011, that the cyber threat has increased and may be associated with the error in basic coding, like buffer overflow, denial of Service, arbitrary code execution, and format string vulnerabilities.

However, it has been noticed that the trend is less important from the year 2010 to 2012. The espionage cyber-attack is on the increase with a raise to 82 per day from 77 per day in 2011 in comparison to the previous year. (Urciuoli, Männistö, Hintsa, Khan, 2013, 56).

1.10 Classification of cybercrime

Cybercrime can be classified based on their type and their software that is been used in each of their cases, which are phishing, Identity theft, cyberstalking, DDos, cyberterrorism (Gordon & Ford,4).

Example	Type	Software	Crimeware
Phishing	I	Mail client	No
Identity Theft	I	Keylogger, Trojan	Yes
Cyberstalking	II	Email Client, Messenger Clients	No
DDoS	I	Bots	Yes
Cyberterrorism (communication)	II	Steganography, Encryption, Chat Software	No

Table 1. Cybercrime by type and software been used for each of the cases (Gordon & Ford 2006, 4)

Here is a description of a Dos attack

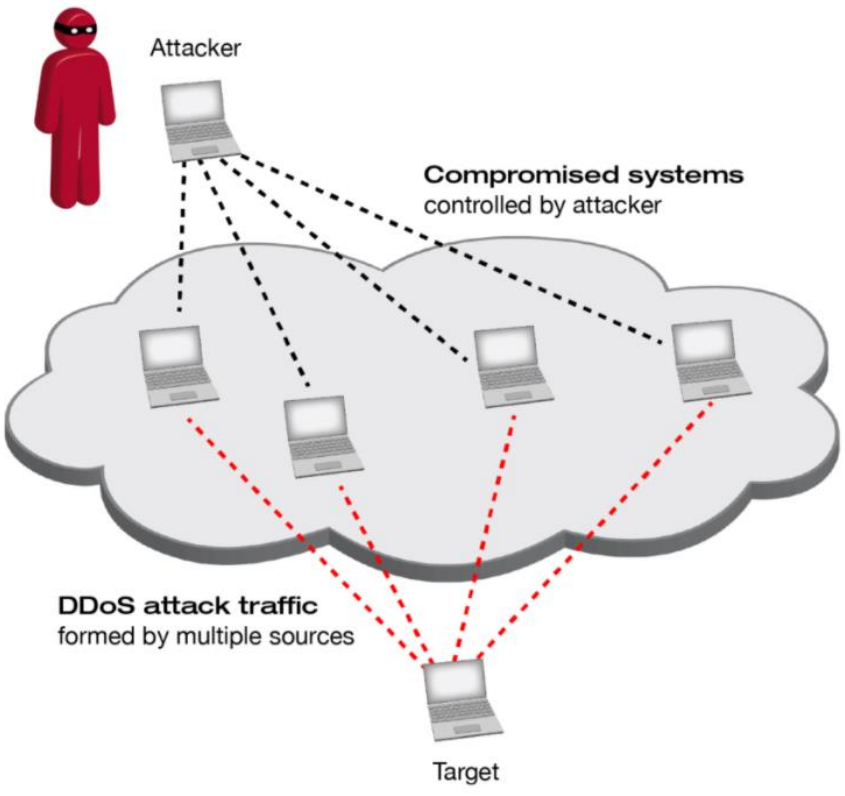


Figure 1. DDoS attack on Target (Xantaro 2018)

1.11 The effect of cybercrime on productiveness in logistic company

Having a critical look at the diagram below reveals the list of 10 industries worldwide, which have been faced with series of targeted cyberattacks in the year 2019.

According to Hornetsecurity, the leading Cloud email provider of security of over 45000 Organisations with 1700 plus platforms with 250 plus five-star reviews and the first on Spiceworks, has revealed different industries with their percentage of attacks. However, the logistic industries tend to occupy the second position with 14% with only a 2 % lower than the energy industry (Hornetsecurity,2020,6)

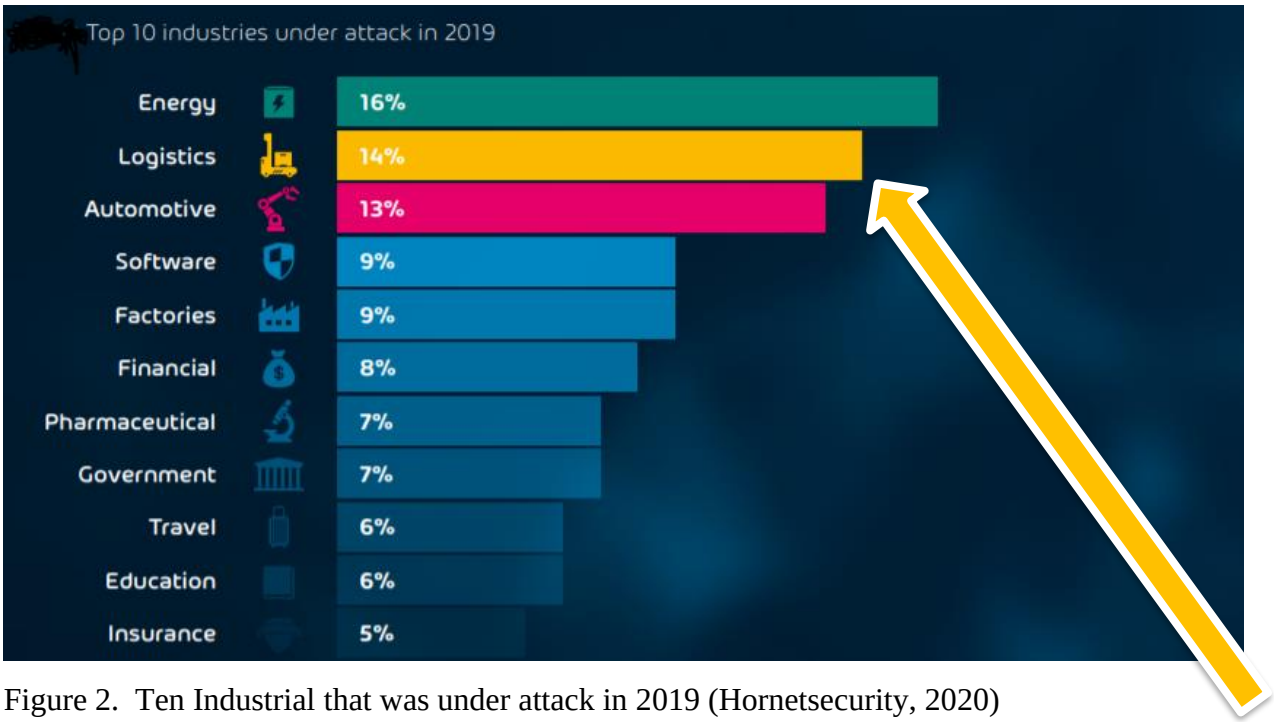


Figure 2. Ten Industrial that was under attack in 2019 (Hornetsecurity, 2020)

TAPA which stands for "Transport Asset Protection Association" is a forum that helps the Global manufacturers, logistics, and carriers of freight with law enforcement agencies made a leading security standard for the supply chain, for minimizing transport crime, theft as well as loss of goods. They stated that, including German and other European countries amounted to about 91.8% of all incidents with loss (24 losses of goods) to the TAPA IIS of their database of worth €21m of an average of crime alone €677,010 and exceeding € 100,000 from April to June 2019. (Brett.D,2019).

As the damages of cybercrime begin to increase in a very fast rate in the world according to Law enforcement agencies and IT specialist, has led to about 6 trillion dollars annually by 2021. (Hornetsecurity,2020)

These effect on the logistical world in Germany and around the world does not leave without its effects, which are:

- The damage of such cybercriminal acts leads to losses, manipulation, or theft of the company's internal personal and financial data.
- The disruption of business operations
- The damaging of systems and networks that are needed for managing of processes of the supply chain.
- The effect on the company's reputations and image representation to the public as well as the direct client repercussion. (Hornetsecurity,2020,7)

- DHL, the logistic and transport company has reported multiple attacks on their supply chain and process with cybercriminal defrauding internet shopper with unauthorized DHL names and brand for the users via email by communicating with clients through graphics that seem to resemble the original DHL emblems. These occur mostly, with the internet online, where clients are requested to make payment, and well as the spoofed DHL delivery services for collecting data, personal information from clients, and credit cards of victims (Nair. P,2021).

- The increased risk that it poses to the logistic company, due to the intrusion from third parties into their system or network and financial damage as well as the pressure of the government as these companies are functioning essential part in the economy (Hornetsecurity, 2020,1-2).
- The intrusion into security and warehouse control facilities led to the loss of data and the introduction of malware into the system, like "zombie zero" which takes advantage of a zero-day vulnerability, the charge of a global resource planning software with the sole aim of exfiltrating of data and record of the company internal ERP systems, causing both capital and personal, productive (Hornetsecurity,2020,3).

- The presence of cybercrime tends to slow activities and deliveries within the supply chain and creating loopholes for hackers (Reuters, 2017).

As the expansion of digital infrastructure is becoming numerous with opportunities so has cyber-attack increased, due to the loopholes that have been discovered by hackers through social engineering, phishing, assessing of email and other online accounts due to multiple reasons are caused by the following as:

- Outdated servers
- Lack of employee expertise and unpatched systems in the field of technology
- Interconnectivity of devices with permanent internet connections Hornetsecurity,2020,7).

1.12 The German view on cybersecurity

The issue of cybersecurity and the German public perspective on the instrumentation of cybersecurity, challenges, and procedures has developed along three lines, which are as follow:

- The connection of cybersecurity with data protection and privacy issues
- Dealing with technical hazards through regulation as wells as engineering and mechanisms through risk prevention.
- The Snowden revelations for the debate of "digital sovereignty."

(Schallbruch, M & Skierka, I.M. 2018, 6)

Along these lines which cybersecurity has developed in Germany, was triggered by reactions from the cyber-attacks in 2000 for efficient cybersecurity, for data protection and privacy, as well as finding ways in handling the hazard from technical cyber-attacks. These were through regulation and engineering means for prevention from government policies with information security, laws from German technology law, for both individual and national security.

Conversely, it is for the protection of citizens, individuals and industries, and states surveillance by the introduction of legal and political measures from foreign intelligent agents where cyberspace is secured, and an operational capability is well handled.

Even when the German government has made progress in securing solid and legal protective measures, in structuring appropriately the informational technological systems, against misuse of the network system, the prosecution by the law due to violations of IT infrastructure that are critical, because of the importance of security in the world. They (Germany) have made a huge investment in cybersecurity.

However, the complexity and the ever-changing environment (vulnerabilities) in the cyberworld for cybersecurity, have revealed that Germany's organizational and technical measures have not adequately been able to protect companies as well as authorities. The reason is that there are no complete defensive and strategic measures for effectively preventing cybercrime, but even technological sovereignty has its shortcoming in the technical level of security. (Schallbruch, M & Skierka, I.M. 2018, 1–7).

2 THE PRINCIPAL OF CYBERCRIME

Since information is becoming easily accessible to all, however, comes with its consequences such as the attack against infrastructure, data, and as well as online fraud and hacking.

The financial consequences from such an attack are enormous, exceedingly over 100 billion dollars in 2007, which tends to supersede the illegal drug trade. Nearly 60% of US businesses believe cybercrime is more than physical crime. This shows the need for information/data protection. (Gercke, 2012,2).

Encryption is defined as a technique of turning plain text into an obscured format using an algorithm (Gercke,2012, September,81). So, therefore, the use of encryption technology is part of the major factors which make investigating cybercrime complicated by blocking access to non – authorized people.

Since early 1980 a series of surveys/reviews carried out by international bodies, which include the UN, Council of Europe, G8 and Interpol had led to the global awareness of cybercrime challenges, because of the nature of cybercrime.

The need was for creating some degree of harmony between countries for effective regulation as well as government, industry, and enforcement agencies. Even though these unifying regulations are desirable, the true consensus is unachievable because of the country's rights, laws, and standards.

The cybercrime convention came into force on the 1st of July 2004 after the signatory in November 2001. It has undergone several ramifications and it is now the cybercrime convention international comprehensive response for problems of cyber- crime.
(Clough. J,2010, 21-22).

Since cybercrime is a typical transnational crime that involves different jurisdictions, usually, different countries are involved or affected. Therefore, the principle that is involved, varies based on the offender, victims, and the information and infrastructure that are involved (Gercke, 2012,235).

The principle of cybercrime was based on the “jurisdiction” (which means various legal issues) and upon the principle of public international law and the authority of a sovereign state for the regulating of conduct in 2005, and the authority of the state to enforce its domestic law. 2007. In enforcing the law is the need for a country to have jurisdiction. (Gercke, M. 2012,235).

2.1 The principle of cybercrime:

- The principle of territoriality/principle of objective territoriality, which is the most common, is applicable when an offense is committed regardless of the nationality of the offender or victim within the sovereign state territory. Therefore, the territory would exercise charge over that individual or legal persons.

- The flag principle is like the territorial principle, but it extends the application to domestic laws to aircraft and ships.

- Effect doctrine /Protective principle: The effect doctrine deals with the enforcement of jurisdiction for crimes made by foreign nationals occurring outside his territory that have some substantial effect within the territory. But in the case of the protective principle, they established jurisdiction where a fundamental national interest is been triggered.

- The principle of active nationality is when the state legislates regulating the citizen conduct abroad or illegal activities, which occur more in civil law countries than common law countries.

- The principle of passive nationality allows in some limited cases to administer jurisdiction in trying a foreign national for offenses made abroad which affect their citizens.

- The principle of universality allows any state to prosecute or arrest any perpetrators of international crime irrespective of their status, rank, or position.

