Universiteit Leiden

MSc. ICT in Business

Cybercrime as a driver to security innovations in Dutch SMEs: *A comparative case study*

Name: Alexandra Naron

Student number: s1462059

Date: 27/10/2017

1st supervisor: Prof. Simcha Jong Kon Chin
2nd supervisor: Dr. Arno Knobbe

MASTER'S THESIS

Leiden Institute of Advanced Computer Science (LIACS)
Leiden University
Niels Bohrweg 1
2333 CA Leiden
The Netherlands

Table of contents

ABSTRACT

Technology development has become an important source of value. It provides new opportunities for both criminals and organizations worldwide. Nowadays, with the emergence of more sophisticated forms of cyber threats companies need to be prepared to fight back in the form of innovations. Developments in both cybercrime and cyber security provide enormous boost to the overall technological development as new software and security means are emerging each day.

Innovation is a phenomenon that not only represents means to increase competitiveness and market share but also appears as a change and adaptation instrument necessary to survive in the environment in which organizations operate. Both opportunities and needs can arise as a result of cybercrime and different perspectives, strategies and organizational goals can affect the types of adjustments necessary for minimization of its impact. Based on this, innovation can be expressed in a form of initiative, organizational strategy, new product or service, paradigm or process as a reaction to internal and external forces caused by cybercrime. In this respect, innovations are these countermeasures that help organizations to respond to future or past events and experiences related to cybercrime.

Small and medium enterprises are nowadays more vulnerable to attacks than larger organizations due to various factors, such as shortage of funds to provide sufficient level of protection, lack of awareness and low defence barriers. This research presents a description of four types of innovation among SMEs in the Netherlands that originated as a direct or indirect response to cybercrime. The types of innovations considered are based on the 4Ps framework that identifies the most common innovation types: product, process, paradigm and position innovations. The aim of this research was to illustrate all four forms of innovations that originated as a response to cybercrime, so the choice of companies was based on availability of each particular innovation in each case organization. Another goal was to discover through literature study and interviews whether cybercrime can be seen as a driver to security innovation. This is a new perspective on the cybercrime and due to shortage of literature on that particular point of view on cybercrime, various aspects related to innovation, cybercrime, technological and organizational development were considered.

Various innovations help organizations to achieve certain business goals, maintain or increase the level of profitability, make operations more efficient or bring financial and socio-economic gains and benefits. Criminals have also their motives, mostly related to receiving financial gains or obtaining valuable information, which is illustrated in some of the case organizations. As a result, it was discovered that the cybercrime phenomenon can affect organizations in very different ways and be a driver to security innovations. It was also discovered that the mechanisms for the innovation on both cybercrime and security sides are based on the needs and demands, that are mostly financial. The common conclusion of four innovation case studies was that if cybercrime would not have taken place there would have been no need in fast innovations and improvements to a certain degree on security side. Proceeding from there was presented a summary, assessing dimensions of innovation based on various characteristics that are linked to cybercrime dimensions, such as type and generation of the crime and its motives and impact levels. The following table is presented in the conclusions part and contains summary of the findings of four innovation cases considered in the thesis. In the empirical findings part it is described that some forms of criminal innovations can also have a business value for the firms not involved in the crime, but could have rather exploit creativity of outlaw innovations in their own business interests. It is also defined why cybercrime can be seen, in some cases, as a change agent making organization adapt to new circumstances and environments where they operate. This change can be compared to organizational changes in previous decades where companies were going “green” and by doing that, proved to be trustworthy. This applies well for companies that employ security measures and are willing to provide securer services for their customers and enhance their corporate image.

To summarize, this report is aimed, with the help of literature and case study analysis, to illustrate a new cybercrime phenomenon from perspective of a driver to security innovations among SMEs in the Netherlands and its implications to organizational development and adaptation mechanisms.

Key words: SMEs, cybercrime, innovation, threat, countermeasures, malware.

List of figures

List of tables

1. Introduction

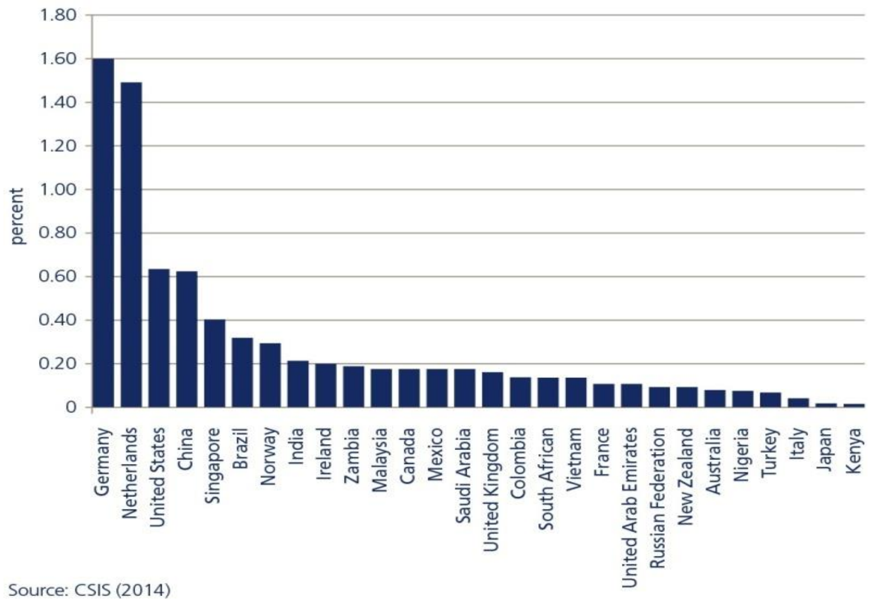
The topic of a cybercrime is gaining more popularity each day and is being one of the hottest topics on the news, and challenging at the same time. Each day organizations in the Netherlands as well as around the globe face cyber attacks undertaken for the purpose of sensitive data theft, exploit of program vulnerabilities, service type attacks and spread of viruses and malicious programs. For example, the malware WannaCry and Ransomwire have recently brought a tremendous damage to not only European region, but have literally affected organizations on a global scale. And this trend seems to increase which indicates that the cybercrime is one of the biggest issues in today's society [1].

According to Deloitte, only Dutch organizations lose 10 billion euro each year from cyber attacks, and, in the worst case scenario, an individual organization can experience losses up till eighteen times higher than anticipated [2]. The consequence of this comprehensive problem is increasing need for different organizations to be able to adapt and respond to existing and new forms of threat that comes with cyber criminality. This may lead to changes and different innovative projects and initiatives undertaken within different types of organizations that are aiming to adjust and to continue their operations within a current not always safe environment and to develop more business-driven security models [3]. In this respect, cybercrime can also be seen as a contributing factor to innovation within organizations who are currently adapting not only in terms of new software tools and applications but through changing their entire strategies and mental models in accordance with new cyber security requirements. Hence, here the cybercrime can be seen partially or fully as a motive or driver for these companies to innovate.

The current thesis presents relevant concepts on cybercrime and innovation and explores cybercrime influence innovation and organizational development and adaptation processes which is illustrated more in-detail through case studies. These case studies are analyzed with help of the literature and through empirical survey among four different SMEs in the Netherlands which implemented the following four main types of innovation: product, process, paradigm and position innovation. As a result, the analysis of innovation dimensions and related cybercrime dimensions and the impact are presented in the summary table in conclusions part which describes these innovations, originated due to direct or indirect impact of cybercrime phenomenon. That table summarizes concepts on different innovation dimensions and can be used as a framework to describe innovation more in-detail applying any other driver.

1.1 Cybercrime in the Netherlands

The cybercrime is seen as an international issue. The figure below shows the percentage of the cybercrime associated with cost levels per country, with the Netherlands being one of the leading countries that are exposed to cybercrimes.



Source: CSIS (2014)

FIGURE 1. COUNTRIES' COST OF CYBERCRIME AND ESPIONAGE COMPARISON IN PERCENTAGE GDP

Furthermore, according to the report provided by security entity – Symantec, the Netherlands is perceived as a number one country in Europe and fourth in the world that is the most exposed to cybercrime because Dutch servers are processing a large amount of spam, phishing, botnets and other digital threats. It also indicated that the Netherlands is highly popular among cyber criminals due to an excellent network of fast and reliable connections with Amsterdam having one of the largest Internet junctions in the world [4].

The Netherlands is seen by the cyber criminals as a one step in an attack and the threat here is difficult to trace [4]. According to the report provided by Centraal Bureau voor de Statistiek (CBS), nearly 20% of Dutch entrepreneurs become victims of cybercrime each year and from 2,5 million cyber incidents that were detected in the Netherlands in 2016 only 27% were reported to the police [5].

According to Cyber Security Assessment Netherlands 2017 (CSAN), the digital capabilities to defend against the threat are insufficient nowadays. The government, businesses and citizens are taking steps forward to increase their digital resilience. Currently, businesses are investing a lot in development of digital security items as well as in the necessary knowledge and expertise in the field of cyber security. This trend is predicted to increase, according to CSAN. The four main trends in ever increasing threats to digital data are as follows [6]:

- Professional criminals have become mature players that implement long term and high-quality operations to outperform security experts
- The digital economic espionage by foreign intelligence puts the competitive capabilities of the Netherlands under pressure
- The malware becomes more sophisticated and advanced
- Advertising networks are not able yet to tackle the problems of malvertising.

According to CSBN, there is a lack of knowledge and investment in cyber security among the population to be able to defend against threats. The cyber security issues and challenges are also highly popular among CEOs [7].

The industry of cyber security is predicted to grow to more than $170 billion by 2020 compared to $75 billion in 2015, according to Cybersecurity Market Report [8]. According to Cybersecurity 500, a worldwide compilation of leading companies that provide innovative cyber security solutions and services also include three Dutch companies, namely, AVG Technologies, BWise and Eclectic IQ [9].

An increased investment in cyber security and innovation among enterprises can be seen as implicit evidence that the rise in the cybercrime has led to the development of new technologies and innovative products as countermeasures to defend against attacks.

1.2 Study relevance

The topic of cybercrime is highly relevant to the society nowadays. The interest in cybercrime and security and their impact on social, economic and technological spheres is rapidly increasing. The research in the field of data security, data breaches and their consequences is more relevant than ever before and the demand for this knowledge is increasing. For the current thesis it was important to show the link between crime and innovation, which can help to see the patterns and dynamism of this relationship and what kinds on innovations can originate as a result of cybercrime.

Small and medium enterprises were chosen as a sample for the current research since SMEs are more exposed to attacks compared to previous years [10]. Being a highly vulnerable segment in the Netherlands which scores high on security breach ranking [5], it was important to show how it responds to cybercrime and what kind of security innovations can be implemented. The study also helps to see the impact size and economic benefits and gains of implementing these innovations.

The interest in the topic can lead to increased awareness on cybercrime in general among organizations that are willing to adapt to the changing environment. The ability to mitigate possible threats and be proactive or event-oriented in their approach to deal with security issues is highly important nowadays. Furthermore, companies, especially SMEs, can no longer ignore the threats. If they do, they can become a victim on the short notice, hence, it can be more expensive not to invest in security.

The following thesis is relevant to the field of study on cybercrime, cyber security, innovation, organizational and technological development. It provides a new and wider perspective on the cybercrime phenomenon as a driver, which brings a deeper understanding of the development of Internet technology in general and its consequences to the society.

1.3 Problem description

The space technologies and nuclear experiments are examples of innovations that were developed as a result of military research and development, due to the threat of war and other threatening factors. Cybercrime also falls under that category in a certain way since new protection tools are being introduced on a continuous basis as natural reaction of organizations to protect their assets. The problem of cybercrime is highly relevant to the society. The Netherlands, for example, is one of the countries that ranks the highest on the list of data breach occurrence worldwide [5]. Therefore, a lot of investment in security measures have been made which resulted in different types of services and software products and innovations in general. However, not all the organizations have been hit by a cyber threat directly yet, or experienced it in full, thus, they have a lack of awareness on that topic which makes them reluctant to change.

Previously, not much research has been done on the view of a cybercrime as enabler of innovations. However, these types of innovations exist and shape the modern society. For that reason, it is essential to have an understanding of the cybercrime phenomenon as a driver and how different parties influence each other's surroundings, hence, forming societal development as well as economic and technological development. SMEs are more vulnerable to cyber attacks nowadays [10] than larger organizations, for that reason it is important to know what kind of innovations they can implement to defend themselves from cyber attacks. And the Netherlands ranks high on cyber breach [5], so it is also vital to investigate how SMEs sector here engages in innovative activities and how it responds to threats through innovations.

The most basic forms of innovation that organization gets involved into consist of product, process, paradigm and position innovations according to Tidd and Bessant [11]. So, it is important to see how innovations evolve in all these types. It is also vital to see the cybercrime as one of the driving forces of innovation on one side and cyber security measures on another where cyber security takes a form of counter innovations. There have been little or no literature paid to the notion of cybercrime as innovator, for that reason the issue of this research is also to make that statement more explicit.

As it has been mentioned earlier, there has been little or no literature earlier to draw a direct link between the cybercrime and innovation. In order to assess the potential impact of the cybercrime, which is mostly perceived as negative, it is also necessary to look at it from the positive perspective that leads to new insights. It is also difficult to assess what kind of new developments were initiated due to cybercrime, however, using related literature, theories supported by empirical survey of main organizational innovation aspects and their approach to addressing the cybercrime threat can help to answer whether the cyber criminality can be looked upon as a necessity to innovate and to develop new approaches to security in general.

1.4 Research questions

The formulated research questions are aiming to illustrate what kind of innovation were provoked by cybercrime phenomenon, the relationship between cybercrime and innovation aspects within different organizations and the role of cybercrime as a factor leading to innovations. The main research questions are as follows:

1. *How can security innovations among SMEs in The Netherlands arisen as a consequence of cybercrime be characterized?*
2. *How can cyber criminality be seen as a driving force to innovations?*

1.5 Purpose

The purpose of this research is to show how cybercrime can be perceived as a driving force to innovation among SMEs in the Netherlands and to describe innovations that were provoked by cybercrime based on types defined by the 4P’s framework. The purpose is to describe four types of innovations, namely, product, process, paradigm and position innovations within chosen case SMEs that have these innovations in place. So, in general, the purpose is to provide a better understanding of the cybercrime phenomenon and its relation to innovation and technology with the help of supporting literature, theories and in-depth interviews. The purpose is also to take a new perspective and angle with respect of known things, e.g. to define the possible relationship between the cybercrime and counter cyber security measures and how cybercrime pushes innovation development among SMEs. Furthermore, the purpose is to explore more the cybercrime phenomenon from a driver perspective to innovation further, by looking at its impact on technology and organizational development and adaptation mechanisms since there is a shortage of scientific literature on that new perspective.

1.6 Study significance

Internet criminality is hugely affecting a wide range of spheres and activities on the net. Security measures to defend against the threat appear continuously with developers coming up with more sophisticated software tools that are increasingly adopted by individuals and organizations. Various cyber security measures are increasingly implemented by organizations. However, not much is known in academic context on the perspective of cybercrime as a necessary factor for companies to engage in innovative activities. Also, not all the small and medium enterprises recognize a fear of cyber threat before it hits directly. Therefore, it is useful to illustrate cybercrime as a driver, forcing organizations to introduce innovative solutions or modernize existing systems and to show the possible outcomes of these initiatives. The novelty of the thesis is that it examines cybercrime from perspective of a driver for security innovations, and its impact on organizational and technological development and organizational adaptations that can come in different forms of innovation. Seeing cybercrime as enabler to change, enterprises can learn to adopt better to the environment and sufficiently meet internal and external security demands. An analysis of the innovations within organizations also helps to reveal some dependencies and patterns, which can be helpful in defining dynamics between cybercrime and cyber security developments.

