Cybersecurity - the threat of social engineering

Kalajžić, Ivan

UNIVERSITY OF ZAGREB - CROATIA
FACULTY OF ECONOMICS AND BUSINESS
MASTER DEGREE IN MANAGERIAL INFORMATICS

MASTER THESIS

Subject: Information System Auditing

Topic: Cybersecurity – The Threat of Social Engineering

Academic year: 2018/2019

Mentor: Mario Spremić

Student: Ivan Kalajžić

_____

Ime i prezime studenta/ice

IZJAVA O AKADEMSKOJ ČESTITOSTI

Izjavljujem i svojim potpisom potvrđujem da je _____

(vrsta rada)

isključivo rezultat mog vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu, a što pokazuju korištene bilješke i bibliografija. Izjavljujem da nijedan dio rada nije napisan na nedozvoljen način, odnosno da je prepisan iz necitiranog rada, te da nijedan dio rada ne krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Student/ica:

U Zagrebu,_____ _____

(potpis)

Acknowledgements

To my family:
I would like to extend my everlasting gratitude and love to my mother Anita and my brother Josip. You have been my rock, my fortress, my everything; you have proven to me that we can accomplish anything we set our hearts to as a family. You have shown me that I should believe in myself and my abilities. Without you in my life I would be lost.

I would also like to express my deepest thanks and love to my grandmother Marija, grandfather Ivan and aunt Lidija for always being supportive and believing in me. For showing me the love and care that I needed when I had to go through the hardest periods of my life. You have taught me that there are is no stronger bond than that of blood and for that I will be eternally thankful.

My gratitude goes to “My Lady” aunt Nada for offering to edit and proofread the thesis with her expertise in the English language. For showing me that there is kindness and happiness in the world when I needed it the most. I will keep you close to my heart forever.

To my mentor:
I would also like to convey my sincerest thanks to my mentor Prof.Dr.Sc. Mario Spremić for his guidance, support and advice that helped me tremendously in writing this thesis. For putting faith in me that I will be able to successfully complete my thesis.

Without the continued love and support that I have received from the people that mean the most in my life, this thesis would not exist. I will keep the advices and wisdom given to me in my mind and heart for any future endeavors I choose to embark on.

Table of contents

1. Abstract

The exponential development of digital technologies and the ever-growing perforation of such technologies into our lives has made today's society increasingly aware of the opportunities and threats presented by these digital technologies. Some individuals, organizations and governments have decided to use these technologies for malicious purposes such as unauthorized data interception, unauthorized data collection, data alteration and possibly even data destruction, data selling, hardware and software destruction while others have been using these technologies to create means of protection from such malicious actions. These malicious agents are targeting the weakest points of the security wall presented to them which is the human being itself otherwise known as wetware. These threats are known under the umbrella term of social engineering. Malicious agents are targeting wetware as it is much easier to circumnavigate the hardware and software defenses put in place by security experts when wetware can easily override such protection measures and provide access to valuable information. Precisely because of these developments in cybersecurity field a growing amount of effort has been shifted from purely technological orientation towards striving to understand the importance of the human role in the system of cybersecurity and thus mitigate the threats of social engineering. This thesis will strive to examine the threats of social engineering attacks, methods used by malicious agents, examine and analyze real life cases through case study analysis as well as discuss and propose protection measures against such threats.

2. Introduction

2.1 Subject and Goal of Thesis

The development of digital technologies that enabled the cyberspace can be found in the roots of the internet, internet technology has irreversibly and dramatically changed our lives for the better and for the worse – the sheer ability to connect with other human beings across the globe and easy, instant access to what is essentially all of humanity's knowledge gathered in one place is unprecedented in history of humanity. These relatively new circumstances have created a need for today's specialists, policy makers and society in general to be growingly informed and vigilant about the threats and opportunities presented in the realm of internet called cyberspace. Needless to say, that such threats and opportunities must be a concern of any information technology expert as they are of vital importance to the stability and security of any society.

This is increasingly important due to ever growing dependence of private, public and governmental organization on the use of digital technologies which presents a possible weakness in any society. Weakness that could be potentially exploited by a possible malicious agent and profoundly affect the victim's lives. Naturally with any relatively "new" technology great effort should be placed into researching and developing means of protection against unwanted and malicious uses of such technology. This thesis will provide a closer look at cybersecurity as a whole and will strive to provide us with the conceptual framework needed to understand underlaying operations of cyberspace as well as conceptual framework of security measures and potential threats. However, in order to fully understand the subject, it is not nearly enough to solely examine the conceptual and technical framework of the issue at hand. Thus, a case study of real-life events is necessary to examine real world errors, results and implications from such attacks. Examination of technical framework and real-life events should lead us to logical conclusions about the possible improvements to protection measures as well as point us a way towards future trends in the cybersecurity field.

2.2 Sources of Data and Collection Methods

Methods of research used in this thesis will include qualitative data research gathered from published literature, research papers, internet sources, an interview might be conducted with an expert from cybersecurity field in order to obtain first-hand experience if the opportunity to do so arises. Additionally, multiple case study analysis under the same framework will be used to supplement the qualitative data obtained.

2.3 Content and Structure of the Thesis

Naturally, the thesis will start with an abstract and introduction that will outline the importance and provide a brief summary of the thesis, as well as collection methods and an outline of the thesis structure. Naturally, we shall begin with conceptual framework for cyberspace in general followed by conceptual framework of cybersecurity in order to get an understanding of the foundation that makes it possible as well as security options available to cybersecurity specialists and everyday users. Once we have examined protection measures, the following section shall focus on the threats presented to us in cyberspace, in this case the focus will be on social engineering threats as that is the subject of the thesis. Now that the complete conceptual framework is established, the following section will examine real-life cases in order to gain an understanding how the conceptual framework is applied in practice. The next section will offer a discussion of the case studies as well as possible improvements to the security measures model and possible future trends that the cybersecurity field is heading towards. The conclusion will outline everything presented in the thesis so far as well as offer authors final thoughts.

3. Overview of Cybersecurity

3.1 The Internet

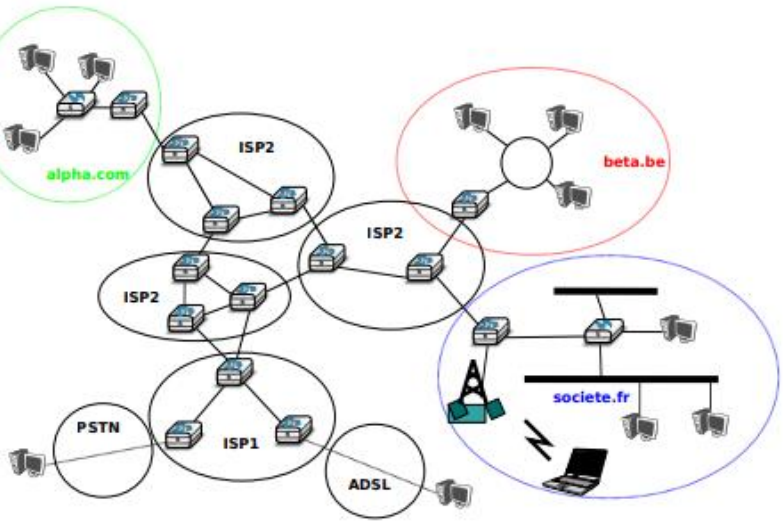
Before examining the topic of the thesis in greater detail it is important to take a look at the foundation of cyberspace. That foundation is called the internet. The groundworks for what was to become the internet as we know it today were laid during the Cold War period of the 1960's when the United States Ministry of Defense commissioned the development of new telecommunications systems intended for command and control of its various military installations located all around the world. Naturally, any effective military is designed around a highly centralized and hierarchical structure and thus were the newly commissioned telecommunications solutions being developed. However, due to the emerging threat of nuclear weapons developed during World War II and a possibility of war with the former Soviet Union in which case the command and control structure could be easily annihilated using nuclear weapons, it was concluded that it would be in the military's best interest to develop a decentralized system instead. Such a decentralized system could not be destroyed in one single strike and could continue to operate even in the worst-case scenarios of system fragmentation. The task of creating such a system was given to the "Advanced Research Projects Agency" (ARPA) with the specified requirements:

- Telecommunications system cannot be centrally dependent
- Telecommunications system must continue to operate even in event of damage of some parts of it

As the research progressed ARPA started collaborating with privately owned enterprises, civil institutions and most notably major universities across the United States. This resulted in development and foundation of the ARPANET in 1969 as test ground for new telecommunications technologies. The first interconnected nods of ARPANET appeared in three major universities in the United States and in 1970 a separately developed network ALOHANET of the university of Hawaii was connected to the ARPANET. The system continued to grow in two directions; one was called ARPANET which served the civilian purposes and other was MILNET which served military purposes. In 1986 a network of supercomputers called NSFNET was integrated into the system. Although limited in use and in bandwidth when compared to today's standards, the successful operation of NSFNET is considered to be an event that is the precursor to today's internet network (Pande, 2017).

One way we can define the internet is as a global network system of computers, servers and cellphones that transmit data across various types of media using a TCP/IP protocol otherwise known as Internet Protocol Suite (IPS) (Investopedia, 2011). Additionally, the internet can be seen as: "*an interconnection of networks, often called domains, that are under different responsibilities*."[1]Alternatively, the internet can also be viewed as a global information-communications systems that interconnects various computer networks of individual countries and organizations and in doing so enables the users of computers around the globe to communicate with each other, share information and use numerous other tools and services through their local networks and telephone lines. In a physical sense, it is a series of interconnected computer networks organized in a specific way with common communication protocols and network services. It is the most important global infrastructure that facilitates education, information flow, research and public and economic activities (Dragičević, 2004). Simply put, the internet represents a global public computer network that uses a hybrid architecture (Spremić, 2017). Figure 1 represents an internetwork otherwise knows as a network that connects to various other networks. This very principle is used by the internet except on a much larger scale than shown in the figure 1 which is a mere illustration of the concept (Bonaventure, 2015).

Figure 1:



Source: (Bonaventure, 2015)

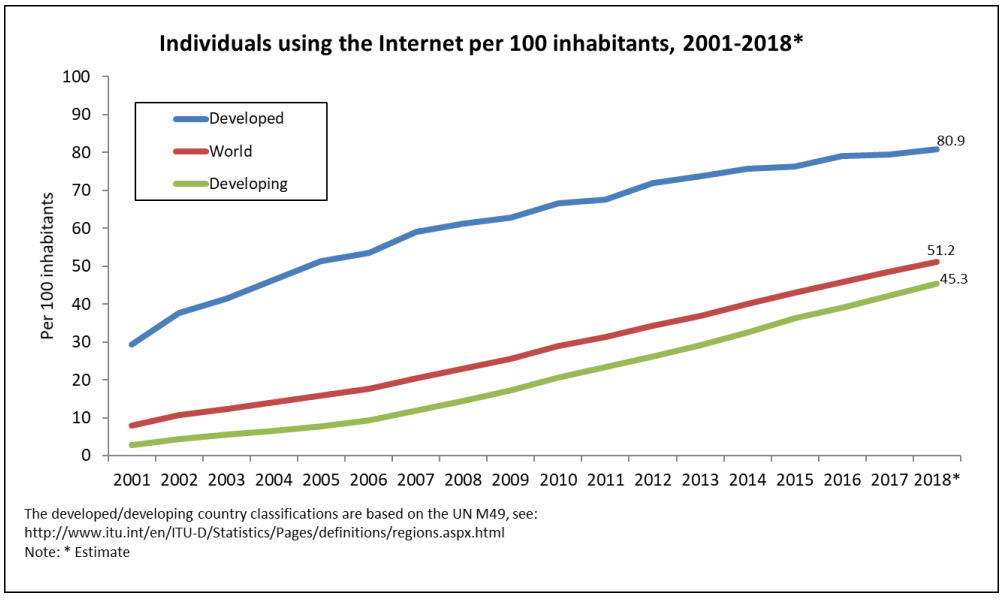
As previously mentioned, the inner workings of internet can be found in Internet Protocol Suite (IPS). Because the internet today is built of layers of hardware and software, IPS provides a communication standard to enable communication between layers. More precisely, IPS

[1] Bonaventure, Olivier (2015.) „Computer Networking: Principles, Protocols and Practice"

specifies how the data should be packetized, addressed transmitted, routed and received. The functionally of the tasks of IPS is divided into four layers. The application layer is the highest layer in the TCP/IP architecture which serves as an access point to network services and protocols for any type of content exchange, additionally it contains other protocols such as HTTP, FTP and SMTP. The second layer is known as the transport layer and it enables the session and communication with network services. It contains protocols such as TCP and UDP. Thirdly, the internet layer is responsible for direction, creation and assignment of the IP addresses to data packets. Finally, the last layer is known as network access layer and it is responsible for delivering data packets to and from the network the user is connected to (Spremić, 2017).

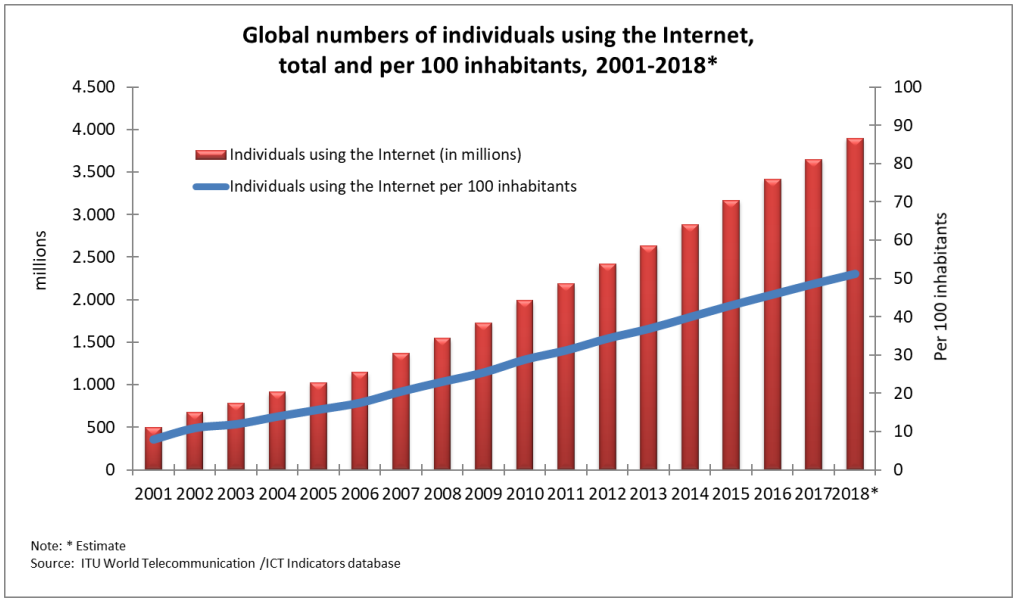
According to International Telecommunication Union (ITU) statistics from the year 2001 to 2018, as presented in figure 2, the number of individuals using internet has reached 51 out of 100 inhabitants worldwide. The number of internet users for developing regions is 45 out of 100 while in the developed regions that number is much higher where 81 individuals out of 100 use the internet. This data point reinforces the fact of all-around presence of internet technology among today's world population. However, it is important to note that the numbers presented in the following figures are an estimate based on available data collected by ITU.

