Cybersecurity Research on the Increasing Technological Automation of Society

Danniel-Lea Trimble Kummerow

Kaplan University

Professor Chicone
IT595 Capstone

# Abstract

Cybersecurity is one of the growing research areas in requiring special attention to standardize the performance of the automated systems. Considering these systems rely on a network protocol to execute functional connectivity, they are vulnerable to espionage, hacking, unauthorized access, and security override. Other potential internet-based risks affecting the performance of the automated systems include cyber stalking, spying, and decryption of confidential data. As a result, information systems must be optimally designed to protect the organizational critical assets from exposure and compromise by securing the information system. One of the contributing factors to the increased prevalence of cyber threats is ignorance and improper resource execution. As such, this study aims to identify the key functional factors that affect security systems in automated information management and networked protocols for highly vulnerable industries such as the online retailing, artificial intelligence, and banking that count on system safety and encryption for data safety. Research needs to be conducted to come up with better ways of ensuring that the cybersecurity threats are tackled. The following research project will look at the increase of the technological automation in the society and perform a deep analysis of the causes, consequences and the solutions to cybersecurity concerns.

# Table of Contents

[Abstract 2](#_Toc509105575)

[Table of Contents 3](#_Toc509105576)

[Introduction 5](#_Toc509105577)

[Background Information 5](#_Toc509105578)

[Problem Statement 8](#_Toc509105579)

[Problem Justification 8](#_Toc509105580)

[Research Objectives 9](#_Toc509105581)

[Literature Review 10](#_Toc509105582)

[Research Theories and Principles of Cybersecurity 10](#_Toc509105583)

[Nature of Cybersecurity Threats 11](#_Toc509105584)

[Malware 12](#_Toc509105585)

[Cybersecurity Risks Trend 14](#_Toc509105586)

[Top Espionage Targeted Industries 16](#_Toc509105587)

[Banking and finance 17](#_Toc509105588)

[Healthcare 17](#_Toc509105589)

[Online Retail 18](#_Toc509105590)

[Education 18](#_Toc509105591)

[Artificial Intelligence and Cybersecurity 19](#_Toc509105592)

[Autonomous Systems 21](#_Toc509105593)

[The Internet of Things (IoT) 23](#_Toc509105594)

[Cyberattack Awareness Campaign 26](#_Toc509105595)

[Methodology 28](#_Toc509105596)

[Data Collection 28](#_Toc509105597)

[Primary data 28](#_Toc509105598)

[Reliability and Limitations of Interviewing Process in Obtaining Primary Data 33](#_Toc509105599)

[Secondary Data 33](#_Toc509105600)

[Reliability and Limitations on Ways of Obtaining Secondary Data 37](#_Toc509105601)

[Data Analysis 38](#_Toc509105602)

[Solutions to Cybersecurity Threats Based on the Literature Review and Data analysis 40](#_Toc509105603)

[Estimated Cost of Solving the Problem and Return on Investment 44](#_Toc509105604)

[Conclusions and Recommendations 46](#_Toc509105605)

[Conclusions 46](#_Toc509105606)

[Recommendations 49](#_Toc509105607)

[References 51](#_Toc509105608)

# Introduction

## Background Information

Cybersecurity is the process by which information systems (applications, data centers, databases, computers, and networks) and information itself are kept safe and protected using the necessary technological and procedural security measures. Throughout the years, an immense technological growth has been witnessed as well as the rise of the cybersecurity concerns. According to Dua and Du (2016), the level of cybersecurity warfare, on the other hand, has also been decreasing over the recent past. Due to rising technological innovations, many companies have developed modernized devices with a programmable interface without any security measures against cybersecurity threats. This lack of measures on cybersecurity threats has made it difficult to curb the growing security concerns which have doubled on a daily basis with the increase of the technological automation (Singer & Friedman, 2014).

In the contemporary era, where the basis of our normal lives has been established in a technologically automated society, it is understandable that it has become difficult to live without the constant advancements in technology. It has taken over all of our social amenities, not to mention hospitals, which we cannot live without, banks where we keep all our savings, planes that we use to fly, the cars we drive and the general infrastructure at large that runs our cities. Due the emergence of the growing automated society, cybersecurity has become a major concern due to the new threat it poses in our everyday life (McCarthy, Harnett, and McCarthy, 2014).

Cybersecurity is the control measures programmed on several devices and media channels to control information in them (Alison, 2017). Cybersecurity applies to both private and public networks and its main purpose is to safeguard computer-based services and data from any form of manipulation and unauthorized access. Due to the wide Internet connectivity, there is a backlog of information from many people and organizations which necessitates the implementation of cybersecurity measures so as to guarantee safety and privacy.

Magoni & Panisot (2001) argue that cybersecurity deals with the handling of any form of imminent danger that may be caused by people having malevolent or harmful and spiteful intent like computer viruses, malware, and spyware. These computer viruses allow a hacker to fully access information from any automated device including automated cars or airplanes and even bank ATMs. The information acquired can be used for malicious reasons which could have adverse effects to individuals, organizations, governments and also the entire society. A Trojan horse is also another threat which appears like a normal program but when executed, it turns into a virus and performs fictitious and forbidden commands which might end up corrupting the data available on the device or erasing the device’s memory.

Cybersecurity involves several steps but the most important step is being aware of the types of imminent dangers that the systems we are making are likely to pose (Mehmood, 2017). Once this has been realized, then measures and strong security systems are implemented to curb any attack on the system from happening. With all these rising issues concerning cybersecurity, it is necessary for research to be undertaken to put measures across to limit security breaches on any computer network and also in any device which has a network interface.

**Paper Structure**

The Capstone project is a research project about cybersecurity in a technological automated society. The research will look at the rise of cybersecurity threats in relation to a technological automated society and come up with solutions to mitigate these growing threats. With the increasing levels of technological advancement all over the world, there has been lack of control on the situations over rising cybersecurity concerns. Chapter one briefly gives a background statement on cybersecurity. Then it explains the research problem being tackled in the paper and justification on the same. It also highlights the general and the specific objectives of this research.

Chapter two covers the literature review. Here, the paper focuses on developing an in-depth understanding of the background information about on the effective cyber-security measures for an automated system. It is a detailed evaluation of the pre-existing secondary information sources such as scholarly articles, books, and strategic reports. Under this, it further explains the nature of cybersecurity threats, risk trends and the top espionage targeted industries by cyber-attacks. It also explains the theory behind Artificial Intelligence and Autonomous systems and how they have led into a rise in the cybersecurity threats.

Chapter three covers data collection, analysis, and solutions to the growing threat on cybersecurity. In this chapter, the type of data collected plus their methods of collection, as well as their validity, reliability and limitations, are also explained in detail. A deep data analysis is also done so as to ensure that a solid solution to the problem is obtained. The estimated cost in solving the problem has also been highlighted as well as the return on investment. All these have been done depending on the governmental and organizational basis. Chapter four focuses on the conclusions and recommendations based on the literature review as well as the data analysis done on the data collected in chapter three.

## Problem Statement

With the advancement of technology all over the world, there are an increase on cybersecurity concerns. Cybersecurity has now become an important aspect to consider in the new technological era. The cybersecurity scope is increasing on a daily basis which makes it a growing concern for companies manufacturing new technologies to look in to the complex issue of security. Security to them comes second whereas it should have been the first thing before they introduce the technology onto the market (Rajeyyagari and Alotaibi, 2018). Globally, trends show that the levels of cybersecurity concerns have risen by 39% within the last two decades and it is predicted to double in the next decade coming considering the high levels of technology growth (Rajeyyagari and Alotaibi, 2018). This has therefore posed a great problem and danger to the computer-based world of information and something needs to be done.