Furthermore, the novelty of the current work is in the problem that has not been investigated in-depth before from an explicit perspective on innovation. Apart from being a highly sensitive topic for many organizations, part of innovation research is characterized by an economic perspective, where technology and innovation are mainly seen as something that provides economic benefits to organizations. In the literature on organizational adaptation, there was nothing found that is somewhat related to crime and its impact on organizational adaptations and development. As a result, this study is considered as a useful contribution in a way that it helps to look at innovation from a new angle where an attempt is made to define the link between the crime and a need for innovation as a consequence and natural reaction.

All new knowledge that contributes to a broader understanding of a phenomenon and provides additional insight can be considered useful. The topic of the thesis focuses on a way that is slightly similar to military innovations, because innovations mainly appear as a consequence of a non-commercial threat. This way it is a contribution to a new approach to understanding of some forms of innovation that were particularly provoked by cyber security demand. Apart from this, the research also partly provides an insight into certain areas of organizational development and correlates with the three information security pillars which are people, processes and technology. Here, the people aspect or the users of technology in the context of innovation are perceived not only as passive consumers, but as individuals contributing to the development of technology and producers of innovation. This interaction leads to innovations that shape and further develop the technology itself.

Since there is a lack of literature on direct or indirect dependence of innovation from rising pressures on information safety, the study has a valuable contribution in general on subjects of cybercrime, security, innovation, technological and organizational development, business processes redesign, adaptation mechanisms and business strategy.

1.7 Limitations

The aim of this study is to define the link between cybercrime and development of security innovation. One of the limitations is the lack of scientific literature on cybercrime from perspective of a technology enabler. Also it can be difficult to assess the impact of cybercrime on a regional or country basis. Therefore, the scope was limited to four SMEs belonging to different industries in the Netherlands, each having own particular innovation in place, product, process, paradigm or position innovation. This is done to illustrate more in detail how SMEs can be affected by cybercrime, what kind of innovations they can implement and, hence, in order to describe the cybercrime from perspective of enabler of innovation.

The limitation of this research is that it is focused on the business context only and doesn't include individual innovations. Research is also limited to chosen industries and doesn't take into account all the possible innovations from other industries. This is also not a complete representation of the cybercrime and innovation relationship in the whole of the Netherlands. Since the interviewees share their own experiences within their companies, other individuals that were involved in the innovation process are not considered. Certainly, the changes don't depend only on one factor, and, normally different factors are taken into account when companies innovate, which is another limitation. In that sense, the research is limited only to one factor of cybercrime and its role as contributor for each particular innovation. There was also chosen only one company per each innovation type. Nevertheless, the chosen participants are considered as a representative sample since problems related to cybercrime and security are unified and are applicable to any organizational context within any industry.

2. Methodology

There are two main research questions that must be answered in this research. The combination of different approaches was used during the research process in order to give an answer on them. The main approach is a comparative case study among SMEs by providing examples of four main types of innovations that have been introduced due to impact of cybercrime. Using this method, it is possible to draw a common conclusion based on the various and coincidental findings within the companies on innovation types and on cybercrime as a driver. In order to fully illustrate the answer on the research questions, scientific literature was used on cybercrime, innovation, organizational aspects such as development and adaptation and associated theories, online resources and in-depth interviews.

2.1 Research design

The research design process consisted of several steps depicted in the figure below.[1]

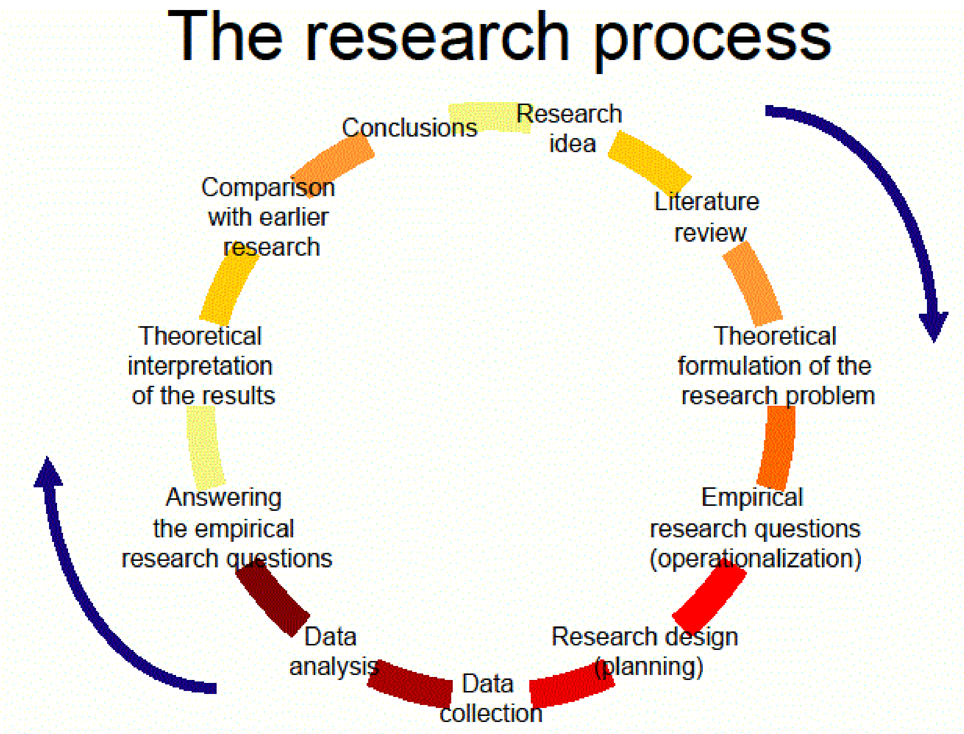

The research process
Research idea
Literature review
Theoretical formulation of the research problem
Empirical research questions (operationalization)
Research design (planning)
Data collection
Data analysis
Answering the empirical research questions
Theoretical interpretation of the results
Comparison with earlier research
Conclusions

FIGURE 2. RESEARCH PROCESS FLOW

Step 1. Research idea generation and formulation of the research topic and establishing the general direction of the field of interest for the study; definition of the most relevant key words for the search.

Step 2. Literature review. A preliminary library search including online databases and catalogues, Google Scholar search engine, Academia.edu website, scientific articles, journals, news sites, dedicated to particular topics of security websites, reports.

[1] https://academichelp.net/blog/research-process.html

Step 3. Theoretical formulation of the research problem. At this stage the needed amount of knowledge of the topic is compiled and the problem is formulated. The gaps in the literature identified. Also established certain links between the literature and the topic on what is known and what haven't been researched yet.

Step 4. Empirical research question is formulated that support the main problem and seeking to receive an answer as soon as the survey is complete.

Step 5. Research design is outlined, the necessary steps, time frames and participants are identified and questionnaire is prepared.

Step 6. Data collection on secondary data and appropriate theories that are most applicable for the topic. Primary data collection by means of in-depth interviews with company employees.

Step 7. Data analysis. Analysis of the secondary data along with primary data that was received after the interview. No special tools were used except Excel and Word tools for a better visual representation.

Step 8. Answering the empirical research question.

Step 9. Theoretical interpretation of the results and gathering data in a certain format according to the framework, aiming to describe different areas of focus.

Step 10. Comparison with earlier research. The empirical results will be combined with earlier research on the problem. Elaboration on the topic will combine both theory on cybercrime and innovation as well as data obtained during qualitative research.

Step 11. Conclusion is presented in the form summing up the findings and outcomes of the data collection and the answer on the research question.

2.2 Data collection

Data collection is based on two main sources: 1) Review and analysis of available literature and sources relating to cyber crime and innovation 2) Qualitative in-depth interviews with four SMEs in the Netherlands.

2.2.1 Scientific literature

In order to conduct a literature study, library search, Google Scholar, white papers, journals, articles, scientific publications, market research reports were used. Earlier publications on cybercrime and innovation were scanned as well as related theories, especially on availability of cybercrime as a driver statement. Since this perspective is new and is explored in the current study, all newly published works were looked through on availability of information to consider cybercrime from that angle.

Since Google Scholar has an extremely large database containing thousands of articles, different keywords were used during the search process. The literature search approach was based on the basic components that constitute the problem, namely, innovation aspect, innovation drivers, cybercrime, technological and organizational aspects. The research on these topics was also performed in the library where earlier publications were taken into account and scanned. The review of the literature gave an overview of the topics of innovation and cybercrime and the extent to which they were highlighted in the literature earlier. Among other things the relation between innovation and innovation dimensions, sources and motivation as well suitable framework on innovation types were considered and applied in the context of the cybercrime as an innovation driver.

The innovation theory offers different typologies, categorizations and definitions of innovation, and therefore the research was limited to those that are most relevant to the analysis and explanation of the empirical material and the findings in relation to the problem statement. The figure below represents the 4 types of innovation by Tidd and Bessant [11] which was used as a framework to describe innovation types within case SMEs.

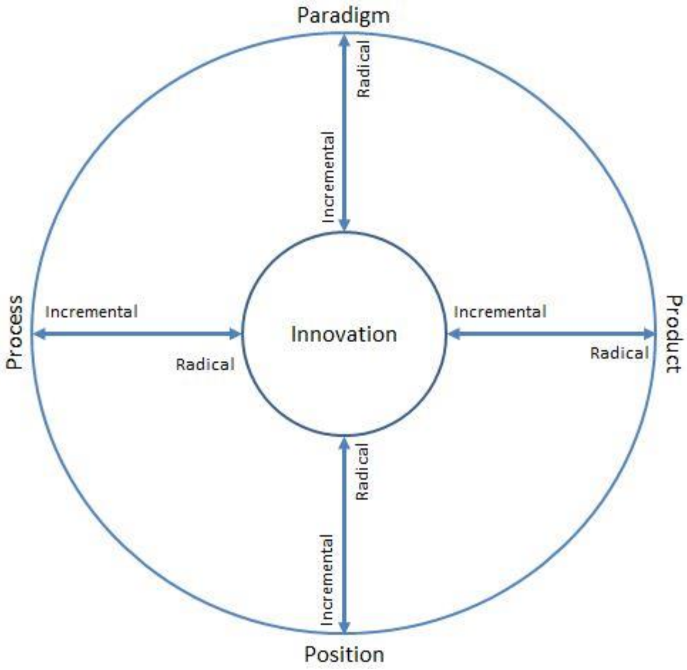


FIGURE 3. INNOVATION TOPOLOGY

Since the perspective on cybercrime as innovator is not provided by the literature from perspective as the following thesis does, different related aspects and surrounding topics were considered in order to answer the research questions. Hence, there were used various theories on organizational development, types of gains and benefits, the nature of innovation and cybercrime phenomenon, functional sources, motives for innovation and other mentioned in the literature review. In the analysis part, literature was used to link main findings with appropriate concepts and to provide certain conclusions on cybercrime as a driver, to identify innovation type and cybercrime that contributed to such developments within organizations. The findings part is based on the literature review and empirical results obtained during in-depth interviews.

In order to have a more comprehensive overview on the main and to some extent scientifically new topic of the dissertation, all the related topics and issues on organizational aspects, cyber security, cyber threats and statistics have also been reviewed.

2.2.2 Qualitative data collection

The survey was conducted in the form of a literature study and in-depth interviews with representatives of four different SME companies in the Netherlands. Motivation for the interviews was to get more in-depth knowledge on the matter of innovation, the type of innovation that was implemented on the enterprises and how it was influenced by the cybercrime phenomenon. The aim was to discover what type of innovation was implemented and to what degree cybercrime had influenced its development and implementation, as well as to find a link if the introduction of innovation was a direct response to it.

The chosen companies were directly or indirectly influenced by cybercrime which has led to innovation activities. The 4P's framework was used to map the innovations according to their type. The concepts found in academic literature were used to classify the type of cybercrime and innovation, the gains, motives and other dimensions, and to see whether certain innovations had elements of other types provided by the framework. In the findings section, the main research question on whether cybercrime can be seen as a driver to innovation is discussed in more detail using results received with the help of literature and qualitative data collection. The results part shows analysis of empirical data collection applied to related theories. In order to conduct a fully illustrated empirical results not only in-depth interviews and literature were used, but also information taken from the companies' websites as well as additional online articles and blogs on their activity.

Below is the table listing all the participants. The responses obtained during in-depth interview were used in results and findings sections. Along with the analysis of received data used for the results part, the responses received from participants were marked as R (respondent) with the number with corresponds with companies they are in.

#	Company name	Industry	Rep. name	Occupation
R1	Verwey Grafische Produkties	Publishing	P.V.	CEO
R2	Elcatronics	Cloud provider	J.K.	CEO
R3	Whitecliff Ltd.	Trust	E.R.	Finance and operations manager
R4	Contec	IT	R.G.	Security support engineer

TABLE 1. SURVEY PARTICIPANTS

The choose of in-depth interview as a qualitative research method for empirical data collection was based on opportunity to obtain information through open questions, how and why questions. The reason to choose this method was also formed due to the need to find what type of innovation was implemented in detail and what were the causes to its implementation. This type of empirical data couldn't have been easily received through other survey types and closed types of questions due to its complexity and versatility. Since cybercrime phenomena haven't been researched as a driver scientifically before, in order to understand this concept there must be performed a collection of data on its various aspects. So, this can also be done better though in-depth interviews with participants that are accustomed to the issue, considering the fact that other questions not included in the questionnaire may follow occasionally.

2.3 Participants

The qualitative in-depth interviews were held with 4 SME organizations in the Netherlands of different industries which have been directly or indirectly affected by a cybercrime phenomenon and have certain experience and the overall knowledge on it. The enterprises from different industries were chosen and considered representative since it gives the most comprehensive overview of the impact of the cybercrime on different organizational aspects, and helps to see the situation more in-depth. Due to limitations of the survey, there are only 4 organizations are chosen. But each organization represents each particular innovation within 4P's innovation space framework, e.g. product, process, paradigm and position. Hence, participants were chosen also on availability of these innovations that are implemented as a direct or indirect response to cybercrime. The purpose of choosing SMEs was with the intent to illustrate how the common issue of a cybercrime can affect various business areas, and because SMEs often fail to safeguard their businesses carefully. Besides, it was important to demonstrate that the very same phenomenon of cybercrime can cause different types of innovations and different types of industries, and other aspects described in the results part.

The chosen participants were those individuals who were able to share their knowledge and provide their opinions on the research topic. Since the cyber threat doesn't distinguish industries in its attacks, apart probably finance and electronics where more attacks are detected, the issue concerns all types of industries and company sizes. According to the latest research conducted in the field of cyber security SMEs are most vulnerable to the cybercrime since many employees are not having standardized policies and procedures and the general awareness and defence level is lower than in large companies. Small and medium enterprise are also easier to target since employees in large organizations barely share any information concerning data breach, which can have a negative impact on their reputation. The survey itself was constructed in accordance with a prepared questionnaire. Therefore, SMEs were chosen as an interesting sample that is also the most vulnerable, so it needs more research it that area.

2.4 Analysis of the results

In order to be able to answer the main research questions, literature study, empirical data collection and analysis of literature, case studies and interviews were performed. For the analysis no special tools were used. All information gathered was interpreted literally to answer the main research questions and subsequently incorporated in the results analysis and findings parts. The findings of each case were mapped according to the theoretical framework chosen for this research for a better understanding to which areas the innovations in the case correspond. The case studies analysis provided a comprehensive overview of possible causes from cybercrime and how it affected organizations in general and in terms of gains they received from countermeasures. The typology of a cybercrime is described as well as the functional relationship on innovation based on the literature. The scientific literature was used in combination with empirical findings in order to elaborate on the main research topic more in-depth in the findings part.