Figure 2:



Source: (ITU, 2018)

Figure 3:



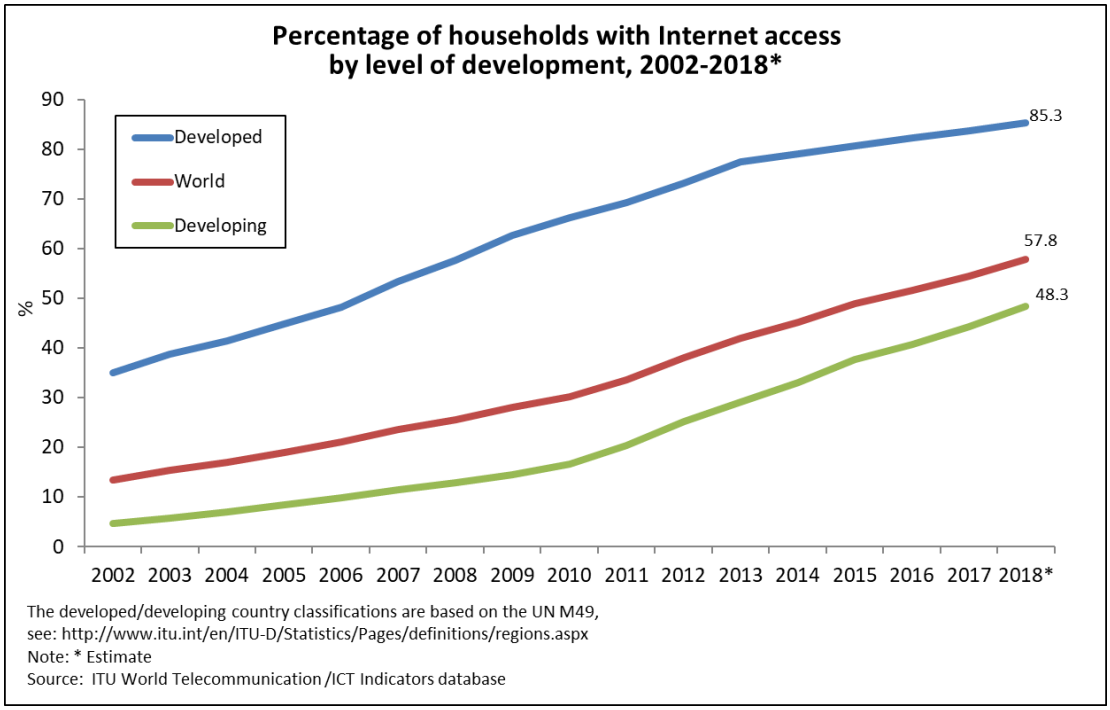
Source: (ITU, 2018)

Figure 3 presents the raw number of individuals using the internet expressed in millions compared with the number of individual users of internet per 100 inhabitants marked by a blue line. It is clear that over the course of the last two decades internet usage among world's population has significantly increased no matter what metric we observe. In terms of individual users of internet per 100 inhabits that number has almost quintupled from 2001 to 2018, while the raw number of individuals using the internet has increased by roughly 7 times from 500 million users in 2001 to 3500 million users in 2018. This further reinforces the fact of pervasiveness of internet technology among today's population.

Household internet adoption rate expressed in percentages of total number of households per region can be seen in figure 4. The numbers presented in figure 4 mostly align with the data presented in figure 2 and figure 3. We see that the adoption rate of internet or simply put percentage of household with internet access is 58 percent of households on the worldwide level which is a significant increase from 2002. The highest percentage of households with internet access is present in developed countries with 85 percent of households having internet access. In developing countries that number is 48 percent of households. However, if we examine the graphs more closely, we can see that the number of households with internet access has seen a sharp increase in the past decade indicating that an ever-growing number of households in the developing countries are rapidly gaining internet access. This data point could suggest that the developing countries are rapidly closing the gap in regard to infrastructure and technology

development when compared to the developed countries. It also clearly shows that in the developed countries nearly every household has internet access.

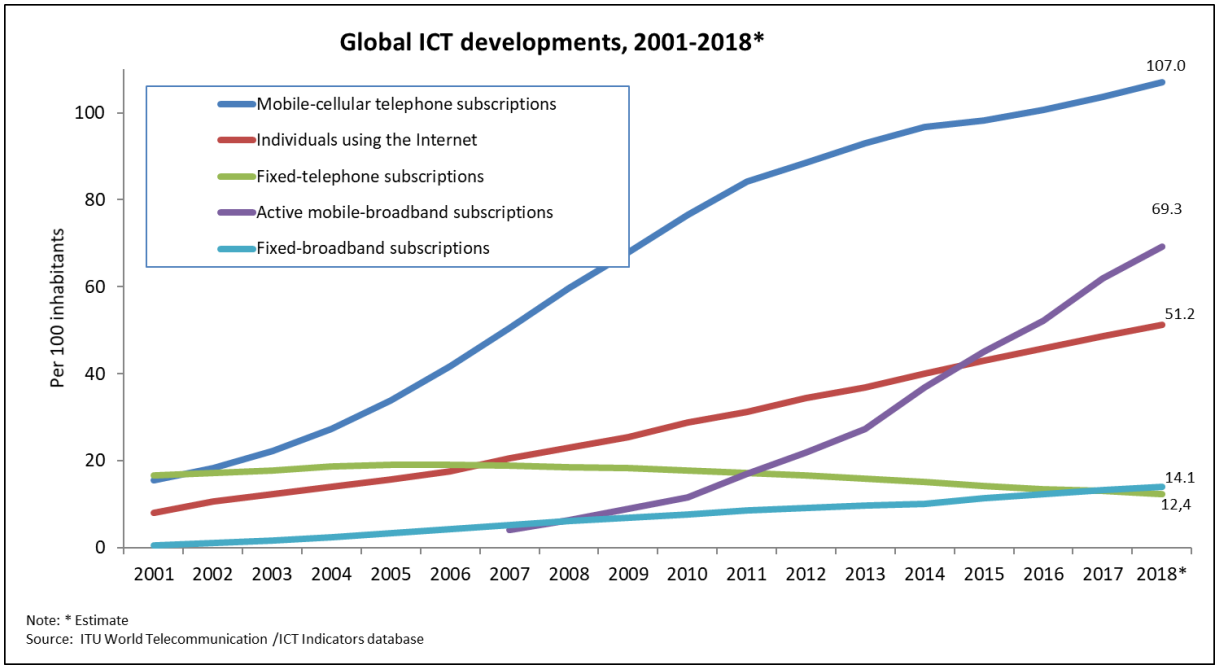
Figure 4:



Source: (ITU, 2018)

Another interesting trend that is present in the information and communications technology (ICT) field can be seen in figure 5. In red we can see the number of individuals using the internet on the global scale as already shown in figures 2 and 3. However, what is interesting is that the fixed telephone subscriptions, which is the technology that virtually started widespread adoption of internet, is on the decline with only 12 users per 100 inhabitants in 2018. Fixed broadband subscriptions are showing a small albeit steady increase of users over the years to 14 users per 100 inhabitants in 2018. What is most interesting is that emergence of active mobile broadband subscription technology in 2007 and its quick adoption and spread rate now covers majority of internet users in 2018 at 70 users per 100 inhabitants. This data points us towards new trends in internet technology where most users that use the internet are mobile users exclusively which is interesting and concerning to cybersecurity specialists given the widespread usage of mobile phones all over the world, even in developing countries, as well as their portability and ever improving technical capability.

Figure 5:

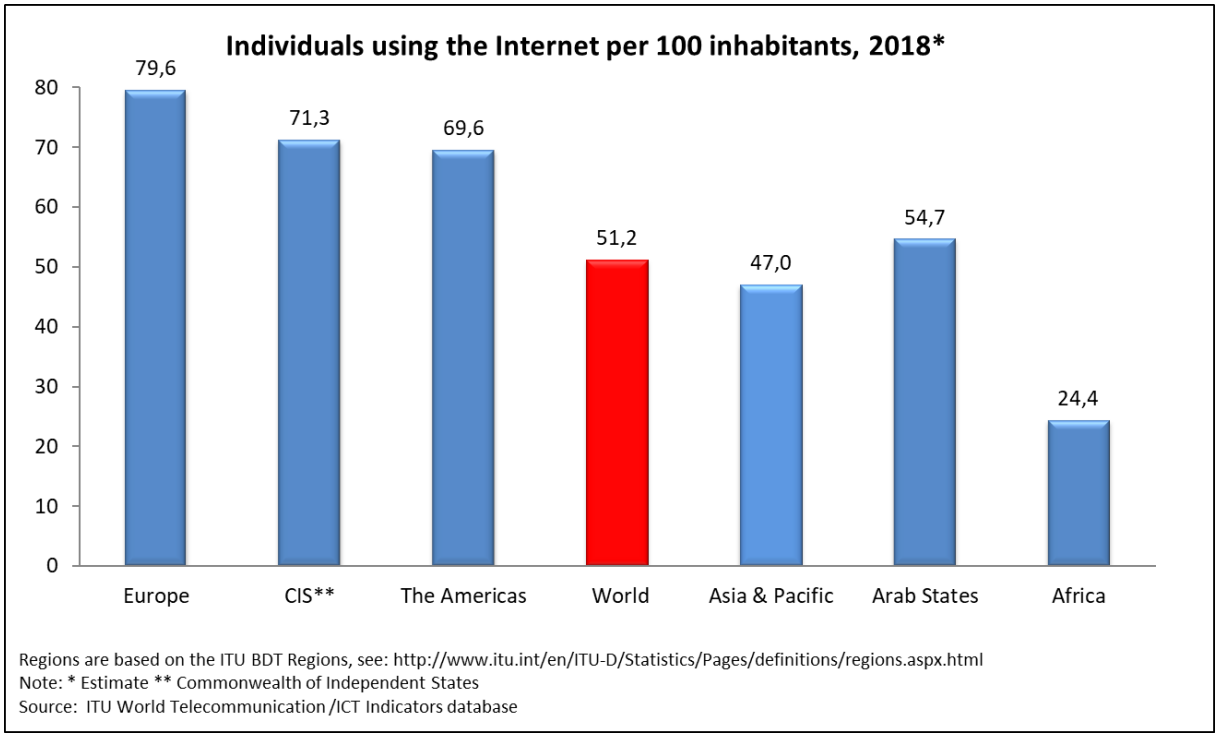


Source: (ITU, 2018)

It is also interesting to see the breakdown of number of individuals using the internet per 100 inhabitants according to the regions of the world as seen in figure 6. A clear trend is visible immediately, that aligns with the data from other figures already presented, in which the developed regions such as Europe, CIS and The Americas are ahead in terms of number of individuals using the internet per 100 inhabitants. More precisely, in Europe that number is 80 individuals per 100 inhabitants. In Commonwealth of Independent States (CIS), which is a regional intergovernmental organization composed of mostly former Soviet Republics meant to serve as a counterweight to the European Union and the United States, the number of internet users is surprisingly 71 users out of 100 inhabitants. In the Americas, which includes both the United States of America, Canada and the countries of South America, that number is 70 users out of 100 inhabitants. It is important to note that most of the countries located in South America are classified as developing countries which points towards a lower number of internet users in South America when compared to North America thus skewing the region number of users downwards. Regions such as Asia & Pacific have a 47 internet users per 100 inhabitants, presumably this is mostly due to poor infrastructure present and inaccessibility due to most of these countries being island nations. In the Arab states number of individuals using the internet per 100 inhabitants is 55 users which is the highest out of developing regions. The lowest number of internet users is in Africa at only 24 users per 100 inhabitants. However, this data

point alone does not provide the complete picture. Along with other figures presented in this section it is clear that the future trends for internet usage are definitely positive and that the number of users will continue to grow especially in developing countries as their infrastructure and technological level improves thus creating a need for cybersecurity specialists not only in developed countries but also elsewhere in the world.

Figure 6:



Source: (ITU, 2018)

3.2 History of Cybersecurity

When talking about cybersecurity in terms of history, it is necessary to closely couple it to the history of internet. The reasons behind the development of internet and its intended purpose are often forgotten. As already mentioned previously in this thesis, the initial purpose of internet was not commercial nor even remotely connected to what the internet represents today in terms of geographical area coverage, number of users and possibilities offered, but rather its original function was telecommunications capabilities intended for the sole purpose of the U.S. military. Therefore, in the early days of the internet not much thought was given to the concept of security as it was presumed that there would be a low number of users that can be trusted with sensitive information. Instead the early internet was developed with efficiency, flexibility, openness and modularity of the system in mind. The detrimental goal envisioned in the first iteration of the internet was to ensure the most convenient and fastest access to the information inside of the network without any limitations to the user. Although, the concept in its original form was what

was indeed necessary for its intended military use, today it is proving to be the weak point of internet especially when it comes to its usage in the commercial and governmental institutions (Dragičević, 2004).

In the very beginning when internet was still known under its developmental name ARPANET, the user base consisted of a very small number of military and governmental institutions whose members often knew each other on personal basis. Therefore, first "security breaches" were often small and harmless breaches that could be classified more closely as mere pranks that the scientist played on each other. Such pranks are described in detailed in the book *"Hackers: Heroes of the Computer Revolution (1984)"* written by Steven Levy for those who are more interested in the subject (Dragičević, 2004). First of the many more serious breaches of ARPANET occurred in 1986 and 1988. The incident in the year 1986 involved an intrusion into the ARPANET network by Cliff Stool who was at the time a system administrator at California's Lawrence Berkley National Laboratory. His intrusion was enabled by a fault in data concerning computer connectivity which allowed him to connect to the ARPANET network and download a copy of information not only from other universities computers, but also governmental and military computers connected to the internet. In 1988 a much more serious intrusion occurred when Robert Morris unleashed the Morris Worm also known as the Internet Worm upon the ARPANET network. This incident is considered to be the first automated network security attack. Robert Morris wrote a program with which he could connected to another computer, locate and use one of its weakness to copy itself and spread to other computers connected on the network, not only that but once the host computer was infected the worm would use so much of the systems resources that it was virtually unusable. This task was done infinitely until the worm spread across the whole network and thus it was called a self-replicating automated network attack tool. The result of the first ever automated breach was some 6000 computers infected which at the time represented about 10% of the total number of computers on the network. Since at the time the ARPANET architects did not have any tools to combat and stop the spreading of the worm the solution was to disconnect almost all remaining computers from the network to stop further spreading. Robert Morris was the first person in history to be criminally charged and sentenced according to the "Computer Fraud and Abuse Act" of 1986 (Dragičević, 2004).

By 1989 more internet worms are written and unleashed this time on the VMS systems connected to the ARPANET by using a program intended for sending and receiving mail. By

1994 a series of programs called packet sniffers first appeared whose intended use was to intercept and copy data travelling over the network and potentially obtain usernames and passwords allowing for access to a certain subsection of the network. In order to combat this by 1995 a "trust relationship" program is developed which enables two or more computers, that are connected to the internet, a secure and fast access to one another. Immediately after introduction of those security measures program tools are developed that are intended to discover and simulate such "trust relationships" enabling a third-party to have computer access to such a system (Dragičević, 2004).