- The procedural law allows the rules of the court to hear/ determine what happens in the civil, administrative, and criminal proceedings (Gercke, M. 2012, 235- 238).

3 THE COST OF CYBERCRIME/SECURITY AND THEIR EFFECT

Cyberattacks a criminal activity, which is conducted through an organization's IT, infrastructure, that could be either internal or external networks or through the internet. It also includes the infiltration of industrial controls of the company's core network system. The process of consideration does not include a plethora of attacks, which the companies firewall defends (Accenture & Ponemon, 2019, 30).

The calculation of the cost of cybersecurity is a huge and complex problem, due to the number of variables that are required in assessing the economic cost.

Another facet, which adds to the complexity is what to be measured, what economic model to apply, how are the computer breaches, accurately? and how the criminal acts are been reported and their impact. The public media, reporting the "cost of computer crime" from multiple sources will elevate cost estimates and affect accuracy (Johnson, T.A. 2015, 255).

3.1 Cost framework for cybercrime

In calculating the cost of cybercrime is the need to consider both the direct and the indirect cost of cybersecurity.

The direct costs are incurred from owners or providers of the infrastructure, including repairs to the network when damaged, while the indirect cost is connected linking to third parties who are not the victim in the direct link to the cyberattack, but who is responsible for the maintenance of infrastructure. (Mendel, 2019, 29)

The opportunity cost is also included in the cost calculation which is resulting from the opportunities lost due to the consequence of reputation based on the activity-based costing framework.

Additionally, are both the internal cost activity center, including (detection, investigation, containment, and recovery) and the external consequences and cost having (Information theft or loss, Business disruption, Equipment damage, and Revenue loss) to the calculation.
Accenture & Ponemon, 2019,33)

. The direct and indirect costs of cyber security attacks

Direct costs	Indirect costs
operational disruption, replacement or upgrading of damaged goods and equipment (or infrastructure) including spare parts	a decline in future revenues
a business continuity plan	insurance
cyber security service level agreements	market failures due to cyber-attacks may also impact cyber security regulations which have a consequent economic effect on the market
physical security including: security information and event management (siem), access control procedures and computer room controls	government activities associated with the cyber-attack
business income disruptions	lost productivity
insurance charges	privacy violations and future privacy protection
recruitment (because of special talent requirements potential candidates may not wish to work in a firm which has suffered a cyber-attack)	the recovery process
intellectual property (IP) losses	increased cyber security investment (such as installing additional cyber security technologies and procedures/policies, hiring cyber security experts and adding external audits)
recovery process	reduced foreign investment in the country or region which had the cyber-attack; the cyber-attack may cause investors to move out of the high-risk domain and territories
risk assessment	the economic impact of investors that may look for countries whose governments are pro-actively investing in cyber security
damage to trade name	stock market losses
lost customer relationships and contracts	
loss of human life and health	
lost revenue from disruption to an organization's internet sites/webpages	
it staff and external contractors working to bring organization systems back to full functionality (including on-line systems)	
legal complaints including privacy violation issues	
security product license fees	

Table 2. Direct and indirect cybersecurity attack cost (Mendel, 2019, 29)

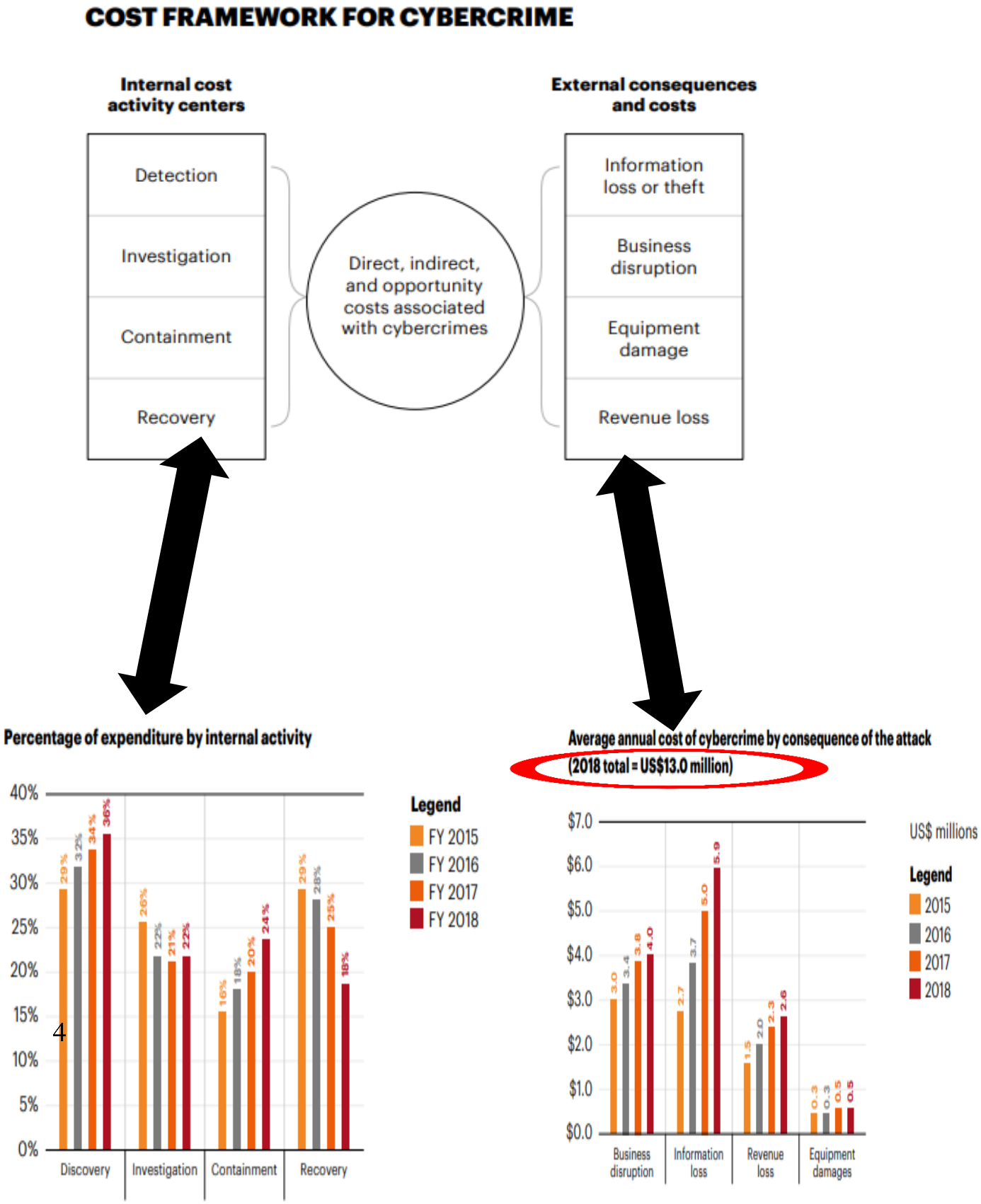


Figure 3. Cost framework of cybercrime (Internal & External) and average cost/Internal activities expenditure (Accenture & Ponemon, 2019, 17, 22, 33)

As cybercrime costs are increasing, it takes more time to resolve, as well as expenses for organizing, according to Accenture and the Ponemon Institute of their ninth annual cost of cybercrime study week release. (Accenture & Ponemon, 2019, 10).

Considering, that the cost of cybercrime has increased to $13.0 million on an average in 2018 in comparison to the previous year (2017), with an average number of breaches in the security in the previous year with an 11 percent increase from 130 to 145 (Accenture and Ponemon,10)

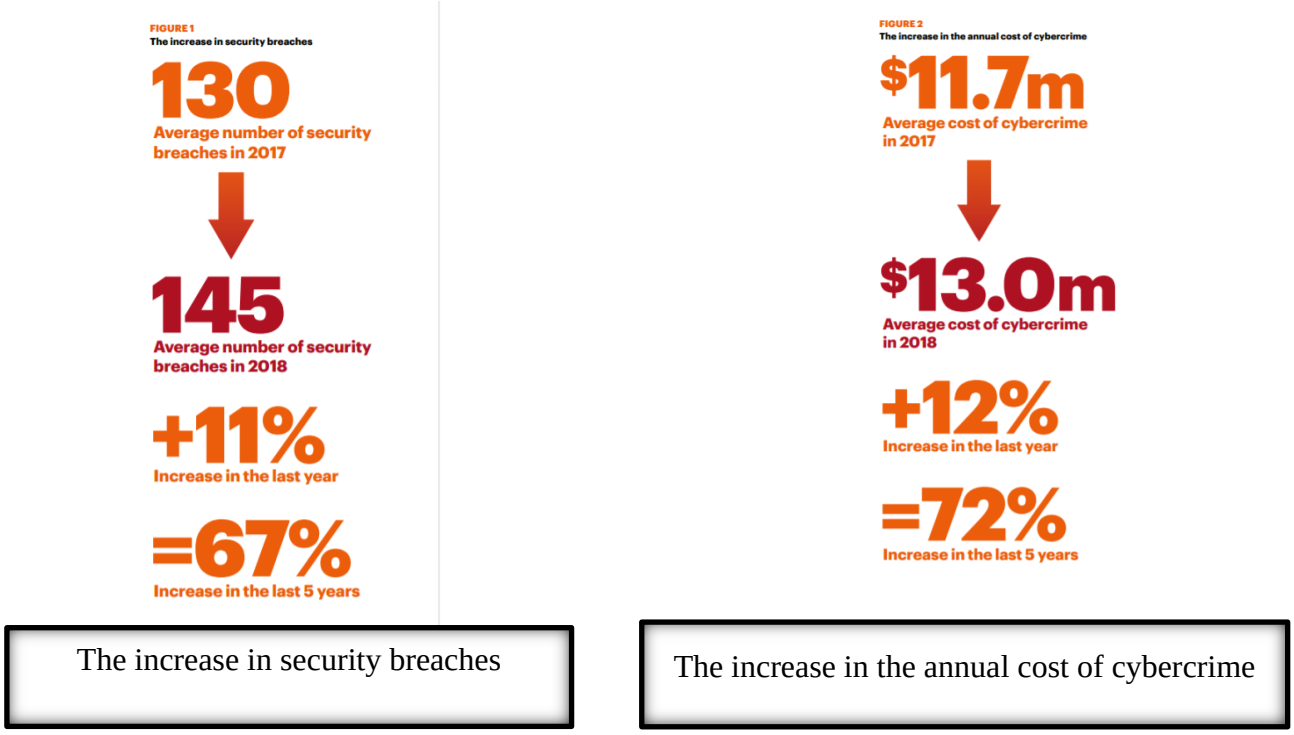


Figure 4. Security breaches and the annual cost increase of cybercrime (Accenture & Ponemon, 2019, 10 – 11)

The calculation also includes a forward projection of the value economically, which is at risk from the cyberattacks in the future for the next five years from 2019 till 2023. This is the second side of the same coin or where cybercrime increases the cost but for the immediate, it increases the disruption of services and data loss and in the long run the financial cost for the future.

As the cost of cybercrime is rising, the expected cost of cybercrime as a percentage from the revenue of companies in various industries (the data collected from 355 companies in eleven

countries around the world including Germany, Finland, etc. and information from IT expert, security practitioner with cyberattack experience and knowledge with cybercrime incidence) for the creation of an economic model for assessing the value, which is at risk globally over the next five years.

The estimated value of the cost in the next five years was gotten by the multiplying of the industry revenue with those of cybercrime cost percentage which is US$5.2 trillion for the cost of cybercrime across the chosen industries as (Travel, Insurance, Logistic, IT, etc.) globally.

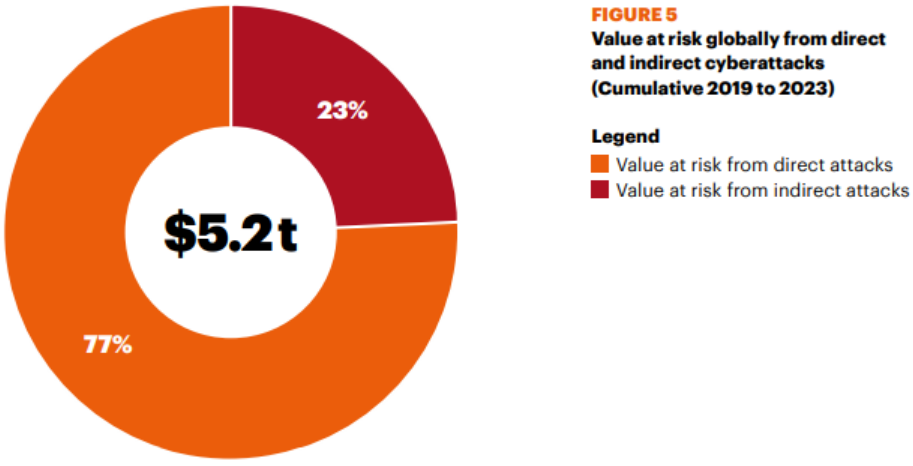


Figure 5. Global value at risk from the indirect & direct cyberattacks (Accenture & Ponemon, 2019, 14)

Direct attacks are where hackers gain entry to computers and can directly download data as well as gain information for exploitation and unethical purposes. While the indirect attack is an attack launched through third parties' computers, which are difficult to track their origins like malware, viruses, worms, and Trojan, etc.