The problem statement will be deeply expounded using data based on the trends and the levels of technological scope. Using tables, graphs, several personal professional views, as well as principles and theory related to cybersecurity science, will be used to relay the problem we are facing, as far as cybersecurity is concerned.

## Problem Justification

 For the last decade, technological advancements have been doubling on an annual basis (Ted, 2014). This is the same case to cybersecurity threats which goes hand in hand with the advancements and it cannot be easily controlled. Many governments all over the world including the United States, China, Japan, India, Australia, United Kingdom, Germany, Mexico and South Africa among others have been putting in place several measures to ensure that awareness about cybersecurity threats is vastly spread (Dua and Du 2016). The expensive technology has seen businesses and institutions invest significantly in cybercrime prevention and security sustaining measures. To generate information and pave way for continued research, authorities have extended efforts to provide cybersecurity training and services at tertiary and vocational institutions around the world (Ted, 2014). However, with all these efforts the cybercrime threats have not dropped not even by a single percent, but rather they are increasing (Rajeyyagari and Alotaibi, 2018).

Therefore, the need for research in this area is undoubtedly clear. Research needs to be carried out to come up with better solutions to be implemented by the various governments all over the world. The solutions need to be realistic and should be able to take the shortest time in terms of the payback period, as well as, return on investment. It will also be easy to conduct research in this area since many companies know of the threats.

Many cybersecurity professionals have even opened their firms to offer cybersecurity services to other companies since they need them (Dua and Du 2016). These professionals can be interviewed, and qualitative as well as quantitative data can be easily retrieved from them. This data from several professionals can be used to come up with solutions best for limiting cybersecurity threats.

## Research Objectives

**General objective**

1. To address the critical security issues underlying automated cyber networks and information systems.

**Specific Objectives**

1. To identify potential cyber risks in information and network systems.
2. To come up with a solution to limiting cybersecurity threats in Artificial Intelligence (AI) and autonomous machinery based on analytical and critical thinking analysis of the qualitative and quantitative data obtained during the research process.

# Literature Review

This chapter will look into the evaluation of theories, frameworks, principles and the best practices related to cybersecurity science and technology by reviewing and accessing the recent cybersecurity literature and industry publications.

## Research Theories and Principles of Cybersecurity

The basic theories, frameworks, as well as the principles and fundamentals of cybersecurity, will enable us to come up with various solutions on limiting the problem. We need to understand the nature of the threats and identify the most targeted areas and how vulnerable they are. Then determine also how the new technologies like Artificial Intelligence (AI), which means the ability of a computer to carry out tasks associated with intelligent human beings, has been of help to cybersecurity or has been promoting cybersecurity threats and if so, on which percentage level. This way, we can be able to understand how today’s technology is operating, hence easier to identify the vulnerabilities which will eventually drive us into obtaining better solutions to limiting cybersecurity threats.

## Nature of Cybersecurity Threats

Due to the rate of technological growth, in order for us to get the glimpse of how our systems became vulnerable to cybercrime, it is important to know first the nature of threats and their exploitations in as far as the technological systems are concerned. According to Mankiw Derek who is the Global Security Strategist of Fortinet Solutions International, he argues that there are more than five hundred thousand attacks in the cyberspace every minute. This indicates that with the expanding cyberspace, there are thousands of attacks every day making user’s information to be vulnerable. (Turkina, 2018). The shows how the absence of cybersecurity exposes a lot of data and private information to unauthorized access.

Jasmine (2017) argues that the only reason why our technological systems are vulnerable in the first place is the issue of trust. Since the inception stage of the Internet, it was not designed with security threat in mind for the future. Currently, more things are connected to the Internet than people, this exponentially expands the attack surface for hackers. This can be illustrated by companies which manufacture machines, wearables, cars, airplanes, smartphones and any other device with a network interface in them and do not have the security protocols in all of their design scopes (Dua and Du 2016). With the limited scopes they have, it is not often designed to keep up with the increasing threat trends. This means that even with a lot of awareness in today’s world, you can still go to the shop and buy a device like a smartphone with no security measure against malware and viruses at all. A recent study showed that 70 percent of Internet of Things (IoT) devices contain critical vulnerabilities (Jasmine, 2017). Further research into this will identify and help come up with better ways to implement the security-focused design which is lacking. This will remove the idea of trust from the ancient technological stereotypes and ensure that our systems are much safer against vulnerabilities than they are now.

According to a case study research by Choo (2001), cybercrime comes in many different ways including which mainly include Distributed Denial of Service (DDoS) attacks done on websites in form of destruction, manipulation, extortion, blackmail, and theft among others. Various ways in which this is done is through certain tools like physical devices alteration, social engineering, and malware which is the most used According to Peng, (2016) Malware is responsible for over 90% of the total cybersecurity threats all over the world.

## Malware

Malware is the leading cybersecurity threat tool used all over the world (Jasmine, 2017). It is just like a normal program which skims through the Internet finding vulnerabilities in systems. When malware is downloaded, it turns into a malicious software by decrypting itself, then it accesses all the personal data by monitoring access activities of the user. According to McCrohan, Engel & Harvey (2010), they expound that there are several forms of malware performing different functions.

**Spyware;** this is the type of malware whose function is to monitor access data and takes the needed data to the hacker (Jasmine, 2017).

**Ransomware;** this malware blackmails the user of the device by locking the user from the reach of their data. Then the device is unlocked until the user pays a certain amount of money as ransom. According to Robin Harvey, a professional cybersecurity analyst, the use of Ransomware has turned into a big global business for hackers with an average hacker making over $7 million on an annual basis.

**Viruses;** these are codes which are malicious in nature and they stick themselves onto a program. Then it runs the same program by replicating what the user is doing (Jasmine, 2017).

**Worm;** According to Jasmine (2017), this is a type of malware which does not depend on any executable file or program to maneuver through the system like a virus. Rather, and without any user’s help, it duplicates itself by the use of any service which may be available on the computer. A worm usually enables a hacker to have access to the system. It then replicates multiple times and at a faster rate each turn, which eventually takes up a lot of memory space of the server until the server stops working due to the small memory space available. The website will then go down with all the information in it.

**Trojan;** is commonlyknown as Trojan horse. It is a type of malware which always appear legit but once installed and initiated in a computer or any device with a network interface in it, it immediately creates a way for the hackers to access your data (Jasmine, 2017).

**Scareware;** this is a type of malware which disguises the user by giving him or her some warning-like messages in form of reminders and popups. Once the user clicks on them, they automatically get downloaded (Jasmine, 2017).

Malware is used everywhere even in Automated Teller Machines to get away with the details of the user (McCrohan et al., 2010). The only basic and easiest way to protect several systems against malware, however, is by installing firewalls and ensuring that the systems are always up to date. In this modern world, anything that can be technologically controlled is vulnerable to cybersecurity threat. Over the past five years, there have been many cases of cybercrime upon major social and basic amenities (Ted, 2014).