There were several key factors that contributed towards further spreading and usage of internet and by extension the development and rise in various kinds of cyberattacks but cybersecurity measures as well. This development in the cyberspace could be viewed as a sort of an arms race between the cybersecurity specialists and malicious agents who are constantly trying to gain an advantage over each other. The first key factor can be found in sudden development, introduction and expansion of the electronic business on the internet which enabled a means or a platform for various large public and private sector institutions from which they could connect directly to a large number of potential customers and thus more effectively offer their products and services. The aforementioned development went hand in hand with the development and widespread use of the World Wide Web and other programing languages, that are a standard today, which opened up new possibilities of attacks and intrusions for malicious agents (Dragičević, 2004). These possibilities will be discussed further in this thesis.

3.3 Conceptual Framework of Cybersecurity

In the following section a conceptual framework of cybersecurity will be examined in order to gain a knowledge foundation needed to understand the methods used to employ protective measures in the cyberspace. Before even approaching cybersecurity as a concept it would be wise to discuss the concept of security in general terms and the philosophy behind it in order to gain a better understanding of the underlaying concept of cybersecurity.

Security can be viewed from two sides. It is usually viewed from the inside as we humans seek a sense of comfort and assurance, it is innate for us humans; we believe that our homes are safe, we believe that our walls are high enough, that our doors are strong enough and our guard dogs are fierce enough. We tend to focus on the positives of our security solutions and usually end up in a positive feedback loop in which all of our security solutions appear to be good enough and thus our system or home safe. Therefore, we stop improving and improvising and keeping

up with the latest trends in security solutions. Until that one today when our walls are breached, our doors kicked down and our guard dogs dispersed. Suddenly, our perspective shifts and weaknesses in security solutions are exposed and seem almost obvious. The second side of security can be viewed from the outside; from the perspective of thieves and hackers that are looking for the gaps in the system. They operate outside of the system and thus have a different view of the security system. Their thinking is outside of the box and different from the one who built the walls meaning they could develop unexpected techniques and solutions in order to overcome a security system. When envisioning a security system, it is important to concede that any system is vulnerable and can be compromised because no matter how secure a system appears to be there is almost always a way to breach it (Hadnagy, 2011). It is necessary to keep such a philosophy of security in mind, no matter if a cybersecurity system or a tangible home security system is being designed, in order to not underestimate your opponents and to keep up with the latest developments in the security field and thus minimize the risk of a security breach.

As with any security system, whether it is a cybersecurity system or a home security system, we can tie the concept of security and risk together. A security level of a system can be rated as a risk of breach; the higher the risk of breach the lower the rated security level of the system. "*In general, risk can be defined as a likelihood that an appropriate source of threat will exploit the vulnerability of the system, and consequently cause some harm to the organizations assets*."[2] In the information technology sense, we can distinguish IT risks as the risk associated with the intensive use of information technology in performing organization's activities. More accurately, IT risks can be seen as a function that represents the interaction of three variables that are: assets, threats and vulnerabilities. Assets represent the value of the organization which can be either material or financial. Threats represent outside and possibly inside incidents such as breaches, cyber-attacks and even natural disasters. Vulnerabilities refer to the existence and effectiveness of controls created and implemented which measures the weakness of a system. A subsection of IT risk is called cyber risk. It is a type of risk that refers to the extensive use of digital technologies in governmental and private organizations as well as everyday life. Due to the prevalence of digital technologies in our lives and daily activities it is easily concluded that most of us are exposed to a certain degree of cyber risk depending on our actions, digital technology usage levels, security measures and knowledge levels. (Spremić, 2018).

[2] Spremić, Mario (2018.) „Enterprise Information Systems in Digital Economy"

Risk management is conducted by placing effective controls which serve as a means of detecting and preventing threats and unwanted events from occurring therefore lowering the risk. It can be also viewed as lowering the risk occurrence or lowering the risk frequency as it is not possible to eliminate risk all together. In order to successfully manage risks, it is necessary to constantly evaluate the effectiveness of controls put into place. Therefore, it can be said that the most important factor in managing risk or in other words lowering the risk frequency can be found in techniques of risk management and proper control management (Spremić, 2018).

Simply put, defining cybersecurity can be as easy as stating that it is the state of being protected against the criminal, unauthorized and unwanted use of your personal digital data as well as the measures undertaken to achieve this protection (Gardner, 2017). Alternatively, cybersecurity can be viewed as a holistic model approach to designing, creating, managing and ensuring the functioning of a modern information system which includes technological, organizational and social aspects as opposed to more traditional procedures towards information security which are mostly focused towards technological solutions. Cybersecurity is the umbrella term for all measures of protection and control which protect individuals and organizations from intentional, sophisticated and malicious cyberattacks which are generally hard to detect and prevent. The main goal of cybersecurity measures is to prevent or at the very least lessen the consequences that cyberattacks can cause (Spremić, 2017).

There are three main pillars of information security (Spremić, 2017):

- Confidentially which refers to ensuring exclusive and safe access to the information system to the authorized user. In other words, confidential information is only available to the users authorized to access it and such information generally holds economical value. The loss of confidentially of information can lead to the loss of competitive advantage, loss of client trust, financial losses and even regulation and law non-compliance charges.
- Integrity of data refers to the protection of completeness and correctness of the user data. Integrity denotes protection from accidental or intentional malicious alteration of data which includes subsequent addition, alteration or deletion of information without a log of actions conducted. The loss of data integrity can lead to making the incorrect decision, loss of client trust and regulation and law non-compliance charges.
- Data availability means that the authorized user can have timely and constant access to the information system and data contained within. The loss of data availability can lead

to inability to deliver services and goods to clients, inability to meet contract obligations, loss of client trust, financial losses and regulation and law non-compliance charges.

In a broad sense we can ensure the confidentially of data by implementing protection measures to the access layer of information system in the form of identification and authorization of user attempting to connect to the information system. Data integrity can be insured by implementing protection measures that protect the data during transmission or that protect the data during quiescence. This can be achieved by data encryption, establishing security protocols during data transmission or by restricting information system access. Availability of services and data can be accomplished by controls related to managing the continuity of business both before and after unexpected and unwanted events (Spremić. 2017). Protection measures that shield these three pillars of information security will be examined in greater detail further in this thesis.

3.4 Forms of Cybersecurity Measures

As mentioned in the previous section a cybersecurity specialist can establish control measures in order to ensure the wholeness of the three pillars of information security and reduce the risk connected with the use of digital technologies. Therefore, this section will discuss the technologies that are the core of such control measures. As previously stated, we can group the control measures and therefore technologies used in three distinct categories. Identification technologies include the use of passwords, usernames, cookie data and various other authentication procedures. Surveillance technologies include identification and location of users, data transmission interception, monitoring communication channels and surveillance of computer network activities. It is important to mention encryption technologies as they are usually used in conjunction with surveillance technologies in order to ensure the second pillar of the information which is integrity of data. Investigation technologies are linked with creating a database collected with the help of surveillance technologies, they also include data storage and processing in order to ensure integrity. It is important to note that in some cases same technologies can be used for the various purposes such as identification, surveillance or investigation and therefore it is almost impossible to make a clear distinction between the various technologies (Dragičević, 2015). Thus, it is prudent to examine each measure individually in order to see how it can be implemented into a possible cybersecurity system.

Naturally, the most common measure of protection is the technology of authentication. Authentication or identification process can be defined as a process of identifying and verifying the individual is the same individual that he or she claims to be when accessing a computer

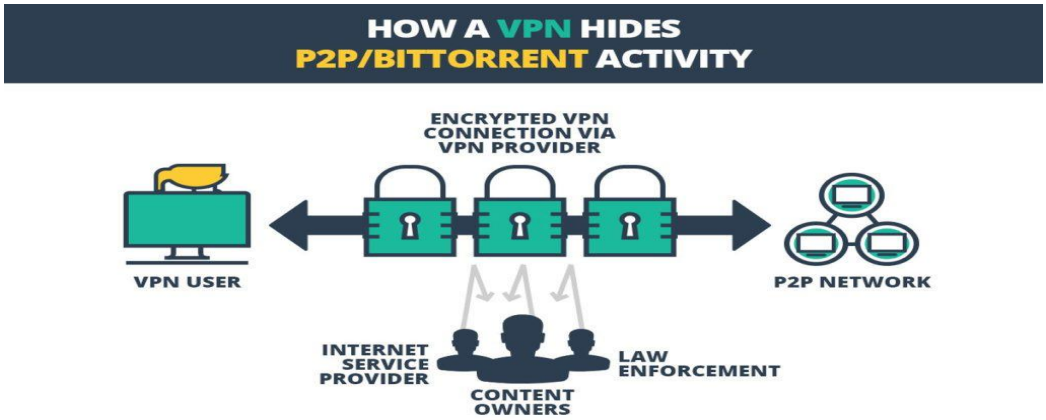
network (Pande, 2017). In other words, it is the process of user login to an information system by using physical, logical or biometric parameters in order to verify its credibility. The purpose of identification process is to prevent any unauthorized access to the information system (Spremić, 2017). The most common method of authentication over the internet denotes username and password usage which is a logical identification of a user's credibility. However, such measures are only rudimentary and suffer from various vulnerabilities such as human error and ease of hacking. This is due to the fact that most of the casual users typically use simple passwords that are easier to remember but also leave them vulnerable to hacking software or they use important dates and numbers that any potential malicious agent can learn using social media and other tools. The second way of identification is physical based; however, it refers to two different concepts within which are object-based and biometric-based physical identification. Object based physical identification can be used to supplement logical based authentication in the form of two factor authorization (2FA). It is a method in which a one-time password (OTP) which as the name suggests can be used only one time and it is sent over a text message to a registered mobile number or to an email account associated with the service, thus a user trying to access the information system would need to have a logical component (password) and the physical component (mobile phone or email account). Similarly, banks have begun offering authentication methods using physical token cards. Token cards function in a way similar to the 2FA method in a sense that they generate and display a one-time password that the user then uses in conjunction with the logical authentication such as the username to enter the information system. However, it is safer than 2FA method as the token also requires a password input that is correct before displaying a one-time password that will grant access to the system. Other forms of object-based authentication include identification cards with coded information required for identity confirmation which enables instant access to the information system (Spremić, 2017). Alternatively, users can use biometric-based authentication which denotes the usage of some biological trait of the user in order to access the information system. These biological traits can be fingerprints, voice, facial recognition software, iris recognition software and even DNA recognition procedures. However, these methods are fairly new and costly to implement as a technical and reliable solution. They are plagued with problems such as false negatives and false positives in identification resulting in locking out the true user and other times granting access to an unauthorized person as a result of a software error. Additionally, due to the cost related in implementing such method on the scale of the whole business it is not a realistic option for most businesses that require their users having to go

through some sort of authentication process (Spremić, 2017). Implementing the procedures and methods discussed in this section will lower the risk of the confidentially pillar being violated.

Once the user is authenticated and connected to the information system and the confidentially pillar is preserved the potential danger does not cease. Data transmission is a particularly vulnerable area of any information system as the data being transmitted leaves the zone of security and privacy of the intranet and could potentially be available on any public or private network (Spremić, 2017). As previously mentioned, it is indeed possible to intercept and thus interfere with data being transmitted by either stealing it, altering it or by simply destroying it. In order to protect information systems from such threats it is prudent to use a combination of surveillance and encrypting technologies and various protocols in order to ensure data integrity during transmission. The first and the most basic forms of protection for transmission of data can be found in the use of various internet protocols. The choice of protocol used for protection will depend on the use case and the way information is being transmitted. These protocols are: FTP, SCP, SSL, TLS, HTTPS and IPsec to name a few. The most basic and almost universal at this point are the file transfer protocol (FTP) and secure copy protocol (SCP). They differ in the fact that SCP better handles one-time data transfers within one network. On the other hand, FTP is better suited for encrypting communication between distant servers. What they share in common is the transfer speed and the fact that both operate in the application layer, but SCP has an advantage in terms of encryption level offered making it better suited for encryption of sensitive data. Security socket layer (SSL) is a protocol that uses encryption to protect the data much like the first two protocols; however, this protocol offers procedures for identification of the server and of the client. Transport layer security (TLS) is a protocol that can be viewed as an upgrade of the SSL protocol in the sense that it creates a tunnel otherwise known as VPN connection between the server and the client. The most common security protocol used today is the HTTPS protocol and it is an upgraded security version of the HTTP which enables webpage viewing in the first place. HTTPS is commonly used for encrypting highly confidential data such as online banking transactions and internet shopping. IPsec refers to the newest family of internet protocols intended for securing internet data communication through authentication and data encryption procedures. Its advantage is high flexibility and degree of security no matter which device or web browser is being used to access the information system (Spremić, 2017). However, internet protocols alone are not enough to stop unauthorized access during data transmission and thus solutions such as virtual private network (VPN) can be used. Naturally, VPN uses the internet as a means of data transfer and communication, but privacy is achieved

by using methods of encryption and tunneling. Because the traffic between the device and the network is encrypted, the communication and data transfers remain private and protected throughout the transmission process. Virtual private network can be imagined as a tunnel between the client device and the server that is virtually invisible. It works in such a way that the client computer connects to a VPN server, which can be located anywhere in the world, which then connects to the destination server. When using a VPN network, it is extremely difficult for potential malicious attackers to steal any information or redirect the client device to another server. Also, it is difficult to even track which pages are being visited by the client device at all. Even if they manage to get insight into location from which the website is accessed, they will instead see the site of the VPN server and not the client device thus ensuring privacy and data protection (Kelam, 2018). In order to ensure maximum anonymity and security over the internet a user can decide to use the onion router (TOR) system. TOR system is designed with layer encryption in mind which means the data is encrypted several times over during each passage through a randomly selected node. Additionally, the relay circuits are reset every 10 minutes by random selection so that these actions cannot be linked to a single user. Communication over TOR network is routed through a distributed server network – the so called server onion which protects users from websites that attempt to tamper with client information and from attackers attempting to gain access to potentially sensitive data and even from the onion server itself as it stores no user data at all, it is merely a channel for transmission. TOR system also represents a platform that allows creation of new application with already built-in security and privacy features. VPN and TOR system can work in together in unison and this solution is called TOR over VPN which ensures the best possible anonymity and security over the internet provided that the user is knowledgeable and will not access malicious content intentionally (Kelam, 2018). Figure 7 represents VPN system solution applied in real world.