3.2 Cybercrime annual average cost by country

Here, on the diagram are the various countries with their different average annual cost of cybercrime. With America at 29 percent in 2018 with a cost reaching US$ 27.4 million, while the United Kingdom reaching US$ 11.5 million with a 31percent. Germany was about 18 percent with a slight difference from the year 2017 to 2018 (Accenture Ponemon, 2019,12)

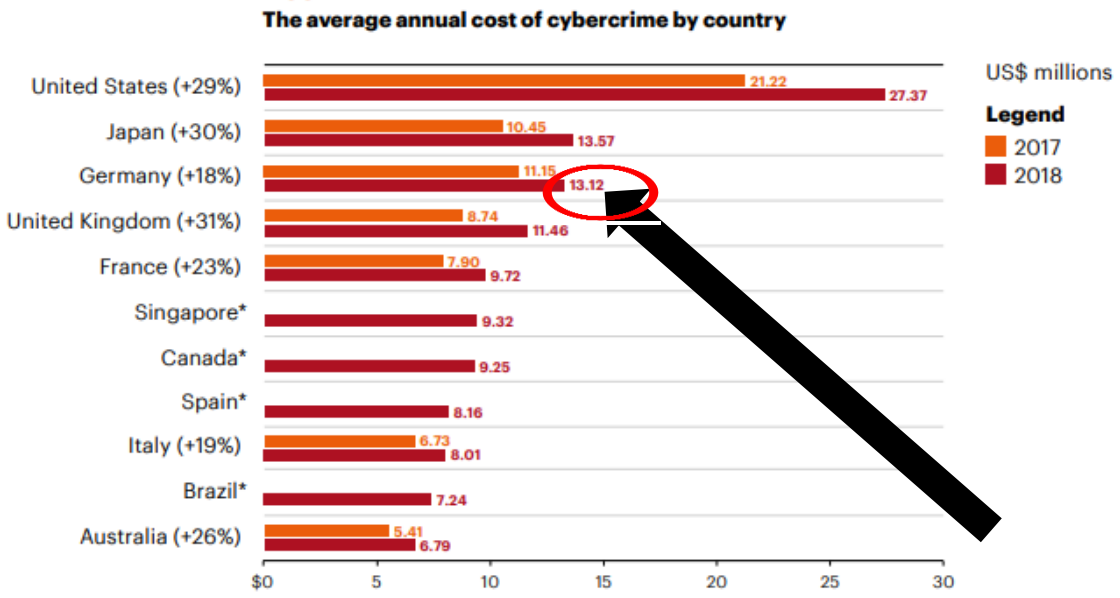


Figure 6. The average cost of cybercrime by country (Accenture & Ponemon, 2019, 13)

3.3 The cost of cybercrime (annually) by attacks

As the presence of the different cyberattacks and their consequence is annually increasing with the continuous attack on systems, facilities, and processes in companies and organizations, are multiplying the cost with the huge impact on revenue losses. Therefore, malware is the costliest with an increase of 11% in comparison to the previous year and the malicious insider attack by 15 %. web-based attacks are also growing with the ransomware of 21%. The cost of the attacks is amounting to US$13.0 (Accenture & Ponemon, 2019,17)

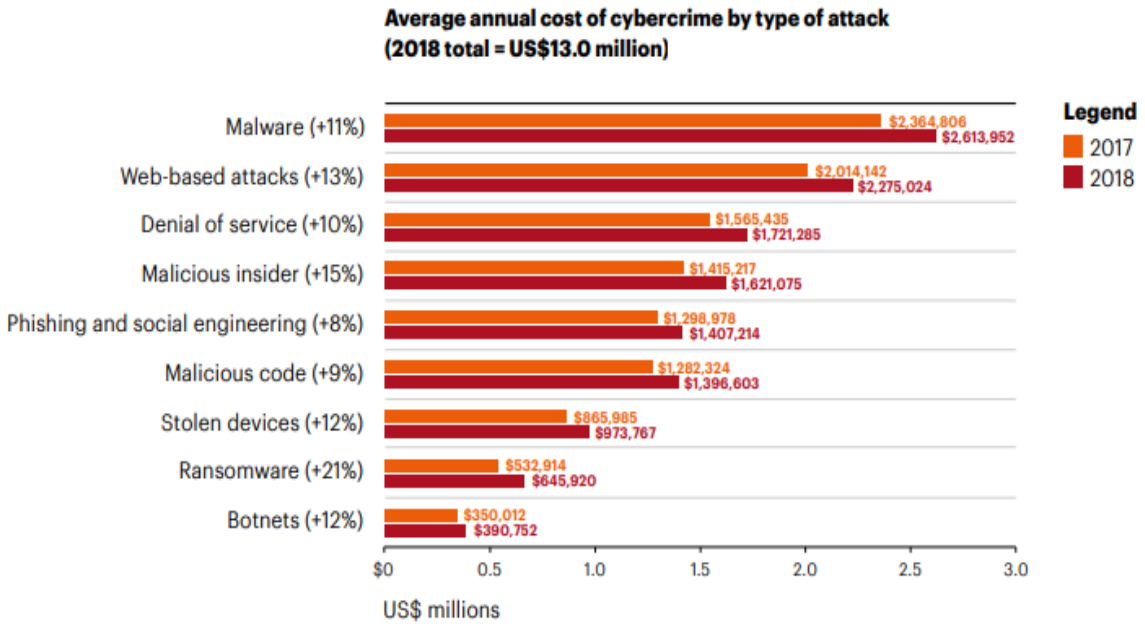


Figure 7. Annual average cost of cybercrime by attacks (Accenture & Ponemon, 2019, 17)

3.4 Some of the limitation in the research of the average cost

The study of the cost of cybersecurity and crime by the institution Ponemon revealed some limitations, which were included in the calculation.

One of the limitations is that the research was done through descriptive inference, in collecting organization data from those who have experience pre-attack cybercrime, within 4 weeks with a nonstatistical result.

The non-response approach was through the collecting of samples by a small representative that includes about 355 companies for the provision of usage benchmark survey. The sampling frame bias involves a framework that is inconsistent with companies whose security programs are more matured (Accenture & Ponemon, 2019, 41).

3.5 Effect of cybercrime on business

With the rising amount of attacks on both businesses, individuals, and governmental bodies, the cost of cybercrime around the world, according to McAfee is around $ 600 billion, or 0.8% of the GDP globally. It is ranking (Cybercrime) as a third crime with global impact. (McAfee)

As the effects of cybercrime are predominant, it causes loss of IP and confidential business information, online fraud crimes with financial implications, because of stolen personal information.

Emphasizing, in 2004, the report reveals that cybercrime produces higher payback than drug trafficking and their effect is growing exponentially as technology expands into developing countries. (Saini, Rao & Panda ,2012 ,205).

4 CYBERCRIME AND WHO LOSSES IN THE PROCESS

Cybercrime is becoming an increasing effect in our society and every area of an organization. The issue is not a matter of how, and not one organization is free from these acts, but it is a matter of when, it is likely to occur.

Then, the effect on lives is in form of information, password, credit card theft, financial and emotional involvement from the shock and uncertainty that are involved.
However, the effect of cybercrime on a company like DHL would be an instant loss of finance as well as other investors and partners (Gone phishing Tournament,2020,5)

Other short-term issues to the company involve exposures to vulnerabilities and the disruption of the supply chain, their partner, investors, and third-party vendors - let alone the huge long-term reputational risk, which could harm their trust by citizens, their image, and consequently loss of their market position, and mentioning their competitors taking the loophole in ruling the market and driving change.

An organization like DHL will lose in non-monetary form as in work hours, loss productivity, damaging of the staff morale, waste of resources (Smith, Lostri, Lewis,2020,4).

4.1 The need and role of cyber technology in a logistic company

As cybercrime has developed a complex ecosystem, which is made of hackers, facilitators, and funders with different motives ranging from pure and profit-making to political gain, but corporate companies need to understand the risk that is involved in cybersecurity to mitigate them by minimizing the threat (Sharrock. J,2018, 2).

The adversarial landscape according to OTORIO divides the threat into different actors with different goals, techniques, and tactics as well as offensive goals (OTORIO report, 2021,10)

Attacker Type	Attacker Nationality	Goals	Techniques	Notable Tactics	Impact
Nation state backed groups (Financial)	China, North Korea, Vietnam, Russia, Iran	Competitive espionage, technological advantage	Clandestine, persistent, wide network attacks	Supply chain attacks, attacks on third parties	Theft of intellectual property and business secrets
Nation state backed groups (Political)		Psychological warfare, damage to sensitive facilities and processes		Supply chain attacks, insider threat	Cutting off or disrupting critical processes and infrastructures
Cyber-Criminals	International	Financial profit through ransom blackmail	Network attacks to steal data or impact production, ransomware to claim money	Phishing, increased use of remote connection solutions (RDP, Citrix)	Production slowdown / halt, business disruption, loss of reputation

Table 3. Potential threat adversarial in the industry landscape (OTORIO, 2021,10)

The table above shows the different attackers with the impacts and motives.

As the presence of cybercrime is becoming eminent and the attacks skyrocketing, as well as the number of users of the internet, are rising with the execution of their day-to-day business.

The need for the provision of cyber tech is for the benefit of the entire organization which is:

- Cyber technology help to assist in the delivery of service to the customer efficiently and effectively.
- It helps in smooth and effective communication between colleagues in the workplace as well as between vendors, investors, and third-party partners.
- They are important for the prevention of customer information, which is crucial.
- It helps for the identification of vulnerabilities in the system or network which would save but financially and reputation-wise.
- Cyber technology is of great importance in the saving of work hours.

While logistic companies are lagging in comparison to other companies which have adopted modern technology. However, recent times show that they have aggressively modernized everything from warehouses to management of logistics through the internet of things (IoT) by connected

objects, cloud computing in all levels of the supply chain, thereby increasing visibility for internal or outsourced and cost-saving processes.
What is lacking is the ability to manage the risk involved with the digital rewards. According to PwC, 38% of logistic companies have unsolved issues significant issues with data privacy and security.

logistic and transport industries can maintain long-term stability in their industry by investing in cybersecurity integration into their core operation. However, it is important to note that, it is shown there is a known technological solution that can provide total protection against cyber-attack (Sharrock. J,2018, 1-2).

4.2 Some of the need for cyber technology are:

- Having a long-term and continuous investment for monitoring, planning, and personal training of personals with robust technology application.
- The utilization of the technology for increasing visibilities and managing risk is a key strategy.
- Detecting vulnerabilities on time and responding quickly is the easiest way to minimize cost and reducing breaches in system data (Sharrock. J,2018,2)

4.3 Operational definitions

Cyberspace: Cyberspace is defined as a space built around connected computers, which store legitimate information that is large for the beneficence of those who are seeking information (Mitra, 2010,19)

Cybercrime: which can be defined as crimes committed using a computer either as a tool or a targeted victim occurring on the internet. Using the computer as a tool requires the technical knowledge of the perpetrator while as the influence of human weakness for exploitation. (Aghatise J,2006).

Cybersecurity:

“Cybersecurity entails the safeguarding of computer networks and the information they contain from penetration and malicious damage or disruption.” (Lewis,2006)

Or according to Dan Craigen, Nadia Diakun-Thibault, and Randy Purse (2014)

Cybersecurity: Cybersecurity is the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems.

Data breach:

It entails the releasing of vital information to an unsecured environment, thereby leading to data loss and misuse.

Spyware:

“Spyware is software available to attackers which gathers information about users without their knowledge or conscious permission – and can be used in taking control and seizing of user’s data or system.” (Jenab & Moslehpour, 2016, 11)

Encryption:

It is used in the process of altering message content, in such a way that, only the reader and the sender can read it. (Mitra.A,2010,64)

Cyberattack: As the disruption or the corruption of the targeted system deliberately, by one state of a system to another state through an assault from a cybercriminal by either malicious or breaches (Checkpoint)

Malware:

Which is for short, is originally” malicious software” can be defined as any software that can be used to disrupt computer operations, as well as the gathering of sensitive information, thereby gaining access to private computer systems and displaying unwanted advertising (Creutzburg. Reiner, 2016) The malware is also called computer virus by Yisrael Radai.

Social Engineering:

It's a type of attack that is carried out, is used in tricking of users for the breaking of security procedures, to gain access into information that is very sensitive and protected from the public. (Seemma. P.S, Sundaresan, Sowmiya M 2018, 125)

Hacking & Cracking :

It is the act of breaking into computer and or networks system with ready-made programs for computer destruction, as well as the making of this hacking. Which could be either for monetary purpose and leaving the computer prone to risk and or crackers, as the stealing of important data and thereby inserting virus and other worms for the damaging of the system. (Vadza, 2011)

Phishing :

These are carried out in the form of an email which is fraudulent in the act of getting their victim in believing those emails are relevant. They later utilized it for obtaining data and important credit card and login information, thereby leaving their victims vulnerable to attacks.
(Seemma. P.S, Sundaresan, Sowmiya M 2018, 125).

Vulnerability:

Cybersecurity vulnerability: According to the Oxford lexicon vulnerability is "The quality or state of being exposed to the possibility of being attacked or harmed," (Oxford dictionary)
this means the exposure of an organization or governmental or private individual in broader terms, a weak spot in their defense.
While Cybersecurity vulnerability is the exposure of an organization to any kind of exploitable weak spot in their fence to data protection. (Logsign)

4.4 Cyber technology advantage and disadvantages

Some of the advantages of cyber technology are for the protection of the system against viruses, malicious code, and unwanted infectious programs as well as the protection of sensitive data from been hacked while enhancing accessibility of information to those who are authorized.

On the other hand, some of the disadvantages of cyber technology are, it is costly and requires high professional skill, the need for constant security patches, which are difficult to keep up to for the updates. The high risk of digital ambushes which are a result of the ever-changing and advancing nature of cybersecurity. (Assignment Help4Me)

4.5 Types of cybercrime

Cybercrime is defined by the Institute of Risk Management as "any risk of financial loss, disruption or damage to the reputation of an organization from some sort of failure of its information technology systems. (FIATA,5)

Cybercrime is spreading wide and fast through the entire internet, stealing data, defaming others online, gaining unauthorized access to use computers as well as companies' systems. It also involves the overriding encryption for the making of illegal copies, breaking of secured code to intellectual properties, and both copyright and trademark software licensing overtaken.