2.5 Validity

The data received from empirical research described in 4 case studies is explanatory in terms that it aims to highlight the aspect of a cybercrime as a driver to innovation within different organizational contexts. The fact that the cybercrime phenomenon is not to be attached to a particular industry or business sector and can affect individuals as well as corporations, the sample consists of various industries respectively which makes the sample more representable. The chosen companies were only those that were gone through changes brought by incidental cyber threats or exploiting a market opportunity in this field to supply safety products or services. The empirical data is collected from employees who have knowledge or experience of the topic. The choice of participants was also based on their openness to discuss the sensitive issue of this research. Here the focus was made not on discussion of reasons of organization to innovate, but rather on contributing factor that pushed the chosen companies to innovate due to cybercrime to a certain degree. Hence, other factors leading to innovation were not considered. The aim was also to provide an overview of 4 different types of innovations using an innovation space framework. The findings were analyzed and elaborated upon with the use of primary data received in combination with scientific literature. The analysis of results was linked to key theories on innovation, cybercrime, organizational development and adaptation. The validity of results was also supported by gathered information and statistics on different aspects of the topic. In order to be able to generalize the main findings and apply them to a certain degree within other organizational contexts, the most common types of innovation were described. It was also done to prove a causal connection between cybercrime and innovation. In this sense, it was shown that all the organizations had a common denominator which is cybercrime. Certainly, any innovation is unique in its core and depends on many other factors like size of the company, industry and other. Though, similar organizations or those that has been affected by a cybercrime to a certain degree and their innovation activities can be mapped and analyzed in similar ways. Though, the topic is not to provide a framework for analysis but to find the possible cause to innovate which are formed by cyber security need.

2.6 Reliability

The reliability of the empirical data was mainly dependent from participants’ openness towards the topic of this research as well as on their honestly in providing information in details. The following research can be seen as highly reliable since the sensitive information was shared and it can be also compared to other cases and statistics provided by previous surveys in this field. Large amount of statistical data on data breach incidents and possible causes of data breach is available online as well. So, basically the information that was received is accurate to the findings on cybercrime in organizations worldwide. Also the type of survey was not to get a numerical data which can be inaccurate or actual but rather on occasions, experiences and knowledge received that was later transformed in the form of innovation. That makes it possible to provide a more in-depth overview of the causes, hence, links between cybercrime as innovator to a certain degree.

2.7 Ethical considerations

The information provided by organizational sensitive issues can be used for a better security awareness among SMEs as well as other organization. The disclosure of information was agreed prior to interview and was given away only with the agreement of organization on this disclose. Some organizations may fear to share their experience with data breaches, which can lead to lowered reputation and loss of trust among the clients. So, the confidentiality and integrity aspects were taken into account while preparing a survey. Only those participants who was able to share the information was interviewed. Some of the employees are, however, willing to share their personal experiences to show that there is a reason to public be more alert. Moreover, it is seen as ethical to disclose some information to the public to raise the awareness, instead of keeping it unspoken. Hence, the knowledge and experience received from case organization in general terms can benefit the society and boost the interest to the topic and can lead to generation of new ideas.

3. Literature review

An approach to cybercrime as a driver to innovation, that was taken for the thesis, hasn't been discovered in existing literature. There is also no evidence that cybercrime phenomenon could have been approached methodologically from perspective of a driver. For that reason the literature review is focused on aspects that can describe dependencies between cybercrime and innovation and its surrounding topics such as relation between innovation and technology, innovation and organizational development, cybercrime and innovation motives, cybercrime and innovation phenomena in general and their characteristics. The description of these topics has also helped to characterize types of innovations among case study SMEs whose innovation originated as a result of direct or indirect impact of cybercrime.

3.1 Cybercrime and SMEs

The sector of SMEs is critical for reaching long term and sustainable economic growth [12]. IT have proven to be a vital contributor to business efficiency and market expansion for SMEs. By exploiting the opportunities provided by IT has also allowed SMEs to establish new ways to deliver their products and services as well as to approach their target segments and customers. The use of technologies and networking has also shaped the security needs for SMEs. An insufficiently secured network is "potentially the weakest link" in the cyber security chain [13], [14]. Hence, development of appropriate business models through investments or innovations is vital to provide a sufficient level of security internally and externally when dealing with customers [15].

The is a numerous amount of cases when small businesses are becoming victims of cyber criminals. Some experts say that small businesses do not fully recognize the potential impact of cybercrime if it had never caused a disaster to an enterprise. Smaller businesses are convinced that due to their size they are unlikely to be seen as a perspective target for criminals. However, this is reversed to the reality since smaller businesses usually have lower defence systems due to lack of financial resources, knowledge or expertise compared to large corporations. Furthermore, smaller businesses are seen as a favourable attack vector due to their belonging to a niche market or possession of innovation, idea, intellectual property or valuable customer base, especially if smaller firm is contacting larger organizations harder to target directly [10]. Since 2015 small businesses become more in favour of cyber criminals according to some field experts [10]. According to "The latest Government Security Breaches Survey" nearly three quarters (74%) of cyber breach fall for SMEs [16]. The statistics released by Symantec showed that nearly 52% of phishing attacks were carried out within SME sector in 2015. In 2017 the Dutch cyber threat landscape has increasingly developed, however, there are no significant changes or improvements in cyber security landscape. According to Deloitte's "Cyber Value at Risk in The Netherlands 2017" report, SMEs require special attention from the wider community. The expected cyber risk for Dutch SMEs is estimated around €1 billion. It also says that SMEs are unable to provide an adequate protection of their businesses against cyber attacks partly due to the high IT costs. Larger organizations are unwillingly exposed to third party risk from SMEs through their supply chains. Raising third party risk combined with increasing sophistication of cyber threats reinforces continuous exposure to cyber threats. As a result, the value of cyber threat is increasing while returns on cyber security investments are declining [17].

The raising security concerns within SME sector in The Netherlands is considered for the following research since smaller organizations are less protected and more vulnerable to cyber threats. So, it is important to see how SMEs are able to respond and innovate against cyber attacks. Not only the tendency among smaller businesses to take the initiative to defend their systems against the threat, but also a rising number of start-ups and small businesses that are focused on development of security solutions is rising compared to earlier years which signals the impact of the cybercrime rise and development. Hence, it is vital to see how companies innovate pro-actively and not making improvements only as a result of a cyber attack.

3.2 Drivers for innovation

Driving force or a driver – is the main factor that causes something to happen; the impetus, power, or energy behind something in motion [18]. Since there is no direct evidence in the literature that the cybercrime can be perceived as a driver for innovation and a factor of growth, different market reports were used to identify that.

There is a vast majority of different drivers for innovation in different industries. In the field of cyber security, organizations are actively engaging in protecting themselves, their data, resources and customers from sophisticated cyber threats. They develop new and dynamic approaches to tackle cybercrime issues that fuel innovation in IT and cyber security sector in order to make their organizations more effective and trustworthy. The demand in security products as a response to cyber threat rise is forcing IT innovator to be more wise and creative.

For the following thesis the most relevant enablers are chosen. The relevancy is based on the appropriateness of their application to the context of cybercrime and innovation phenomena and the field of cyber security. Among the most relevant drivers of security innovation are knowledge, creativity and organizational culture.

3.2.1 Knowledge demand

Knowledge is one of the key resources for innovation where knowledge transfer is a crucial when organizations engages in innovation activities. Hence, the knowledge possessed by employees and the general knowledge pool within organization is beneficial when innovation is created [19].

Knowledge and technology demand push and demand-pull concepts are referred to as key drivers for innovation. This is because they complement each other and mean that the needs should be fulfilled for an innovation to succeed. Very often knowledge requires research and development specialists to be set to solve a challenge or a problem. This type of research normally leads to breakthroughs, which can be used for innovation development. It also deals with exploiting the opportunities that come as a result of scientific research. Hence, a new knowledge is promoted and absorbed as an opportunity and often depends on a kind of demand [11].

Knowledge demand is characterized by the need to be fulfilled which often happens through innovation opportunities and generation of new knowledge. Hence, users see the benefit of adopting innovation or are motivated to change. An innovation is in most cases is a response to a need, whether it is the perception of a need or a real need but without such a need innovation will have little chance of success [11].

3.2.2 Creative thinking

Creativity is identified as a vital source of innovation [20] that must be embraced by organizations in order to be able to promote innovation. Creative intelligence and design thinking are central concepts in innovation capabilities of organizations. It refers to the ability of employees to think outside the box and use multiple approaches in problem solving and decision-making activities. This ability also contributes to creation of innovation culture within organization. Creative environments are considered to make a positive impact on knowledge creation and on the overall organizational performance [21], [22]. Creativity by definition means not only creation of something new but also improving something that already exists [23]. It is often attached to the notion of originality, however, creativity is not individualistic in its core but is attained from a relationship with a piece of work, product, experience and so on. Hence, it is a connection point between two separate incidents [24]. Creativity is also perceived as a core driver for economic value and growth with creativity knowledge as a major competence of innovation [23]. However, the lack of connectivity and knowledge transfer possibilities is seen as a barrier to innovation and innovation acceleration.

3.2.3 Organizational culture

Certain studies focused on more on organizational culture and its influence on transfer of innovation. Organizational culture is comprised of deeply rooted beliefs and values of human behaviour and interaction [25]. Organizational culture is one of the sources of innovation when organization is open to innovative activities and not keeping tight to established routines. When organization is inclined towards innovative activities and creation of innovation culture is a desirable process, these activities can result in new or improved ideas, products, services and business practices. There are a number of factors that contribute to creation of innovation culture: external environment, response to critical incidents, organizational structure, resources and technology [26].

3.2.4 Drivers for cyber security market development

Cyber security market opportunities and forecasts 2016-2022 report [27] highlights the demand drivers and growth stimulators for cyber security: rise in security breach targeting enterprises, need for stringent compliance and regulatory requirements, rise in the adoption of cloud-based security solutions, the emergence of risk-based frameworks for cyber security. It also indicates restraints for cyber security market which are high cost of innovation, budget constraints and increased usage of free or pirated security solutions.

Global Smart Grid Cyber Security Market [28] defines following driver: Increased complexity of cyber threats; challenge – lack of defensive measures; trend – increased use of off-the-shelf applications.

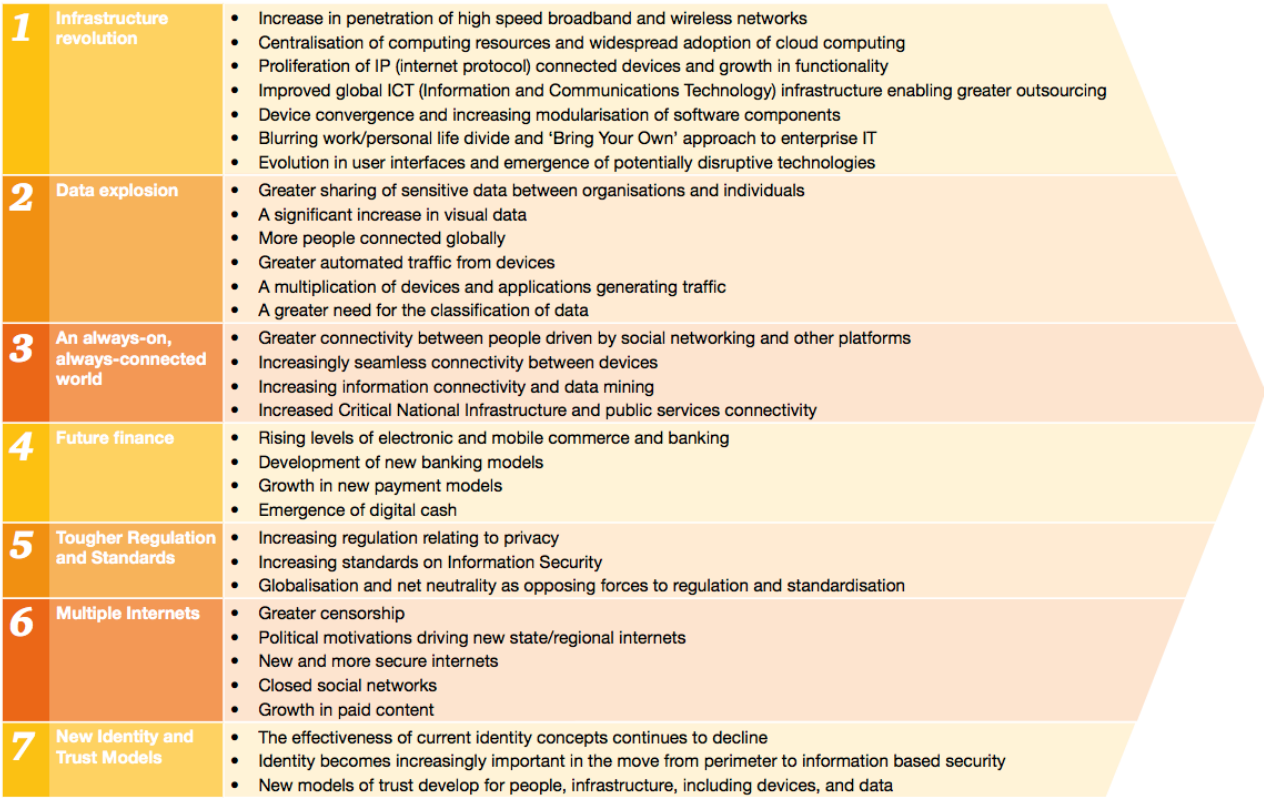
According to Cyber Security Market in India 2012 report [29], the concept of cyber security is evolving with myriad growth opportunities across different sectors including a prospective opportunity in SMEs which has recently emerged as a target for cyber attacks. Drivers: increased wired and wireless internet usage, rapid computerization, presence of smart handled devices, growth of e-commerce, growth in cloud computing, rise in cyber attacks. Challenges: availability of pirated software, lack of interest in updating software. Trends: cyber security players foray into mobile security, cyber security, virtualization, training institutes design courses on cyber security.

The Cyber Security Market report published by Allied Market Research [30] the cyber security market is expected to grow to $198 billion by 2022. The future is characterized by globalization of threats and development of solutions such as security incident management, Unified Threat Management (UTM), risk and compliance management, Identity and Access Management (IAM) that enable organizations to secure infrastructure and data from harmful cyber threats and vulnerabilities. According to the report, SMEs and projected to grow in cyber security market by 18,5% worldwide.

Among the main drivers of the cyber security market are [31]:

- Increasing cyber threats, both from new actors and new threat vectors (the paths that attacks can take).
- Greater vulnerabilities due to the more extensive use of technology, in particular mobile devices and cloud technologies.
- Increasing awareness by organizations and consumers of the current and potential threats.
- Changes in technology driving product and service innovation of security solutions.
- Increasing regulation, particularly those enforcing the requirement to secure personal data.
- Changes in outsourcing; some organizations are increasingly relying on partners for security, whilst others are growing internal security spending to maintain greater levels of control.