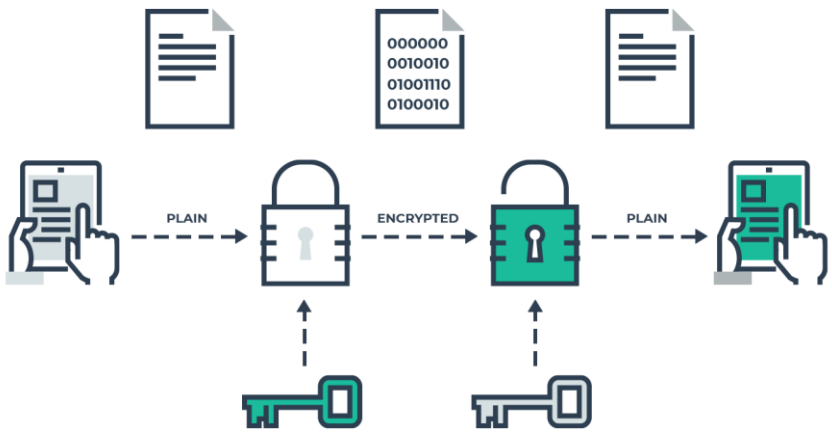
Figure 7:



Source (Pixel Privacy, 2019)

So far in this section, only protocols and tunnel solutions were discussed as a means of securing data during transmission. However, encryption is another technique which can be used to convert data into an unreadable form before even transmitting it over the internet, thus even in the event of data being intercepted the attackers will have no value of their plunder as it will be unreadable to them. Encryption provides a high level of protection and is considered as the best practice to employ in order to protect valuable information. In essence, encryption is a process in which data is transformed into binary non-sensical string making it unreadable without a key. Algorithms such as the BASE64 can be used in order to encrypt the data (Veinović, Adamović & Milenković, 2010). Generally speaking, there are several methods of encryption available to the user on the market. Firstly, symmetric key encryption denotes an encryption method in which both the sender and receiver have a single key which can both encrypt and decrypt the data. The second method, and generally considered a more secure method, is the asymmetric key encryption otherwise known as public key encryption. Meaning all the users on the network have a key that can be only used to encrypt the data, while only one or several key figures in the network possess a key that can be used to decrypt data. Naturally, this method is also deemed as the safest method of encryption before data transmission due to the difficulty of obtaining a decrypting key (Pande, 2017). Figure 8 illustrates public key encryption.

Figure 8:

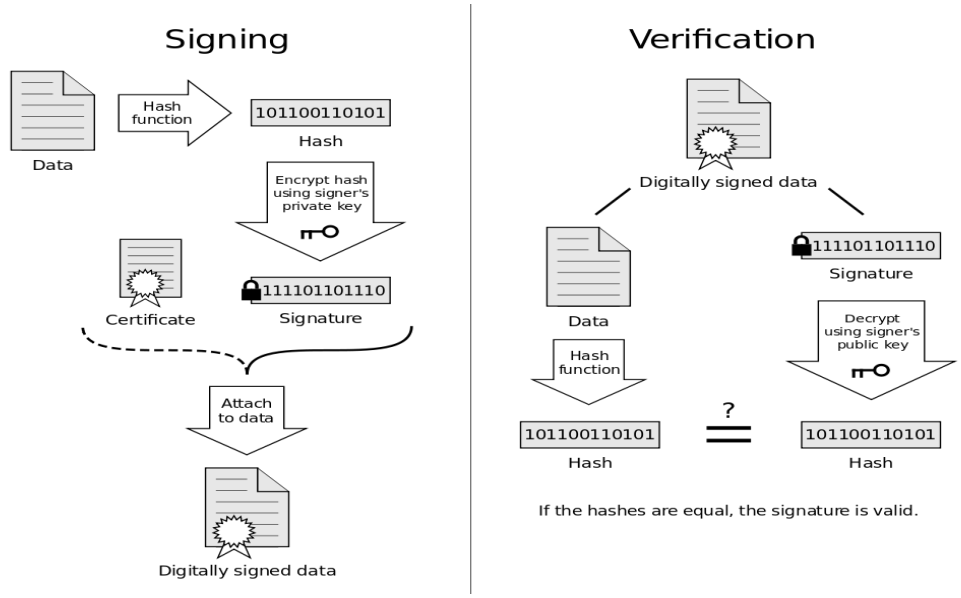


Source: (Pixel Privacy, 2017)

A combination of authorization and encryption techniques is known under the term of digital signature. It is a technique for data validation which is a process that ensures the content of the received data is certified and the sender is identified. In other words, it is an electronically generated signature assigned to the data being transmitted. Both the sender and the receiver create a pair of complementary keys, one public and one private key. Both sides exchange their public keys. When they want to communicate and send data to each other the private key is

used to create a digital signature in the data. Only by using the public key of the sender, the data can be verified by the receiver, and the contents of the message considered authentic. In the case that the data is tampered with in any way during transmission, it can no longer be re-encrypted as the private key is possessed only by the original sender and thus when it arrives to the receiver the data will not be verified as it does not possess the required digital signature anymore. Apart from security and privacy concerns this method also addresses legal concerns in cases where necessary as the sender's authenticity can be checked and verified (Spremić, 2017). Figure 9 illustrates the process of creating a digital signature.

Figure 9:



Source: (Mailfence, 2019)

Another tool at cybersecurity expert's disposal is the firewall which can be hardware-based or software-based and offers external protection to the information system. Its primary role is the scanning and control of incoming and outgoing network traffic. The firewall analyzes incoming traffic and checks for matches in the malicious code database. Any matches of the incoming traffic to the signature of the malicious code is stopped immediately and blocked from entering the information system. Firewall creates a bridge or a gate between the trusted local network and the untrusted outside network such as the internet which is considered unsafe and unreliable. The inner local network is often called the demilitarized zone (DMZ) which represents the safe and reliable sections of the information network. This enables uninterrupted communication between computers on the inner trusted network while protecting them and the data contained within from potential harmful code located somewhere on the outer network. Generally speaking, it refers to an actual piece of hardware backed up by sophisticated software

solutions that are responsible for checking incoming network traffic. Naturally, there are different configurations possible depending on the safety requirements and the network properties. Today, an ever-growing share of firewall solutions are solely software based and are packaged with other solutions as we will discuss in the following section (Spremić, 2017).

Antivirus software is dedicated to protecting your systems from a number of malicious threats that range from various kinds of viruses, worms, trojan horses to rootkits and other malicious code that spreads across the internet. Similarly, to the firewall solution, the antivirus software uses a detection engine that scans your computers data and checks it for a match against a database of malicious code signatures. If a match is found in your system that means a threat of some kind is likely present, and in the default settings the antivirus software usually destroys it automatically. However, it is recommended to adjust user settings so that the antivirus software firstly quarantines the suspected malicious code and enquires the user to examine the incident personally before destroying it. This is done in order to prevent false positives from occurring and resulting in the antivirus software automatically deleting necessary or wanted non-malicious software present on your computer. Today most of the antivirus software solutions on the market offer real time active system protection. Additionally, as previously mentioned most of antivirus software today is bundled together with firewall solutions. This is done in order to achieve all around protection both from outside threats and from threats that have potentially compromised the outer firewall and managed to infiltrate the information system (Pande, 2017).

Lastly, steganography can be defined as the technology and the art of hidden writing. It not only applies to the sphere of digital technologies, but it has been used in many forms over the past centuries to hide confidential information in plain sight. Today, steganography is used to insert information in the unused section of the information packages that are transmitted over a network. The hidden data can be transferred in seemingly meaningless content such as document files, images, audio files, programs or protocols. The transmission, security and integrity control are handled by communication protocols as it is assumed that it is not necessary to further encrypt the data since no one suspects it hiding a secret message. This information is virtually undetectable and requires specialized software in order to read it (Dragičević, 2004). Naturally, the tools presented in this section do not cover all the tools available to the cybersecurity specialists today as that would venture beyond the scope of this thesis whose primary focus is the threat of social engineering.

4. Overview of Social Engineering

4.1 The History of Social Engineering

Social engineering has been a part of the human history for as long as there was known civilization. Although no nations or intellectuals of the history ever developed specified theories for it, the underlaying concept was certainly used by many governments and organizations throughout history. The term social engineering or (*sociale ingenieurs*) first appeared in an essay by the Dutch industrialist J.C. Van Marken in 1894 which outlined the idea that modern employers needed the assistance of specialists in handling the human "problems" of the world just as they needed the technical expertise of ordinary engineers to deal with the problems of the machines. Therefore, in the wider sense of the term social engineering refers to altering social circumstances for the benefit of a third party. Needless to say, those that carry out the social engineering must have reliable information about the society and effective tools in order to fulfill the wanted result. These tools and techniques were often employed by brutal totalitarian regimes of the history such as the Nazi regime in Germany, communist regime in Soviet Union and Communist China and in many of the dictatorial regimes throughout the world and history. According to Podgorecki, social engineering can be viewed as a paradigm for developing and promoting socio-technics that could serve as an alternative to traditional top-down social engineering methods. Socio-technics were used a concept that described certain forms of social intervention in the political context and only sometimes as a label for academic discipline of studying different forms of governmental and social strategies. In other words, it is an analytical discipline of making the rational choice in political processes and social practices that produces a certain wanted result. However, socio-technics can be applied on the level of the individual, family and not just in terms of political programs. Therefore, it means the application of the theory on both the macro-sociological and micro-sociological level (Podgorecki, 1996). What is common for all these various theories of social engineering is the idea that the opinion of humans both on the individual and societal level can be influenced by employing certain techniques without the subjects being aware of such techniques being applied to them. Therefore, an organization or a government could use such techniques to sway the opinions of the society in their favor and thus influence the results of an election or a business deal. These techniques could be used for both positive and negative actions. Thus, when talking about social engineering in scope of the thesis, we shall discuss the use of social engineering techniques through the use of digital technologies.

4.2 Conceptual Framework of Social Engineering

The following section shall outline a conceptual framework of social engineering that will be crucial in understanding the methods used in conducting social engineering attacks in the realm of cyberspace. While in the previous section we have explored the general terms related to social engineering and the philosophy behind it in order to gain a better understanding of the underlaying concept, this section will provide a in depth look at the concept.

There are many definitions of social engineering depending on the author and sphere of thought we observe. In a broad sense, social engineering can be defined as the act of manipulating a person into taking an action that may or may not be in its best interest which may include gathering or divulging information, granting access to a place or a system or performing certain actions. This definition of social engineering can be applied to everyday life; it is used in the way professors interact with their students, parents with their children, doctors with their patients, lawyers with their clients, politicians with their voters and even in dating (Hadnagy, 2011). However, such a definition is indeed a very broad one, therefore it is prudent to come up with a narrower definition in terms of digital technologies. A closer definition of social engineering states that it is: "*the name of the category of security attacks in which someone manipulates others into revealing information that can be used to steal data or money, steal access to systems of cellular phone or even steal your identity. Such attacks can be very simple or very complex. Gaining access to information on the phone or through the web sites that users visit has added a new dimension to the role of social engineer."* [3]Alternatively, social engineering can be viewed as the subsection of cyberattacks that do not take advantage of the operating systems, security protocols, application vulnerabilities or control measures put in place but rather the attack is directed towards the weakest section of the systems which is the human factor (CarNet, 2006). In other words, it can be described as the term that hackers use to describe attempts to obtaining information about information systems through non-technical and non-software solutions (Winkler, 2010). Whichever definition of social engineering we choose to follow, one common factor is clear among them all. Social engineering is designed to be a sophisticated attack that aims to circumnavigate the strong defensive points of the systems by aiming at what is traditionally the weakest link in any systems – the human itself. It is important to note that social engineering attacks are highly sophisticated and usually follow a preplanned course of action thus maximizing the threat of such attacks.

[3] Peltier, Thomas (2006.) „Social Engineering: Concepts and Solutions"

Such a preplanned course of action that the attackers undertake each time a potential victim is approached is often called “The Cycle”. The cycle consists of four distinct phases which are information gathering, relationship development, exploitation and execution. It is important to note that even when this cycle is followed, each social engineering attack is unique to each victim and thus each attack carries a possibility that it might involve other traditional techniques of attack in order to achieve the desired end result. Such a unique approach to each attack means that these attacks are often hard to detect and prevent (Allen, 2006). Information gathering refers to a variety of techniques that the attacker can use to find out specific information about the victim. This information can be used to build a relationship with the target or used to outright threaten the target with revealing the potentially damaging information. Developing relationship with the victim refers to freely exploiting the willingness of the victim to establish a rapport in order to put themselves into the position of trust with the victim. Once a position of trust has been established with the victim, the attacker proceeds with exploitation phase in which the victim is coerced into either revealing sensitive information or performing an action that they would not conduct under normal circumstances. Performing the wanted action by the victim could signal that the execution stage of cycle has been reached and that the goal of the attack has been fulfilled. In other cases, it might mean a beginning of a new cycle and the second stage of an attack to another victim or a system (Allen, 2006).

The motives behind the attacks can be numerous and dependent on whether the attacker is working individually or as a part of some larger organization. However, in many cases of social engineering attacks the motives are uniform. First possible motive for a would-be attacker could be found in the potential financial gain achieved from carrying out such an attack. Some attackers may have a self-interest in carrying out the attack such as finding, accessing and/or altering information stored about themselves or other individuals. In some cases, revenge may be motive behind an attack, an individual or organization may be targeted by an attacker for reasons only known to them in order to satisfy the emotional desire for revenge. Rarely, some attackers may be externally pressured by a third party into committing such an attack for any of the reasons mentioned above (Allen, 2006).

Whatever the motives behind an attack may be, it is clear that these attackers are often referred to as the “Black Hat” hackers. Black hat hackers can be seen as individuals who conduct unauthorized intrusions into various information systems for any of the motives mentioned above. Generally speaking, in order to avoid suffering legal repercussions black hat hackers

often target organizations and individuals outside of their country of origin thus not violating the laws of their own country. However, much effort has been placed into cooperation between legal entities of various countries precisely with regards to violations in cyberspace and equalization of penal and criminal laws so that the attackers suffer the consequences of their actions no matter their country of origin which is especially true for economical and political unions such as the European Union. Distinct from the black hat hackers are the "White Hat" hackers which are individuals who perform security assessments as specified within a contract. In other words, organizations and institutions may hire hackers in order to purposefully and with permission attack their information system in order to find the vulnerabilities of the security system and thus propose solutions to those vulnerabilities. Additionally, a category of "Gray Hat" hackers can be seen as the group of people who typically conduct themselves within the boundaries of the law and the contracts signed by them with various organization for whom they may be working as white hat hackers. However, they tend to push their attacks further than specified by their contract or perform reverse engineering of proprietary software and code mostly with no intent of obtaining financial gains but rather out of pure curiosity and interest (Wilhelm, 2013). Whatever the motives, causes or purposes various attackers have for their attacks, they share the tools and techniques used for carrying out such attacks. The techniques and tools used by social engineering attacks will be discussed further in this thesis.

4.3 Types of Social Engineering Threats

As we examined in the previous section; social engineering threats usually denote avoiding technical attacks on systems and instead they prefer to target the human component which can be then manipulated into providing access or information. However, social engineering attacks can also include a form of technical attack. Therefore, it can be said that social engineering attackers are multileveled and could use tools and techniques that include physical, social and technical aspects. Social engineers can conduct their attacks by using a single aspect or could combine different aspects in order to perform a much more complex attack. Therefore, we can define a combination of attack aspects as the socio-technical approach to social engineering attacks (Krombholz, Hobe, Huber & Weippl, 2014). This section will strive to examine all aspects and forms of social engineering attack no matter are they purely social, technical or socio-technical forms of attacks in order to achieve a full understanding of the array of threats faced. In addition, this section will briefly examine other more traditional malicious code-based threats that often come packaged with social engineering attacks or their deployment on a network or information system constitutes the end goal of a social engineering attack.