In the United States alone, some of the cases reported according to Steve (2018), ranges from medical services where ‘hackers sent fatal dose to pumps which transported drugs in a pharmaceutical manufacturing plant in California’. There was also a case involving cars where ‘three jeeps crashed on a highway leaving several injured and one casualty in Cleveland, Ohio’. Other cases were about toys where ‘Barbie Wi-Fi was hijacked by hackers in order to investigate and spy on small kids’ and also some water supply systems where ‘on 28th October 2016, some parts of Brooklyn in New York State as well as Manhattan lacked water supply for two days after hackers hacked into the controls of water supply at the main intake’.

This shows how much the world will be at its highest risk for cybersecurity threats in the near future. Thorough research in this area is needed to come up with the necessary system-security solutions that will save our world from the losses it is undergoing due to the lack of cybersecurity and cybersecurity research. Research shows that over $650 billion is lost globally due to cybersecurity threats (Naveen, 2017). Some of these amounts could be saved and the economy improved only if we come up with cheaper and better ways to curb cybersecurity threats.

## Cybersecurity Risks Trend

About two decades ago, there were no such things as cybersecurity risks. People still trusted technology, but as time went by, cases about the security threats started rising. The first computer worm was created and introduced by Morris Robert in 1989. The worm was like a virus which had the ability to self-propagate so rapidly and aggressively causing a large percentage of the Internet to close (Reveron, 2012). This worm set the state for hackers to realize that they can create a virus and shut down a computer or steal some files.

In the 1990’s there was the creation of many computer viruses. The famous ones being ILOVEYOU and Melissa viruses which caused the shutdown of many PC’s and leaving others infected (Steve, 2018). It was during the late 90’s specifically in 1997 when the first antivirus was created. People had realized that it was not safe anymore and they had to create something to counterattack the viruses and worms.

In the late 2000’s hackers advancing their skills and started stealing information from debit and credit cards. A famous case scenario is when information and data was stolen from over 47million payment cards by Gonzalez Albert in a retail store in the United States (Grupta, Agrawal et al, 2016). Since then, there has been a tremendous growth in terms of cybersecurity attacks. This has been attributed by the growing technology which is estimated to be doubling on an annual basis and it is expected to triple in the next two decades.

The invention of Automatic or Artificial Intelligence, has also brought in new technological cyber threats with it. Grupta et al. (2016), argue that AI is used in making self-driven cars as well as robots working in various warehouses and manufacturing stores. An example of this is the Amazon Inc.’s 45,000 robots working at over 50 warehouses around the United States. As far as these robots making work easier, faster and simpler, hacking into devices and machines using the Artificial Intelligence technology is very easy since it has many devices with a network interface in them, for example, a Bluetooth or an ECU usually found in self-driven cars.

With these increasing trends, Naveen (2017) predicts that it will become very costly to curb cybersecurity threats, especially in the near future. A decade ago, the cybercrime damage cost was around $200 billion on an annual basis. A decade later in the year 2017, cybercrime damage cost is averaging to almost $1 trillion. It is forecasted that in the next five years, the damage cost will increase by 600%, going over to $7 trillion. The global spending on cyber security services and products is expected to rise exponentially from the recent $90 billion to over $1 trillion in the next five years (McCrohan et al., 2010).

Moreover, with the increase in population as well as technology, Steve (2018) predicts that by the year 2023, there will be over 6 billion Internet users from the 2.1 billion in 2015 and 3.9 billion in 2017 (p. 32). With these figures, cyberattacks will increase, and based on the recent trends, 6 billion people will have a high risk for cybersecurity threat. Global damage costs on ransomware are as well predicted to increase immensely in the next five years to come from $400 million to over $15 billion in 2022 (Steve, 2018, p. 33).

With all this information, we can clearly see that we are heading somewhere not so good, as far as cybersecurity is concerned. This is happening due to the lack of security measures put in place by the manufacturing companies of various devices having a network interface in them (Jasmine, 2017). Research is, therefore, necessary to ensure that a better solution to this problem is obtained including best policies that can be implemented by the government to ensure reduction on these cybersecurity threats and risks.

## Top Espionage Targeted Industries

With this modern age of technological advancements, many companies, as well as organizations, face a continuous barrage of cyber-attacks (Jasmine, 2017). It does not matter whether it is a technical or a non-technical organization, any industry is undeniably at a great risk, especially with the data and the forecasts seen above. It is the high time that industries realize the stark reality of cybersecurity threats (Gao, 2011). Attackers who are highly skilled can perform limitlessly in as far as cybersecurity threats are concerned (Gao, 2011). A testament to this fact is when 76% of the internet itself got disrupted in August 2016 after the attack on the DDoS by highly skilled hackers (Jasmine, 2017). Having mentioned this, there are several industries and organizations operating under them which are the most target by cybersecurity attackers. In the descending order of attacks, they include banking and finance sector, healthcare, online retail, education, and manufacturing. This is according to a report published in August 2017 by Global Sign Internet Group.

### Banking and finance

Hackers have found the finance and banking industry to be by far the ideal target (Gao, 2011). This is because companies in this industry have got all the vital information that hackers need. These include private financial information, home addresses, bank account numbers, and identities of their clients among others. According to a survey conducted in January 2017, banks encounter on average around 90 serious breach attempts annually and out of these attempts, 39% of them become successful in taking vital information of their clients (Turkina, 2018).

### Healthcare

This is also another industry which carries with it a heavy load of sensitive information. Healthcare industry as well has got intensive information. This information that is targeted by hackers includes financial details, physical conditions of the patients, home addresses, and their full names. All these information is available since all organizations working in the healthcare industry like hospitals, for example, have full access to the intensive healthcare records electronically (Turkina, 2018). These records contain all the above information.

The recent ransomware attack called WannaCry ruined all the health records completely. The devastation brought the operations of Britain’s National Health Service (BNHS) to a standstill and the care of the patients was highly impacted.

More of this will be seen in chapter three under data collection.

### Online Retail

Due to the fact that these online retail platforms have got valuable information about their customers in their databases, it has made them very vulnerable to attacks (Turkina, 2018). Attackers are interested in this information. Moreover, retail organizations are more open to cyber-attacks when they move their services and products on an online basis. Hackers and attackers also have a great opportunity for online retailing services as they have a high number of employees and customers who are distributed all over the world making the attack surface to be distributed widely (Turkina, 2018).

In 2015, there was an attack on a home development retail company called Home Depot. The company had to pay over $20 million to all the customers in the United States who had been affected by the attack. At least the company had money to pay the affected customers otherwise it could have been a different case if a small company had been attacked. Both the company and the customers would have suffered a huge loss.

### Education

As of the year 2010, Turkina (2018) argues that the education sector had not been a big target to the attackers. Things have however changed in the recent past. Hackers have started targeting all the organizations working in the education industry like colleges, universities, technical institutions and even medical institutions among others due to the worthy academic research they produce. An example of this kind of attack was witnessed in an Engineering College in China in 2005, where the attack caused a huge compromise on records of over 19,000 people. Other examples of industries that are still under high target include the manufacturing, transportation, real estate as well as utilities (Turkina, 2018).

The table below shows the trends of attacks on various industries since the year 2007 when the age of cybersecurity attacks came into place up to 2017 (Jasmine 2017).

*Figure 1: A Graph showing the trends of the most targeted industries globally*

### Artificial Intelligence and Cybersecurity

Artificial intelligence is the theory where machines display intelligence known as machine intelligence, which is in contrast with that intelligence displayed by animals or human beings called natural intelligence (Passeri, 2017). In the recent past, since the development of the Human-Machine Interface (HMI), it has opened new technological doors for the development of machines aided by artificial intelligence. With Artificial Intelligence, (AI), it is possible for machines nowadays to have the ability to perform tasks usually performed by human beings, adjust to new inputs and learn from their past experiences and adjust to the same. Some of the examples include the driverless cars and computers which can play chess just like human beings.