All these lead to computers been compromised and privacy infringement, which is through the loopholes in network and security systems (Seemma. P.S, Sundaresan, Sowmiya M 2018, 125).

According to Vadza, cybercrime is an unlawful act that is committed using a computer as a tool or as a target, leading to forgery, fraud, theft, etc. (Vadza. K. C,2011). Categorizing by Vadza covers either cybercrime as a target on a computer or its use (computer) as a weapon in committing further fraudulent activities.

Irrespective of the difference in choice of categories between Vadza and Seemma, Sundaresan, Sowmiya, they all cover the issue and the mode of their act of cybercriminal.
Cybercrime can be classified based on its motive into three categories (Seemma. P.S, Sundaresan, Sowmiya M 2018, 125) which are:

Type 1: Cybercriminals who are Hungry for recognition.

- Hobby hackers
- IT professionals (Social engineering)
- Politically motivated hackers

- Terrorist organization.

Type 2: Criminals – they are not interested in recognition.

- Psychological prevents.
- Organized crime
- Corporate espionage (Financially motivated hacker)
- Sabotage (Sponsored hacking)

Type 3: Cybercriminal – insiders' threat

- A former colleague who is seeking revenge
- The use of employees from competing companies through damage of theft. (Seemma.P. S, Sundaresan, Sowmiya M 2018,)

Considering Type 3, which is the insider threat. These insider threats are usually overlooked by the organization, but the threat can either be by employees who may be currently or formerly, employed, partners of contractors. They could carry a variety of disruptions by damaging or erasing sensitive data or data breaches.

The insider in the logistic company could compromise personal information or customer, intellectual property, report sheet of the company, and the undertaken of the security control, which places them in the category of negligence (redscan,2020).

What could be realized is that the insider threat could also occur in the malice, were they connive with a competitor, organized hacker group which would steal data, corrupt system virus and steals confidential data or the misuse of the access to the system. (redscan,2020).
The insider threat could be divided into three parts based on the riskiness of behavior, which are:

- Malicious insider
- Careless insider
- A mole

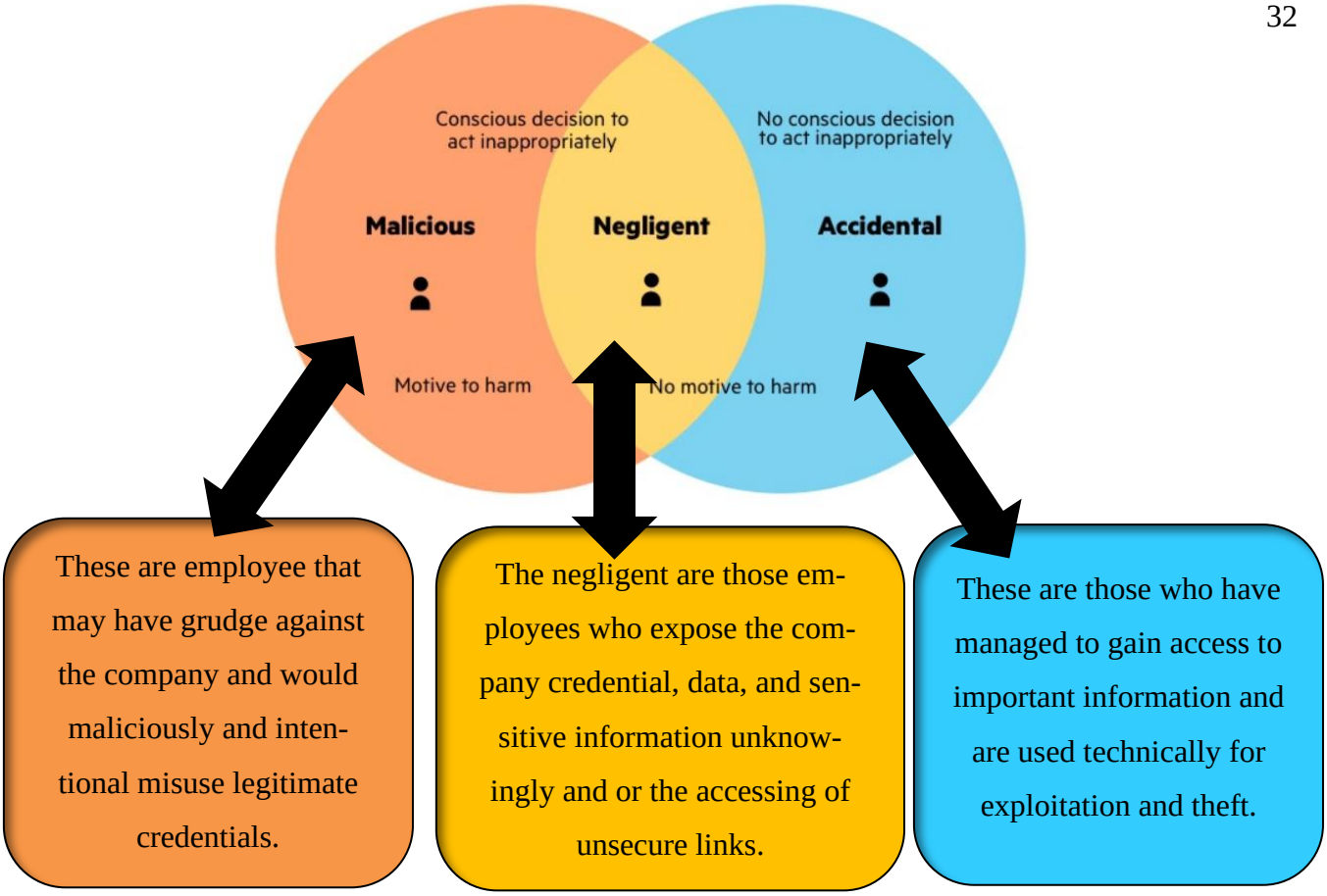


Figure 8aTypes of insider threats (Imperva, 2020)

There are multiple attacks that companies are facing and the need to understand their nature of the cyber-attack would aid in better equipping, the facilitation of understanding, coordination, and communication in the supply chain. These attacks are as follows (DHL,2021).

4.6 Types of cyber-attacks

Thus, the diagram shows the various types of Cyber-attack.

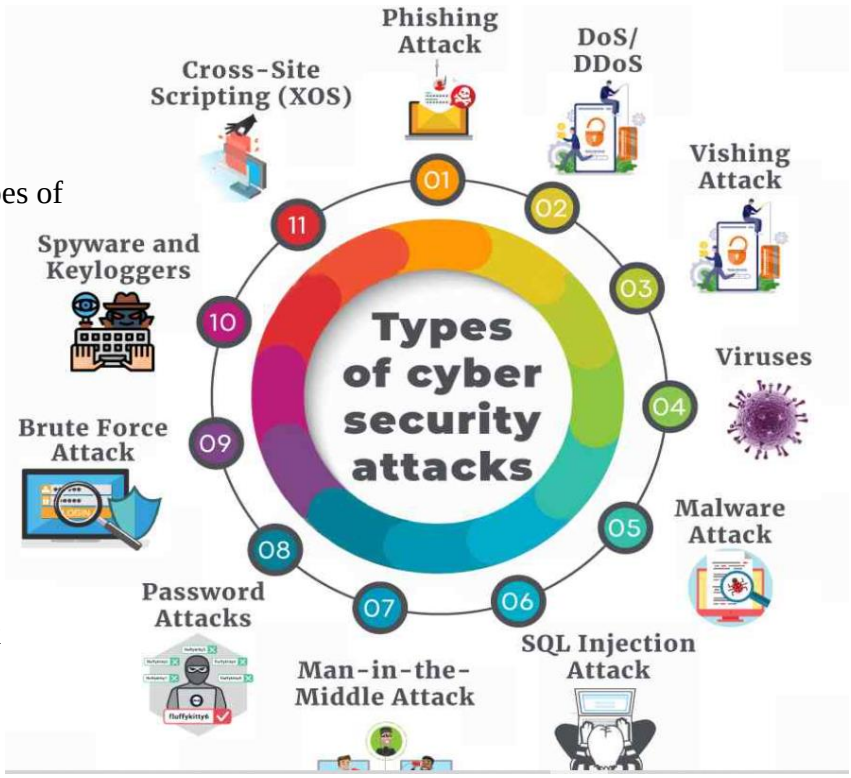


Figure 8b. Various types of cyber-attack (Assignment help4Me)

5 HACKING

Good or bad, hacking is an important aspect of network security.
Hacking is defined as the identifying of weakness in computer systems and or networks and exploiting the weakness to gain access. Which is through the bypassing of the login algorithm in gaining access to a system (Teimoor, 2017)

A Hacker is someone who gains access to and sometimes to data and information which could be used, misused as well as for legal or illegal activities according to Merriam Webster.
(Merriam Webster)

Hackers are as well skilled computer programmers with the knowledge of the security of a computer. (Teimoor, 2017)
Not all hackers are bad, but the mainstream media has a bad connotation of the word "hacker", but a hacker can be divided into 3 based on their motive and whether if they are breaking the law.

- White hat (Ethical hacker)
- Black hat (Crackers)
- Gray hat

Below is a pictorial representation of the hackers.

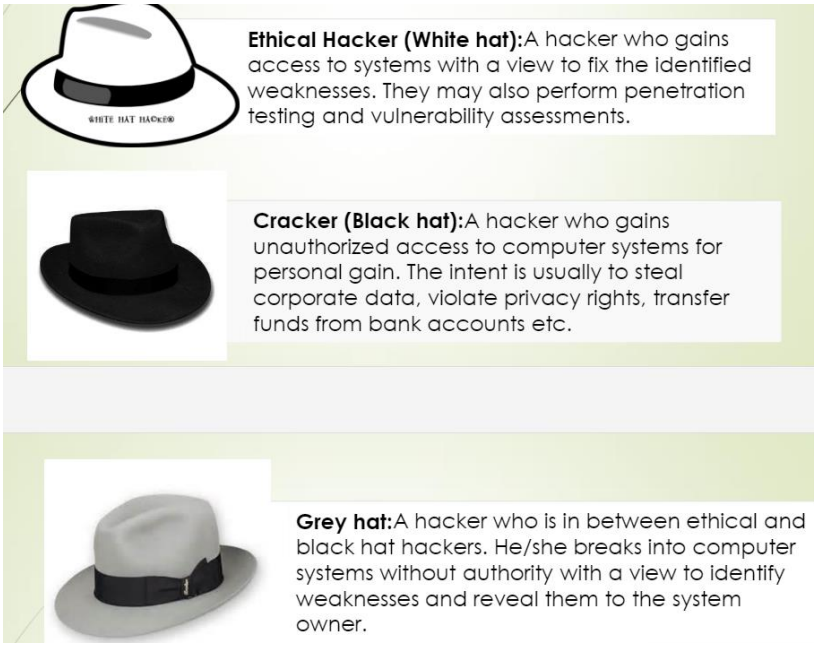


Figure 9. Different types of hackers (Teimoor, 2017, 5- 6)

They are of different categories, based on either monetary gain or simply out of curiosity, which are for the accessing of sensitive information, passwords, and credit card numbers. (Melendez.S,2019).

Hacking could be unlawful access to a system or network, known as a mass phenomenon, involves illegal password obtaining with setting up “spoofing” where users are made to disclose their password and software-based keylogging that record every keystroke. Those attack computers would be put in their botnet and be further used in attacking others (ITU,2012.17).

The University of Maryland suggested that any computer that is unprotected when connected to the internet is most likely to be attacked with a higher risk than the ones been protected. but even a successful attack against really protected computer systems only proves that the technical protection measures can never be able to stop attack completely. (ITU,2012.17).

While some of the hackers circumvent their act in proving their abilities and other causing manipulation and data espionage and denial of service (DDoS) attack (ITU,2012)

Whenever hackers gain access to the organization or individual information, it could be dangerous, leading to loss of data which could lead to legal consequences. It could also be embarrassing when e-mails, text messages are stolen. (Melendez.S,2019)

To the extreme, these hackers could use that stolen information or data for the extortion of money from their victims by demanding ransom, by encrypting data and rendering them unusable or inaccessible as well as the destroying of data in targeting their victims.

Furthermore, they could use those hacked computers in further hacking other computers or making zombies in an endless malware army. (Melendez.S,2019)

5.1 Different types of hackers

Figure 10. Hacking titles (Cisco (CCNA Security)

- The Hacktivist attack for attention
- State-sponsored are attack who are sponsored and guided by the government for lunching operation ranging from cyber espionage to intellectual property theft.
- Cybercrime attacks are those that are involved in it for financial gain.

As the increase of technology usage is becoming demanding in our society, so are the risk and the threat which most organization may undermine, but the hacker is becoming sophisticated in their act.

Considering" NOTPETYA" as malware which was used by the hacker in affecting a lot of companies like Maersk company losing millions of dollars, disruption in their supply chain and about 10 days delay, with over 4,000 servers been affected. (Hornetsecurity,3)

DHL the German mail and logistics firm (Deutsche Post DHL Group) also confirmed the effect of the attack of the NOTPETYA which led to the loss of resources. (Reuter,2017)

The head of technology in Maersk company, made claims of huge disruption to systems and other communication, hampering coordinated response, thereby, exposing weakness in procedure and behavior, even where their software was patch appropriately. but the malware NOTPETYA has explored its weaknesses. (Ritchie, 2019)

About 10,000 mailboxes in phishing attacks have hit FedEx and DHL Express with the extracting of the user's e-mail account for the sharing of pretentious information about shipping parcels for extortion. ((Zurier, S. 2021,17)

Unsafe DHL pack station

Figure 11. DHL Pack station (German dude)

This is a typical pack station in Germany, that operates 24/7 hours in standby, used for sending and picking parcels.