Since social engineering attacks do not necessarily rely on the social and technical aspect of the attacks, the attack can therefore take a purely physical form. One of the most common techniques of physical based social engineering attacks is known as shoulder surfing. This denotes a scenario in which an attacker is physically present with the victim and is discretely looking while the victim types in confidential information such as username and password. In such a way, the attacker can simply access the account or network from another computer with ease thereby compromising security of the system. Due to developments in mobile and laptop technologies such attacks are much easier to carry out and generally occur in public places such as coffee shops, airports, malls and other venues. A variant of the shoulder surfing technique can also be done by simply listening to a conversation between two people as sometimes people discuss and divulge sensitive information in public assuming that no one is listening to what they are saying (Kelam, 2018). Another method that is often used can be referred to as dumpster diving which denotes an attacker searching through an individuals or organizations rubbish. This technique works due to the fact that most people assume that no one would go searching through their rubbish willingly and thus tend to toss out potentially valuable information such as personal data, manuals, memos, print outs of sensitive information and sometimes even written down credentials (Krombholz, Hobe, Huber & Weippl, 2014).

The social aspect of social engineering attacks can also be considered as the most crucial aspect of the attack that influences much of the effectiveness of the attack. By using social aspects, the attackers mostly rely on socio-psychological techniques such as the Cialdini's six principles of persuasion in order to manipulate their victims as outlined in the book *"Influence: Science and Practice (2001)"* written by Robert Cialdini which is interesting material for anyone interested in the inner working of human psychology. Briefly stated, Cialdini wrote that any individual can be influenced and will be influenced in some manner. The underlaying goal is to understand what creates that influence. In Cialdini's opinion influence is created by six principles which are: social proof, commitment, reciprocation, liking, authority and scarcity. For instance, one common principle that the social engineering attackers often use is the authority principle. This denotes falsely presenting themselves as figures of authority in order to obtain sensitive information or access. By presenting themselves as figures of authority the attackers automatically place themselves in position of trust with their victims in order to take advantage of that trust. It is interesting to note that most of the social aspect attacks are conducted over the telephone (Krombholz, Hobe, Huber & Weippl, 2014).

Solely technical aspects of social engineering attacks are mainly carried out over the internet. There are a number of ways social engineering attackers can use the internet to gather sensitive information without necessarily ever contacting their victims. It is often easy to harvest passwords as users often use the same simple passwords for their various accounts. Some users who are not so tech savvy may even be freely providing confidential information on the internet without them ever being aware of it. Thus, attackers will often use search engines, social networks and internet forums in order to gather personal information about their potential victims. There are also tools such as the "Maltego" that automatically gather and aggregate information from various internet sources (Krombholz, Hobe, Huber & Weippl, 2014).

It is important to note that usually the most successful social engineering attacks often include a combination of several or all of the various approaches discussed above. As previously mentioned, this combination of various aspects into a single social engineering attack is known under the term of socio-technical approaches. Today a wide variety of socio-technical attacks exist, and they compose a majority of social engineering attacks carried out every year. This section will explore such techniques.

Phishing is one of the most common threats present on today's internet. In the recent years phishing attacks have increased both in number and in the level of sophistication. It can be said that almost everyone who uses the internet in some capacity has been a potential or indeed a victim to a phishing attack. Phishing derived its name from the actual activity of fishing, and it is much similar to fishing in a lake, but instead of trying to capture fish, phishing attempts to gain access to sensitive information. It can be viewed as a form of online theft that aims to steal potentially sensitive information such as usernames, passwords, credit card information, social security numbers and other valuable data (Chhikara, Dahiya, Garg & Rani, 2013). However not all phishing attacks are the same and we can distinguish between several categories such as: vishing attacks, spear phishing attacks, pharming attacks and smishing attacks. Firstly, spear phishing attacks are almost identical to a standard phishing attack however they differ in the fact that spear phishing attacks are usually targeted towards a single individual or a specific organization. Pharming attacks are more sophisticated and involve creating a fake version of a legitimate website. When users try to access the legitimate site, they can be rerouted to the fake version and thus their input information such as username and password stolen. Smishing attacks are also very common and very similar to phishing attacks, which is especially true today as modern mobiles more closely resemble computers, however the only difference being

that smishing attacks are conducted through the use of text messages. Lastly, newer and more sophisticated attacks are known under the term of vishing attacks. They can be classified as an attack conducted through the use of voice over internet protocol (VoIP) technology. This can be considered as a strategy that is similar to attacks conducted over traditional phones (Kelam, 2018).

A recent development is called a water-holing technique. Instead of targeting an organization or an individual through more traditional means such as spear-phishing, the attackers create falsified websites with content that they expect their victims to visit based on the information about the organization and hide malicious code within, in order to infect the victim's system. In other cases, they infect already existing legitimate websites that their specific victims visit with malicious code (Krombholz, Hobe, Huber & Weippl, 2014). Such a method is much more complex to implement especially if the targeted website is a part of another large organization that may possibly possess security features. However, if infection of the targeted website is successful then it is much harder to detect and prevent and thus effectiveness is potentially high.

Another common method of social engineering attacks on the internet is the baiting method. It can be seen as a combination of the phishing and trojan horse attacks. It is usually employed on physical devices such as CD-ROMs and DVD-ROMs or USB drives in order to appear legitimate. However, such a drive actually contains malware that offers access to the system or information in some way to the attackers. The attacker relies on the curiosity or the greed of the victim who finds and uses the device thus enabling the installation of malware on the victim's computer and potentially infecting an internal network if the computer happens to be a part of some organization's network. In some cases, instead of leaving the device in random locations and hoping a victim picks it up, the attacker can hand out devices as a part of falsified promotional campaign offering free music, movies or as rewards for participating in their questionnaire or other contests (Jain, Tailang, Goswami, Dutta, Sankhla & Kumar, 2016).

Pretexting attacks are another common method widely applied on the internet. It denotes inventing a false but a convincing scenario in order to gain a position of trust with the victim and thus potentially gain access to valuable information. The attacks can be performed through a variety of media such as phone calls, emails and even physical media. Pretexting is more than just mere lies and it can denote creating entire new identities which are then uses to establish trust and gain information. Needless to say, those attackers that carry out pretexting attacks

need to be very well informed about their victims in order for the pretexting manipulation to be convincing. For instance, it can be an offer to perform a service, a job offering, helping a friend to gain access or any other number of scenarios (Salahdine & Kaabouch, 2019). Pretexting attacks are also known under the name of reverse social engineering. It is a similar concept only much more complex than a simple pretexting attack. The goal of such an attack is to make the potential victim approach the attacker himself. It consists of three steps which are: sabotage, advertising and assisting. For instance, an attacker can purposely sabotage an organization's information system, then the attackers advertise stating they can fix the exact problem that occurred. The attacker will then help resolve the problem while inquiring for sensitive information such as password or coercing the victim to install certain software in order to fix the problem (Krombholz, Hobe, Huber & Weippl, 2014).

Tailgating attacks are known under several names such as piggybacking or physical access. In a broad sense it means accessing an area, building or a system by following someone who has authorized access to the target. Usually areas with restricted access require their employees to have some sort of authorization method such ID cards or RFID cards. The attackers can simply ask the victim to hold the door because they forgot their own credentials. Alternatively, they can gain access to a cellphone or a computer belonging to the organization and install malicious code allowing them information needed (Salahdine & Kaabouch, 2019). More specifically: "*RFID attacks can be performed over several layers of the interconnection system model (ISO). For instance, at the physical layer, the RFID devices and the physical interface are targeted to manipulate an RFID communication. These attacks can cause temporary or permanent damage to the RFID cards. At the network layer level, the attacker manipulates the RFID network such as the communication between the RFID entities and data exchange between these entities*."[4]

Another major threat is in the form of ransomware attacks which can target both individuals and organizations. Ransomware attacks are employed in such a fashion that malicious code is installed on the victim's computer that restricts and blocks access to the data by encrypting it and to the system resources by slowing down performance. In order to remove malicious code and regain access to the valuable data the victim is extorted into paying a ransom. Most frequently, the attackers request payment in bitcoin currency as it cannot be traced to the attackers easily. It is important to note that ransomware attacks are generally highly

[4] Salahdine, Fatima & Kaabouch, Fatima (2019.) „Social Engineering Attacks: A Survey"

sophisticated and complicated and involve six stages in order to be employed. First stage consists of writing the malicious code that will encrypt the victim's files and restrict system resources. The second stage is the deployment of malware into the victim's system. Once deployed the malicious code is installed. Naturally, in case of ransomware code command and control of the malicious code is required, attackers begin directing the code towards the data on the computer. Once the data has been located destruction phase begins in which the malicious code starts blocking system resources and encrypts the data within. When the victim's system is fully blocked the extortion process begins by contacting the victim and demanding a certain ransom. As with any type of ransom attacks, it is not guaranteed that after fulfilling the attacker's requests that access to the system will be restored (Salahdine & Kaabouch, 2019).

Pop-up messages can also be considered a form of social engineering attack although they are not necessarily always malicious in nature. Instead pop-up messages can be used in advertising and promotion campaigns. However, when used for a malicious intent they can take numerous forms. For instance, a pop-up message may appear on the user screen alerting the user about the loss of connection prompting him to input his login data once again. In such a way attacker can gain access to valuable information. Another way pop-up attacks can manifest themselves is in the form of advertising pop-up that a user may click on and instead of leading the user to a legitimate site it will instead lead the user towards a falsified website designed to deploy malicious code. Some pop-up's may alert the user of potential malicious code on their system and recommend an anti-virus solution download which is in fact the malicious code. Pop-up usually exploit the panic reaction of their potential victims in order to infect the system (Salahdine & Kaabouch, 2019).

So far, we have covered most of the forms of social engineering attacks and along the way we have mentioned more traditional methods of attacks such as malware. This is due to the complex nature of social engineering attacks which employ various solutions across multiple aspects such as technical, social and physical as previously mentioned. Thus, it would be prudent to briefly examine methods of attacks that are traditionally technical and aimed at computer systems rather than the human factor in order to gain a full understanding of the potential magnitude of social engineering attacks.

Malware which is otherwise known as malicious software is a widely used term for computer code that is designed to gain access and install itself into the target system without the consent

of the user. Once installed on a target system, malware performs unwanted and usually malicious tasks for the benefit of a third party. Another side effect of such malicious code is that it can seriously impact the performance of the host machine. Malware is a broad category of malicious code that includes a variety of cyber threats such as viruses, worms, trojan horses, rootkits, backdoors, spyware, adware and botnets (Pande, 2017).

Viruses virtually became a synonym for any malicious code that is found on the internet. Viruses are written to specifically damage the host computer by deleting or altering files, occupying memory space by replicating copies of the code and slowing down the performance of the target machine by disrupting system resources. Due to the severity of impact of such code and its widespread usage among attackers it has become the most publicized threat. It is also dangerous because it can spread via email, USB drives, digital images, audio and video files and virtually any other type of file. However, one disadvantage of the virus is that unless the executable file of the virus is initiated by a human the virus cannot be triggered (Pande, 2017). Worms are very similar in terms of code to viruses; however, they differ in the fact that worms do not require human intervention to activate themselves. Worms automatically travel inside the network in order to spread on all the machines on the network. They also replicate themselves endlessly and damage the host system much like the virus (Pande, 2017). The most dangerous and the hardest to detect malicious code is called a trojan horse. The malicious code received its name after the legend of the wooden horse that the Greeks used to enter Troy as is written in Homer's epic Odyssey. Its name is no coincidence as trojan horses disguise themselves as useful software. Often the user opens a link, clicks on a pop-up window or downloads a file claiming to be legitimate software. Apart from damaging the recipient machine in a similar fashion to worms and viruses, trojan horses can also create a backdoor in the victim's system allowing for remote control by a third party. Additionally, systems affected by a trojan horse can be incorporated into a botnet and thus used for whatever purpose the person controlling the botnet has in mind (Pande, 2017).

This thesis already explored means of protection available to cybersecurity specialists today, however, that exploration was in general terms and thus the following section shall explore protection measures that are designed specifically to combat social engineering threats.

4.4 Methods of Defense Against Social Engineering Threats

As we have previously mentioned, cybersecurity can be viewed as a holistic model approach to designing, creating, managing and ensuring the functioning of a modern information system which includes technological, organizational and social aspects. This definition of cybersecurity is even more important when discussing means of preventing social engineering attacks. This is due to the fact that social engineering attacks are much more complex and wider in scope than regular cyberattacks. This multileveled threat means that we must not solely focus on the technical aspect of defense but rather consider other approaches to defense as well. Therefore: "*The defense must have several layers of protection so that even if a hacker were able to penetrate one level, there would be other levels at which the attacker would be stopped. Since social engineering attacks are multi-layered a defense strategy is critical*."[5] Additionally, we can distinguish method of defense against social engineering as applied to an organization and to each individual. Such measures and approaches will be discussed in the following section.

When designing methods of defense on the scale of an organization - the first step is ultimately the most important one. Each organization should create and clearly define a security policy for their employees to follow. Sadly, most organizations tend to focus only on the technical aspects of the security policy and do not consider the human factor at all when implementing the policy. In order to fully solve the security problem, the organization or individuals in charge must understand the importance of development and implementation of quality, easy to follow and complete security policies, guidelines and procedures. Achieving efficient application of security policy underlines the full support and dedication of all members of the organization (CarNet, 2006).

Second and almost as important step is raising awareness and knowledge levels for all employees. Naturally, it is of great importance that all employees in the organization understand and recognize potential threats and are aware of the details of security policy put in place. However, not only potential threats and defense details are enough. It is also important to make the employees aware of consequences of social engineering attacks. This means that a good training and awareness raising programs for employees must be diverse and must go through as many possibilities and tools in order to achieve maximum effectiveness of the training

[5] Gragg, David (2003.) „A Multi-Level Defense Against Social Engineering"

program. There are three common techniques that organizations can use in order to train their employees: they can create a formally documented security policy and employee education policy, organizations can provide basic security training for all employees within the organization, organizations also need to document, monitor and periodically repeat training program for all the employees. Ultimately, it is not about creating a short-term program that the employees will have to go through out of obligation but rather about the necessity of creating and nurturing a corporate culture and a set of standards that everyone should adhere to in their lives (Kelam, 2018).

Naturally all employees should be trained at least in some capacity. However, key personnel of the organization should undergo a special and extended resistance training program. Firstly, the organization should clearly define what is meant by key personnel which can range from assistants, secretaries, customer service personnel to system administrators, engineers and managers. In a broad sense, key personnel can be regarded as anyone whose responsibilities include dealing with the general public and those who enjoy escalated rights and access to the organizations network. In essence, resistance training denotes hardening the employees to persuasion techniques. Several resistance training techniques can be used from the field of social psychology in order to prepare key personnel (Gragg, 2003). Resistance training techniques are (Gragg, 2003):

- Inoculation which as the name suggests works on a similar principle as preventing the spread of disease by the use of vaccines. Key personnel are given a similar argument as they would be given to a social engineering attacker but only weakened. Therefore, key personnel are trained in employing strong refutational arguments that buffer the attacker. Disadvantage of such technique is that it presumes that the employee will foresee the attempts of the attacker.
- Another technique is called forewarning. Forewarning denotes training in which key personnel is warned about the contents and the intent of an incoming message by an attacker but is not offered solutions on how to deal with such an attack. It was found that once the personnel knew concrete information about the message, their responses automatically increased in resistance. Additionally, forewarning of content produced a greater resistance than forewarning of intent. Therefore, it is important to forewarn key employees that an attacker will attempt to persuade them but also that the contents of their arguments will be manipulative and insincere. It is also important to note that in

order for forewarning training to be effective employees must come to regard attackers solely as criminals who are intent on performing malicious actions.