Based on a 2017 report by Webroot Inc, where an American corporation is providing businesses and consumers with security against cybersecurity threats, it argued that artificial intelligence posed both negative and positive impacts in as far as cybersecurity is concerned. The United States was among the first adopters of AI. More than 88% of the American companies incorporates AI in their operation as well as against cybersecurity threats (Passeri, 2017). The report also says that over 92% of professionals in cybersecurity are concerned that some of the workers working for these AI companies will turn against them by using the AI technology in cyber-attacks. This will be the worst cyber-attack as it cannot be detected with ease of the current cyber-attacks such as malware. They are also vastly sophisticated. Artificial intelligence as well can be of great use in curbing cybersecurity attacks. Artificial intelligence uses Machine Learning (ML) algorithms which detects any form of cybersecurity threat easily (Passeri, 2017; Naveen, 2017).

However, due to AI, there has been an increase in the levels of cybersecurity threats and risks. For example, take the case of self-driving cars. Self-driving cars have many devices on board having a network interface. These include USBs, Bluetooth, BRX-based receiver, Remote key, Airbag ECU, Vehicle access ECU system, engine and transmission ECU, Interior and Exterior lighting system ECU, TPMS, ADAS system ECU and a Passive key entry among other onboard devices like a GPS tracker (Yan, Qian, Sharif, & Tipper, 2018). All these features and devices found in a self-driven car have a network interface which can be easily hacked using a laptop or even a smartphone. All the cars have been designed without any security concern in mind. They do not have any form of security against any form of cybersecurity risk like malware (Yan, Qian, Sharif, & Tipper, 2018).

The other case applies to the automated teller machines (ATMs). They have been created without any form of security measure against any cybersecurity threat. As seen earlier, there have been many cases where hackers hack into these ATMs and steal personal information of the users (Yan et al., 2018). Therefore, there is a need for research to come up with better solutions to curb new cybersecurity attacks caused by Artificial Intelligence technology. These solutions could include policies set by governments or ISP providers. These solutions are going to be explored in chapter three.

### Autonomous Systems

As technology goes into being part of our lives, people have started integrating with it rather than operating it. This is a fact with autonomous systems as they have been made in such a manner that they have turned out to be part of us and is second nature to many through the blend they bring to the society. An autonomous system in technological perspective is basically a system in which many systems are collected under one network then supervised and managed by a single entity (Alison, 2017). The system integrates transport networks like the case of self-driven cars, critical infrastructure like power networks and payment systems, points of sale and ATMs, and also the wearables among others. Having integrated all these essential facilities under one network, it has then become a target priority for hackers as it holds vital information about people just as we had seen earlier (Yan, Qian, Sharif, & Tipper, 2018).

Self-driven cars are a good example of systems taking over the limelight of systems being autonomous. There are several features and devices in a driverless car which are all connected and controlled from one point inside the car. These include USBs, Bluetooth, BRX-based receiver, Remote key, Airbag ECU, Vehicle access ECU system, engine and transmission ECU, Interior and Exterior lighting system ECU, TPMS, ADAS system ECU and a Passive key entry among other onboard devices like a GPS tracker (Yan et al., 2018). There have been several cases reported however showing how these cars are very weak in terms of being vulnerable to cybersecurity threats (Grupta, Agrawal, and Yamaguchi 2016),

A case study report carried out by Grupta, Agrawal, and Yamaguchi (2016), Over 1.7 million Cherokees Jeep in 2015 were recalled by attackers that they were able to take over the control of the cars remotely through the sound system in the cars by the use of the onboard Bluetooth in the Mp3 player. Other cases were as well reported last year on 2017 August demonstrating how Fiat, Audi, Toyota, BMW and Mercedes self-driven cars did not have any form of security feature at all that protected it from any form of cybersecurity threat. According to an online blog by Technopedia, data forecast shows that there will be over 250 million autonomous cars on the highway by 2020 (Grupta et al., 2016). Further research is needed to improve the policies and solutions to cyber threats to reduce cases of cyber-attacks against these autonomous systems.

In the case of Points of sale and ATMs, in the past, since the only banks were being protected against fraudsters, they used the RFID chips to protect their systems. However, with autonomy in place now, complex cases like skimming where information in a debit or credit card can be read and transferred directly during its operation in an ATM machine (Jasmine, 2017). This is because ATMs were created without any security risk in mind. Therefore, to protect them against cyber-attacks, research needs to be conducted so as to find out better solutions to protect the same. According to Robbins Chuck, CEO of Cisco, the autonomous system market is expected to be worth $10 trillion by 2022 (Turkina, 2018). This will then make it be a target for the attackers. New research needs to be done to come up with solutions and policies to curb the same against any form of cybersecurity threat.

### The Internet of Things (IoT)

Having discussed Autonomous systems, the IoT is yet another form of many systems being interconnected together. According to Mehmood (2017), Internet of things is basically the interconnection of many products that can be seen and those that cannot be seen. They may include products like Laptops, Smartphones, Smart watches, wearables, Smart TVs, webcams, smart cameras among other tangible products with a programmable interface in them.

Other products which you cannot see including actuators, sensors, electronics and software which is built into everything including your fridge, television, homes like technology to switch on lights when you enter the doo, technology to unlock the doors; technology to allow the traffic lights and the cars to communicate with each other and prevent further accidents; the technology to allow cities all over the world though hundreds of thousands of sensors communicating with each other to control water supplies, manage distribution of energy, and regulate air quality in real time (Grupta et al., 2016). All these have been made possible simply because of the tremendous technological growth which cannot be controlled.

According to a research conducted by Hypercom Consortium and River Clyde Homes in the United Kingdom (UK), 25% of the biggest cities in the world will be using the IoT technology by the year 2030. The technology has been tested by the firms in the United Kingdom in two cities already and it is working, they can monitor communal lighting, smoke detection, lift maintenance, potential gas leaks, and carbon monoxide levels (Jang-Jaccard et al., 2014). All these, provide a real-time feedback to the server rooms on the state of the city as they communicate to each other. The feedback is then used to minimize safety and health risks. “The Internet of things can monitor everything from local weather to temperature and all the way to carbon monoxide levels among other things” (Elon, 2018).

However, this is just the beginning of IoT. In the near future, Alison (2017) argues that it is able to engulf a lot more products. These includes feedback sensors for rescue and search emergencies, field threat detection devices for the army, monitoring environmental waste, animal transponders on farm, food pathogens, as well as implants on the heart, kidney, brain and liver among others. This is therefore to mean that the potential upon which IoT can go is limitless and in the future, everything will be interconnected.

A research carried out by a security firm in the United States showed that the IoT industry is growing at an average rate of 12.7% on an annual basis. According to Steve (2018) and Cisco’s CEO, Robbin Chuck, the IoT industry alone is expected to reach a tremendous worth of over $US22 billion by 2022 on a global basis. This therefore means that in the near future, the level of interconnectivity among devices and various products will mean that in everything that a person do or go, devices will be sharing data and communicating at the same time.

However, in as far as cybersecurity is concerned, the IoT, no matter how amazing it may seem, it is one of the biggest and rising concern. Due to the interconnectivity of devices with programmable interfaces between them puts the society into a great risk. The number of connected devices and products by 2020 is expected to reach 200 billion and over 1 trillion by 2035 according to data forecast researched by Naveen (2017).