This packet station works with an SMS system where the customer is required to make registration by downloading the DHL app and later, after registration with the customer address. The SMS is sent when the parcel is available. Hackers have been able to crack the account of DHL customers by stealing their data and thereby manipulating the information so that when SMS is sent, it is received by the hackers.

The DHL pack station compartment is open with a mobile TAN number which is sent to the receiver’s phone to be able to open the compartment, but the hacker was also able to order goods unpaid worth 100,000 euro. (Morchner.T, 2018)

This emphatically reveals that the DHL network system could still be cracked by using the loopholes in their system for cybercrime activities as well as customer data for dubious activities and taking note of the reputation of the company.

Furthermore, other attacks that have been carried out, had used, the file-borne malware, which is on the rise, with breaches that are new with zero-day attacks and which traditional base anti-virus could not recognize.

In April 2020, the use of Dridex ransomware attacks companies' customers like FedEx and DHL through sophisticated phishing e-mail disguised on DHL, persuades customers to click on links and respond to e-mail. But eventually, it steals data, distributing malware on the computer system.

What is even costly, is the vulnerabilities of the system which could not identify this malware, only after 2days. However, the strain that is put on security teams, coping with the overwhelming daily attack and alert fatigue, a new threat that comes from all fronts is alarming. (Hosgood,2020).

6 VIRUS HORSE AND MALWARE

The threats today are more psychological than technical in the landscape, due to attacker hostility. Users are more targeted by e-mails, websites and been asked to give sensitive information as username and passwords through online login.

These are through a deceptive act by either inexperience of the user or clicking of links to infection and corrupting of their systems,

According to the McAfee site advisers, about 95% of 120000 who took the spyware quiz were unable to identify which site is safe or unsafe to click. Thus, this indicates a stunning result to user's faces. All these are due to a lack of security awareness of users and the malware when clicked would exploit cyberspace, a workstation for confidential information.
(Davis, Bodmer& leMasters. 2010,8).

A virus as it is known is a small script of code that runs as a program with the sole aim of affecting computer system operation without the knowledge of the user's and their permission. It could be able or execute on its own the programs it has been assigned as we as the replication of itself in infecting servers and network system, for it to be a virus. (Checkpoint,2021)

A virus is a program that is designed to alter the targeted system without the user's consent and thereby infecting the existing program and application by infecting the host computer. (Davis, Bodmer & LeMaster. 2010)

The effect could range from small to mild effect on computer and network system or spreading to huge corporate effect on a network system, hardware, software, or total corruption of files. Thereby acting as access to infecting another computer within a short space of time.

Some of the remedies of virus infections could be the current update of anti-virus in order, to patch any vulnerabilities that may be present and reducing or blocking out threats.

A horse is a type of malware that is been downloaded onto computers through disguise believing as a legitimate program by social engineering, hiding malicious code within the software. They are required to be installed by the users.

These users being un -unaware, of the downloaded malicious code. It later gains back access to corporate systems and spying on online activities, sensitive data, which works through the executable (.exe) files, thereafter, spamming, introducing malicious infection to the system. They become active when other malicious programs are run or opened. Examples of some of this Trojan malware are: (Fortinet, 2020)

- Backdoor Trojan
- Downloader Trojan
- Exploit Trojan.
- Fake antivirus Trojan

7 MALWARE

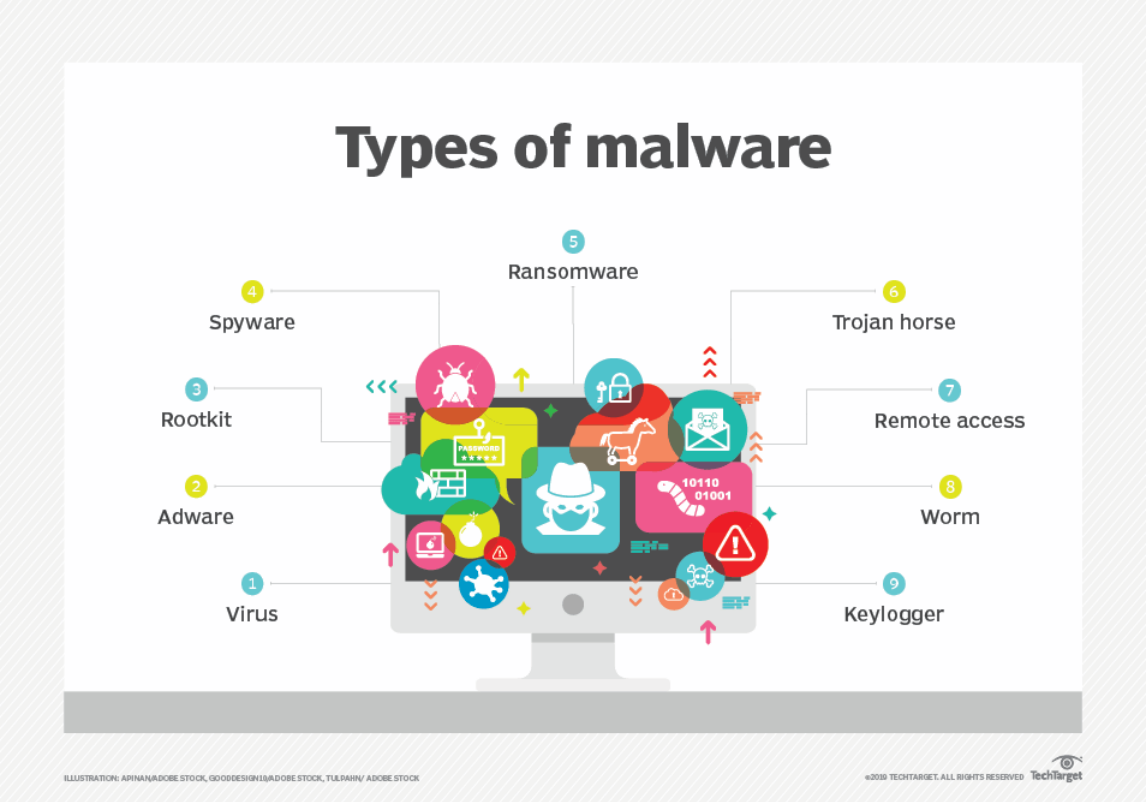


Figure 12. Types of malware (Ben Lutkevich)

Above are the various types of malware. The malware is deceptive in luring users to download or click on links or waiting for a software vendor who releases the update, and they later use the patch by reversing by, developing an exploit from it by creating, a lot of variants in infecting user. (Davis, Bodmer, leMasters, 2010, 9).

They as change the workstation, fraud spamming or remote control of infected workspace and spam relay as well as breaking into the corporate server for intellectual property.

The Russian Business Network (RBN) is known for its malicious activities with the largest in scamming, phishing, malware, and DDoS (Distributed Denial of Service). As cybercrime is becoming a business and due to the lack of Jobs and high-paying IT in Russia and young professional talent with technical experience are driven into cybercrime for getting a technical fix.

The RBN organization has been able to make about 120 million dollars yearly, with the infection of platforms with bandwidth and continuous deploying of the malicious web server, botnet, and control servers. (Davis, Bodmer, leMasters. 2010,13).

7.1 Phishing and spam through e-mail

As phishing and e-mail scams and spam are rising in these current times with the continuous way of lockdown from the corona and due to the increasing presence to remote working from home, has led to a seismic shift and change of organization globally. Due to the epidemic accelerating digital transformation has increased cybercrimes through multiples of phishing attacks and increase vulnerabilities in networks and systems.

Cybercrime has become sophisticated through carefully crafting their SMS, text, and messages. There has been an increase of about 30,000 % increase in attack and related phishing attack of about 667% leading to about roughly $137,000 average cost on data through either malicious e-mail or website wrongly visited or clicked. (Gone phishing Tournament,2020,5)

The findings of Gone phishing Tournament organization release that about 20 % of worker or employee are quick to click on phishing e-mail links- even when they have awareness of phishing attack and security training program. About 10 to 15 % of the staff submitted data in web form. (Gone phishing Tournament. 2020, 6)

Phishing attack clicks and confidential data submission.

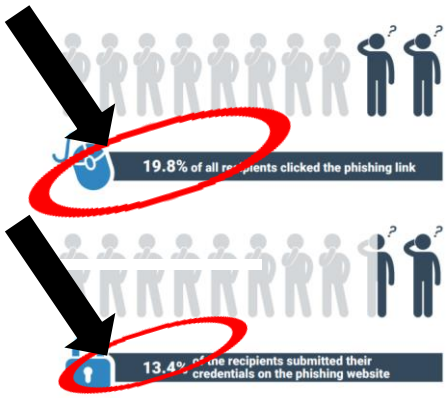


Figure 13. Lack of phishing awareness (Gone Phishing Tournament, 2020, 6)

The Gone organization made the report in comparison of the year 2019 to 2020 with the increase from the previous year from 11% of the employees, who clicked on phishing links and 2% submitted credential and important information to 2020 with about 67% clicking phishing links and about 13% submitted their passwords or information.

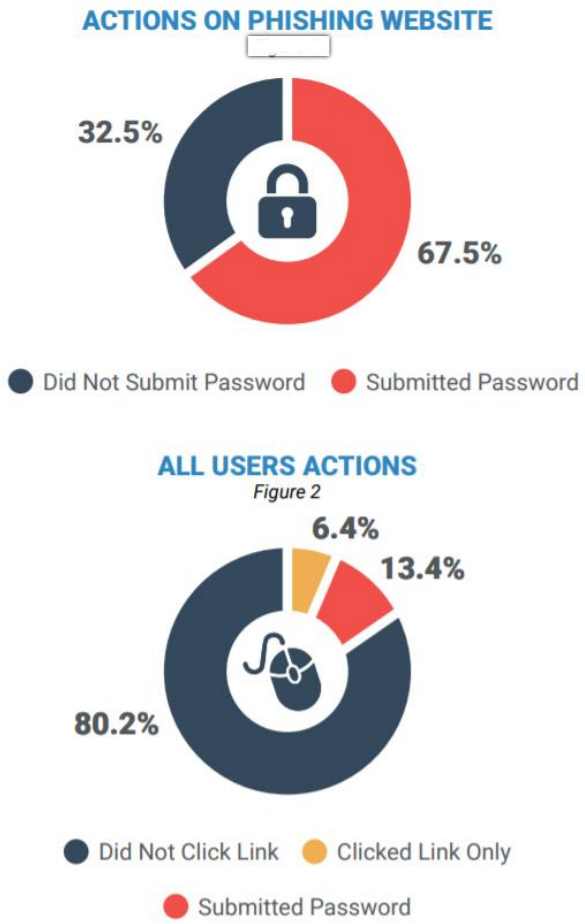


Figure 14. User actions on phishing websites (Gone Phishing Tournament,2020,7)

Phishing is a social engineering method for tricking victims into providing personal information through email, voicemail. etc. There are also phishing – to- services whose aim as fraudsters deceive victims through the mail without the hosting of creating their sites (Warburton 2020, 43).

Check Point, the software Technologies Ltd. made their fourth-quarter release stated that DHL is one of the biggest shipping companies in the world. As the second abuse brand with multiple attacks of phishing and scamming with an 18% increase. This was in comparison to Microsoft leading at 43%. (Check Point,2020).

7.2 Top phishing brands in the 4 quarter of 2020

Here are the top 10 ranking brands with their appearance in phishing attempts:

- Microsoft (related to 43% of all brand phishing attempts globally)
- DHL (18 %)
- LinkedIn (6 %)
- Amazon (5 %)
- Rakuten (4 %)
- IKEA (3 %)
- Google (2 %)
- PayPal (2 %)
- Chase (2 %)
- Yahoo (1 %)

(Check Point,2020)

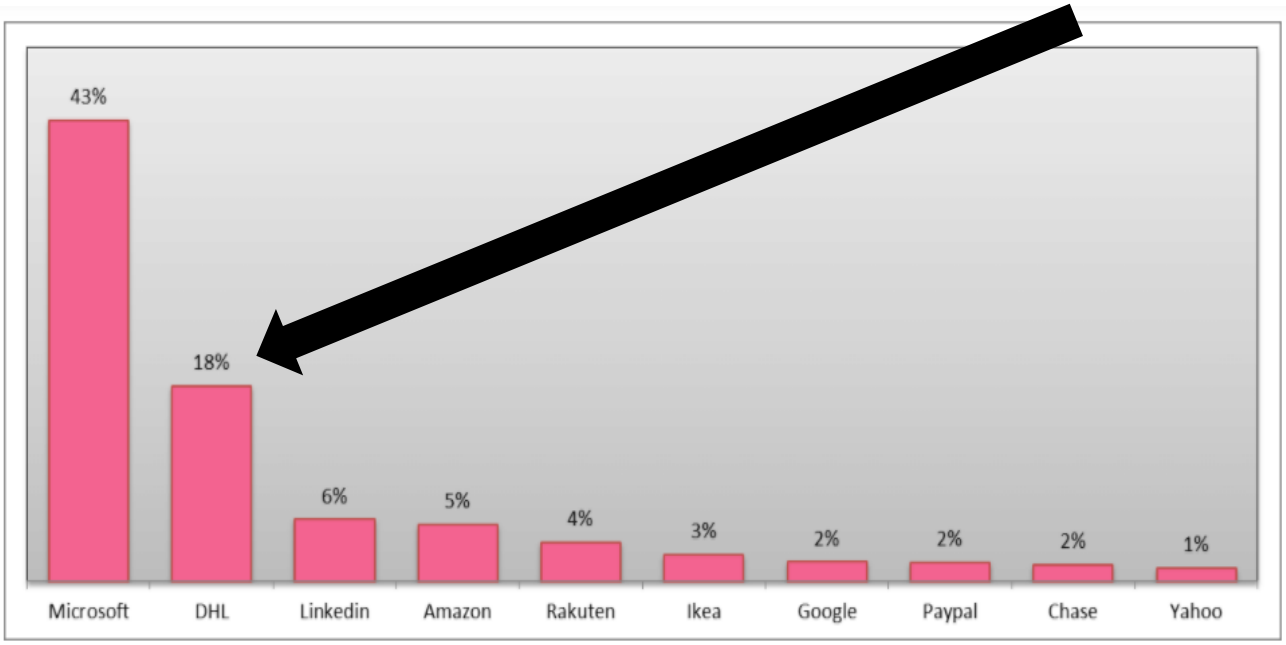


Figure 15. Phishing attacks according to brands (Check Point, 2020)