- Reality check is another technique used in resistance training. As previously mentioned, when discussing the psychology of security, most people tend to have unrealistic expectations about attacker's abilities and unrealistic optimism about their own invulnerability. This perceived invulnerability can lead to personnel ignoring risks and failing to put measures into place that combat such risks. Therefore, as a part of reality check techniques personnel are often intentionally fooled in order to demonstrate to them that they are indeed vulnerable and to teach them not to underestimate the attackers. This technique is often applied before other training techniques.

Another way to stop social engineering attacks can be found in a technique called social engineering land mine (SELM). Much like the name suggests, these are traps just like the mines on the battlefield that are set to "explode" in the face of an attacker. It is designed to expose the probable false scenario the attacker is trying to perpetuate and thus stop the attack. There are several techniques that can be employed such as: the justified know-it-all, centralized security log, call backs policy, please hold policy and key questions. Justified know-it-all refers to protection against physical based social engineering attacks. It is an employee whose sole responsibility is to know each employee of the organization on an individual basis and thus easily recognize a potential outside attacker and stop him in his intentions (Gragg, 2003). Another SELM techniques is called centralized security log which denotes having a log of security events that is being constantly monitored by information security personnel in order to prevent a potential attack. This log can be used to recognize patterns of attack as usually an attacker will try multiple vectors of attack until successful. A centralized log system can be used to recognize that events are connected to a single attacker (Gragg, 2003). Call back policy is common and well-known procedure. It denotes that system administrators or customer service representative do not fulfill personal information requests such as passwords resets or username inquires, and other questionable requests right away but rather insist on calling back at a later date. In the meantime, the calling number is checked for any inconsistencies and verified against a database. If the phone number is not listed as approved then the employee has the freedom to deny request of the caller (Gragg, 2003). Key questions rule is useful for verifying the identity of a caller asking for internal information or password requests resets. It denotes setting up specific questions for each employee that only they should have knowledge of. If the caller cannot correctly answer the question being asked of him then the requests for

personal information or password reset are dismissed and the event recorded in the security log (Gragg, 2003). Lastly, please hold policy counterattacks the psychological principle that people are easily persuaded to act against their will or undertake questionable actions once there is pressure and surprise. Therefore, a please hold policy is a SELM technique that is employed in order to combat any suspicious calls or any other calls asking for personal information or password resets by asking the caller to standby and putting them on hold. This will stop the pressure put on the employee and during the hold period the employee can log the request, discuss possible solution and decide how to verify the identity of the caller. Naturally, it is still prone to human error of the employee, but it is at least providing a chance for the discovery of the social engineering attack (Gragg, 2003).

However, these levels of defense need to be backed up by offensive actions taken against the attacker. This level is often referred to as the incident response. This is critical due to the fact that social engineering attackers usually try multiple times to breach the same organization by trying their luck with different employees. This process allows for an employee to initiate a process in which the attacker is labeled and other potential victims within the organization are notified and thus aware of the probable repetition of the attack. Thus, organizations would be prudent to employ a single individual whose responsibility is to track these incidents closely and recognize a pattern. Naturally this employee should have full access to the centralized log system in order to be effective (Gragg, 2003).

Now that we have discussed most common methods of protection against social engineering attacks on the level of an organization, it would be wise to discuss protection possibilities on an individual level as social engineering not only target organizations but individuals alike.
As already mentioned, any individual using digital technology is exposed to a certain degree of risk of falling a victim to a social engineering attack, thus it is also important to implement defensive measure on the level of individual as well. However, the most common issue faced is that most individuals think that the probability of something like that happening to them are extremely low and thus they need not worry about the threat. Another issue is that people overestimate how secure their information is and thus stop improving their security measures. Logically, this can be solved by educating individuals about the threats and consequences of social engineering. On the other hand, this is easier said than done as individuals do not gather around a centralized system such as an organization that makes organization of education and training easier. Thus, we must resort to other methods of education such as advertising

messages, news bulletins, newspaper articles, internet forums, social media and many other means. However, individuals can follow certain clues and indicators that they might be a victim of a social engineering attack. These indicators include; recognizing that someone is creating a sense of urgency in order to force the individual into making a rash decision, take note of individuals seeking information to which they do not have access to or they should already have knowledge of, notifications that are too good to be true such as competition or lottery winnings. Needless to say, if any of the aforementioned suspicious behaviors is noticed then it is prudent to cease all communication with such an individual and in some cases even warn legal entities of such attempts (Kelam, 2018). A general guideline for anyone using the internet can look this (Kelam, 2018):

- Pay attention that online transactions you are conducting are done over HTTPS protocol and make sure the website is legitimate
- Do not reveal personal information over telephone especially to unknown callers
- Never click on links, download files or other email attachments from unknown sender
- Check the legitimacy of a website before filling out any forms that request personal information
- Social media users should be careful with what they publish. Do not reveal personal information such as photographs of your house, street or house numbers or vacation schedule to name a few
- Do not download suspicious applications
- Do not download suspicious files especially those promising free music, movies or video games
- Employ various technical protection measures designed for commercial users such as email filters, antivirus software and firewall software solutions
- Be suspicious of any email communication requesting personal and financial data which are threatening the closing of an online account unless the information is provided
- Falsified and malicious email usually will not be personalized and will begin with a generic message intended for wide use
- Do not use a simple password with numbers that signify something meaningful to you such as birthdates, wedding dates and similar occasions. Instead use complex passwords that contain symbols, upper-case and lower-case letters and numbers.
- It is recommended to regularly change passwords on all of your online accounts. The recommended period can vary but usually a period of 6 months to a year.

5. Overview of Case Studies

5.1 Literature Review on Operation Aurora

One of the most famed examples of social engineering attacks was named "Operation Aurora". This attack can be classified as a text-book example of a spear-phishing attack. The attack originated from China and targeted the U.S. private sector and military defense companies in 2009. The attacks were performed by a hacker group known as "Elderwood Group" located in Beijing. It is important to note that the hackers had assistance from the Chinese government and the People's Liberation Army. However, any involvement was categorically denied by the Chinese government and army which issued a statement that these were rogue agents operating on their own volition. The attacks were aimed towards organizations such as Google and dozens of other such as Adobe Systems, Juniper Networks, Yahoo, Symantec, Rackspace, Northrop Grumman, Lockheed Martin, Morgan Stanley and Dow Chemical to name a few. The goal of the attack was to steal confidential and classified information especially information from military defense companies. Google was the only organization to publicly claim that it was targeted and admitted that Google accounts of certain Chinese human rights activists have been breached (Cyber Operations Tracker, 2010). The name "Operation Aurora" was given by Dmitri Alperovitch, who is a Vice President of Threat Research at the well-known cyber security company McAfee. A research was conducted into the attacks by McAfee. The post attack research uncovered that "Aurora" was the file path name on the attacker's machine that was included in two of the malware binaries. McAfee researchers stated that they believed this was the internal name given to the operation by the attackers (Wired, 2010).

The cyberattack was first initialized against American companies such as Google, Boeing and Lockheed Martin by sending emails to a selected group of employees within these companies which were disguised to look as if they came from acquaintances of the employees. A second venue of attack was through the "Microsoft Messenger" instant chat software in which the employees received a link to a malicious website. Once a targeted system was compromised, a backdoor was installed which disguised itself as an SSL connection to command and control servers in Illinois, Texas and Taiwan thus appearing legitimate. The infected machines then began exploring the protected intranet that they were a part of and started searching for other vulnerable system sections as well as sources of intellectual property and contents of source code repositories. In such a way the Chinese hackers obtained access to Boeings network and its top secrets such as the U.S. Department of Defense plans, engineering details and classified

Pentagon files. The backdoor stayed operational and provided access to Boeings network for almost two years before being discovered and terminated (Shakarian, Shakarian & Ruef, 2013).

The result of the cyberattack was that Chinese hackers managed to obtain roughly some 630000 files related to the development of the C-17 transport aircraft which at the time aggregated a research and development cost of $3.4 billion making it the third most expensive aircraft ever designed in the history of U.S. military. Consequently, by 2013 the Chinese People's Liberation Army successfully managed to reverse engineer the aircraft from the stolen technical files and brought it into service under the Y-20 Doppelganger designation. Similar attacks were conducted against Lockheed-Martin and U.S. drone manufacturing companies which are suspected to have stolen technical files related to development of advanced radars and sensors, radar absorbing materials, stealth technology and military drones (Shakarian, Shakarian & Ruef, 2013).

5.2 Literature Review on Northeastern U.S. College Phishing Attacks

A college in the Northeastern U.S. which shall not be explicitly named found itself in myriad of cybersecurity issues. The college itself was founded in 1800s and housed a population of 7500 students and 1400 faculty and staff members. The school periodically suffered from classical phishing attacks resulting in some security breaches. As the college did not have any on-line or in person training specifically dedicated to cybersecurity the awareness of possible threats and consequences was low. As a result of inadequate security measures, the security breaches increased in frequency and severity. At a highest peak of threats, the college recorded 5 to 6 successful phishing attacks each month. Luckily, the college administrators noted that college's fundamental operational resources were increasingly vulnerable to attack and thus began seeking a solution to the threat presented to them (Wombat Security, 2018).

The attack that prompted the college administrators to finally put measures in place occurred when a cyberattack came in the form of a fabricated email that appeared to come from the new dean's email address. The phishing attack addressed new policies and staffing changes, meaning that the attacker had information about the intended victims, and requested updates to personal information log. The attack was successful, and the attackers gained a significant amount of personal information. However, it also spurred the responsible administrators into action and towards a solution (Wombat Security, 2018).

The administrators began searching for an awareness training program that could help the faculty and all of its staff to recognize an cyberattack in the first place and to teach them how to respond properly to such a threat. What they found is that many organizations offered training via basic tools such as presentation slides and videos followed by simple quizzes. However, the administrators were aware that in order to successfully stop the threat a more comprehensive and in-depth training program was needed. They needed a training program that would give their staff interactive training and firsthand experience with simulated phishing attack. The solution was found in the form of Wombats Security Education Platform (WSEP) (Wombat Security, 2018).

WSEP primarily focused on raising awareness of cyberattacks and alerting staff behavior in order to give the best possible opportunity for a long-term defense strategy against cyberattacks. The implementation worked in such a way that initially the Wombat Security Anti-Phishing Training Suite was issued to 300 of its faculty and staff members. Within a year, it was expanded to another 300 staff members. This training suite includes a simulated phishing attacks as well as multiple interactive anti-phishing training modules. Once the training began Wombat would initiate a series of simulated phishing attacks which were then repeated every few weeks in order to evaluate if the training modules were indeed helping the faculty staff. The training modules were adjusted if the staff was having difficulty or they were not effective for that particular individual. The training program is still under effect until all the faculty and staff members are trained and proficient in dealing with cyberattacks. So far, the number of trained staff members in dealing with security attacks is 600 staff members (Wombat Security, 2018).

The results of such an extensive training programs was that when exposed to real-world phishing attacks there was a 90% reduction in the number of successful phishing attacks. Other results of the training program were that the college experienced an increase in the number of users reporting phishing emails as well as quicker response times to said threats. This means that the training program also helped increase pro-active defensive measures as well. The college is also planning to continue with training but to increase it in the level of sophistication and a number of simulations conducted. Most importantly the response of the staff exposed to the training program has been incredibly positive which is a signal for nurturing a proper organizational culture of security (Wombat Security, 2018).

5.3 Literature Review on Sagawa Express Smishing Attacks

There is a new incident in which SMS phishing attacks otherwise known as smishing attacks are claiming to come from a parcel delivery firm Sagawa Express Company. The smishing attacks involved attackers which are sending short text messages to their victims intended on guiding smartphone users towards a fake website via which they are prompted to input sensitive personal information (The Japan Times, 2018).

Apparently, the attacks are varied in complexity and not every victim is approached in a same manner. For instance, a man in Mie Prefecture received a text message claiming to come from Sagawa Express Company notifying him of an attempted delivery that included a website address appearing to be legitimate. The man was unsure if he ordered anything from the company but decided to check the website regardless. The site appeared legitimate but urged him to install an application on his smartphone. Luckily, he found the request strange and decided to call the telephone number listed on the falsified website, only to reach a man who had nothing to do with the Sagawa Express Company. According to Sagawa Express, messages and the linked websites are falsified and designed to persuade a potential victim into installing an application that will steal their personal information such as ID information, passwords and even credit card information. In some cases, the installed application can end up taking over the victim's smartphone and be secretly used to send even more smishing messages. Apparently, there are over 20 different versions of text messages and Sagawa Express Company warned their customers that they never contact them through text messages (The Japan Times, 2018).

The organization immediately notified the police in order to stop the criminals. The police issued a statement saying that they are of opinion that the rise in smishing reports are in accordance with increase in home parcel deliveries brought about by e-commerce. This statement is backed up by the Information Technology Promotion Agency (ITPA), which stated that recently the smishing attempts specifically related to Sagawa Express Company have skyrocketed from about 10 attempts to 110 attempts in a period of 6 months. The ITPA is warning people and especially customers of Sagawa Express not to visit any dubious websites or allow installation of applications from anonymous providers. If they happened to have such an application already installed on their smartphone the ITPA advised to switch the smartphone into airplane mode and then delete the application in order to ensure the application is destroyed. Similar statements and advice were issued out by Tokyo's Metropolitan Police Department. As of yet the responsible attackers have not been found (The Japan Times, 2018).

5.4 Literature Review on ChronoPay Scareware Attacks

This study case refers to a series of recent scam attempts that used a falsified security alerts on the Mac platform in order to coerce users into purchasing a security software that in reality did nothing for the user. The software was in fact bogus. The software that was recommended for installation is the property of ChronoPay which is the largest online payment processor and a rogue anti-virus software company based in Russia. ChronoPay responded to these incidents by issuing a public statement in which they are denying any involvement in the cyberattacks (Krebs, 2011).

Since the begging of May 2011, various security firms have been issuing warning to Apple users to be on the lookout for new scareware threats such as MacDefender and MacSecurity. It is believed the attack originated and spread through infected Google image search results. The victim would search for an image on Google search and once they have found the image they would generally click on the image in order to be directed to the website where the image originated from, however the website was falsified and malicious script was initiated warning the user of a security breach and recommending the user to download the anti-virus software in order to be safe. At first, the attacks required users to provide passwords in order to install these fake anti-virus programs, but later variants of the attack did not require any permission and installed themselves automatically. Once the anti-virus program was installed it began directing users to pay for software via domains such as mac-defence.com and macbookprotection.com. (Krebs, 2011).