The most comprehensive overview of drivers of the cyber security market is presented in the table below [31]:



1	Infrastructure revolution	• Increase in penetration of high speed broadband and wireless networks • Centralisation of computing resources and widespread adoption of cloud computing • Proliferation of IP (internet protocol) connected devices and growth in functionality • Improved global ICT (Information and Communications Technology) infrastructure enabling greater outsourcing • Device convergence and increasing modularisation of software components • Blurring work/personal life divide and 'Bring Your Own' approach to enterprise IT • Evolution in user interfaces and emergence of potentially disruptive technologies
2	Data explosion	• Greater sharing of sensitive data between organisations and individuals • A significant increase in visual data • More people connected globally • Greater automated traffic from devices • A multiplication of devices and applications generating traffic • A greater need for the classification of data
3	An always-on, always-connected world	• Greater connectivity between people driven by social networking and other platforms • Increasingly seamless connectivity between devices • Increasing information connectivity and data mining • Increased Critical National Infrastructure and public services connectivity
4	Future finance	• Rising levels of electronic and mobile commerce and banking • Development of new banking models • Growth in new payment models • Emergence of digital cash
5	Tougher Regulation and Standards	• Increasing regulation relating to privacy • Increasing standards on Information Security • Globalisation and net neutrality as opposing forces to regulation and standardisation
6	Multiple Internets	• Greater censorship • Political motivations driving new state/regional internets • New and more secure internets • Closed social networks • Growth in paid content
7	New Identity and Trust Models	• The effectiveness of current identity concepts continues to decline • Identity becomes increasingly important in the move from perimeter to information based security • New models of trust develop for people, infrastructure, including devices, and data

Source: PwC / Technology Safety Board Information Security 2020 report

FIGURE 4. LONG TERM DRIVERS SHAPING THE CYBER SECURITY

As a result of reviewed market research reports on the cyber security market, there is a lot of evidence on cybercrime being one of the factors or drivers for innovation growth and security market expansion.

3.3. Key cybercrime concepts

During the 10th United Nations Congress on the Prevention of Crime and the Treatment of Offenders, there were two definitions generated with respect to the cybercrime term. The following definitions are [32]:

"Cybercrime in a narrow sense (computer crime) covers any illegal behaviour directed by means of electronic operations that target the security of computer systems and the data processed by them."

"Cybercrime in a broader sense (computer-related crimes) covers any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network."

With the development of technology, the cybercrime sophistication develops respectively. The evolution of the cybercrime is illustrated in the figure below [33]:

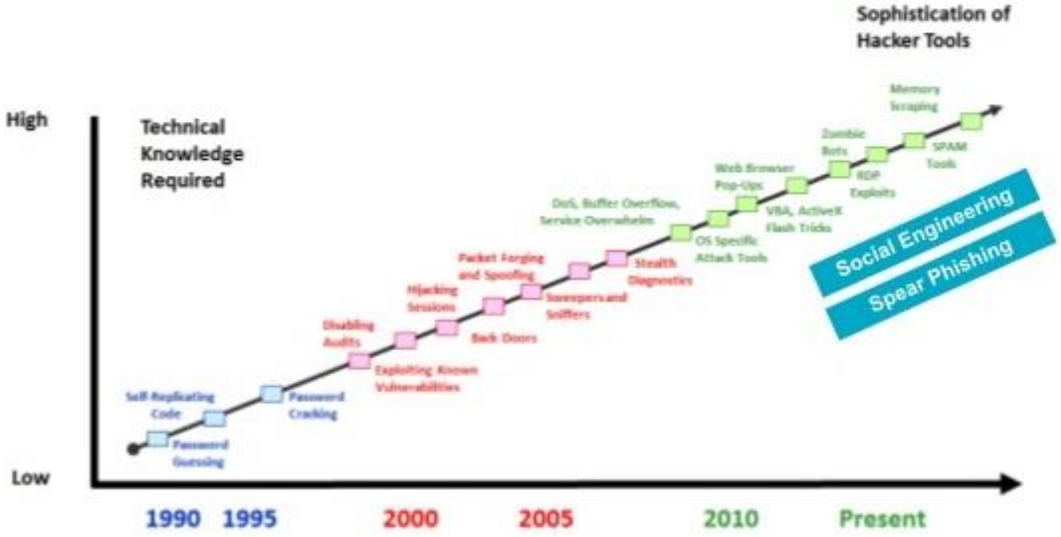


FIGURE 5. EVOLUTION OF CYBERCRIME OVER TIME

A major problem with cybercrime is that it cannot be fully covered and monitored by laws and regulations. In particular, the issue of ownership and control has dominated long debates over the Internet and what measures to take since the cybercrime act and individual performing that act can be difficult to spot [34]. The problem of acquiring knowledge about cybercrime lies in the fact that crimes do not follow the traditional pattern commonly considered for the threat level and severity and the damages are often difficult to measure in financial terms. Furthermore, statistics have long been characterized by the fact that much cybercrime has not been registered because it is not always reported or detected [35].

3.3.1 Generations

The cybercrime phenomenon can be described in three generations associated with its development along the development of technology. The following categorization was proposed by Wall D. [36] and it best describes the level of severity and scope of the criminal opportunity at each stage.

In *the first generation* of cybercrime, computers were used as a means for performing traditional type of crime. For example, computers were used in the preparation stage for obtaining information or as communication means. In this type of crime, computers and network technology can contribute to the criminal activity. But if these technologies are eliminated, the crime will still take place. The first generation is mainly characterized by the criminal exploitation of mainframe computers and their discrete operating systems. It usually involves the acquisition of funds or unauthorized access to sensitive information . An example of the first generation of cybercrime is Salami fraud.

The second generation is often called “hybrid” and involves the possibility of cross-border crime and overseas crime provided by network technology. In this case, the Internet represents an opportunity for traditional crime to be carried out on a global level. In this case even if the Internet is excluded, the crime will still take place.

Third-generation cybercrime is a “true cybercrime” that is automated and mediated by network technology. This category is using a distributed and automated software-controlled features. The criminal activities are, to a lesser extent, depend on social manipulation as opposed to first and second generation cybercrime. This type of crime cannot be initiated without broadband technology and the Internet since it stretches only to cyber space. So, if the internet factor is eliminated the crime wouldn’t be possible to commit. An example of this type of crime is spamming, phishing, social engineering.

3.3.2 Methods and classification

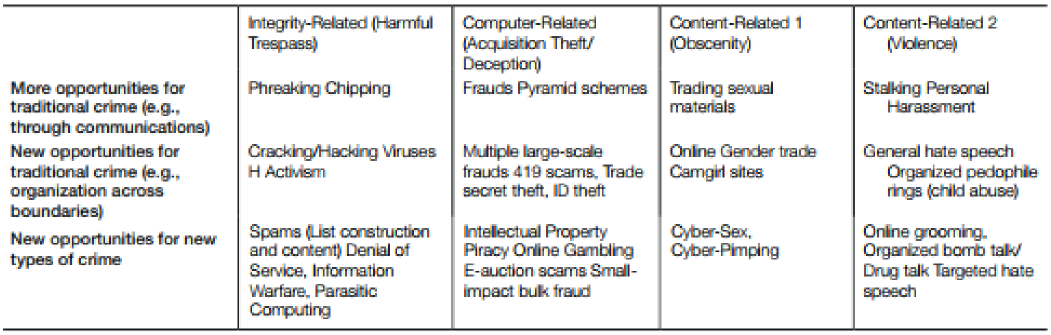
There are several different classifications of cybercrime. One of the methods of classification provided by Wall [36] is by distinguishing three main categories of cybercrime, namely, content data integrity crime, data-assisted crime and data content crime. Data integrity crime deals with the security of network access mechanisms and includes service attacks, hacking, phishing. Data-assisted crime use computers that are connected to the Internet with the purpose of, for example, obtaining goods or money illegally. The data content crime is about illegal content distribution on network-connected machines, such as child pornography and distribution of spam.

Computer integrity-related crime is the form of a cybercrime that involves hacking, cracking and service attacks on computers on a network. These are attacks that compromise integrity of computer systems in general. Such crime can further cause impaired confidence to those who use computer systems that were under attack. Such attacks may be stretched to another crime, such as the creation of a back door in a system that can be used to re-enter the system at a later date, allowing criminals to retrieve information that may be used later. Examples of such information may be username and password, personal information or company information.

Computer-assisted crime involves offenses where criminals use network-connected computers. Wall draws three distinct groups under this form of a crime, namely, virtual theft, bankruptcy and a fraud. The virtual theft involves appropriation of intangible assets, bankruptcy with abuse of financial assets and the fraud involves an internet-assisted fraud of any kind. These groups involve everything from phishing to fraud auctions and fake advertising. This type of crime has radically changed together with technology development over time.

Content-related crime deals with the distribution of an harmful content via the Internet. Such crimes can be, for example, recipes to create weapons and drugs, cyber-stalking and pornography, violence encouragement, bullying and racist utterances. Although, the cyberspace is outside national jurisdictions and the restricted content is only a representation of the information on the web, the power of the image or an advice can send a distracting message that can encourage people to unlawful actions [34].

Cyberspace creates opportunities for criminals to commit crimes through its unique features. The “transformation keys” that provide opportunities for cyber criminals include globalization, distributed networks and data trails. In order to fully grasp how new opportunities and criminal behavior are generated, the following matrix was provided by the Wall [37] that shows different levels of opportunity that can be enabled by each type of crime.



	Integrity-Related (Harmful Trespass)	Computer-Related (Acquisition Theft/ Deception)	Content-Related 1 (Obscenity)	Content-Related 2 (Violence)
More opportunities for traditional crime (e.g., through communications)	Phreaking Chipping	Frauds Pyramid schemes	Trading sexual materials	Stalking Personal Harassment
New opportunities for traditional crime (e.g., organization across boundaries)	Cracking/Hacking Viruses H Activism	Multiple large-scale frauds 419 scams, Trade secret theft, ID theft	Online Gender trade Camgirl sites	General hate speech Organized pedophile rings (child abuse)
New opportunities for new types of crime	Spams (List construction and content) Denial of Service, Information Warfare, Parasitic Computing	Intellectual Property Piracy Online Gambling E-auction scams Small-impact bulk fraud	Cyber-Sex, Cyber-Pimping	Online grooming, Organized bomb talk/ Drug talk Targeted hate speech

FIGURE 6. MATRIX OF CYBERCRIME: LEVEL OPPORTUNITY TYPE OF CRIME

3.3.3 Motivation factors

One of the main reasons of the cybercrimes committed is money and valuable information. Criminals can gain an access to personal data or user identification of bank account, access credit card information or any kind of personal data. Posting an inappropriate content online is another way for a criminal to act, which is supported by more intrinsic motivations to harm the other people or social groups on social network sites, for example. This can be caused by a motive of revenge or any other intrinsic reason that makes criminals undertake cybercrimes [38]. Apart from performing an act of committing a crime on the web, information on how to conduct a crime can also be shared [36].

The attackers can be found both inside and outside of organization [39]. The focus of the thesis is on outside threats and attackers, so the motives for outsiders will be described. The classification of attackers coming from outside of organization can be based on their organization, motives and professional level: amateurs, professional hackers and organized hackers. There are three broad categories of motives that attackers can be guided by [39] which the thesis focuses on to a certain degree:

1. Political motivations – destroying, disrupting, or taking control of targets, espionage, making political statements and protests).
2. Economic motivations – theft of intellectual property or other economically valuable assets such as funds or credit card information, fraud, industrial espionage and sabotage, blackmail.
3. Socio-cultural motivations – attacks with philosophical, theological, political and humanitarian goals. These forms of motivations may also include entertainment, curiosity, and a desire for publicity or fame.

According to Wall [36] cybercriminal motivation can also be divided in seven groups: complacency, need for respect from peers, desire to impress potential employers, criminal gain or competitive advantage, revenge, distance to victims and politically motivated protests.

Types of cybercrime and generations will be used in describing innovation types within SMEs as characteristics taken to measure the impact of crime. However, crime motives on behalf of criminals will not be fully disclosed in the cases, since the research is not about motives on behalf of criminals and what makes them involved in criminal activities. Though, some motives will be mentioned along two case company examples where the criminal act had an internal and direct impact on organization. Other two case organization didn’t have a direct contact with crime, since they are being service and security providers, so, here description of motives are not applicable.

3.4 Key innovation concepts

Innovation is the process of translating an idea or invention into a good or a service that creates value for the user and satisfy a need of a user. Innovation involves deliberate application of information, imagination and initiative in deriving greater value of resources. It includes all the processes by which new ideas are generated and are converted into useful products and services. In business terms, innovation often results when ideas are applied by organizations in order to satisfy the needs and expectations of the customers or users of innovation [40].

Innovations often deal with familiar things in new ways [41]. An innovation does not need to be new to everyone, but must be experienced as new to those who implement it [42]. The table below provides some definitions of innovation in different contexts [43]:

Definitions of innovation

“Industrial innovation includes the technical, design, manufacturing, management and commercial activities involved in the marketing of a new (or improved) product or the first commercial use of a new (or improved) process or equipment” (Freeman 1982)

“Innovation is the specific tool of entrepreneurs, the means by which they exploit change as an opportunity for a different business or service.” (Drucker 1985)

“Innovation is the successful exploitation of new ideas” (UK DTI 2004)

“Successful innovation is the creation and implementation of new processes, products, services and methods of delivery which result in significant improvements in outcomes, efficiency, effectiveness or quality” (Albury 2005)

Innovation is “the successful development, implementation and use of new or structurally improved products, processes, services or organisational forms” (Hartley, 2006). Innovation is “something new being realised with (hopefully) added value” (Jacobs and Snijders 2008).

The context of innovation can determine whether something is perceived as new according to criteria such as new to the world, new to society, new to the business and community or for a particular individual. Innovation requires diffusion and an assumption that society, or at least part of a society can make use of it [42]. Innovation also does not have to be always spread across large parts of a society. As long as an idea is developed and implemented, it is perceived as new to those who implement it, and is leading to changes in routines and processes for a particular segment of users [44].

3.4.1 Dimensions of innovation

Innovation is not only an idea, it is also the implementation of it. Some authors differ in including or excluding the commercialization phase of the innovation process [44].

Innovation comes in a variety of types and dimensions. Innovations vary along at least five dimensions such as type of innovation, degree of novelty, type and size of the organization in which the innovation project originated, the environment or sector in which the innovation was developed. Main distinctions are made between innovations that take place in private or public organizations. Some authors distinguish innovation type according to product, process and service innovations and their approach to innovation either reactive or proactive [45]. The degree of novelty is considered along an axis from incremental to radical [46] where radical innovations create major disruptive changes, whereas incremental innovations continuously advance the process of change. In general, radical and incremental innovations concern the degree of novelty and impact on market and on economic activity of organizations on the market. Here radical innovation can come in the form of a new or breakthrough product or process that haven't been introduced before while incremental concerns an existing product, service, process or method whose performance was enhanced or modified [47].

The size of organization is also considered as one of the dimensions of innovation since innovation implemented at SMEs can be radically different from those of larger organizations. At last, the stability of environment or sector is considered to determine to what extend it can affect organization.

The link between entrepreneurship and innovation is very tight, since entrepreneurship sometimes comes in the form of innovation itself and brings with it innovative product and idea to the market. Entrepreneurship refers to the necessity-driven and opportunity-driven business models [11]. Here innovations are based on availability either demand for innovation or due to opportunities on the market.

3.4.2 Sources of innovation

There are two main important sources of innovation that are identified in the literature, namely, internal and external which also contain different sources of innovation in each [48], [20]. Internal innovations come from R&D department, initiatives, ideas, programs, internal collaboration between departments, etc. External innovation refers to an idea or innovation that comes from outside of the company, for example, from stakeholders, suppliers, customers or other external forces and environmental forces. Open innovation, creative intelligence, knowledge diffusions can be sourced both internally and externally.