Due to the interconnectivity and the ability of the devices to send and receive data while at the same time be able to communicate with each other poses a great danger to cybersecurity threat (Mahmood, 2017). Hackers and attackers will just have to find a loop hole or a weaker point of the entire link for example use a Bluetooth in a fridge at home then access the mobile phone then the laptop and slowly even access important government files and other huge firms. Therefore, with the technological growth, it is important to conduct a research in order to identify the real problem and ways of solving it in as far as cybersecurity is concerned.

According to Jasmine (2017), consider the following line graph showing the trends in level of technological growth, growth of IoT industry and the levels of threats over a period of ten years starting from 2018 to 2028.

*Figre 2: A graph: showing the forecasted trends of technological growth, IoT industry growth and cybersecurity threats growth from 2018 to 2028*

From the graph, we can clearly see how technology is expected to grow tremendously as well as the industry of Internet of Things (IoT). When this happen, the levels of cybersecurity threats also rise exponentially following the industry’s growth. This therefore means that it will be hard to control the growth rate and this calls for a research to be taken in order to come up with a better solution which will help curb the rising cybersecurity attacks.

## Cyberattack Awareness Campaign

With all the literature review vividly explained above, cyberattacks awareness campaign is an important tool and feature against cybercrime that should be enhanced. Cyberattacks awareness campaigns are basically simple initiatives taken by the government or any other concerned non-governmental organization to make people be aware of the existence of the cybersecurity threats and their consequences. This is usually done through posters, billboards, seminars, conferences and educational talks in various learning institutions.

However, in as far as this method seem to be the way to go, according to Passeri (2017), the levels of cyberattacks awareness campaigns have drastically dropped as compared to the rate of technological growth as well as the number of cybersecurity attacks on an annual basis. This has led to the increased cybersecurity attacks. Consider the following line graph showing the annual trends of technological growth, cyberattacks awareness campaigns and the levels of cybersecurity attacks since the year 2010 to the year 2017 on a global basis.

*Graph: Annual Trends on Technological growth rates, cyberattacks awareness campaigns and cybersecurity attacks since 2010 to 2017*

From the line graph above, we can see that the rate of technology has been on the rise since the year 2010 and it exponentially increased till 2017. To be precise, technological growth cannot be controlled. We can as well see that the level of cybersecurity attacks has been on the rise proportionally to the technological growth. However, since the year 2014 when the levels of cyberattacks awareness dropped, the levels of cybersecurity attacks also rose exponentially than before. This therefore tells us how important awareness campaigns are important in as far as cybersecurity is concerned. This calls for serious research to be taken, to curb the immense problems of the loss control over the governance of cybersecurity, as it concerns today’s increasing high levels of technological expansions.

# Methodology

## Data Collection

To actualize this research process, data was collected through both online and offline sources, such as journals, textbooks, and interviews conducted via from others who have interviewed top technological companies. Data was collected to show the trends of global spending on cybersecurity.

The bar graph below shows the estimated spending on global cybersecurity since 2000 to 2025:

**Data:**
The data was obtained from online library sources, government sources, corporate filings, Annual reports from major world service providers, and reliable technological websites. Both qualitative and quantitative data were obtained from secondary sources. However, qualitative data have been explained in the literature review in chapter two. The following is the quantitative data obtained from the sources.

According to Information Security Timelines and Statistics report of 2017, there has been an increase in cybercrime in 2017 as compared to 2016 (Jasmine, 2017). Moreover, hacktivism has risen charts as well as cyber espionage but a decrease in cyberwarfare and awareness (Mehmood, 2017). The following pie-charts show the trend.

*Pie-Chart 2: Trends and Motivations behind Attacks*

Alison (2017) argues that malware has been the major form of attacks technique since the recent past. It has been increasing exponentially throughout the years. Other techniques include account hacking, targeted attack, DDoS, vulnerability, Defacement, advertising, DNS hijacking, SQLI, and unknown techniques among others (Alison, 2017). Since malware is the easiest ways to gain access to personal files just as explained earlier in literature review back in chapter two, it is the reason why it is the leading technique.

The following bar graph shows the top ten attack techniques and their trending percentages since 2015 to 2017.

*Graph 3: Top Ten Attack Techniques 2015 vs 2016 vs 2017*

There has been an increase in malware. According to the Computer Crime and Intellectual Property Section (CCIPS) (2018), it reports that in the third quarter of 2017 alone, more than 23 million new samples of malware were captured. This means an average of 300, 000 per day. Among these, ransomware has been the highest. On a daily basis, more than 11, 000 ransomware attacks are occurring on a daily basis. This is a 280% increase over 4, 000 attacks in 2016 (Naveen, 2017).

According to a 2017 report from the FBI, it reported that phishing and ransomware worked together. Ransomware that was contained in phished emails increased to 98.5% during the third quarter of 2017 up from 93% in third quarter of 2016 (Steve, 2018). According to a print out by Kaspersky (2017), it reported that more than 80% of email users are aware of the ransomware risks but they still click on them. In a case study carried out by Gmail, it showed that more users actually clicked on the ransomware links than those who admit that they did.

It is also recorded that 55% of all the organizations which are victims of successful cyber-attacks in the year 2016 did not make any changes in 2017 in as far as their cybersecurity is concerned (Alison, 2017). The same case applies to their budgets. According to a case study report carried out by Barkly Security, it recorded that 45% of the same organizations do not change their budgets in 2017 and 8% reduced their budgets. 37%, however, were willing to increase their budgets but small amount went to security and 10% were not sure of anything (Mehmood, 2017). Consider the following pie charts for the two case scenarios so as to visualize the picture.

*Pie-Chart 3: Security plans and Budget Forecast for the affected organizations*

It is also reported that hackers are targeting Android as a platform for attacking Windows. This is because it is much easier to breach Android since it does not have any form of security measure to protect it from any form of cyber security attack. According to Swimland Security (2017) which is an online blog, it records that more than 82% of victims whose data have been breached, do not have any system in place to protect their data. Instead, they rely on a third-party to inform them that there is a breach. This takes a long time of up to 160 days for them to realize that they have been compromised. However, if they had a security system of their own, this time could be reduced to 12 days.

According to a 2017 report produced by Microsoft, it showed that the potential cost of the attacks on cybersecurity has been increasing exponentially since 2007. In 2017, it has reached a whopping $US 765 billion (Naveen, 2017). As per this data, $3.8 million on average, goes to data breach cost per company. This is actually a lot of money which demonstrates the need for action in curbing cybersecurity threats. Consider the line graph below showing the trend between the cybersecurity threats and the level of technological growth since the start of the 21st century.

*Graph 4: Trend of Technological growth and Cybersecurity Threats*

### Reliability and Limitations on Ways of Obtaining Secondary Data

The importance of using an integration of primary and secondary data is to create room for comparison of facts and figures. This allowed for rigor and validity sustenance by cross-checking the precision, reproducibility, and repeatability of findings. It is notable that literature review’s secondary data was selected via keyword search to ensure relevance of the selected sources to the study objectives and topic. Through library reading, an in-depth understanding of the background of the topic was developed to guide hypothesis formulation.

The major limitation of the method used in obtaining secondary data is that they are hard to find. Most of them even need someone to be a member first. Online libraries like the Wiley requires one to pay a small fee so that you can access their research materials. Documents sometimes may as well lack legitimacy and authenticity.