7.3 Spam through e-mail

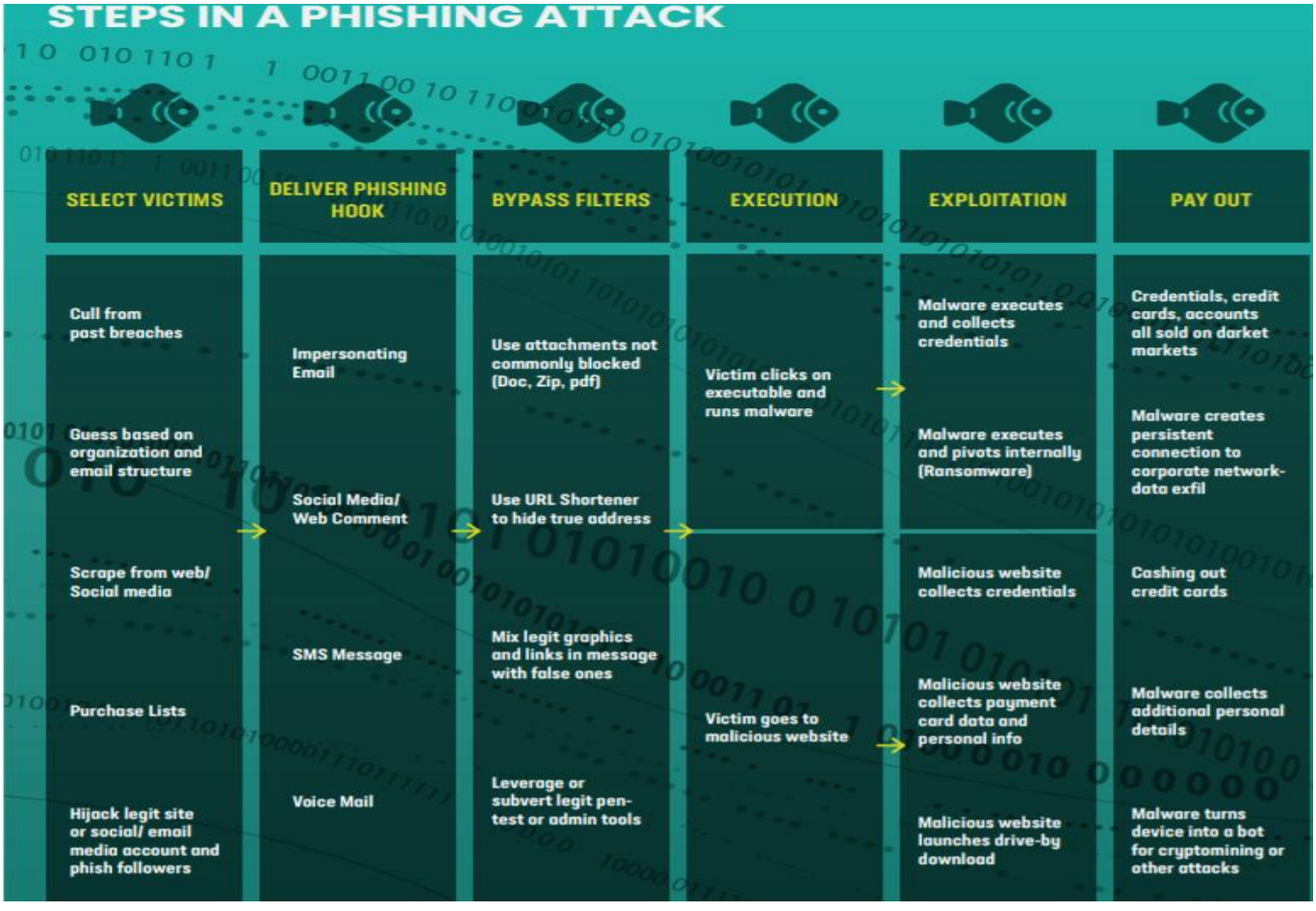
The spamming through e-mail be either through hacker, luring their victims into providing of confidential information and passwords, for which the victim would be affected and the Intrusion in to company's network system with malicious wares.

7.4 DHL phishing email – password theft

Reports from Check Point software has made the report of malicious phishing e-mail which impersonate the DHL brand with the attempt to steal password that was sent from spoofed e-mail address like Parcel.docs@dhl.com, were used for informing the customer when to pick up their parcels, through making the victim click on those links for inputting of their data. As well as the cracking of code in receiving of SMS through mobile TAN for the compartment in pack station. (Check Point 2020).

All these various acts would be of detrimental effect to the customer but in the long run to the reputation of the shipping giant DHL in terms of loss of trust (reputational risk) and financial cost when victims switch to new brand and means of purchase.

Figure 16. Phishing attacks steps (Warburton, 2020,10)



7.5 Real-time phishing proxies (RTTP)

The RTPP whose increase is becoming noticed with the capturing of MFA codes is being utilized by hackers for intercepting users which acts as a person in the middle for the user by intercepting user transactions with the real website. Since these occur in real-time, the malicious websites can then automate the entire process by capturing and replaying the authentication base such as the code from MFA codes (multi-factor authentication) (Warburton,2020,34)

7.6 The reusing of a victims' data in real-time

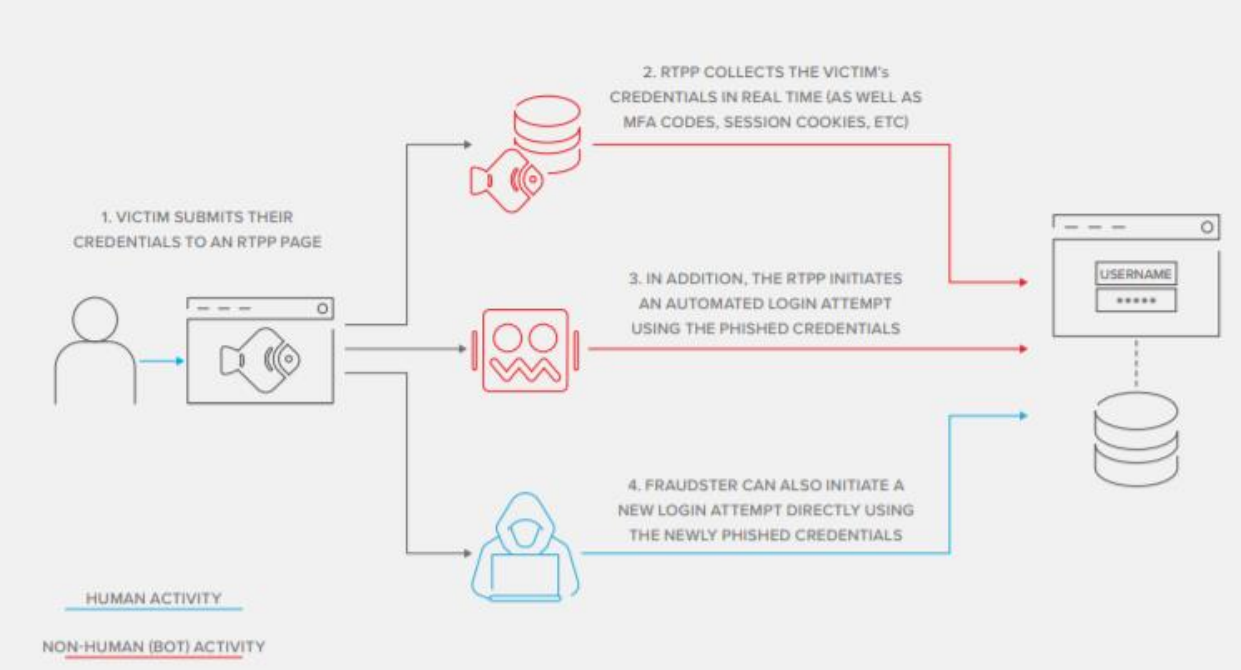


Figure 17. The reuse of a victim's data in real-time (Warburton, 2020, 34)

Here is the difference between traditional phishing and the real-time proxy

	Traditional Phishing	Real-time Phishing Proxy (RTPP)
Method	Fraudster creates a replica of the target website using a clone or phishing kit.	RTPP acts as person-in-the-middle, dynamically intercepting requests from the client and initiating a new connection from the attacker to the target site.
Timing	Asynchronous; credentials are harvested for use hours or days later	Synchronous; attacks conducted in real time as user interacts with phishing site
Information gathered	Usernames, passwords, answers to security questions	Usernames, passwords, answers to security questions, MFA codes, session cookies
Pros (for fraudsters)	Easy to set up	Difficult to detect and shutdown, able to defeat MFA schemes
Cons (for fraudsters)	Services exist to detect and shutdown phishing sites	Requires advanced knowledge to set up

Figure 18. The differences between the traditional and the real-time proxy (Warburton, 2020,35)

7.7 Network segmentation.

Network segmentation helps in the increasing of the security of system /network through separation or the creation of sub-network in a network. As an in-depth strategy against cyberattack, all because it greatly deters hackers in comparison to traditional networks, that are easy to attack.

Because of their non-sophistication (Traditional network) with only an initial firewall and no further preventive majors against ever-advancing changes, in the cyber world thereby creating patches in software updates. (Metivier, 2017)

Network segmentation assists in preventing sensitive data from intruders unlike the traditional flat Network with servers and workstations in the same LAN (Local Area Network). They can be physical or virtual.

Here is an example of a Network segmentation that assists to secure sensitive data and prevent intruders.

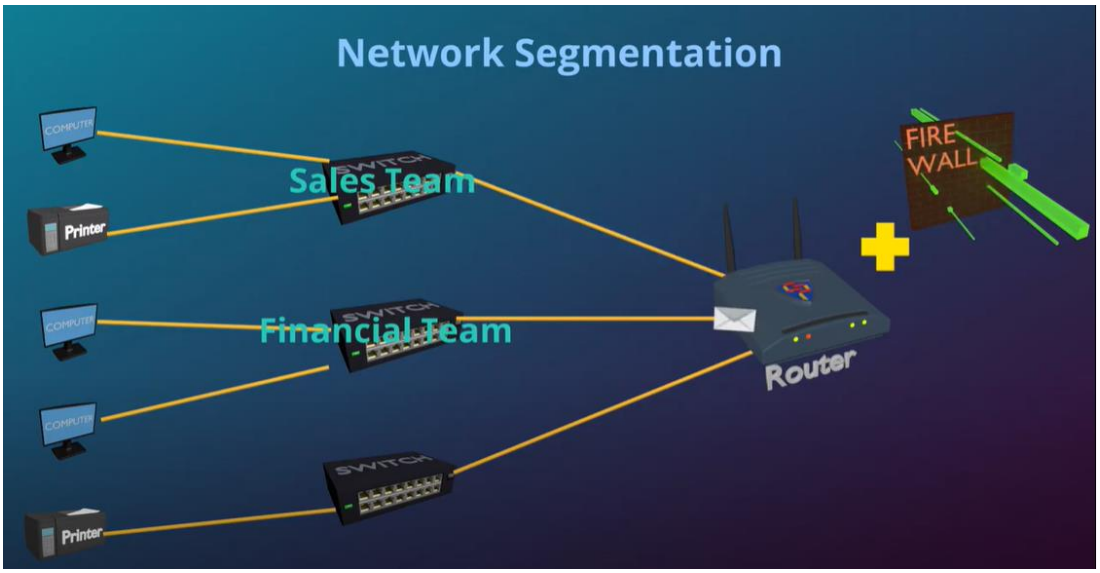


Figure 19. Network Segmentation in a Network (CyberProtex, 2019)

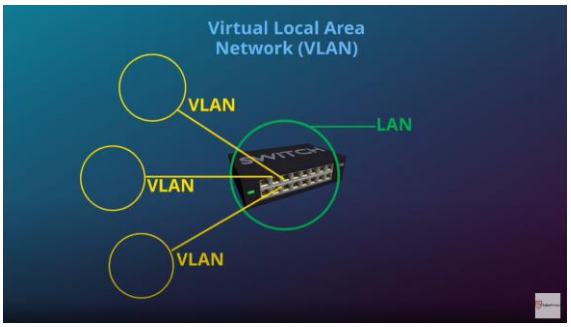


Figure 20. Virtual Local Area Network for Network Segmentation (CyberProtex, 2019)

Some of the benefits of Network segmentation are that it helps to organize the system effectively, reduces the size of the broadcast domain and improves monitoring of the Network, Better access control, and performance improvement. (Metivier, 2017)

7.8 Computer protective awareness and collaboration

The need for protective majors is required in an industry that is already facing a lot of attacks with the rapidly- growing threats on their logistics, transportation system.