Another view on sources of innovation is through the functional relationship of innovation with an emphasis on the role of users in the innovation process which was considerably explored by E. Von Hippel in his book "Sources of Innovation" [49]. Sources of innovation and user role are interrelated because user innovation by definition can also be about process innovation [50]. In particular, firms can have different functional relationship to a certain technology and innovation. E. Von Hippel describes this as follows: *"Users are firms that expect to benefit from using a product or service. In contrast, manufacturers expect to benefit from selling a product or service. A firm can have different relationships to different products or innovations."* Hence, in order to identify the functional source of innovation, companies and individuals are categorized according to functional benefits they acquire from a particular product, service or process innovation [20]. The difference between producer and user of innovation is that the producer benefits from selling a product while a user benefits from using a product [49]. One can also distinguish them from perspective where a user is an innovator because he or she has a direct benefit or advantage of using innovation, whereas a manufacturer only gets a financial benefit of it from selling the innovative product. User and producer are the two main innovator categories, but there are also other functional relationships between innovation and innovator which can be conducted on different levels. An innovator is an individual or an enterprise which develops and introduces an innovation in order to receive a reasonable return [51]. In the context of user innovators, a lead user term is used. It is a “user” that goes ahead of the majority with a market trend and tries out first what was issued by the innovator. This makes the first-mover innovations, from managers perspective, create a solution to meet the users’ needs which is attractive for producers to commercialize upon. Generally, unlike producers, users will think of their own personal or corporate benefit received from the use of innovation, while producers are only interested in innovations that help to increase the potential market and financial gains [51]. User innovations can also be freely spread their among others without any financial interest, which is termed as open innovation [20]. In general, open innovation can also refer to open sharing of knowledge and ideas without having necessarily finished products [52].

The following theory on the source of innovation is considered relevant for this research because it helps to define the functional relationship and the type of a user that produces or consumes the innovation in case organizations.

3.4.2.1 Outlaw innovation

Some studies distinguish between invention and innovation, where innovation is about taking the idea or invention and gaining certain benefits from exploitation of it which is often linked to the commercialization process. However, reserving innovation only to commercial products and services has its limitations, thus, eliminating a lot of innovation activity such as outlaw innovations [53].

One form of a user innovation is a lawless innovation type or outlaw innovation. Criminals are also users of technology and criminal users can be defined as lawless users. That are users who, either individually or as part of a group, actively oppose or ignore the restrictions they encounter from proposed or established technical standards, products, systems or the law and regulations. This user category can create or use new hardware or software modifications to existing products, or exploit security vulnerabilities for unauthorized access to systems.

Lawless innovations cannot be patented as well as some of non-producer innovations, which is roughly said to be user innovations. It can be of administrative, intangible and of non-marketable nature, and may not need to increase earnings or increase efficiency in the organization [53].

The following concept deals mainly with the producer and user relationship [49] where in addition to sharing information the changes are made to a product function or its intended use. Here exploits are designed to make failures, perform attacks or breaks of security systems. This can in turn push manufacturers and producers to innovate or improve existing products to meet the new needs and demands. Furthermore, innovation may concern, for example, those users who illegally release game codes and hackers who violate a corporate intellectual property rights and pose a direct threat [54].

Outlaw users are not associated only with direct interaction with software and internal systems. Many outlaw users can also be those who, for example, download music illegally, e.g. those individuals who take an advantage of technology in lawless ways [53].

3.4.3 Motivation factors

There are numerous reasons why companies engage in innovation processes. It can be done for the purpose of market share increase or for having a competitive advantage, improved efficiency of internal processes or communication or a brand of the company to name a few. However, the most basic principles that motives can be summarized to are based on needs, benefits or gains that organization is trying to achieve or fulfil through innovation. Hence, an innovation must fulfil a need, be beneficial for the user or the company and thus provide a desirable gain for the user or the company. The knowledge on what are the motives and desirable outcomes of the innovation are considered relevant for the following thesis in order to describe the reflection of innovation to cybercrime along above mentioned motive categories, e.g. the needs that must be internally or externally fulfilled, who benefits from the innovation and possible gains that it brings along [55].

Innovation is not only limited to individual needs. It is also about meeting social needs, e.g. the concept of innovation is not limited to commercial market and consumer needs only [44]. In addition, there are certain aspects that must be taken into account in terms of innovation gains. An actual idea or invention spread and used by the wider society can bring welfare or socio-economic gains [56]. There is a belief that there has been a democratization of innovation due to an increase of the ability among organizations to innovate as a result of IT development. This has provided more widespread access to tools and means needed for innovation, while increasing an access to richer innovation community [51]. The benefit of user innovations is in increase of social welfare through users getting exactly what they need and the product or service being sold to more users.

Innovation can bring different types of benefits and gains. E. Hippel attempts to look at the functional relationship of innovation in order to establish who is the innovator (as an actor) through the benefits brought by innovation [49]. Another way of looking at innovation in order to get an understanding of the benefits is through the extent to which innovation can affect the user and provider and how it can be perceived as an innovation. This can be done by considering several categories of gains: business gain, private gain, socioeconomic and welfare gain [51].

Business gain and financial profitability is a driver to invest in innovation from the business perspective. Considering functional relationship, this separates the private economic gain from a user gain, since user innovation does not assume a financial gain provided by innovation. Often socioeconomic and welfare gains exceed the corporate return from socio-technological innovations. A user innovation can provide personal economic gains, business gains and socio-economic and welfare gains. User innovations can boost social welfare, hence, it will most likely affect a wider socio-economic spectrum in turn. So, an innovation therefore does not need to bring direct or indirect financial benefit to businesses or individuals, but can benefit the society in general [49].

3.5 Technology and organizational development

Previous research has often been focused on market opportunities, enterprise sizes and internal capabilities as determinants of corporate innovation when looking at factors that drive technological innovations [57]. In addition, much attention has been paid to innovations that involve economic benefits only. Such an approach is slightly limiting the concept of innovation and omits other forms of innovation that arise from technological and other drivers with certain drivers coming also from the cyber threat due to development of technology. Nevertheless, the economic approach as well as the organizational and management approach takes it as a prerequisite that there are several factors that affect innovation and technological development [53].

The evolutionary economic theories draw links to biology by looking at technological development as an evolutionary process that influences the economy where organizations and innovations must adapt to the environment and as adaptations take place there changes are made to organizations, technologies and the social environment. Here the technology, industrial structures and the surrounding environment are seen in a co-development process (co-evolution) [58]. Thus, the changes in technology affect economics, institutions, industries, companies, individuals and the society. In addition, technological developments and innovations are interdependent because the majority of technologies and innovations are built upon earlier ideas [44].

There is an assumption that political and social forces help to shape economic changes and are influenced by the development of technology as well. Public institutions, non-profit organizations, laws and regulations are examples of contextual relationships when technological evolution is encouraged or restricted to a certain degree. Some researchers also refer to the term techno-economic paradigm for the similar context [28]. Also, much attention was paid to information and telecommunications developments to explain how national institutions were eager to adapt to new surroundings. All those dynamics can lead to radical or incremental innovations [46].

Organizations are constantly changing due to changes in the external environment. If the company is adapting to the new settings it firstly leads to changes within [59]. The new technology and developments can also lead to both positive and negative results, and one must have a knowledge and be able to deal with the negative consequences [60].

Some literature on innovation describes two the most dominant approaches, namely, innovation from the economic and managerial perspective. Economic perspective largely focuses on innovation and technological development from an economic point of view, where innovation presumably has a commercialized value and provides monetary benefit by means of efficiency of operations and product development which in turn can generate higher earnings. For example, in the field of evolutionary economics, there is often a focus on innovation and adoption of technology as a necessary step to adapt to the market [61]. Those who fail to adapt will face customers turning to other service providers. In contrast to that, organization and management literature has more focus on innovation from perspective of organizational learning and knowledge sharing skills, leadership, structures and processes as determinants of innovation. Both approaches, however, recognize other factors that can be affecting technology development, economy, organizational innovations. And these factors which arise from mostly external environment, such as cybercrime, affect large parts of society. This is describing an evolutionary approach to adaptation to surroundings [62]. These views were relevant to the research topic, hence the literature on organizational adaptation was used in analysis of the results since it is linked to some extent to the overall evolutionary economics perspective of technology.

This overview on technology and innovation is relevant to the following thesis since it considers social and technological developments such as cybercrime in organizational context and the way it shapes the context of organization in terms of internal and external environments.

3.6 Innovation model

There is a variety of models for innovation exist in the literature. However, the most famous model created and developed by Tidd and Bessant [11] was chosen for this research to describe four different types of innovations that originated due to cybercrime. The motive to chose the model is that it describes basic innovation types that organizations can undertake and that it is applicable to the content of cyber security innovations and types of innovations that can be produced in this sector. The 4P's model/method provides a powerful tool for analysis of companies' innovative sides. It includes 4 main categories within its innovation space: Product innovation, process innovation, position innovation, paradigm innovation [11]. Along these four axis it also has additional dimensions for incremental and radical innovations that are appropriate for the analysis and are aligned with the findings on innovation literature. With the use of this model it is possible to describe all four types of innovations, as well as those that have elements of other forms of innovations and map them accordingly within the framework.

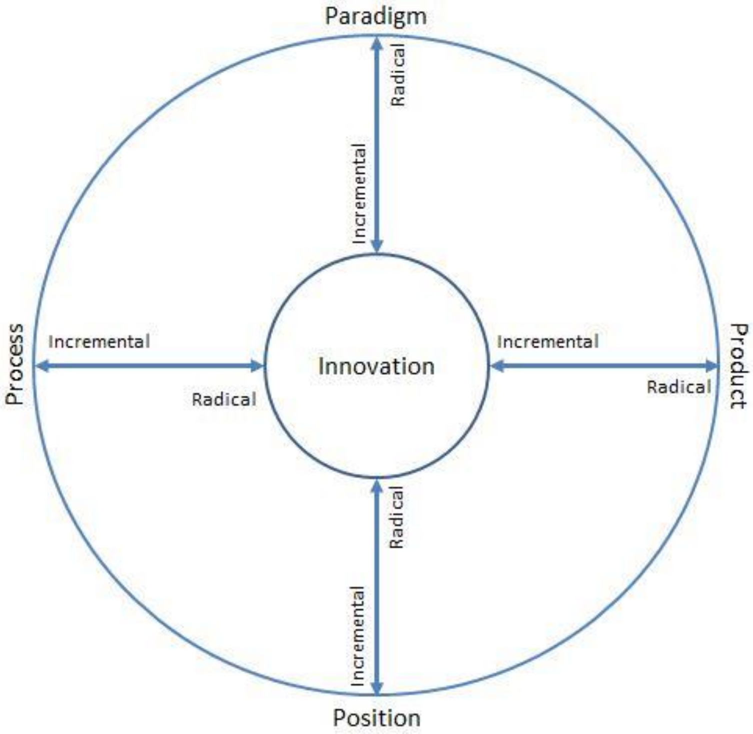


FIGURE 7. INNOVATION SPACE 4P'S

Product innovation includes introduction of innovative products and services which are offered by organization to the end user. The product or service can be new and modified, based on the previous version of that product.

Process innovation includes modernization of internal systems and the ways how products and services are created or delivered.

Position innovation is concerned with changes how a specific process or product is perceived and how products or services are used. Examples are changes in commercial or marketing innovation when organization is changing focus, in terms of market, goals etc.

Paradigm innovation is a change in the basic mental models compared to that was previously established at an enterprise. Paradigm shapes what an organization or business is about.

The changes that take different forms in organizations and countless innovations introduced can be characterized by this model. As it has been mentioned earlier, the reason for choosing this framework is that it describes a four-dimensional innovation space and allows a gradual transition from radical (new to the world) to incremental (minor improvements) innovation type review.

4. Case analysis

In order to illustrate what kind of innovations were caused directly or indirectly by cybercrime among SMEs, four cases are presented and analyzed to depict four different types of innovations defined by the 4P's framework. Through the cases, there was an attempt to define what kind of innovations originated as a result of cybercrime within different organizations. A description of the case company, a presentation of problematic areas revealed during in-depth interviews and an analysis according to the literature and theoretical concepts of cybercrime and innovation are presented in the subsequent chapters. Innovation type and scope are mapped on the 4P's innovation space framework. The analysis of innovation types, their dimensions and cybercrime dimensions which had an impact or related to each particular innovation, was summarized and presented in the Table 9. The summary presented in the table contains each particular company's relation to a type and generation of cybercrime as well as innovation type defined by functional relationship and possible innovation gains.

Four different cases were chosen to illustrate how companies innovate due to influence of cybercrime as one of the driving factors. Speaking of analysis, innovations were typologized and categorized by the type of innovation and where on the innovation map they can best be suitable since some of the forms of innovation can also have attributes or elements of other types. Furthermore, it is discussed whether it is a user innovation or producer innovation by looking at the functional relationship and what kind of needs it covers along with possible gains from its utilization. Then it is separately discussed what relationship or link there is between cybercrime and particular innovation.

Each case is discussed and analyzed separately. In order to get a better understanding of whether cybercrime plays a role in making companies innovate, all the chosen SMEs belong to different industries. This makes the survey broader and more representative since considerations on the impact of cybercrime are not limited to only one industry. Hence, it shows that the impact can be harmful to a wide range of industries and types of businesses, however, due to limitations of the research only these industries were considered.

In each particular case each innovation type from 4P's framework is illustrated, all of which in some way are partly driven by cybercrime. The four case companies are:

Case 1: Contec (Product innovation)

Case 2: Whitecliff Ltd. (Process innovation)

Case 3: Verwey Grafische Produkties (Paradigm innovation)

Case 4: Elcatronics (Position innovation)

The discussion on the main topic of cybercrime as a driver to innovation follows the cases analysis. The discussion is built around empirical data received from respondents which is also linked to the literature on the main topics of the thesis.

5. Case Results

5.1 Product innovation: Contec

Contec B.V. is a distributor of IT security solutions in the Netherlands, Belgium and Luxembourg. The company sees the importance that customers get the most from IT security. Therefore, Contec's portfolio only consists of products on which they have gained a lot of experience. The resulting expertise enables the sales department to tailor-made advice per security issue. Also, partners can always count on the hands-on support of specialized IT consultants. Finally, Contec offers extensive technical and commercial support. Among the benefits that Contec provides with its security solutions are specialized product knowledge, high quality brand portfolio, extensive IT security experience and hands-on mentality.

Cyber breach and security means are among the top issues of organizations that want to secure their data assets. For that reason, different companies such as Contec offer customized or packaged solutions in the form of products or services to their clients. Since the level of cyber breach is rising, many organizations remain vulnerable if certain measures are not have been taken into account beforehand. Most often companies start to realize the level of danger only after the breach of vital and sensitive information took place. In order to prevent this from occurring it is advised to take an opportunity provided by innovative products and services and to invest in their implementation.

Among Contec’s product portfolio there are multiple brands that are tailored for different security issues, such as virtual firewall solutions for perimeter protection in virtual environments, cloud and network protection and security management tools. A particular product of interest is the Server Breach Detection System (sBDS). The product was developed as a direct response to an act of cybercrime. It is a complex product that extends beyond traditional light-weighted protection means such as antivirus or firewall. It can be described as an innovative version of the system solution that is capable of detecting and analyzing the threat within the internal network on a large scale. The most prominent features of the product include threat correlation analytics for advanced threat detection, real-time risk monitoring for internal networks and critical assets and a complete insight into life cycle threats through the Cyber Kill Chain.

By introducing new products and solutions continuously, Contec wants to show the pursuit in further development and extension of existing security product lines related to cyber security, such as firewall, cloud protection and security management tools in order to satisfy customers' evolving and changing needs.

5.2 Process innovation: Whitecliff Ltd.

Whitecliff Group is an international investment management provider that is operating in numerous jurisdictions and financial centers through a network of associated companies. The company provides guidance on transactions of varying levels of complexity and tailor-made legal, financial and project management solutions. Confidentiality and integrity are essential parts of the business and the processes are designed to ensure outmost information protection.

The company operates in a highly turbulent environment that involves a large amount of transactions made daily. Data on various bank accounts and credit cards are highly sensitive and is important to be protected. However, due to the human error certain security issues were arising which led to improvements and innovative approaches to the problem. Here the process innovation took place in order to achieve business goals, enhance internal processes and fulfill the need for a better protection of financial data and assets.