## Data Analysis

From the data, we have seen that trust in technology has grown in a larger perspective to a point where 85% of companies all over the world produce products and services like smartphones, cars, airplanes, banking services, ATMs, home appliances and electronics, and anything that has a user interface between them without any form of security against cybersecurity threats and attacks (Turkina, 2018). This has been brought about by technological advancements. This way, it has become easy for attackers to attack various infrastructure ranging from power lines, banking systems, transport and water systems among others. The attack on the infrastructure has caused a lot of losses as we had seen in the literature review.

Cybersecurity industry is expected to reach $3 trillion by 2025, which means that there will be an increase in dangers associated with cybersecurity (Grupta et al., 2016). The governments will also spend a lot more money in curbing cybersecurity attacks rather than saving some. The increase in ransomware has led to loses and increased costs in many industries. Also, the fact that the United States has got the highest percentage in terms of cybersecurity attacks which means that industries situated in the United States stand a high chance of being attacked. When this happens, the company will suffer loses and so will the economy of the United States.

From the data, the fact that there has been a tremendous increase in cybercrime from 68% in the third quarter of 2016 to 76% in the third quarter of 2017, and at the same time the during the same time period, cyber warfare has dropped from 6% to 2% is a serious problem (Yan et al., 2017). This means that the fight against cybersecurity threats and cybersecurity crime has gone down and at the same time giving room for cybercrime to increase.

Furthermore, due to technology growth, increase in the production of devices having a network interface between them but without any form of security system against any form of cybersecurity threat has led to the loss of control in limiting cyberattacks (Naveen, 2017). This is the reason there is a double increase in cyber-attacks annually. This is also the reason why Android has become the second targeted operating system after windows. This means that more than 75% of all smartphones, tablets, iPads, and any device operating using Android globally are at a greater risk of getting attacked since they do not have any form of security protection against cyber-attacks. This is as well the reason as to why Naveen (2017) reports that malware has increased exponentially since 2015 up to 2017.

The fact that a higher percentage of around 55% of all the organizations which are victims of cyberattack have no plans for any changes to their security plans is devastating (Alison, 2017). This means that there will always be a loss in the grip of curbing cyberattacks and cybercrime at large. This will also mean that the levels of cybercrime will always increase on an annual basis without any change on the same since none of the victims are trying to come up with a better solution to improve their security plans and ensure that cybercrime is curbed.

From the data above, it showed that around 45% of organizations which are victims of cyber-attacks display no change at all in their budgets in as far as cybersecurity threats are concerned (Mehmood, 2017). This means that there will be no extra funds to curb what had happened to them earlier and so these companies will continue to experience attacks annually. They also do not have funds to carry out research and come up with better solutions towards security in as far as cybersecurity threats are concerned. This has led to an increase to the cybersecurity problems due to the lack of comprehensive research that would provide solutions to the problems.

Based on the analysis, we can clearly see that with the rising edge of technology and the ignorance of the existence of cybersecurity threats has led to an increased cybercrime rate. This has then led to the loss of the grip in ensuring that cybersecurity threats are curbed. A solution, therefore, based on research needs to be proposed in order to deal with the emerging crisis. It may be several solutions since one solution alone cannot deal with the cybersecurity problem.

## Solutions to Cybersecurity Threats Based on the Literature Review and Data analysis

In order to propose a solution to the cybersecurity problem based on the data obtained and analysis of the same, we have to understand that in cybersecurity, there are solutions performed by individuals at personal levels, then those by companies and organizations under various industries and then those affected by the state and the federal government. We have seen from the data that the highest level of cyber security attack technique is malware. As discussed in the literature review, malware is basically any form of computer virus be its Trojan horse, worms, ransomware, spyware, and scareware among others. In order to curb this, even without the consent of the manufacturer, according to Gao (2011), Raveron (2012) and Passeri (2017), we need to protect all our devices against any form of malware using the following ways;

1. Installing reputable anti-virus software on all computers including laptops, PCs and all the servers.
2. Updating the anti-virus on a routine basis. Companies and organizations should pass a policy not allowing any computer without an updated anti-virus to be connected to a network.
3. Ensure that there is a firewall employed to ensure network protection.
4. All Internet downloads should be scanned for any virus before they are used.
5. Programs or files of unknown origin should not run or read before they are verified and scanned first for their legitimacy.
6. Ensure that critical data is always backed up. This way, if a ransomware attack should arise, the company can fail to pay the ransom and still have its data in place. This is a way to discourage and reduce the hyped ransomware rate in the recent past.
7. Monitoring systems and logs. This way, it can be easier to identify a problem like a computer virus at an early stage before it does damage on the files. It can even be eliminated with ease.
8. The access of end user to systems should be highly restricted with no administrative favors.
9. They should also come up with a policy on information security.

Also, as seen from the data analysis, it has become hard to limit cybersecurity threats since most companies and organizations which are victims of the same, do not seem to induce any effort into limiting the problem. We saw that the highest percentage of them do not want to change their budget and also do not want to adjust any security plans. In order to start curbing cybersecurity threats, victim companies need to adjust and improve their security plans and also raise their annual budget to cater for the improvements and adjustments that will be done in as far as cybersecurity is concerned (Jang et al., 2014). If the above is done, according to Alison (2017), in reference to a case study research carried out by BH Consulting, a security firm in Cleveland, Ohio, we will reduce malware attack by 34% within the next five years (p. 24).

Still, in malware attack, we have seen from the data that 85% of manufacturing companies around the world do not have any security protocol within their design scope (Turkina, 2018). This means that almost all the devices we have are vulnerable to attack. According to Jasmine (2017), Jang et al, (2014), and Grupts et al, (2016), the following are some of the ways in which these companies can help in improving cybersecurity and reducing threats;

These companies should install a vulnerability management program in all their products (devices) having any programmable or network interface. Doing this, it will enable the users to be notified as soon as there is a detectable virus within its network. Then necessary action can be taken including scanning or clean the device using an anti-virus. Come up with better software for their devices. To do this, it needs an essential cooperation within the technology industry. They should ensure that the new software has got an FTP program which is the best malware detector so far. The new software will ensure that any form of the virus in any device having a programmable interface is detected and a recommended action is given immediately. The government on an international basis has a great obligation in terms of coming up and effecting policies to curb the cybersecurity threats (Rowe et al., 2006).

First of all, from the data, we found out that there is a higher percentage of people suffer from malware through email phishing. A higher percentage of the victims suffer from unawareness while others suffer just because of ignorance not knowing the consequences of opening links and attachments of unknown and unverified origin. This has been brought about the increased cybercrime and the decreased cybersecurity, just as seen from the data collected. In order to deal with this, the government should first increase the cyber warfare first. This can be done through education. People should be educated starting from the lowest level of education like in third grade about the basics of cybersecurity, cyber-attacks, and cyber-ethics. This way, as they grow up they will know the effects of malware viruses and some of the ways in which it can be dealt with. Governments all over the world, especially from those most affected by cybercrime, should form a peace treaty on Internet and cybersecurity (Ted, 2014). As seen from the results they include United States of America, China, Germany, Britain, Brazil, Italy, Japan, France, Russia, Canada, South Korea, and India among others. They can be the top 50 most affected countries all over the world. These governments should form a Geneva Convention for the Internet. This will help form major policies in which all the governments are obligated to implement at whatever cost. This way, the future warfare on cybersecurity will be far more prevented. Even though the level of technology will be growing, the policies that will have been put in place will help along the way as cybersecurity threats increase.