These requirements are needed for multiply reasons such as the prevention of disruptive operational activities and high costs of prevention of ransomware, and other viruses, malware, that affect systems or networks. These attacks could be both locally and international in the industries which can send a ripple wave effect at large. (Slaby. R.J,2021)

In overcoming these effects and bringing the awareness to the company, is the need for protective means for slowing down the effect and aiding the awareness for ransomware, malware, and other attacks from taking fast growth and the hazard, which they tend to pose; including the reputational risk, profits, uptime, threaten in the logistical industry. Below are some of the processes and acts that are required for their prevention, namely:

Here are some of the steps that are Important as stated below:

- Employee's education is important because they are the inner circle in the cybersecurity process. This would help in managing these processes and or slowing the attacks or total prevention. According to Slaby. R.J "employees should be technically educated with the modern and up to date technologies and to be aware to be wary of the emails links which they may receive and avoidance of click on, websites that they visit as well as attachments that they would open "

- The creating of good network and security processes with better hygiene measures where the network can be segmented makes it harder for ransomware, viruses, and malware from spreading from one system to another. Thereby keeping the endpoint anti-malware software updated which would reduce or eliminate the vulnerabilities that exist in the systems been operated and applications, quickly as possible. (Slaby. R.J. 2021).

- Creating imperative systems that would institute a rigorous backup regimen by the keeping of multiple copies of business data that are critical as well as patient data locally in an offsite cloud system. These ways would assist in keeping information safer. Additionally, the inclusion of routine processes that would help in the backing up of data for full-proof defense in overcoming ransomware - is one way of resetting the system that has been compromised with initial onset attack identification on the system. (Slaby. R.J. 2021).

- The investment in safety and security network, recovery strategy is the winning way to keeping the network and minimizing risk. The keeping of backups would save the company in the time of breaching.
- The need for the renewal of outdated systems are ways to reducing the potential risk.

8 THE DHL POLICIES

The risk of cyber-crime produced to any company is enormous and the losses are large because of the great financial significance and business implications, both on the web, email. (Callo. J,2018,)

DHL as a global operational logistic company has a set of processes which, if not carefully attended to, would lead to instability in the environment as well as the lack of security for the various model of transport. (DHL).

8.1 Protective measures

Since the enormousness of threat of cybercrime is increasing, alongside the unauthorized access from external parties as well as attacks on servers, all these could bring a company to their knees or reckless behavior internally, from employees and hackers investing in becoming sophisticated, so therefore, the threats would need some protective strategy in place. (Abolhassen. F, 2017).

Some of the ways for protective strategies include:

- The assessment of risk exposure: through the identification of potential exposures that would pose risk and vulnerabilities in systems and networks. (FIATA,4)
- The adopting of technical standards like ISO/IEC 27000 series for security in the logistic industry.
- Moving from reactive to proactive ways in nipping threats before it because cybercrime attack.
- The need for effective corporate data protection in cloud computing (data storage and sharing). Cloud customer participation is required more than the cloud providers, because of their roles in adverting cybercrime. (DHL,2021)

- Prioritizing your security mailing list for an update in the patching of servers and security vulnerabilities when they are announced. (DHL,2021)

- The creation of secured passwords and regular updating for preventing hacking.

- Making sure the servers by running (SSL) secure sockets layer, which is technological standard for the keeping of secured connection using HTTPS (Hypertext Transfer Protocol Secure) (DHL,2021)
- The organization of constant staff training with new and modern technological programs and education.
- Implementation of swift security person for quick response to cyber-attack and threats.

The findings showed that the company policies have been functioning, in terms of creating a uniform level of conformity within the group by increasing awareness by keeping the workers, customers, and partners informed of the possible risk and the means to minimize them.

However, even when the Secure Socket Layer technology (SSL) helps in encrypting data during transmission, is not a guaranty that emails and other messages cannot be accessed by third parties, leading to possible threats. Therefore, it is a recommendation from the company, that confidential information is sent by post for maximum security. But there are also compensatory measures set in place, in case of data breaches and information theft (DHL,2020).

They have been able with their Data Privacy Policy from (Data protection management) in keeping information secured through awareness training, regular performance check, exchange of information in the global network.

The involvement of internal experts in the simulation of cyber crisis has assisted them in preparing ahead. This entails the inclusion and training of employees for the identification of potential compliance violations and reporting suspicion to a web application and hotlines, which has helped in protecting information and reducing the risk. The mentioned strategies have helped the company in keeping information secured (DHL 2019,45-49).

9 DISCUSSION

The research reported in this thesis contributes to the cybersecurity, importance in highlighting the impact of cybercrime to logistic companies (DHL) with potential losses in terms of financial losses, damage to infrastructure, systems, loss of company hours, reputational risk both internally with staffs and externally with partners as well as to their competitors.

The research contributes by stating the need for preventive majors and taking the lessons learned from other companies or past experiences of attacks for effective improvement of processes and preventing, re-enforcing, and precaution, in avoiding risk, threat before it becomes a huge financial cost and data loss. What my findings are is that systems can be protected through varieties means like Network Segmentation which would assist in the keeping of sensitive data secured when shared with employees or externally with shareholders or partners.

The major risk is not what one would consider a huge threat, even when systems need security and the provision of sophisticated systems but rather, employees who are the biggest focus to be informed of the cost of the risk of cybercrime to the company. Customer data and loss of trust to their partners, long-term loss of integrity, and eventually bankruptcy of the company should be made clear to employees for comprehending the effects and their consequences for active participation.

Employees are to be trained, with threat identification and the needed sophistication in handling malicious intrusion before they cause harm. The involvement of all parties in the company including partners and third parties should be given intensive notion and importance of cybersecurity. Cybersecurity is a continuous process that needs complete attention due to the increasing sophistication in the cyberworld. Another hindrance to an efficient and effective system is a lack of awareness and non-conformity in the network system and inadequate cybersecurity commitment with new patches for an effective update.

DHL is committed to making the security system continuously effective because neither the government nor the company security policies are a total defense but are initial protection to their information, infrastructural, However, the susceptibility and vulnerabilities to cybercrime are high as technology advances and the lack of awareness and lack of professional technicality.

10 CONCLUSION

The issue of cybercrime is not something that attacks only small establishments, but even huge organizations with all the security facilities, experiences in the field, risk, the threat of security, and policies. It is of great concern with every facet in companies and the world at large, with the increasing alarm of daily threats and cybercrime occurring.

I have discovered that the need for companies to involve their teams, employees, and reminding them of continuous learning.

Firstly, learning from the lessons of cybercrimes which the company has experienced, by gaining key insight into the mindset of how hackers and all the challenges their present existing security system pose or practices toward cybercrime.

The lessons would help the team/company in planning how to deal with the different cybercrimes and how they impact even the most resilience of the company's security and policies.

Since cybercrime brings with it complexities, I would comment that having a self-protective model for identifying, prevention of information theft, data, and confidential information through installed, firewalls would aid in handling initial attacks on the company system or network.

The use of network segmentation is the way I found companies to handle their network system, not only for the security of their data but also for the smooth running of processes, which would increase efficiency and trust between employees and their stakeholders.

The need for all these strategic ways for handling the company's data securely is because of their global presence and the integration of all their supply chain, which could be exposed to multiple risks and cyber activities like organized crime, terrorism, piracy, and internet crime.

Therefore, the need for corporate security for the identification of these potential security risks for analyzing them with the threat early identified their impact, evaluation and taking the appropriate action in mitigating them. (DHL,2021).

11 REFERENCES

Abolhassen, F. 2017. Cyber Security simply makes it happen: Springer international publishing. Switzerland

Accenture & Ponemon, 2019. The average cost of cybercrime by country. Accenture security.https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf [Accessed:28th April 2021].

Accenture & Ponemon, 2019. Global value at risk from the indirect & direct cyberattacks. Accenture security.https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf [Accessed:28th April 2021].

Accenture & Ponemon, 2019. The annual average cost of cybercrime by attacks. Accenture security.https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf [Accessed:28th April 2021].

Accenture & Ponemon, 2019. Cost framework of cybercrime (Internal & External) and Average cost/Internal activities expenditure. Accenture security.https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf [Accessed:28th April 2021].

Accenture & Ponemon, 2019. Security breaches and the annual cost increase of cybercrime. Accenture security.https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf [Accessed:28th April 2021].

Aghatise J,2006, 2. Cybercrime definition.https://www.researchgate.net/publication/265350281_Cybercrime_definition [Accessed:28th April 2021].

Aghatise, J. 2006. Cybercrime definition. Referred 01.06.2006.https://www.researchgate.net/publication/265350281_Cybercrime_definition [Accessed:28th April 2021].

Assignment Help4 Me. https://assignmenthelp4me.com/article-advantages-and-disadvantages-of-cybersecurity-342.html#cyber

Azeez, A. N & Osunlade, O. 2009.Approach to solving cybercrime and cybersecurity. Referred 01.08.2009.https://www.researchgate.net/publication/45865451_Approach_To_Solving_Cybercrime_And_Cybersecurity [Accessed:28th April 2021].

Ben Lutkevich. Types of malware. Security search. https://searchsecurity.techtarget.com/definition/malware [Accessed:28th April 2021].

BMBF, 2020. Referred 2020. Cybersecurity research to boost Germany's competitiveness.https://www.bmbf.de/en/cybersecurity-research-to-boost-germany-s-competitiveness-1418.html [Accessed:28th April 2021].

Brett, D. 2019. Air Cargo News. Referred 03.09.2029.https://www.aircargonews.net/airlines/theft-from-aircraft-tops-emea-cargo-crime-stats-for-q2/ [Accessed:28th April 2021].

Brockett, P., Golden, L.L & Wolman W. Enterprise Cyber Risk Management. Referred 01.04.2012.https://www.researchgate.net/publication/224830949_Enterprise_Cyber_Risk_Management [Accessed:28th April 2021].

Callon, J .2018. Cyren Security Blog. Referred 14.05.2018. https://www.cyren.com/blog/articles/cyber-pirates-targeting-logistics-and-transportation-companies [Accessed:28th April 2021].

CCNA Security cisco. https://static-course-assets.s3.amazonaws.com/CCNAS2/en/index.html#1.2.1.2 [Accessed:28th April 2021].

Check Point ,2020.https://blog.checkpoint.com/2021/01/14/brand-phishing-report-q4-2020/ [Accessed:28th April 2021].

Check Point,2020. Phishing attacks according to brands.https://blog.checkpoint.com/2021/01/14/brand-phishing-report-q4-2020/ [Accessed:28th April 2021].

Check Point, 2020. What is a cyber-attack? https://www.checkpoint.com/cyber-hub/cyber-security/what-is-cyber-attack/[Accessed:29th April 2021].

Cisco. Hacking titles. CCNA Security.https://static-course-assets.s3.amazonaws.com/CCNAS2/en/index.html#1.2.1.2 [Accessed:28th April 2021].

Clough. J, 2010. principal of cybercrime. Cambridge university press Cambridge, New York, Melbourne [Accessed:28th April 2021].

Creutzburg Reiner, 2016. Handbook of malware 2016. Referred.07.2016.https://www.researchgate.net/publication/305469492_Handbook_of_Malware_2016_-_A_Wikipedia_Book [Accessed:28th April 2021].

Cybersecurity and Cyberwar. Singer & Friedman, 2014.Oxford University Press New York

Cybersecurity and the threat to logistics.https://www.cybercitadel.com/docs/cyber-security-and-the-threat-to-logistics-a.pdf [Accessed:28th April 2021].

CyberProtex, 2019.Network Segmentation. Referred 17.06.2019.https://www.youtube.com/watch?v=6dghYSZzcF8 [Accessed:29th April 2021].

Davis, M., Bodmer, S & leMasters, A. 2010. Hacking malware & rootkits exposed: Malware and rootkits secret & solutions. New York (NY): The McGraw-Hill Companies

DHL,2019. Sustainability Report. Referred. 2019. https://www.dhl.com/content/dam/dhl/global/core/documents/pdf/sustainability-report.pdf [Accessed:12th May 2021].

DHL, 2020. Data privacy policy summary. Referred.01.06.2020. file:///C:/Users/odhomi/Downloads/dpdhl-data-privacy-policy-summary-2020-06-01.pdf [Accessed:12th May 2021].

DHL, 2021.Cybersecurity: Why ‘Password1’ is asking for trouble. Referred 09.04. 2021.https://www.dhl.com/discover/business/managing-your-business/cybersecurity

[Accessed:28th April 2021].

DHL, 2021.Resilicence Management.https://www.dpdhl.com/en/sustainability/governance/resilience-management.html [Accessed:28th April 2021].

DHL.https://www.dpdhl.com/en/sustainability/governance/resilience-management.html [Accessed:28th April 2021].

Fiata, 5. Prevention of cybercrime. https://fiata.com/fileadmin/user_upload/documents/FIATA_Best_Practice_on_Prevention_of_Cybercrime.pdf [Accessed:28th April 2021].

Fortinet, 2020.https://www.fortinet.com/de/resources/cyberglossary/trojan-horse-virus [Accessed:28th April 2021].

German dude. DHL Pack station.https://german-dude.de/blog/packstation-parcel-pickup_545/# [Accessed:28th April 2021].

German Dude. https://german-dude.de/blog/packstation-parcel-pickup_545/ [Accessed:28th April 2021].

Gone Phishing Tournament, 2020.User actions on phishing websites. Terranova security.https://terranovasecurity.com/wp-content/uploads/2021/01/GPT-2020-Report-EN-1.pdf [Accessed:28th April 2021].

Gone Phishing Tournament, 2020.Lack of phishing awareness. Terranova security.https://terranovasecurity.com/wp-content/uploads/2021/01/GPT-2020-Report-EN-1.pdf [Accessed:28th April 2021].

Gone phishing Tournament,2020, 5.https://terranovasecurity.com/wp-content/uploads/2021/01/GPT-2020-Report-EN-1.pdf [Accessed:28th April 2021].