Further investigation into the issue has shown the distinct marks of ChronoPay involvement. The most damning evidence for this can be found in the information provided by WHOIS tool which allows for users to search various domains and check who is the owner. By searching both domains it was found that they include the contact address of fc@mail-eye.com. In 2010 ChronoPay suffered a security breach in which internal documents and emails of the company were leaked. Cross-referencing these leaks shows that the contact address associated with the domains belongs to ChronoPay's chief financial controller Alexandra Volkova. The domains were quickly suspended by a company in Czech Republic after the attack became public knowledge. However, the contact address was used again to register two more domains related to Mac Security but those have not shown up in attacks yet. It is quite obvious that ChronoPay is behind these cyberattacks as a means of getting the users to purchase their anti-virus software solution which in the least is an unethical business practice if not outright illegal (Krebs, 2011).

5.5 Literature Review on FTC Scareware Case

In 2008 the U.S. District court of Maryland issued a temporary halt to a scareware scheme at the request of the Federal Trade Commission (FTC). The scareware attacks operated in such a way that they warned the users that scans have detected either viruses, spyware or illegal pornography on the user's computer and offered to download security products such as WinFixer, WinAntivirus, DriveCleaner, ErrorSafe and XP Antivirus. Once downloaded the security programs would pressure their intended victims into purchasing full version of the aforementioned security software. It is estimated that this scareware scheme has affected more than one million users (Federal Trade Commission, 2008).

According to FTC, the attackers conducted their attacks through internet advertising networks and popular websites by carrying their advertisements. The advertisement contained hidden programming code that once clicked on would deliver the user to one of the attackers' malicious websites which claimed to scan the user's computer for security and privacy issues. Naturally, the website claimed to have found problems and urged the customer to buy computer security software as mentioned above. The attackers responsible for the scareware attacks were two companies – Innovative Marketing and ByteHosting Internet Services which operated on a variety of aliases and maintained offices in various countries. The FTC complaint also named six individual defendants which have received proceeds from the scareware scheme. In the same complaint the FTC urged the U.S. District court to bar the defendants from engaging in further deceptive marketing and to provide monetary recuperation to the victims or otherwise give up the illegally obtained funds (Federal Trade Commission, 2008).

In 2011 a settlement was reached between the state and the defendants in which two of the defendants were ordered to return up to 8.2 million USD in proceeds obtained from the illegal and immoral action. Two other defendants also previously settled for charges against them for an unknown amount. At the FTC's request, the federal court carried a verdict of more than 163 million USD in damages against the final defendant in the case who was deemed as the leader of the operation. The last defendant was also banned from selling any security software and any other software that may interfere with consumers' computers and from conducing any forms of deceptive marketing (Federal Trade Commission, 2012).

5.6 Literature Review on Phishing Experiment

Not all of the case studies reviewed need to be malicious and have real world consequences in order to be useful in understanding the practical application of social engineering methods of attack. Therefore, this section will briefly overview an experiment conducted by researchers of phishing attacks.

The goal of the experiment was to achieve mutually exclusive categories of being ethical towards the test subjects and being accurate in the real-world application which is a very difficult balance to get correct. The experiment presents an implementation of the designed methods based on the user interface of online auction site such as eBay. The experiment included a sample of several hundred subjects (Jakobsson & Ratkiewicz, 2006).

The design of the experiment was as follows: „*To this end we must carefully consider the features of the attacks above that make them different from a normal, innocuous message (from the recipient's point of view):*

1. *Spoofing is used (and hence, a message constituting one of these attacks may be caught by a spam filter)*
2. *An attack message contains a malicious link rather than a link to eBay.com*

More carefully restated, our goals are as follows: we wish to create an experiment in which we send a message with both of the above characteristics to our experimental subjects. This message must thus look exactly like a phishing attack and must ask for the type of information that a phishing attack would (login credentials). We want to make sure that while we have a way of knowing that the credentials are correct, we never have access to them. We believe that a well-constructed phishing experiment will not give researchers access to credentials, because this makes it possible to prove to subjects after the fact that their identities were not compromised."[6]

The results of the experiments are given with a 95% confidence meaning it can be applied to a real-world scenario. It was found that links containing cousin domains appearing to look like legitimate sources are the most effective with 11% of users yielding credentials as opposed to only 7% of users yielding credentials to an undisguised IP address (Jakobsson & Ratkiewicz, 2006). This indicates that exploiting the authority principle discussed previously yields results.

[6] Jakobsson, Markus & Ratkiewicz, Jacob (2006.) „Real World Phishing Experiments: A Case Study"

6. Research Results

6.1 Overview of Research Results

Case study examination shows that a strong exterior firewall can prove ineffective if attackers can exploit weaknesses in human factor of the system in regard to their lack of knowledge of the cyberspace as we have seen in the "Operation Aurora" case study. Another concerning factor that was seen in the case study was the scale of the attack which affected multiple large organizations at the same time. The cyber attackers exploited the lack of employee knowledge in order to conduct spear-phishing attacks, however these spear-phishing attacks merely served as a means to deploy a backdoor solution on target systems in order to obtain classified information. Therefore, it is obvious that in today's cyberspace social engineering attacks are a complex multidimensional threat that will exert a lot of effort and investment in order to design effective protection measures.

The case study examination of the Wombat Security training program application to a college that found itself under cyber-attacks, has shown us that there are indeed effective measures that can be applied against everyday phishing attacks. However, such a training program needs to be extensive and involve multiple training scenarios and simulations of real-world attacks. Another necessary component is the willingness and dedication of those participating in these training programs. On the other hand, it can be said such training programs have only shown their effectiveness against uncoordinated individual phishing attacks that when compared to the "Operation Aurora" attack, are not as complex. Still, such threats are not encountered on a daily basis and Wombat security case offers insight into possible effective protection measures from standard phishing attacks.

Sagawa Express case study points us towards new developments in the cybersecurity field. As the widespread adoption of e-commerce and smartphone rises so do the opportunities for cybercriminals. The attack vectors are no longer limited to computer networks but rather can be employed over mobile phones with similar effectiveness especially due to the fact that the intended victims are not as aware of threats emerging from mobile platforms. The case study has also shown us that in the real-world tracing and detecting those responsible for the attacks is not a guarantee but rather an outlier circumstance.

ChronoPay case study has shown us that we do not necessarily have to put trust in large organizations having the best interest of the consumers at heart. It is not always prudent to assume just because a solution offered seems to come from a legitimate source that the cause of a problem does not also originate from that same source. It teaches us to always judge situations using our knowledge and not to solely rely on the promises of large organizations who might abuse their authority in order to scam their customers.

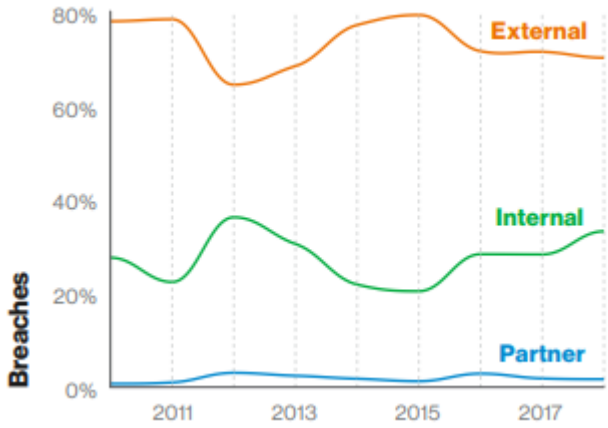
The Federal Trade Commission study case offered insight into similar scareware tactics employed as in the ChronoPay's case study. It offered insight into scale and effectiveness of such attacks and the potential financial gains for the possible attackers. It also teaches us not to always trust our panic instinct as it may be exploited by possible attackers for their own benefit. It also shows us that there are governing bodies and institutions put in place in order to protect users from such criminal acts.

Overview of the phishing attack experiment has shown us that when observing the success rate in absolute terms the overall percentages are quite low. This indicates that the volume of social engineering attacks needs to be extremely high in order to achieve a desired result. However, this fact also suggests that in such a case we can recognize social engineering attacks as they would likely not be personalized but generic attempts at obtaining information. Additionally, it once again shows us the potential for a successful attack when abusing the Cialdini's principle of authority. Attacks that masqueraded themselves as coming from authority figures achieved a higher percentage of successful breaches than those from generic IP addresses.

6.2 Future Trends

In order to anticipate possible future trends in the cybersecurity field it would prove prudent to examine some data points from cybersecurity reports of various organizations. Firstly, we shall examine data points from a Verizon data breach investigation report. Figure 10 represents the origin of the breach, figure 11 represents the motives behind a security breach and figure 12 represents the responsible parties.

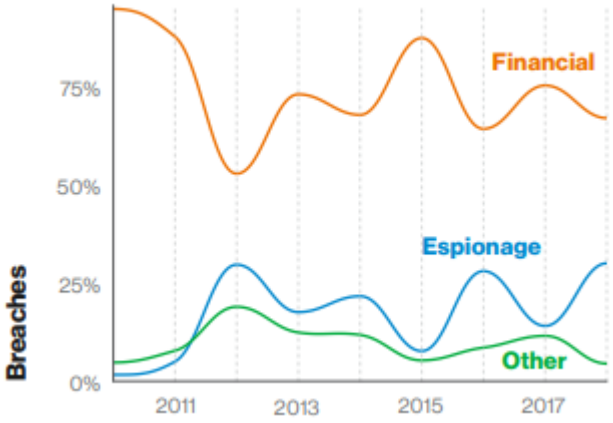
Figure 10:



Source: (Verzion DBIR, 2019)

It is immediately clear from figure 10 that the majority of breaches originated from external attackers. However, a significant portion of attacks has been internal in origin. Additionally, in the past years the number of internal breaches has been increasing. This data point indicates that organizations and those involved in cybersecurity need to be aware of possible internal threats as well as external threats.

Figure 11:

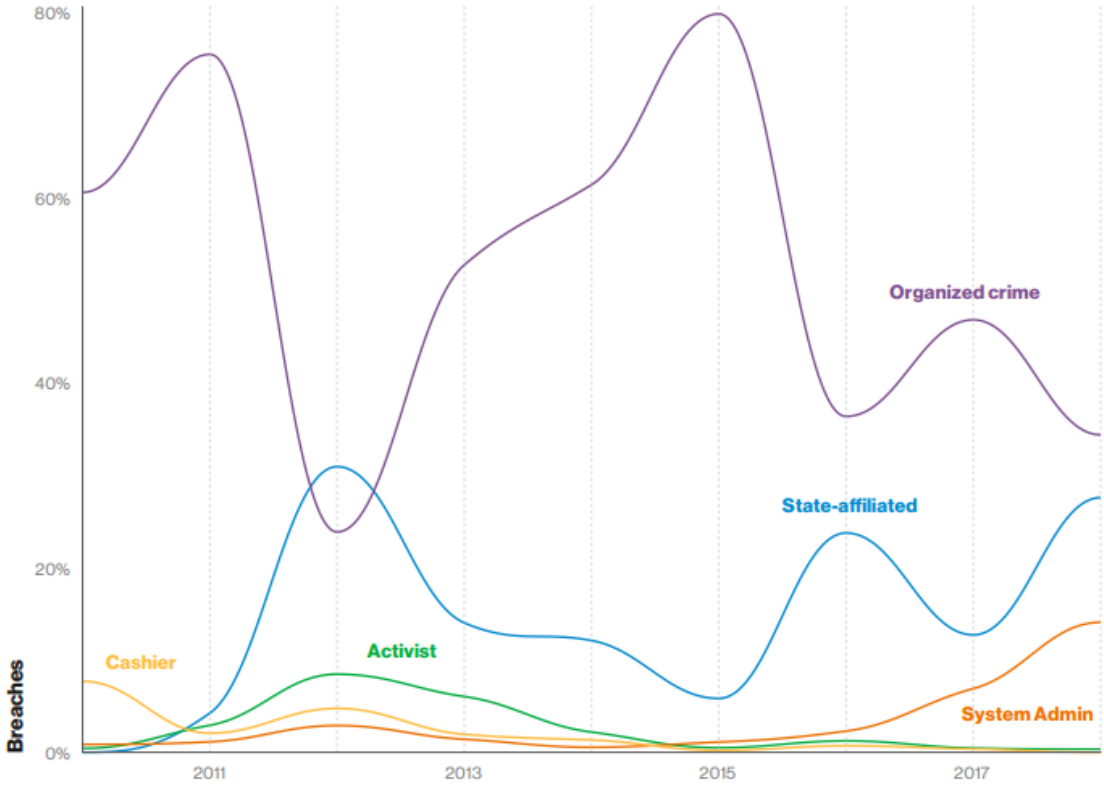


Source: (Verzion DBIR, 2019)

Figure 11 shows us the most common motive behind a cyber-attack. Naturally, the most common motive is financial gain. Significant portion of attacks are also aimed at espionage attempts. In the past quarter such attacks have seen a rise again indicating that organizations may not only be targeted for their financial assets but also for sources of intellectual property. It is also clear that other motives are decreasing in frequency indicating that it may not be worth

it for the attackers to attempt a cyberattack if they expect the risk to be higher than potential gains.

Figure 12:

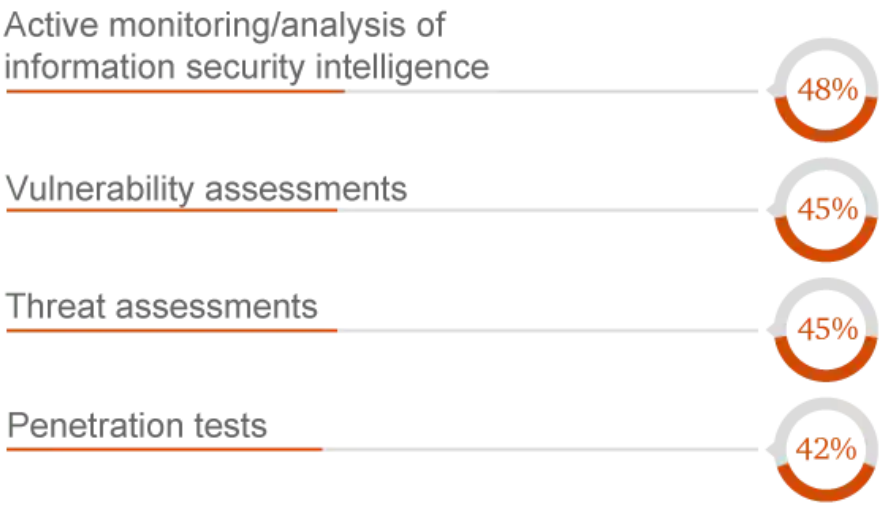


Source: (Verzion DBIR, 2019)

An interesting trend is almost immediately visible in figure 12. It shows that organized crime perpetrators are on the decrease while state-affiliated attacks are on the rise. Cross-referencing data from figure 12 with data from figure 11, we can conclude that the rise in espionage attempts could be correlated with rise in espionage as a motive. This indicates that organizations and institutions need to be aware of hostile state cyberattack attempts which are generally incredibly complex and difficult to stop. This will require new innovations and improvements in security measures.

Other interesting trends can be observed by examining the PricewaterhouseCoopers Global Information Security Survey of 2018. Figure 13 represents the adoption rate of various security measures while figure 14 represents the belief which position in the organization, and thus which individual should bear the responsibilities for cybersecurity measures and implementation.