One of the issues that has occurred multiple times at the enterprise is that an email with a virus was disclosed. As one of the examples of how the malware affected the company in recent time was a story provided by a respondent on a e-mail phishing case. The following email was sent as a spam listing the name of the right recipient, which was one of the company's suppliers, but despite the correct name the e-mail contained a malware instead. Due to the lack of awareness among employees the virus has infected all the word documents on the stationary computers in the office as well those documents that were stored in Dropbox including other offices of the company. Adding to that, the virus asked for money to be paid to restore the data. Eventually it was prevented by an external IT supplier and the backup of the files was performed and files restored. However, there was a loss of files of this same day and vital information concerning transactions, correspondence and other sensitive information was irrevocably gone. For that reason, the company started to reorganize its processes and raise the awareness among employees.

Since the company is handling very sensitive data and involves financial transactions in large volumes and basically operates finances on the large scale, the need in new security measures was inevitable, which would differ from usual performance ways. Therefore, apart from installation of basic software for protection of internal systems the company has also developed a new way of handling its operations and security issues with the help of an external consultant. The guidance on the policy and procedures document was developed accordingly and highlighted the most important areas on dealing with sensitive data in strict and specific ways. The following document contains information on the most important areas of information security, such as legal rights on the information, classification of data and its storage particularities, user identification and authentication, e-mail, physical security, operating system, Internet, mobile message exchange, remote access.

5.3 Paradigm innovation: Verwey Grafische Produkties

Peter Verwey Grafische Produkties is a full service graphic design company that focuses on design and lay-out of physical and online publicity. The company is running its business for over twenty years and have produced a large number of books, covers, brochures, advertisements, websites and other graphic material.

Verwey G.P. is a running business for more than 20 years. However, only recently the business felt a need in a better security means, measures and a security-oriented mindset. The need for security measures appeared due to multiple fraudulent occurrences at an enterprise. Some of the insights were brought up by a CEO of the company who faced a direct threat from a cybercrime and reassessed the general approach to security systems and beliefs at the enterprise. The CEO of Verwey G.P. had faced a theft from the company account of nearly

10.000 euro. After investigation it was revealed that the corporate account and the credit card number was compromised. Since the company isn’t large by the number of employees the following theft was rather considerable and represented a vital financial asset of the company.

In order to minimize the possibility of occurrence of these kinds of events the CEO of the company had updated the security software and tools and introduced an awareness program after consulting its external IT provider, with check up on personal details, enhanced password combination and keeping and access to corporate accounts. The issue had also influenced other employees and raised an awareness among other employees, since the same could have happen also with their personal accounts. Through the initiatives of CEO, the new paradigm on security was introduced. Also, he shared some knowledge and insights on Internet security issues with the employees and on relevant events that can follow and measures taken in case of a security breach.

5.4 Position innovation: Elcatronics

Position innovation means changes in the context in which the products or services are introduced. Cloud technology helps organizations to store all their data on virtual server which is highly vulnerable to different types of crimes and frauds. Very often data is not managed directly by the client but by the provider instead. According to CEO of Elcatronic, the cybercrime is no longer a threat to personal computers only, cloud environments and virtual servers are becoming under attack more in the past couple of years, which makes it hard to provide a fully reliable service. The types of attacks performed might be unrecognized by internal systems that monitor and control that process. Eventually the damage done can be enormous, especially for the consumer.

Due to the rising alertness on behalf of the companies and customers of Elcatronics, apart from the core business proposition as internet and cloud service provider it is also targeting its services as more secure and reliable compared to competitors. One of the steps towards a shift from the original service proposal was made through cooperation with Gemalto to increase its trust among the customers and to be outstanding among its competitors adding the focus to enhanced security tools. By exploiting this strategic goal, Elcatronics is aiming to remove barriers to adoption of cloud which still exists due to security issues and to create differentiation of its service on the market. The main advantages of using a solution is to improve its current services and enhance their authentication, encryption and data management processes. By providing safer services Elcatronics is aiming to change the image of the cloud and IT supply among its customers, showing this way its own position compared to similar businesses in this field.

Elcatronics can be said is contributing the public and community in general through the services it provides in terms of the enhanced safety and, therefore, quality. During an in-depth interview there were several steps how the business changed due to security reasons. Firstly, the backup service was improved a couple of years ago. The company used to do backups in their own office, with a second mirror backup at one of the employees' houses since insurance companies demand a backup to be done outside the facility. Since in case of fire there must be a second location, so backups can be restored. The next step was in placing raid systems at the client’s location. A raid system is a backup system with 10 one terra byte disks. If one disk fails, the other disks are a mirror, so the broken disk can be restored from the other nine. Another point of attention is that the company received many complaints on security breaches from their clients. Usually it was due to human error, by opening a phishing email, or an email that contained a Trojan horse. These raid systems were in the client's network, otherwise backups would not be possible. The company was forced to take action and think of a system that was more secure so a special facility was rented in the Schiphol region. The servers there are protected with the highest encryption and two phase identification. Also installation of anti-virus software with a client is an obligatory part of the contract. The company has bought and further developed a program called Crashplan. This way clients can easily access their data, without the risk of a security breach. It is a backup program, that encrypts data. Only the end user (the client) has the key to de-encrypt the data. So, that way even data that is intercepted is useless to the hacker. Same way websites that run on company’s servers are protected with extensive spam filters, that immediately compare e-mails to known e-mail addresses and IP addresses that send spam or phishing mails and these lists are being continuously updated. The same is also implemented for visitors of the websites. Their IP address is compared to know lists of perpetrators. Connections from suspicious countries are blocked until the client approves such an entry.

In case of target group, the company started to focus more on bigger companies, because a security breach in big companies is largely scaled. In smaller companies its far easier to set a protocol and make staff stick to it. In larger companies it is much harder to identify the one person that caused the breach or violated a protocol. All the cybercrime attempts on the enterprise itself to hack the servers or backup systems have been successfully blocked. So, Elcatronics promotes itself as a safer IT service provider in terms of marketing to give more confidence to the clients and trust in their services. Even though the company the company is currently protected it continuously look for even better solutions. According to the interviewee, new threats appear every day but working together with third parties that develop software to protect data has proven to be a good way to stay ahead.

6. Analysis of results

6.1 Product innovation: Contec

Contec belongs to SME segment and specializes on providing security products and solutions. The company provides solutions to problems that echoed in previous negative experiences with cyber threats, that is why it has its own place on the market and a need for its products. Hence, the company is trying to fulfil the existing customer need. The most important targets are a second and third type of cybercrime generations that company provides protection from. Products and services provided by the company are developed as a direct response to potential or past cybercrime experiences as well as for the analysis of internal systems and threats. Hence, it doesn't concern general means of protection only (antivirus, firewall), but is being rather an innovative version of the solution that is capable of detecting and analyzing the threat within the internal network on a large scale.

The innovation example is the sBDS product itself, which wouldn't have been created without a prior need for that product. It was also introduced to show that this was a necessary step to further develop extended security product lines related to cyber security, such as firewall, cloud protection and security management tools in order to satisfy customers' evolving and changing needs. The company is using a product innovation strategy by introducing new means of cyber protection. So, the manufacturer of the software is a producer of innovation. Here through open innovation the manufacturer of that particular innovation is responding to customer demand in order to fulfil the existing demand. This is a producer innovation due to the functional innovation relationship since innovation here is a marketable solution which provides the direct benefit for the producer.

Innovation brings a corporate gain to the producer in terms of direct revenue through sales and increased market share. This is the main reason why the innovation was introduced and the direction of the company's security mission in general. Yet, product innovation brings a prosperity gain through the fact that it's a crime-fighting and anti-fraud innovation, which can help the user to minimize the amount of cyber attacks to customers' networks. This gives a benefit to those who use it as well, thus eliminating the financial costs that may arise from being affected by the cybercrime and its consequences. The socio-economic gain is provided since the product is available to a society in general and is beneficial for the society. The product provides in this case also financial gain from the sale on behalf of the producer and better protection from the cyber threat while minimizing associated costs of possible impact on the consumer side.

The following product innovation can also be characterized as position innovation because the company has its own unique perspective on the delivery of the services and the solution provided is positioned differently from other products of its kind. The change approach originated from previous negative experiences resulting in innovation. Another dimension that can be added is that it is radical innovation since it didn't go through an evolutionary process and having similar products in the past, but represents a new solution of its kind. It can be similar to many other security solutions, but it has its own unique features.

Crime as innovation driver

Threats and risks experienced by end users, individuals or organizations has led to the emergence of technologies that can help to minimize those risks. Contec as well as many other product developers or service providers in that area ensure that the protection measures are created to meet the current customer needs and are able to provide protection against the newest forms of cybercrime. Some of the attacks can be highly critical to organizational assets stored online. Hence, the appearance of the companies and products, particularly specializing on defence measures can be seen as a direct response to the cybercrime that takes place. Since there is a demand in that type of product or service, means that the problem isn't eliminated. If the problem didn't exist the need in defence products and enterprises will be useless as well. The innovation type presented in the case with Contec is corresponding with data integrity crime in the form of third generation of cyber crime. Innovation also presumes that certain gains are achieved when innovation is created. The main gains are received from selling and using an innovative product, so it is beneficial for both producers and the users.

6.2 Process innovation: Whitecliff

The type of innovation at Whitecliff is linked to the method of doing routine things in new ways, hence, it is as a process innovation. This type of innovation is focused on internal processes and involves much attention to the human factor. The innovation that took its existence at Whitecliff originated from the negative past experiences with cyber threat as well as in the case with Contec. However, here the need came internally due to several fraudulent occurrences at the firm, unlike with Contec where the need originated externally. Here the innovation is largely about solving problems in new ways or about improving old ways and adding new elements to it. This is a form of incremental innovation at the enterprise, since the new ways of handling the processes are based on old systems combined with new knowledge aiming to improve the old system that was more prone to vulnerabilities.

Whitecliff has no commercial interest in this innovation, since in financial terms it doesn't bring a direct profit. It is more aimed at protection against some form of a secondary generation of data content crime. The following innovation has been developed as an aid for a larger process and can also be classified as a user innovation. The functional relationship with innovation lies in the use of the methods or tools that were developed specifically for the company. It is also driven by a need to solve a problem that together with appropriate knowledge makes innovation beneficial for organization in the long run. However, there are no expectations of a private or corporate economic gains since it is not the type of innovation that can be purchased or sold.

Crime as innovator

The relationship between crime and innovation is in the increasing use of the tools among criminals as a medium to perform second generation data content cybercrime. The crime motive is economical and the type of threat is phishing, since the malware destroyed certain corporate files and asked for money to restore the data.

Financial institution or organizations are among the most targeted among criminals. Older software and protection methods are less efficient nowadays. In order to provide a proper protection, not only new software tools must be implemented, but also the ways in which processes are handled in general. This type of innovation primarily concerns the internal processes itself, though it can also be shifting to the point where it transforms to a paradigm innovation. Here the change from the usual ways moving to new ones as a consequence of the cybercrime, also alter the way employees approach security in general. Nevertheless, the measures wouldn't have taken place if there was no demand for the change of processes.

Also, if the occurrence of the cybercrime breaches wouldn’t exist the company would barely spend additional funds for security matters, especially if they wouldn’t lead to direct financial gains. So the need in security is fulfilled on behalf of the enterprise itself. There are no direct financial gains from this innovation because the security need was internal, and the gains received from a safer environment in this case are difficult to quantify.

6.3 Paradigm innovation: Verwey Grafische Produkties

The type of innovation implemented at Verwey G.P. is a paradigm innovation since due to the influence of CEO and his past negative experiences with cyber fraud the mindset of individuals and of the firm was changed towards creation of more safe environment and accountability. Here knowledge sharing and awareness in combination with security means takes place. Innovation is not radical since organization left the same processes as earlier, however, the working attitude has shifted to a safer patterns of communication. The views on how availability and accessibility of data is approached have changed dramatically as well.

If there were no fraudulent incidents occur at the enterprise, there won’t be a need to make these changes. The following innovation is incremental, since it represents a next logical step followed by data breach and leads innovation in approach to security. Innovation in this context is a user innovation because the benefits are linked directly to the new established mindset of those who are involved. It is not able to receive a direct profit or gain since this time of innovation is not marketable. However, in the long run it can be externally beneficial for the company and can help to save its assets that currently non-measurable but can worth more than innovation implementation itself in the future. In addition, since the level of possible fraud is minimized in this case, it can be concluded that this type of innovation is in conjunction with a welfare gain in terms of safeness of the company’s assets where risks from cybercrime are minimized. A socio-economic gain is also likely in this case since it would involve less costs of possible investigations and improved loyalty of the customers.

Crime as innovator

Verwey G.P. was mainly affected by data integrity type of crime of first generation when personal or in this case corporate sensitive data was violated or hacked. The motivation behind the cybercrime is classified as economical, since the prime reason of the crime was the theft of corporate financial assets. The criminals had found the way to the knowledge of credit card data and this belongs to a category of second and third generation of cybercrime. The reason behind such an occurrence can be laid within internal company systems which were proved to be unsafe as well as in the banking system in the Netherlands. The banking is a suspect in this case, due to widespread use of banking apps, which can also be easily hacked. The innovation paradigm to get a safer working environment was primarily provoked by such an occurrence, so in this respect the act of a cybercrime served as a driver for a change of the mindset and approach to personal and corporate safety. It is also a security demand factor that played a role to raise the level of awareness among employees and enhance their knowledge. Also the importance of the security was recognized only after the incident took place, so in this respect the company was driven by cybercrime as by cause of a change.

6.4 Position innovation: Elcatronics

Elcatronics’ innovation is in the way how services are currently delivered against the past and the unique position of the company to provide its services and products in this particular and safer way. The following innovation can also be described as a business model innovation since it changes the direction and image of the company through improved delivery model. The innovation of Elcatronics is intangible, so it is not possible to sell or have a direct gain from it. Even though they are suppliers of the service, the service itself wasn't directly affected by the cybercrime, thus, it remained unchanged. As with the paradigm innovation, it is difficult to classify the type of innovation in terms of company's unique position when the benefit is not direct and doesn't fall completely under user innovation definition. However, the following innovation is partly a user innovation because it is beneficial for customers, that receive more safety in a service proposition and the company in turn receives a positive feedback from the satisfied customer. This type of innovation can be in the long term also beneficial for the society in its attempts to be outstanding compared to the competitors, and can serve as a motivator for other like-minded companies in the field to adopt a similar approach. In this respect the type of innovation is also in conjunction with paradigm innovation. Furthermore, the unique attitude and position of Elcatronics can be not new to the world, but new to those who adopt it, so the unique position in their approach to security and service delivery is an internal innovation of the company. In order to be able to adapt to changing circumstances and needs, the company is involved in innovation processes, thus, fulfilling also own business goals and needs that require flexibility nowadays. The position innovation expressed through the case study, however, also intersects with a product innovation in terms of development and adding additional features to the existing Crashplan software program. The program itself is based on an older version of the product and is an incremental product innovation.

Crime as innovator

There was no direct impact as far as it is known on the company itself. But the raising alertness on behalf of consumers served as a motivator to introduce new safety ways on the delivery of more secure services. This was partly done also to increase the trust and commitment of the clients and to attract more prospective customers who are still being anxious to use cloud services for safety reasons. Hence, here is an indirect impact of a cybercrime on internal innovation processes, which are seen as natural in cause and effect terms due to raising number of data breaches worldwide.