Geers (2011), maintains that another policy that should be passed by the government is on the protection of the ‘little guy’. Hackers nowadays have found it easy to steal $1 from 2 million people than stealing $2 million from one person. When these people report to the police, the police do not bother using government resources tracing $1. The government should, therefore, pump in more funds to help in the investigations of attacks by the police rather than leaving the matter to the police. If this is done, it will reduce the rate at which hackers steal $1 from several people. Cybercrime will as well reduce and so will the losses that the victims suffer in case of an attack.

## Estimated Cost of Solving the Problem and Return on Investment

The total the total cost of cybersecurity stands at $750 billion and is expected to rise to $3 trillion by the year 2025. As outlined in earlier in the literature review and in data analysis, according to Herjavec Group, it has been forecasted that the damages due to cybercrime will rise to over $10 trillion by 2025. A case study research given out in a 2017 FBI report showed that if we implement the above-mentioned solutions, we will at least increase the cost we are using right now by 30% (Steve, 2018). This means that in the United States alone since the government is using around $31.5 billion, it will then instead use around $45 billion. According to Alison (2017), organizations, on the other hand, are expected to use a quarter of their total earnings on cybersecurity. This, therefore, depends on the size of the business in terms of production and profit margins. The estimated start-up cost, therefore, will be ¼ of their total earnings. This cost will keep on reducing after some time, say a period of five years. This is because the software and programs already existing in the systems will only need to be updated on a timely basis hence it will not be incurring a lot of costs as it was during the startup cost.

In order to calculate the return on investment, we first have to consider the net profit of the organization and the total cost that will be incurred in solving the problem and in this case, it is the total investment cost. In the case of the manufacturing companies as mentioned above in the solutions to the cybersecurity problem, ¼ of their total profits is the total investment.

If a company say Company X has a profit of $600 million, then a quarter of this is given by;

$\frac{1}{4}×\$600million=\$150million$

$therefore;totalinvestment=\$150million+\$600million=\$750million$

Return on Investment = (Net Profit/Total investment) multiplied by 100%

$=\frac{\$600,000,000}{\$750,000,000}×100=80\%$

Depending on the timeframe the company or the investor is planning on investing, then the time that the return will be expected can be calculated. All these depend on the start-up period. According to the Global Inc. Cyber Security Company’s research report released in September 2017, it showed that as time goes by, the return on investment decreases (as cited in McCrohan et al., 2010 p. 35). This is because, when the cybersecurity costs are reduced due to ransomware among others, then profit margins will increase due to the trust the company will have on the products the company is producing hence increasing its market scope.

The following graph shows the trend on return on investment for 8 years as from the year 2017;

*Graph 5: Trends on Return on Investment in the next eight years*

We can see from the graph that there is a reduction in the return on investment as time goes by. This means that an investment is done on curbing the threats caused by cybersecurity, losses due to the same will be reduced and hence profit margins will rise again. Also, since only maintenance costs will be incurred in updating the already existing system of security protection, then it will mean faster return on investment as less investment is used and more results or say profit is obtained.

# Conclusions and Recommendations

From the data analysis above and based on the literature review as well, several conclusions can be drawn as well as recommendations.

## Conclusions

According to Alison (2017), there has been a great deal of rising in technological growth as well as cybercrime. Technological growth has been doubling on an annual basis. There has been also been a great deal in the drop of cyber warfare. With these mere facts, many people have been affected since they do not really even understand what cybersecurity all about is.

Malware has been the most used technique for attacking over the past ten years and it has increased over the past three years. This has been brought about by companies not coming up with new software but rather keeping the old ones without even correcting the loopholes existing in them. This has made hackers perfect their malware skills, especially with the current rising technological rate. Due to this, it has become hard to control or even have a grip on dealing with cybersecurity threats.

Over 85% of total manufacturing companies all over the world produces products and services like smartphones, cars, airplanes, banking services, ATMs, home appliances and electronics, and anything that has a user interface between them without any form of security against cybersecurity threats and attacks (Jang et al., 2014). This has made it easy for the attackers to hack into the systems and devices with ease and b doing so, it means that the grip of dealing with the cybersecurity concerns is lost. Cybersecurity threats usually and mostly base their attacks on major social amenities. These include banks, hospitals, universities, and colleges among other schools, transport systems like cars, ships, and airplanes as well as the infrastructure at large. 95% of the total attacks occur on infrastructure and therefore this means that the effects are devastating as seen from the data obtained (Shafqat and Masood, 2016).

Many companies which have suffered from cybersecurity attacks show no positive effort at all in dealing with the problem. A higher percentage, as seen from the data obtained, do not want to either change their annual budgets but rather reduce it nor even try to adjust their security plans. This has led to a series of loses by many companies and organizations due to the multiple attacks they are facing on an annual basis. The companies do not care at all. With this level of ignorance and naive in major organizations around the world, it becomes hard to take care of the rising concerns of cybersecurity.

Cybersecurity threats have caused a significant drop in the profit margins of various companies as well as individuals on a personal basis. Due to these losses, it has seen a great impact on the economic scale all over the world with the top leading being the United States, China, Britain, Canada, Germany, India, Japan and South Africa among other countries. According to Steve (2018), the government is to blame due to the rising cybersecurity concerns. This is because it has failed in ensuring a vast spread in the cyber warfare campaigns so as to ensure that people understand what cybersecurity threats all about are and also the consequences of the same. People should be taught on the basic ways to prevent themselves from cybersecurity attacks like installing a legit anti-virus in their PCs and ensuring that they are updated. But since the government has not pumped in enough money to deal with the situation, many people have suffered deeply through e-mail phishing.

There is no set of education curriculum in 96% of schools on a global basis that ensures children are taught of cybersecurity from third grade as soon as they know how to use a computer or a mobile phone (Jasmine, 2017). This has led to the development of an illiterate society all over the world in as far as cybersecurity is concerned and this has made it hard to deal with the looming concern in the cybersecurity threats.

Cybersecurity attackers have become clever. According to Turkina (2018), they cover their tracks using certain software tools like the VPN and therefore it has become hard to deal with the looming cybersecurity concern. It also turns out that most specialized hackers prefer not working for the company or becoming the ‘good guys' but rather the opposite which has really become a challenge in most countries when dealing with the problem.

As stated earlier, Elon Musk (personal communication, January 20th, 2018) claims that artificial intelligence has brought in more problems by increasing cybersecurity attacks. AI, as we saw in the literature review, uses the autonomous system technology. This means that all the sub-networks of devices having a programmable network interface are connected together and operated under one network. AI has seen a huge development in self-driven cars, automatic airplanes, industry robots as well as intelligent phone applications. When all are connected by one network it becomes easy to infiltrate the whole network by finding just one weak sub-network and since they do not have any form of security measure, they are easily attacked. With the rising AI technology, therefore, it has led to the lack of grip in addressing the looming cybersecurity concerns.

## Recommendations

Based on the literature review, data obtained and its analysis as well as the conclusion above, the following recommendations can be drawn to help improve alleviate cybersecurity threats while adopting automated systems. First, the electronic devices operating without any form of security system should install a vulnerability management program in the programmable, and network access system. This will enable the users to be notified as soon as there is a detectable virus within its network. Then necessary action can be taken including scanning or clean the device using an anti-virus (Wong, 2018).