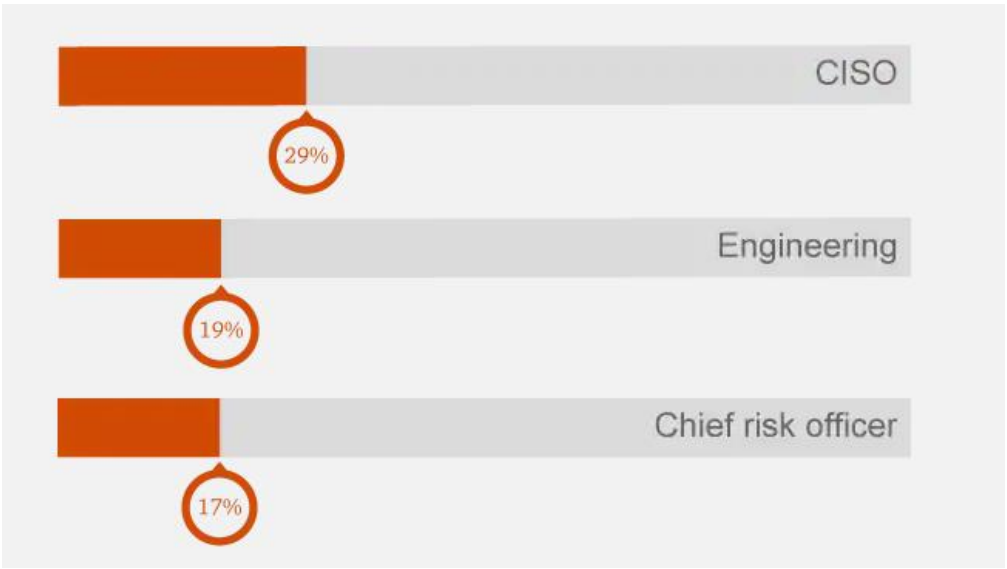
Figure 13:



Source: (PwC GISS, 2018)

Figure 13 shows the percentage of survey respondents that have adopted any of the key processes listed that are responsible for lowering the risk of cybersecurity breaches. It is incredibly concerning that less than half of the respondents have adopted a key process. This indicates that organizations are still not aware of the risk presented to them in the realm of cyberspace. This means that a majority of organizations that have been respondents to the security survey are exposed to a great deal of cybersecurity risk.

Figure 14:



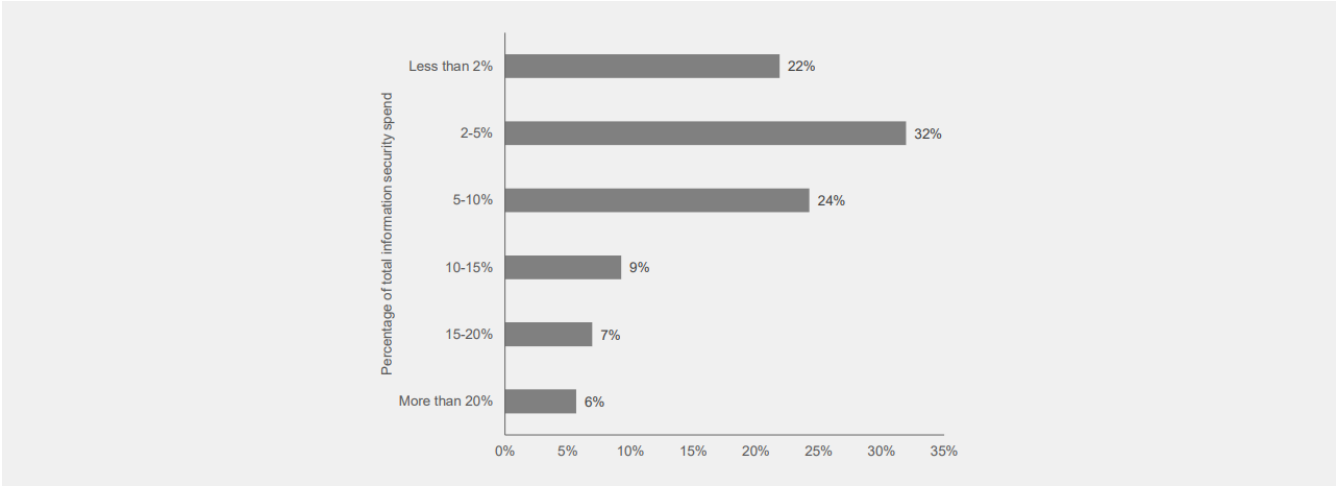
Source: (PwC GISS, 2018)

Figure 14 shows the data collected from a survey question in which the participants were asked which position should bear the responsibility for handling cybersecurity issues. 29% of

respondents indicated that this should be the responsibility of the CISO, 19% responded that the engineering should bear the responsibility while 17% of the respondents concluded that chief risk officer should bear the responsibility. This data point is also concerning as it indicates that on the industry level the consensus has not been reached on which position within an organization should bear the responsibility for handling cybersecurity risks. Naturally, this means that the set regulation and policies have not been put into place in most of these organizations.

Additional trends can be examined in the Ernst & Young Global Information Security Survey. Figure 15 represents the spending of respondents on cybersecurity in relation to the total IT budget expressed in percentages, while figure 16 represents the expected change in the IT security budget in the following year expressed in percentages.

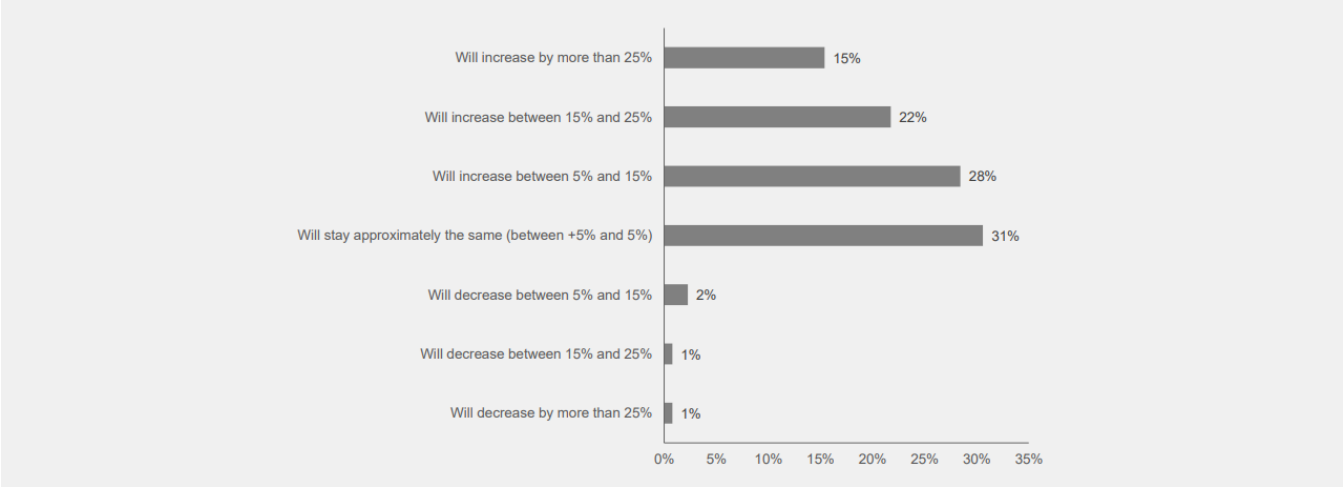
Figure 15:



Source: (Ernst & Young GISS, 2019)

It is immediately clear that a vast majority of respondents have limited or very limited budgets in terms of cybersecurity. 22% of respondents have a budget of less than 2% of the total IT budget, 32% of respondents have a budget between 2% and 5% for cybersecurity while 24% of respondents have a budget of 5-10%. This is extremely concerning meaning that in most organizations only a small amount of funds is being directed towards cybersecurity issues. This means that the specialists dealing with cybersecurity issues have extremely limited funds available to them and thus their options in dealing with cybersecurity threats are limited as well.

Figure 16:



Source: (Ernst & Young GISS, 2019)

However, the data point presented in figure 16 is more encouraging in terms of cybersecurity budgets for the following year. 15% of respondents expected to increase the cybersecurity budget for more than 25%, 22% of respondents expected to increase the budget between 15% and 25% while 28% of the respondents will increase it between 5% and 15%. Only a minority of respondents are expecting a decrease in the cybersecurity budget. This indicates that the future outlook of the respondent organizations has shifted more towards cybersecurity. The organizations are increasing cybersecurity budgets as a response to the myriad of potential threats in today's cyberspace.

Overall, several trends are visible. There is an increase in hostile state-affiliated espionage cyberattacks aimed at stealing intellectual property and other valuable information. The current spending and adoption rates of key cybersecurity processes are concerning and questionable at best. However, the spending rate on cybersecurity and thus presumably the adoption rate of key processes is expected to increase in the following years. However, cybersecurity as an industry has a lot of hurdles to go through in order to be taken as a serious and necessary component of any organization by most of organization's management boards. This will require great effort and precise and correct analysis by cybersecurity specialists today in order to prove that they are needed for safe operation of a business in the cyberspace environment.

7. Conclusion

This thesis has examined the conceptual framework of both cybersecurity and social engineering offering us insight into technical possibilities offered to cyber specialists today and the threats present in today's cyberspace. The thesis strived to emphasize the importance of cybersecurity as one of the principle priorities for all spheres of society such as military, governmental and private in the upcoming decades. The examination of various real-life case study presented in the thesis has demonstrated that an exterior firewall can prove ineffective if attackers manage to exploit weaknesses in human factor of the system. As concluded, this is mostly due to their lack of awareness of cyber threats and the lack of knowledge of security measures. Therefore, it is necessary to adopt a holistic approach to cybersecurity in which not only the technical aspect of the security will be applied but also social and organizational aspects. Extensive and in-depth training and education are necessary to keep the workforce up to date on threats present in the cyberspace. The future trends in cybersecurity are concerning, it is expected that there will a constant rise in cyberattacks especially concerning hostile state-affiliated attempts aimed at stealing intellectual property. However, organizations are starting to recognize the importance of cybersecurity for successful business operation and thus are increasing budgets in order to combat the threats presented. Needless to say, the multidimensional and complex threats of today's cyberspace will require a lot of effort and investment from organizations, governments and individuals alike in order to conceive appropriate and effective protective measures that will ensure security.

8. Literature

1. Allen, Malcolm (2006.), "Social Engineering: A means to Violate a Computer System", SANS Institute
2. Bonaventure, Olivier (2015.), "Computer Networking: Principles, Protocols and Practice", The Open University of Hong Kong
3. CarNet CERT (2006.), "Socijalni Inženjering", CarNet
4. Chhikara, Jyoti & Dahiya, Ritu & Garg, Neha & Rani, Monika (2013.), "Phishing and Anti-Phishing Techniques: Case Study", International Journal of Advanced Research in Computer Science and Social Engineering
5. Council on Foreign Relations. "Cyber Operations Tracker: Operation Aurora": https://www.cfr.org/interactive/cyber-operations/operation-aurora, Council on Foreign Relations
6. Dragičević, Dražen (2004.), "Kompjutorski Kriminalitet i Informacijski Sustavi", IBS Zagreb
7. Dragičević, Dražen (2015.), "Pravna Informatika i Pravo Informacijskih Tehnologija", Narodne Novine
8. Ernst & Young Global Information Security Survey (2019.), "Is Cybersecurity About More Than Protection?", Ernst & Young
9. Federal Trade Commission (2008.), "Court Halts Bogus Computer Scans", Federal Trade Commission
10. Federal Trade Commission (2012.), "FTC Case Results in $163 Million Judgment Against Scareware Marketer", Federal Trade Commission
11. Gardner, Michael (2017.), "Cybersecurity for Beginners: Stay Safe", Wombat Security
12. Gragg, David (2003.), "A Multi-Level Defense Against Social Engineering", SANS Institute
13. Hadnagy, Christopher (2011.), "Social Engineering: The Art of Human Hacking", Wiley Publishing
14. International Telecommunication Union (2018.), "Statistics": https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx, International Telecommunication Union
15. Jain, Akshat & Goswami, Harsh & Dutta, Soumiya & Sankhla, Mahipal & Tailang, Harshita & Kumar, Rajeev (2016.), "Social Engineering: Hacking a Human Being Through Technology", IOSR Journal of Computer Engineering

16. Jakobsson, Markus & Ratkiewicz, Jacob (2006.), “Real World Phishing Experiments: A Case Study”, Semantic Scholar
17. Kelam, Ivana (2018.), “Socijalni Inženjering kao Metoda Otkrivanja Povjerljivih Informacija”, Sveučilište u Splitu
18. Krebs, Brian (2011.), “ChronoPay Fueling Mac Scareware Scams”, Krebs on Security
19. Krombholz, Katharina & Hobel, Heidelinde & Huber, Markus & Weippl, Edgar (2014.), “Advanced Social Engineering Attacks”, Journal of Information Security and Applications
20. Mailfence (2019.), “Secure and Private E-mail Service”: https://blog.mailfence.com/how-do-digital-signatures-work/, Mailfence
21. Pande. Jeetendra (2017.), “Introduction to Cyber Security”, Uttarakhand Open University
22. Peltier, Thomas (2006.), “Social Engineering: Concepts and Solutions”, The EDP Audit, Control and Security Newsletter
23. PixelPrivacy (2017.), “What is Encryption and how does it Work”: https://pixelprivacy.com/resources/what-is-encryption/, PixelPrivacy
24. PixelPrivacy (2019.), “What is a VPN and What Does it Do?”: https://pixelprivacy.com/vpn/, PixelPrivacy
25. Podgorecki, Adam & Alexander, Jon & Shields, Rob (1996.), “Social Engineering”, Carleton University Press
26. PricewaterhouseCoopers Global Information Security Survey (2018.), “The Global State of Information Security”, PricewaterhouseCoopers
27. Salahdine, Fatima & Kaabouch, Naima (2019.), “Social Engineering Attacks: A Survey”, MDPI Publisher of Open Access Journals
28. Shakarian, Paulo & Shakarian, Jana & Ruef, Andrew (2013.), ”Introduction to Cyber-Warfare”, Elsevier Incorporated
29. Spremić, Mario (2017.), “Sigurnost i Revizija Informacijskih Sustava u Okruženju Digitalne Ekonomije”, Ekonomski Fakultet Zagreb
30. Spremić, Mario (2018.), “Enterprise Information System in Digital Economy”, Faculty of Economics and Business Zagreb
31. Technopedia (2011.), “Internet”: https://www.techopedia.com/definition/2419/internet, Technopedia
32. The Japan Times (2018.), “New Smishing Scams Baiting Smartphone Clients of Sagawa Express”, The Japan Times

33. Veinović, Mladen & Adamović, Saša & Milenković, Miloš (2010). “Strategija Zaštite Baza Podataka”, Fakultet za Informatiku i Menadžment Beograd
34. Verizon (2019.), “Data Breach Investigations Report”, Verizon
35. Wilhelm, Thomas (2013.), “Professional Penetration Testing (Second Edition)”, Elsevier Inc.
36. Winkler, Ira (2010.), “Social Engineering and Reverse Social Engineering”, IT Today
37. Wired (2010.), “Google Hack Attack was Ultra Sophisticated, New Details Show”: https://www.wired.com/2010/01/operation-aurora/, Wired
38. Wombat Security (2018.), “Successful Phishing Attacks at a Northeastern U.S. College Drop by 90%”, Wombat Security