6.5 Mapping innovation and cybercrime

In order to understand how innovations are being part of an evolutionary process that has come as a result of cybercrime impact, mapping helps to illustrate that process among SMEs by highlighting their innovation dimensions.

Each case has illustrated different types of innovation within different organizational contexts. For each case there was a short description of the company given and a problem associated with the cybercrime that pulled an innovation to a certain degree forward. According to the respondents, the proposed solution in the form of innovation should be beneficial to companies themselves, end user or a society in general. There are definitely other factors why organizations innovate but the focus was made particularly on security issues and associated changes. After each case it was shown how cybercrime can be seen as a contributing factor to innovations at each enterprise. Below is a schematic representation of each innovation that could take place in the framework of the 4P's within innovation space. The location of each innovation depends also on the degree to which type of innovation it most likely belongs, since some of the innovations intersect or have elements of other types of innovations. Also, it indicates whether each innovation belongs to either radical or incremental type of innovation.

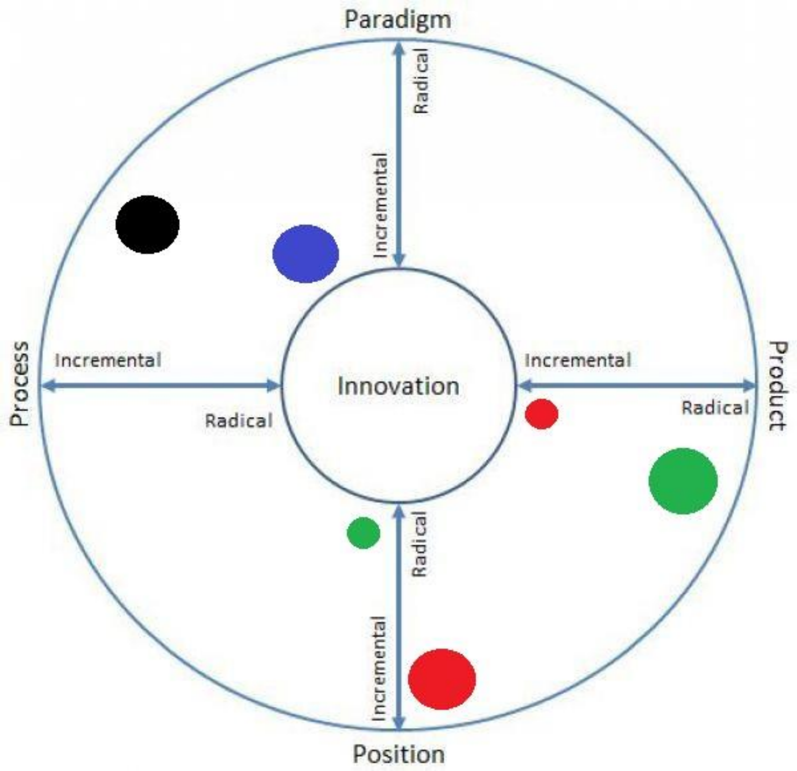


FIGURE 8. 4P'S MODEL IN THE INNOVATION SPACE (RESULTS)

Company:

● Contec (Product innovation)
● Whitecliff Ltd. (Process innovation)
● Verwey Grafische Produkties (Paradigm innovation)
● Elcatronics (Position innovation)

The figure below summarizes the analysis of the cases and shows relationship between cybercrime type, cybercrime generation, innovation type and innovation gains. Here it is shown which individual case innovations belong to each category of cybercrime. The type of innovation, whether it is user or producer is presented, as well as the main benefits that the innovations provide. Hence, the table provides other dimensions to the 4P's main framework:

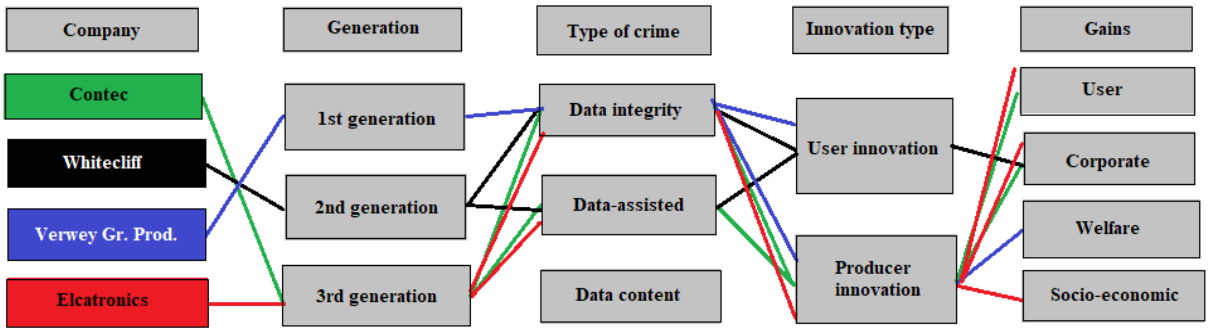


FIGURE 9. CASE SUMMARY ON INNOVATION AND CONSECUTIVE GAINS

The last column of the table which is gain, illustrates those types of gains that were considered in the literature and which are considered to be the most important gains for each organizational case in terms of innovation. With some innovations there is no obvious or measurable gain that can be defined. Some have different gains and benefits and one leading to another. For example, with a welfare gain, in most cases, it can also result in a socio-economic gain, corporate individual gains in the long term. For example, sBDS, which mainly provides a business gain, will probably also provide a welfare gain and a socio-economic gain, since this solution as any other security products serves wider public. And these types of products provide financial benefits also to the shareholders of Contec. So, there are various gains that can be received in terms of utility of innovation, either short term or tong term, and often a synergy of different benefits is brought by innovation. However, the most obvious gains were indicated in the table.

These cases illustrate why and how the organizations have invoked the innovations as a result of cybercrime in those specific cases. It deals with the overall need for change that cybercrime has directly or indirectly caused, and this need for a change has resulted in adaptations that have led to innovations. The innovations in information technology have taken place over the two decades very intensively. They are being a result of the timely changes in technology and crime.

Only one of the innovations provides corporate gains, associated with the selling of the product. The rest of the innovations are more related to welfare gains and socio-economic benefits. Some enterprises such as Contec are more proactive in taking an opportunity to fulfil a demand on the market and the need for safety among the wider public. Others take more reactive approach and are adjusting to the environment and fulfil the necessity for a change as the market requires. Also, there are entities such as in case of Whitecliff and Verwey G. P., where the changes come with new knowledge and experience. The cases except for Product innovation didn’t receive direct financial gains from innovation, though, the gain is seen more as long term. Such a benefit is rather hard to estimate since it is not marketable and doesn’t have a selling value. Furthermore, the need for innovation at Contec and Elcatronics was formed by external development and the cybercrime wasn’t making a direct impact on the enterprise, unlike, Whitecliff and Verwey G.P. that were directly affected by it. In this respect, the first two above mentioned companies’ innovations were triggered by the external environment, technological development and needs while the other two by the internal need for a change.

Nevertheless, all four case companies were affected by cybercrime to a certain degree which has led to innovations. Also, there can be many types of gains brought by innovation, which also depend on the goals of its implementation.

During the analyses of the cases it was also revealed that those companies that Contec and Elcatronics that were not directly affected by cybercrime produced more radical innovations that also coincided with other forms of innovations. Also these companies’ innovations were based on a pro-active approach to cyber security compared to Verwey and Whitecliff where reactive approach to cyber threat was taken. The latter two were directly affected by a cyber crime and didn’t have forms of radical innovations, there was more tendency to improve the existing processes and approach to security. These innovations are incremental in their nature and raised due to internal corporate needs, unlike the first two were originated through external demand and security need.

The following chapter presents a discussion on innovation introduced as a result of cybercrime in different organizational contexts, and on cybercrime on a more general level, using the literature on organizational development and adaptation and qualitative data received from in-depth interviews.

7. Cybercrime as-a-driver: empirical findings

The following section describes different processes that cybercrime and innovation are surrounded by. In order to see the cybercrime as a change agent leading to innovation it is necessary to see how it evolves through technological development against developments in cyber security as countermeasures. Also the cybercrime level, knowledge and skills are considered because it gives an idea on maturity of cyber attackers and how far they can go. This can be seen through the needs they are trying to accomplish. Some of opinions from experts were collected on trends of cybercrime and security and on dynamics of that development revealing the innovative advantages and benefits from innovation that might be on both sides of the cyber race. Here also the description on how can cybercrime enable a change in business models from necessity-driven to opportunity-driven perspectives. Furthermore, there is described organizational development through improved cyber security measures and strategies and the need in adaptation to currently unsafe environment. Seeing cybercrime as a driver, it was also possible to conclude that innovation provoked by that phenomenon brings along efficiency and organizational growth through improved security and innovation. Among other things, the importance of crime leading innovations is mentioned, since any forms of innovation can bring a knowledge value in a business context.

In the conclusion section, data collected during empirical research among SMEs, applied to literature theories, describes various dependencies, motives and other dimensions of innovations that originated due to cybercrime as well as some of the cybercrime dimensions that had an impact or relation to that development.

7.1 Relation to technology development

Information technology has become an all-encompassing technology that provokes radical as well as incremental innovation and changes. It is a complex phenomenon which provides new opportunities and satisfies different business and user needs. But, at the same time, it has caused many new threats and new needs arose that must to be satisfied accordingly. Both criminals and SMEs face the opportunities that information technology offers. "*The rising number of threats and security breaches is leading to the development of new software, tools and programs on a continuous basis. In particular, this creates enormous opportunities for anti-virus developers, because they sell their products, creating a false sense of security. Same goes for companies that offer tools to repair computer systems. Most of these tools are useless (Mackeeper, does more damage than it fixes), and even more dangerous because the average user isn't aware of what he or she is installing. Macs don't need these tools, because the architecture of these Macs has built-in technology, to repair any issue. Windows is more vulnerable to viruses and malware. Many products are offered to repair and protect. They usually solve nothing. McAfee is trustworthy, and so is Norton Utilities. But many other tools contain a lot of errors and require payment to solve the issues, which in many cases do not even exist"* [R4, interview].

Both cybercrime and security push innovation forward. Even in the area of outlaw innovations, there are those products and services that are outstanding and sophisticated. *Lawlessness can lead to new and better products and new markets in the world. And* *criminals can be seen as actors for technological development by modifying and utilizing products and systems to do things beyond what they originally were created for"* [R1, interview].

Organizations tend to innovate as a result of cybercrime for various reasons. This may depend on the type of organization as well as on its purpose. In either case some forms of innovation take place as a direct response to the opportunities and needs cybercrime has caused. "*The possibilities that may arise in the security sector for instance, are premise driven, if there is a need that can be fulfilled. Creating security solutions without the need for it will not bring any benefit or profit. Hence, premises are created as a result of a threat. Protection from the threat appears as a necessity and response to a clear need. New knowledge is created because there is a need for a solution"* [R1, interview].

As all the respondents highlighted, the main challenge of cybercrime is the globalization processes and internet accessibility since the web is boundless and the crime can pass along the borders and legal frameworks. There is no international law or international police with authority operating across the Internet. A world that is becoming increasingly connected is also providing more room for criminals. "*It is seen very clearly, for example, when Facebook got a big deal. Suddenly a lot more malware becomes widespread also through social networks. And this is a tendency that is steadily growing*" [R4, interview]. Adding to that the safeness of technology is rather poor. According to one of the respondents the safeness level is *"extremely bad. We see companies that store total accounting or critical business data in an unprotected environment or on local laptops without anti-virus. Or, for example, in a free DropBox, Google Drive or OneDrive account"* [R2, interview].

This means that the threat can come from anywhere in the world, and can therefore be hardly impossible to trace which makes an enormous impact not only on organizations in the Netherlands but in the world. It also poses a great threat also to national economies in general. "*Organizations, especially financial institutions, prefer not to disclose how much they did lose due to the cybercrime to avoid losing the confidence in their services among the customers."* [R3, interview]. However great sums of money are spent each year to fight against the attackers and for development of new and more sophisticated protection means in the Netherlands. "*Banks were used to replace bankcards without thorough checks. In one particular case this resulted in cleaning out of seven bank accounts because the bank card was automatically connected with telebanking. Identity check failed or was never performed, and the criminals had access to all accounts. As a result, nowadays banks require clients to come to the bank and show proof of identity. But this only applies to business accounts. One would think banks would learn and implement this for private clients"* [R1, interview].

By reviewing the literature on technological development, expert opinions received during interviews on providing connections of interdependence between cybercrime and security and the dynamics of its development, it is possible to conclude that the Internet has linked the world together in one large, virtual community where most interactions of different kinds between users and producers of innovations take place. The internet has been formed by users, but the Internet has also shaped users and communities through technological developments. This illustrates an interdependent and collaborative process that involves different actors, change agents and processes in the Netherlands as well as around the globe and. It also applies to criminal and regular organizations, their interactions and innovations on both sides. In that sense, it can be seen as an evolutionary process where changes affect other changes and evolve in a dynamic process.

7.2 Knowledge and skills

Apart from the literature study, there were certain opinion collected on how cybercrime develops and evolves, and how this development can also be seen as an ongoing process without an end point. Though, it is possible to conclude that this process itself is moving developments of counter innovations forward.

According to one of the respondents, "*In previous years the most common forms of attacks were classical viruses with "immature" hackers bringing a certain amount of damage to individuals or enterprises. Those hackers wanted to possibly show how skilled they were and wished to be largely noticed. Around 2000, the patterns had changed, as more and more criminals used the Internet as a source to commit a crime. Those better skilled individuals could have economic, political or military-strategic motives for stealing information. These, unlike the first category of hackers, preferred to stay less visible"* [R2, interview].

"The attack patterns today are largely tailored to make financial gains, and this tendency is even more strongly felt after 2006. Before attacks were mainly aiming at, for example, stealing credit card information. Today, such viruses as Trojans are upgraded, with the aim of, for instance, stealing both credit card information, passwords and user credentials. Later this information can be sold at different locations in order to be further exploited for financial gains. Also, the spread of ransom software is very excessive nowadays. Computers are blocked, and by paying an amount in bitcoins, their computer is released with bitcoins being untraceable." [R2, interview].

According to another respondent, the biggest of recent times is an identity theft. "*Criminals use social media, like Facebook, to find out all details about a person. Once they have a social security number they can assume that person's identity. The consequences of this can be enormous in terms of damage done. People suddenly discover they can't get a loan, or their bank account has been cleaned out."* [R1, interview]. "*The large part of criminal activity is also done within a dark net. Recently, the Dutch police successfully infiltrated a dark web site, where drugs were sold. They monitored the users for half a year and were able to arrest the criminals and close the site. The Dutch Government has now provided 26 million euro to fight cybercrime"* [R1, interview].

According to one of the respondents, what is also becoming more common nowadays is spread of Advanced Persistent Threats[2] [R4, interview]. This is described as a set of highly advanced computer hacking processes targeting at exploiting vulnerabilities of the system of an entity. Those who develop these systems have an extremely large amount of resources. Phishing is also seen as the worst type of cybercrime in recent years. "*Fake links to certain websites or accounts in a .docx (which include all kinds of macros that make the files*

[2] https://nl.wikipedia.org/wiki/Advanced_Persistent_Threat

encrypted) where money is being asked for. And at the very beginning people often pay because people they assume they did something wrong themselves. This has happened to us twice in a cloud environment, and it's the least harmful here, since it runs 24/7 backup (not just files, but the whole system), so we could turn the time back and restore everything, usually within one day. On a standalone computer, it's a much bigger problem, especially for customers without backup." [R4, interview]

In addition, "*crime has become much more organized, and thus can consist of many development teams. Among them, there are those individuals who do the actual programming job and develop tools. They will not necessarily use these tools themselves, but will be paid for that task. There are also the ones who use the tool and those who launder the money"* [R4, interview].