Also, these organizations should come up with better software for their devices. To do this, it needs an essential cooperation within the technology industry. They should ensure that the new software has got an FTP or a VPN program which is the best malware detector so far. The new software will ensure that any form of the virus in any device having a programmable interface is detected and a recommended action is given immediately. The government should start thorough cybercrime warfare so as to make people understand the existence of the problem and its effects. This will reduce the level of ignorance and several malware practices like ransomware through email phishing can be avoided. The government should finance a new curriculum in schools. If this should be introduced, it will ensure that children are taught about this looming problem as soon as they start learning using a computer, say in third grade (Rodney, 2018).

Those companies that have been attacked and are victims of cybersecurity threats should show an effort to curb the problem. They can do this by increasing their annual budgets and mostly towards securing the security of the company. They should also help in advancing their security plan rather than relying on an older version of the same. Victim companies and individuals should ensure that they back up data on a daily basis. This will ensure that in case of an attack, they will still have their data secured. Having data backup files will also reduce ransomware cases since the company does not have to pay the attackers so that they can have their data back as they have them in backup files (Passeri, 2017).

In as much as technology has led to the increase in cybersecurity threats as well as companies making products without any security measure in their design scope, curbing the problem as well starts from a personal level. It is recorded that 42% of the total cybercrime actions occur at a personal level like opening a link or an attachment of unknown origin in your email. People should, therefore, start ignoring these links and attachments by being responsible and not being naïve all the time. They should ensure that their computers have got updated anti-virus as well as ensure they back up their data on a routine basis (Elon, 2018). Initializing the above-recommended actions will help in reducing the looming concern on cybersecurity threats. We have seen that cyber threats are a serious concern which will become a technological crisis in the future if we do not take the required actions now in ensuring that we curb it.

# References

Alison, D. S. (2017). December 14th, 2017 Tech-Republic Cyber Attacks Report: 91% of

Brinkmann, S. (2014). Interview. In *Encyclopedia of critical psychology* (pp. 1008-1010). Springer New York. <http://www.hatjecantz.de/files/interview_brinkmann_e.pdf>

Choo, K. K. R. (2011). The cyber threat landscape: Challenges and future research Directions. *Computers & Security*, *30*(8), 719-731. Retrieved from; <https://www.sciencedirect.com/science/article/pii/S0167404811001040>

Cybersecurity pros fear hackers will use AI to attack their company. Retrieved from; <https://www.techrepublic.com/article/91-of-cybersecurity-pros-fear-hackers-will-use-ai-to-attack-their-company/>

Dua, S., & Du, X. (2016). *Data mining and machine learning in cybersecurity*. CRC press.

Gao, L. (2001). On inferring autonomous system relationships on the Internet. *IEEE/ACM. Transactions on Networking*, *9*(6), 733-745. Retrieved from; <http://ieeexplore.ieee.org/abstract/document/974527/>

Geers, K. (2011). *Strategic cybersecurity*. Kenneth Geers.

Gupta, B., Agrawal, D. P., & Yamaguchi, S. (Eds.). (2016). *Handbook of research on modern Cryptographic solutions for computer and cybersecurity*. IGI Global.

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats to cybersecurity. *Journal of Computer and System Sciences*, *80*(5), 973-993.

Jasmine, M. (2017). July 26th, 2017 Crayon Data Resource, Big Data Sample: Will Artificial Intelligence takes over cybersecurity? Retrieved from; <http://bigdata-madesimple.com/will-artificial-intelligence-take-over-cyber-security/>

Magoni, D., & Pansiot, J. J. (2001). Analysis of the autonomous system network topology. *ACM SIGCOMM Computer Communication Review*, *31*(3), 26-37. Retrieved from; <https://dl.acm.org/citation.cfm?id=505663>

McCarthy, C., Harnett, K., & Carter, A. (2014). *Characterization of potential security threats in modern automobiles: A composite modeling approach* (No. DOT HS 812).

McCrohan, K. F., Engel, K., & Harvey, J. W. (2010). Influence of awareness and training on Cybersecurity. *Journal of Internet Commerce*, *9*(1), 23-41. Retrieved from; <http://www.tandfonline.com/doi/abs/10.1080/15332861.2010.487415>

Mehmood, H. (2017). August 8th, 2017 Global Sign Blog: How Top Industries Are Preparing ForEvolving Cybersecurity Threats. Retrieved from; <https://www.globalsign.com/en/blog/top-industries-preparing-for-evolving-cybersecurity-threats/>

Naveen, G. (2017). August 23rd, 2017 Cyber Threats Vulnerabilities Report: List of Countries, which are most vulnerable to Cyber Attacks. Retrieved from; <https://www.cybersecurity-insiders.com/list-of-countries-which-are-most-vulnerable-to-cyber-attacks/>

Passeri, P. (2017). September 2017 Cyber Attacks Statistics. *Hackmageddon Information Security Timelines and Statistics.* Retrieved from; <http://www.hackmageddon.com/2017/10/20/september-2017-cyber-attacks-statistics/>

Peng, S. Y. (2015). Cybersecurity threats and the WTO national security exceptions. *Journal of International Economic Law*, *18*(2), 449-478.

Rajeyyagari, S., & Alotaibi, A. S. (2018). A study on cyber-crimes, threats, security and its emerging trends on latest technologies: influence on the Kingdom of Saudi Arabia. *International Journal of Engineering & Technology*, *7*(2.3), 54-58. Available from: <https://www.sciencepubco.com/index.php/ijet/article/download/9969/3500>

Reveron, D. S. (Ed.). (2012). *Cyberspace and national security: threats, opportunities, and Power in a virtual world*. Georgetown University Press. Retrieved from; <https://www.acs.org.au/content/dam/acs/acs-publications/ACS_Cybersecurity_Guide.pdf>

Rowe, B. R., & Gallaher, M. P. (2006, March). Private sector cybersecurity investmentStrategies: An empirical analysis. In *The fifth workshop on the economics of information security (WEIS06)*. Retrieved from; <https://pdfs.semanticscholar.org/a188/0f3fc72ab11f5eca24fa6970eb2a8ab69c4f.pdf>

Shafqat, N., & Masood, A. (2016). Comparative analysis of various national cyber security strategies. *International Journal of Computer Science and Information Security*, *14*(1), 129. <http://www.academia.edu/download/41883983/17_Paper_31121548_IJCSIS_Camera_Ready_pp._129-136.pdf>

Singer, P. W., & Friedman, A. (2014). *Cybersecurity: What everyone needs to know*. Oxford University Press.

Steve, M. (2018). Jan, 23rd 2018 Cybersecurity Bussiness Report. Top 5 cybersecurity facts, Figures and statistics for 2018. Retrieved from; <https://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics.html>

Ted, J. (2014). December 4th, 2014 Info-Security magazine Cyber Attacks trend report: DefiningMoments in the History of Cyber-Security and the Rise of Incident Response. Retrieved from; <https://www.infosecurity-magazine.com/opinions/the-history-of-cybersecurity/>

Turkina, E. (2018). Jan, 2nd 2018 the importance of networking to entrepreneurship: Using AI Intelligently in cybersecurity. Retrieved from; <http://www.information-age.com/using-ai-intelligently-cyber-security-123470173/>

Yan, Y., Qian, Y., Sharif, H., & Tipper, D. (2012). A survey on cybersecurity for smart gridCommunications. *IEEE Communications Surveys and Tutorials*, *14*(4), 998-1010. Retrieved from; <http://ieeexplore.ieee.org/document/6141833/>