Gordon, S & Ford, R. 2006, 1- 4. On the definition and classification of cybercrime. Referred 13.01.2006.http://index-of.es/Viruses/O/On%20the%20definition%20and%20classification%20of%20cybercrime.pdf [Accessed:28th April 2021].

Gordon, S & Ford, R. 2006. Cybercrime by type and software has been used for each of the cases. Springer-Verlag France.http://index-of.es/Viruses/O/On%20the%20definition%20and%20classification%20of%20cybercrime.pdf [Accessed:28th April 2021].

Hornetsecurity, 2020 1-7. https://www.hornetsecurity.com/data/downloads/reports/document-cybersecurity-special-logistics-en.pdf [Accessed:28th April 2021].

Hornetsecurity,2020. Ten Industrial that was under attack in 2019. Hornetsecurity.https://www.hornetsecurity.com/data/downloads/reports/document-cybersecurity-special-logistics-en.pdf [Accessed:28th April 2021].

Hornetsecurity, 2020. cybersecurity special cybercrime threatens the future of the logistics industry.https://www.hornetsecurity.com/data/downloads/reports/document-cybersecurity-special-logistics-en.pdf [Accessed:28th April 2021].

Hosgood,R.2020.Bright TALK .Referred.21.08.2020.https://www.brighttalk.com/webcast/18272/434604/how-fedex-ups-dhl-customers-were-tricked-by-an-advanced-phishing-campaign [Accessed:28th April 2021].

Humayun, M., Niazi, M., Jhanjhi, N, Alshayeb, M., & Mahmood, s 2020, 2020). Cybersecurity threat and vulnerabilities. https://www.semanticscholar.org/paper/Cyber-Security-Threats-and-Vulnerabilities%3A-A-Study-Humayun-Niazi/7fe928acf4a6868124e1f33fbe4cbac1a94eca08 [Accessed:28th April 2021].

Imperva. https://www.imperva.com/learn/application-security/insider-threats/

Imperva. Types of insider threats.https://www.imperva.com/learn/application-security/insider-threats/ [Accessed:28th April 2021].

ITU. Cybercrime 2012. ITU publication. Referred 01.09.2012, http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf?utm_source=Contextly&utm_medium=RelatedLinks&utm_campaign=AroundWeb [Accessed:28th April 2021].

Jenab, K & Moslehpour, S. 2016, 11. Cyber Security Management: A Review, https://www.researchgate.net/publication/305220294_Cyber_Security_Management_A_Review [Accessed:28th April 2021].

John Callon, 2018.Cyren Security Blog. Referred 14.05.2018,https://www.cyren.com/blog/articles/cyber-pirates-targeting-logistics-and-transportation-companies [Accessed:28th April 2021].

Lewis, J. A.2006.Cybersecurity and Critical Infrastructure Protection. Referred 01.01.2006,http://cip.management.dal.ca/publications/Cybersecurity%20and%20Critical%20Infrastructure%20Protection.pdf [Accessed:28th April 2021].

Logsign. https://www.logsign.com/blog/what-are-the-types-of-cyber-security-vulnerabilities/ [Accessed:28th April 2021].

Marco Gercke, M. 2012.Understanding cybercrime. Referred 01.09.2012,http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf?utm_source=Contextly&utm_medium=RelatedLinks&utm_campaign=AroundWeb [Accessed:28th April 2021].

McAfee.https://www.mcafee.com/enterprise/en-us/assets/executive-summaries/es-economic-impact-cybercrime.pdf [Accessed:28th April 2021].

Melendez, S, 2019. Chron. Referred 11.01.2019, https://smallbusiness.chron.com/effects-computer-hacking-organization-17975.html [Accessed:28th April 2021].

Mendel , J. 2019, 29.Economic & Business review.referred.06.2019,https://www.researchgate.net/publication/333943566_Economics_and_Business_Review_CONTENTS [Accessed:28th April 2021].

Mendel, J. 2019. direct and indirect cybersecurity attack cost. Sci-endo.https://www.researchgate.net/publication/333943566_Economics_and_Business_Review_CONTENTS [Accessed:28th April 2021].

Merriam Webster. https://www.merriam-webster.com/dictionary/hacker [Accessed:28th April 2021].

Metivier, B. 2017.The Security benefits of Network Segmentation. Referred 6.6.2017,https://www.tylercybersecurity.com/blog/the-security-benefits-of-network-segmentation

Mitra, A. 2010, 19, 64. Digital security and cyber terror and cybersecurity: Chelsea house publishing: NY (New York) [Accessed:28th April 2021].

Morchner, T. 2018.Cybercrime. Referred 20.07.2018,https://www.haz.de/Hannover/Aus-der-Stadt/Polizei-fass-Bande-von-Computerbetruegern-in-der-Region [Accessed:28th April 2021].

Munich RE, 2020.https://www.munichre.com/topics-online/en/digitalisation/cyber/cyber-insurance-risks-and-trends-2020.html [Accessed:28th April 2021].

Nair, P, 2021.Bank info security. Referred.28.01.2021,https://www.bankinfosecurity.com/phishing-campaign-spoofed-dhl-delivery-service-a-15878 [Accessed:28th April 2021].

OTORIO, 2020, 10 .Industrial Cyber impact,https://f.hubspotusercontent20.net/hubfs/8127371/Industrial%20Cybercrime%20Impact%20Report%20and%202021%20Predictions.pdf?utm_campaign=eBook%20-%20New%20Industrial%20Cybersecurity%20Strategic%20Predictions%20for%202021&utm_medium=email&_hsmi=102511626&_hsenc=p2ANqtz--n6uE_mbOXpAXmgvnU-qaMHbCTfKoBVfQDoroXZaegIOBMdpy-cXJ8ZdyYJz_5Yim4qgxTgB9UUI4fWGf2_aM08w0MyTW9GzGpxX1C_12fSFSixLM&utm_content=102511626&utm_source=hs_automation [Accessed:28th April 2021].

OTORIO. The potential threat is adversarial in the industry landscape.

OTORIO.https://f.hubspotusercontent20.net/hubfs/8127371/Industrial%20Cybercrime%20Impact%20Report%20and%202021%20Predictions.pdf?utm_campaign=eBook%20-%20New%20Industrial%20Cybersecurity%20Strategic%20Predictions%20for%202021&utm_medium=email&_hsmi=102511626&_hsenc=p2ANqtz--n6uE_mbOXpAXmgvnU-qaMHbCTfKoBVfQDoroXZaegIOBMdpy-cXJ8ZdyYJz_5Yim4qgxTgB9UUI4fWGf2_aM08w0MyTW9GzGpxX1C_12fSFSixLM&utm_content=102511626&utm_source=hs_automation [Accessed:28th April 2021].

Oxford dictionary. https://www.lexico.com/definition/vulnerability [Accessed:28th April 2021].

Ponemon Institute and Accenture, 2019, 10- 33.The cost of cybercrime: Ninth annual cost of cybercrime study,https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf [Accessed:28th April 2021].

Redscan, 2020.Referred 25.03.2020.https://www.redscan.com/news/a-guide-to-insider-threats-in-cyber-security/ [Accessed:28th April 2021].

Reuter, 2017.Referred 2.08.2017, https://gcaptain.com/corporate-earnings-feel-impacts-of-notpetya-cyber-attack/ [Accessed:28th April 2021].

Reuters. Referred 08.08,2017, https://www.reuters.com/article/deutsche-post-results-cyber-idUSL5N1KU0S5 [Accessed:28th April 2021].

Ritchie, R, 2019. Global intelligence for digital leaders. Referred. 08.2019. https://www.i-cio.com/management/insight/item/maersk-springing-back-from-a-catastrophic-cyber-attack [Accessed:28th April 2021].

Sain, H., Rao, Y.S., Panda, T.C.2012 ,202- 205.Cyber-crimes and their impacts: a review. Referred 01.012012.https://www.researchgate.net/publication/241689554_cyber-crimes_and_their_impacts_a_review1.pdf [Accessed:28th April 2021].

Saini, H., Rao, Y.S., & Panda T.C,2012. Cyber-Crimes and their Impacts: A Review. Referred 01.01.2012. https://www.researchgate.net/publication/241689554_Cyber-Crimes_and_their_Impacts_A_Review [Accessed:28th April 2021].

Schallbruch, M, M & Skierka, I.M 2018.The Organisation of Cybersecurity in Germany. Referred 01.07.2018.https://www.researchgate.net/publication/326509095_The_Organisation_of_Cybersecurity_in_Germany [Accessed:28th April 2021].

Seemma.P.S., Sundaresan &Sowmiya, M .2018. 12 Overview of Cyber Security.https://www.researchgate.net/publication/329678338_Overview_of_Cyber_Security [Accessed:28th April 2021].

Sharrock, J, 2018, 1-2. Cybersecurity and the threat to logistics. https://www.cybercitadel.com/docs/cyber-security-and-the-threat-to-logistics-a.pdf

[Accessed:28th April 2021].

Slaby, R. J, 2021.Acronis. Ransomware still threatens the transportation & logistics industry.https://www.acronis.com/en-us/articles/ransomware-logistics/ [Accessed:28th April 2021].

Smith, M. Z, Lostri, E. & Lewis, J. A, 2020, 4. The hidden costs of cybercrime. https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf [Accessed:28th April 2021].

Teimoor, R.A, 2017. Knowledge about hack and hackers. Referred.01.02.2017.https://www.researchgate.net/publication/333547044_Knowledge_about_hack_and_hackers [Accessed:28th April 2021].

Teimoor, R.A, 2017. Different types of hackers. computer institute of Sulaiman.https://www.researchgate.net/publication/333547044_Knowledge_about_hack_and_hackers [Accessed:28th April 2021].

The cost of cybercrime. Accenture & Ponemon, 2019. Referred 2019. https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf [Accessed:28th April 2021].

The Council of Europe, conversion, 2002.Referred 26.04. 2002.https://www.everycrsreport.com/reports/RS21208.html#:~:text=The%20Council%20of%20Europe's%20Convention%20on%20Cybercrime%20was%20opened%20for,Internet%20and%20other%20computer%20networks. [Accessed:28th April 2021].

Thibault, 2014. Defining Cybersecurity. Referred 10.2014.https://www.researchgate.net/publication/267631801_Defining_Cybersecurity

[Accessed:28th April 2021].

Thomas, A.J .2015. Cybersecurity.: Boca Raton (FL): CRC press

United Nation.https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html [Accessed:28th April 2021].

Urciuoli, L., Männistö, T., Hintsa, J. & Khan, T. 2013, 55–56. Supply Chain Cyber Security – Potential Threats. Referred 01.01.2013.https://www.researchgate.net/publication/274450273_Supply_Chain_Cyber_Security_-_Potential_Threats# [Accessed:28th April 2021].

Urciuoli, Männisto, Hinta & Khan, 2013. Information & Security, https://procon.bg/system/files/2904_Supply_Chain_Cyber_Security.pdf [Accessed:28th April 2021].

Vadza, K, 2011.Cybercrime and Categories, https://www.researchgate.net/publication/274652160_Cyber_Crime_its_Categories [Accessed:28th April 2021].

Warburton, 2020, 34. The reuse of a victim's data in real-time. Webroot, an OpenText Company.https://www.f5.com/content/dam/f5-labs-v2/article/articles/threats/22--2020-oct-dec/20201110_2020_phishing_report/F5Labs-2020-Phishing-and-Fraud-Report.pdf [Accessed:28th April 2021].

Warburton, 2020,10. Phishing attacks steps. Webroot, an OpenText Company.https://www.f5.com/content/dam/f5-labs-v2/article/articles/threats/22--2020-oct-dec/20201110_2020_phishing_report/F5Labs-2020-Phishing-and-Fraud-Report.pdf [Accessed:28th April 2021].

Warburton, 2020.Phishing and Fraud report. Referred.01.01.2020.https://www.f5.com/content/dam/f5-labs-v2/article/articles/threats/22--2020-oct-dec/20201110_2020_phishing_report/F5Labs-2020-Phishing-and-Fraud-Report.pdf [Accessed:28th April 2021].

Warburton, 2020.The differences between the traditional and the real-time proxy.https://www.f5.com/content/dam/f5-labs-v2/article/articles/threats/22--2020-oct-dec/20201110_2020_phishing_report/F5Labs-2020-Phishing-and-Fraud-Report.pdf [Accessed:28th April 2021].

Xantaro service integration, 2018.Referred 11.05.2018.https://www.xantaro.net/en/tech-blogs/complexity-of-multi-vector-ddos-threats/ [Accessed:28th April 2021].

Xantaro,2018. DDoS attack on Target. Xantaro service integration.https://www.xantaro.net/en/tech-blogs/complexity-of-multi-vector-ddos-threats/ [Accessed:28th April 2021].

Zurier, S. 2021,17. SC media. Referred 23.02.2021. https://www.scmagazine.com/home/security-news/phishing/hackers-hit-10000-mailboxes-in-phishing-attacks-on-fedex-and-dhl-express/ [Accessed:28th April 2021].

12 APPENDIX 1

ABBREVIATION	MEANING
BMBF	Bundesministerium für Bildung and Forschung
SMEs)	Small and Medium seized
TAPA	Transported Asset Protection Association
ISS	Incident Information Service
RBN	Russian Business Network
HTTPS	Hypertext Transfer Protocol Secure
IP	Intellectual Property
IoT	Internet Of Things
MFA CODES	Multi-Factor Authentication
DDOs	Denial of Service
DHL	Dalsey, Hillblom, and Lynn
ERP	Enterprise Resource Planning
RTTP	Real-Time Transport Protocol
CCNA	Cisco Certified Network Associate
ISO/IEC	International Organisation for Standardization
VLAN	Virtual Local Area Network
SSL	Secure Sockets Layer

13 APPENDIX 2

Cyber Risk expectation.

Figure 19. Cyber Insurance. Risks and trends 2020.Munich RE