"Criminals do not follow the same laws and rules and bureaucratic regulations as regular citizens which enables them to stay ahead of organizations sometimes that fail quickly to respond with a change" [R3, interview]. Hence, there is a certain degree of dynamism between criminal innovations and regular innovations.

An increase in the number of individuals with high technical ability explains the rise of outlaw users. These users, in turn, provide an opportunity to outlaw innovation development. According to reviewed articled on criminality levels and statistics, today's IT and technical knowledge levels are much higher than in the past decades, and the violators can reprogram, learn, transmit and share knowledge fast on complex and high-tech products and services. This has resulted in less control for organizations, which is challenging for both organizations and their customers. Hence, modern cyber criminals require a high level of competence and knowledge with regard to ICT. This especially concerns programming skills to be able to develop a highly advanced malicious software. *"The criminal world has developed its own business models, where the programs are sold as tools or as easy-to-use criminal programming tools, often called exploit packs, so that those who use them need minimal technical knowledge to take advantage of it. Hence, someone with a basic knowledge of software can easily find a program on the internet to create malicious software themselves."* [R4, interview].

7.3 Cyber security needs

The idea of crime and punishment in the form of appropriate institutions that define the crime and deal with it has been around for thousands of years. However, what is perceived as crime has changed over time. As society had been developing, different types of preventive measures were developed and continue to develop against the threats, criminal events and those individuals who doesn't want to commit to the common rules.

Along the widespread technological use various needs and opportunities make regular organizations involved in innovation activities. In a technology driven environment different forces are involved in driving innovation forward. The cyber criminality is one of the factors that contributes to it.

The respondents chosen for the thesis have described some critical situations, where the need for change and provisions of cyber security have been necessary steps for their businesses. Therefore, the need for change and the possibilities to implement changes were driven by widespread technological use. The same applies also to cybercrime, partly due to the increased economic potential of the Internet.

Not only recently organizations have felt a strong need for a security. In the business environment it is vital to have a necessary level of competence and resources to be able to fulfil security needs. Organizations largely invest in cyber security nowadays, since its perceived more efficient in terms of tradeoff between possible losses of cybercrime. *“The need in secure authentication, authorization and encryption processes. Backup systems have also become increasingly important. In case of ransom software, a backup can be vital. Companies like Elcatronics, use the highest encryption possible and also use two phase identification. Their servers are located at Schiphol in a highly secure environment”* [R2, interview].

7.4 Change adaptations and organizational development

Organizations are constantly innovating due to changes in external conditions and the environment they operate. These changes in the external environment include innovations from the outside world, competition, public demand and governmental policies and regulations. This entails organizations' requirements for changing processes, products, and strategies to enable organizations to maintain their current operating level. Thus, this supports the assumption that organizations are in co-development with their surroundings. Organizations can stay up to date or stay behind, that is, regarding the organization's ability to perform their tasks. Even a small company like Verwey G.P. faced the need to further protect its data after criminals got access to their bank accounts. According to CEO, *“the company has implemented training for its staff, to learn how to recognize phishing mails and to be aware of spoofing. All computers have been protected with anti-virus software and passwords. These passwords are changed every three months and data is back upped regularly”* [R1, interview].

Outlaw innovation and criminals lead to changes in the external conditions of regular organizations, which means that a certain criminal activity can cause changes to the environment and, thus, affect organizations. The effect of cybercrime has changed the environment of the case organizations respectively. *“Outlaw innovations and criminal activities influence adaptation processes among regular organizations and complement commercial innovation projects and innovation processes through these activities.*[R1, interview].

Innovation, as mentioned above, is not just about increasing competitive advantage, growth and financial benefits, but also for staying at the same or higher level of profitability or in order to enhance operational processes. This is about how the organization manages to solve its issues, dealing with uncertainty and unexpected events, the increased turbulence and complexity in different circumstances. Change and turmoil in society, economics and technology can create crises which also cause threats to organizations. To minimize these, organizations must adapt and change. These changes may in many cases be innovations. Changes in a place will often lead to a chain reaction, forcing others to adapt and to new things created. It is a chain of causal effects and therefore ability to survive and maintain eligibility of an organization. In general, adaptation and change results in organizational development and innovation. Innovation always involves change in routines, but change does not necessarily lead to innovation. The cases illustrate that innovations driven by cybercrime can be developed to increase the market share, to keep business running at the same level or to enhance internal operational efficiency.

7.5 Necessity vs. opportunity business models

Entrepreneurship refers to the necessity-driven and opportunity-driven business model. This is a simple distinction also contributes to the angle of innovation taken in the thesis. Among the case companies, two of the innovations were necessity driven for the innovators (Verwey G.P., Whitecliff), and two were opportunity-driven innovation (Contec, Elcatronics). This coincides with two user innovations and two producer innovation among the cases. The opportunity-driven innovation was sBDS from Contec and a Crashplan provided by Elcatronics, where the need and necessity lay with a potential customer, a lead user. The innovative products by Contec and Elcatronics are opportunity-driven solutions created to solve the problem or to meet the needs of the customer while at the same time bringing a profit to organization, producer of innovation. All innovations in case companies can be looked upon as the result of innovation opportunities that have been introduced by the environment and cybercrime threat in particular. Due to the change in the environment caused by cyber criminality new necessity-driven innovations have been realized as it is shown on the examples of the case companies Verwey and Whitecliff. Here the internal demands for security were prerequisite to change, where the cybercrime had played a role of a pusher to take an action to change the process and the mindset in case of Verwey.

7.6 Benefits from innovation

Through the case companies it was shown how the innovators vary among each other. This deals with the functional relationship of innovation, and relates to the analytical distinction between user innovation and producer innovation. This distinction can be particularly useful because it shows innovation not aiming to bring particularly financial benefit, but that it fulfils a need and can be in a form of idea, process or unique position that makes it innovative.

Since innovation and inventive business ideas are highly risky and expensive to implement, people normally get involved only if they expect a benefit to exceed the estimated cost. Other innovations and inventions that don’t meet these criteria mean that they are random. So, as it has been illustrated in the case companies, not all innovations need to be profitable. The utility can come through a value other than financial profit, which can also make it difficult to measure by economic unit of measurement.

This may suggest another interest in innovating against cybercrime, even though the cost should not exceed the value that is perceived to be brought to organization in terms of innovation benefits. Any innovation processes require commitment to goals and a strong belief in success. Changes in the environment can for example force organizations to reorganize their structures and resources and can involve an emotional aspect as well. As it has been with the case of process innovation in Whitecliff, where external forces influenced internal processes and shaped processes of completing routine tasks in new ways. One of the ideas behind implementing a new system was also due to the fear of a cyber breach which led to the development of a new innovative process, and partly paradigm to ensure the security of data.

Innovation is aimed to be beneficial when it is used. All case innovations have brought benefits to the companies. Here, many of the forms of innovations implemented by the enterprises have been introduced because of the needs created by cybercrime. With the knowledge they possess, some solutions were created to benefit their own companies as well as other, as it's in the case of product development by Contec and Elcatronics. In these examples, innovations have fulfilled completely or partly the need with existed knowledge.

Organizations can receive different experiences through innovations caused by cybercrime which also depends on the type of organization and how it was affected. Below are briefly described some of the most visible benefits that organizations can receive from innovation.

"The benefit of innovating as a reaction to cybercrime and information security associated events for most Dutch businesses is to minimize the financial losses. Economic loss can be direct or indirect, and depend on the event. Many businesses are exposed to cybercrime or information security events without being aware of it" [R3, interview]. *"The reason is often the lack of monitoring and logging of events that are crucial for detecting and preventing security events in the future. Often even simple emails are tailored to infect complex information systems. Whenever an employee clicks on a malicious email attachment, it can be enough for a computer system to become infected"* [R4, interview]. "*Spoofing makes it harder to recognize malicious email, because at first glance the sender seems trustworthy. An email appears to be from Rabobank, but when one clicks on the sender's name, a different mail address is exposed"* [R1, interview].

Another benefit is, for example, through implementation of a new technology or mental model that can increase earnings and minimize the risk of loss. In addition, the organization will probably be perceived as more trustworthy among its customers. This kind of a change was implemented at Verwey G.P.

In some cases, the financial benefit can be difficult to identify in concrete terms. Especially if one is not aware of the fact of the intrusion into the system or data breach incident. It can be difficult to estimate how this information will be used by the attacker and what the consequences would be. Long-term profits from innovations are difficult to estimate in case companies Verwey G.P. and Whitecliff since their forms of innovations are not of the marketable value, and can be beneficial only to internal ecosystems.

“According to Dutch authorities it is assumed that it can be very expensive not to innovate. Furthermore, it is difficult to estimate what kind of benefits innovation can bring in the long term, for example, for the public sector or non-profit organizations, and can also depend on the goal of the organization. It can also be beneficial to take advantage of criminal innovations and solutions for regular businesses.” [R1, interview].

Another benefit is the opportunity to create innovative products or services by exploiting the marketability it provides. Since a security need is arising from cybercrime, one can fill this need by creating security solutions to cover it, as in cases with Contec and Elcatronics. The benefits here may include business development, increased revenue and increased market share.

Many of the benefits are linked to business and private economic benefits for organizations. But there may also be cases where it is more of a welfare gain and a socio-economic gain rather than a direct organizational profitability, which is shown in the examples of some of the case companies. This is due to wider adoption and promotion of security by technology and security driven companies such as Contec and Elcatronics.

8. Conclusion

Innovation is a phenomenon that not only about increasing the competitiveness, market shares or something that will provide financial benefits. Innovation provides measures in relation to various factors that affect the environment and organization in which it operates. In addition to that, innovation is a sort of a solution to a problem that organizations face. It is often driven out of need or demand and is often combined with the knowledge sharing.

Innovations are often about bringing together familiar things in new ways, or modified and improved products or services. Innovation does need not be new to everyone, but must be experienced as new to those who adopt it. Based on this understanding, innovation may be initiatives and strategies of organizations to protect and adapt to various aspects of cybercrime as it has been shown by case organizations. Both opportunities and needs can arise as a result of cybercrime, and different perspectives, strategies, organizational tasks and goals can affect what kinds of adjustments are being implemented.

Innovation is intended to fulfil the need of an end user who receives certain benefits from using it. Users normally don’t receive a direct financial benefit from innovation if they are not being producers of innovation and can’t sell it. Criminals can also be users and produce outlaw types of innovation.

Increased information access through increased use of data and network technology brings more user innovations, which increases social welfare. Innovations can lead to various gains such as private, public, corporate, socio-economic and welfare benefits.

The review of various market research and analysis reports on cybercrime and cyber security provided an indication that cybercrime or cyber threat is one of the drivers of technological development. However, since, there is no methodological or scientific approach on considering cybercrime as an enabler of innovation, the following thesis was attempting to get closer to understanding of the phenomenon from this perspective. An attempt was made to illustrate how cybercrime has driven innovations in four SME organizations in the Netherlands and how it can be seen as an innovation driver.

According to literature and numerous articles that were reviewed, SMEs are more vulnerable to cyber threats compared to larger organizations. This is due to low defence barriers, assumptions about the lack of interest among criminals and often a shortage of funds to provide adequate level of protection. The Tidd Bessant’s 4P’s framework was chosen for mapping four different types of innovations that took place within participating SMEs. The companies were chosen on the basis of availability of each particular innovation at their respective enterprises. This was done with the aim to illustrate how cybercrime can impact innovativeness and how it can be described with respect to different innovation dimensions.

In order to be able to provide an answer to main research questions, there were different aspects considered on innovation and cybercrime phenomena. The summary of innovation and cybercrime elements that were chosen for description of the cases were based on the literature and are summarized in the table below:

Company/innovation dimension	Contec	Elcatronics	Verwey	Whitecliff
Dimension of innovation				
Innovation type				
Product	🟦			
Process				🟦
Paradigm			🟦	
Position		🟦		
Business model				
Opportunity-driven	🟦	🟦		
Necessity-driven			🟦	🟦
Functional relationship				
User innovation			🟦	🟦
Producer innovation	🟦	🟦		
Reaction to the environment				
Internal			🟦	🟦
External	🟦	🟦		
Needs and demands				
Internal		🟦	🟦	🟦
External	🟦	🟦	🟦	
Gains				
Corporate	🟦	🟦	🟦	🟦
Individual			🟦	🟦
Public	🟦	🟦		
Welfare		🟦	🟦	
Socio-economic	🟦	🟦		
Scope of innovation				
Radical innovation	🟦	🟦		
Incremental innovation			🟦	🟦

Cybercrime aspect				
Cyber security approach				
Reactive (prevention)		🟦	🟦	🟦
Proactive (detection and response)	🟦	🟦		
Cybercrime generation				
1st generation			🟦	
2nd generation				🟦
3rd generation	🟦	🟦		
Cybercrime type				
Data-integrity crime	🟦	🟦	🟦	🟦
Data-assisted crime	🟦	🟦	🟦	
Data-content crime				
Motivation				
Political				
Economic			🟦	🟦
Socio-cultural				
Cybercrime impact				
Cybercrime as-a-driver to change	🟥	🟥	🟥	🟥
Cybercrime direct impact			🟦	🟦
Cybercrime indirect impact	🟦	🟦		

TABLE 2. SUMMARY ON CASE STUDY FINDINGS

Cybercrime appeared as an integral part of interaction between people and technology and this interaction is pursuing further developments that aim to fulfil a certain need. With the development of the use of the web in society, the counter destructive developments took a place respectively, leading to the society that continuously adapting to new environments, facing threats and risks and, hence, develops countermeasures. Most considered innovations were made in an attempt to fulfil the security demand or to maintain the business functioning at the stable level by diminishing the possibility of a threat. In the findings section views on various aspects are presented and analyzed with the help of literature and by means of in-depth interview answers provided by respondents of case companies. More general findings were gathered in order to get more understanding of cybercrime phenomena and its influence on innovation as a driver by considering its surrounding factors, such as technological development, knowledge and skills possessed by the criminals, motives, shifts in the business models due to security demands and organizational adaptation mechanisms as well as opportunities and advantage that innovations bring along.

In general, innovation is not only a matter of consideration for those only parties that obey the law. The skills that criminal possess can be sometimes unexpectedly higher, because their creative abilities may not be governed equally by business models, guidelines, bureaucracy, formal education or any types of restrictions including ethical. One cannot either encourage or honor criminals by looking at the topic from only one point of view, which is mostly negative. From the positive side, what it contributes to is providing knowledge and awareness about the world in which organizations operate. Users, both obeying the law and outlaw users help to shape and push forward innovation and technological development. These are important aspects that are necessary for a better understanding why the world and technology eventually take the shapes they currently do. It is also useful for understanding more in-depth why organizations innovate and what kind of innovations take place in different organizations.

The race in cyberspace can be considered an ongoing process with new risks appearing and counter measures to fight against them. The success on behalf of each actor is the speed with which technology develops. Hackers turned out to be both creative and innovative early in the way they can break into the systems, which means that these systems have to be improved and reinvented to be safer. Thus, crime can develop criminal innovations or outlaw innovations.

In the thesis, counter innovations are considered as a result of the crime. These types of innovations are directly or indirectly related to cybercrime which made an impact on their business models and shaped their organizations to a certain degree. Such counter innovations, namely, products, processes, paradigm and position have their own dynamics and scale because they are produced within a self-strengthening process and can be seen as reactive or proactive to developments within the internal or external environment.

Both criminal innovations and counter innovations are produced on a continuous basis and new products are created continuously. It is an evolutionary process because it builds upon previous innovations, knowledge and technologies as well as reflects the consequences of other actors' changes to the environment and other players. One must keep the same pace, thus countering each criminal innovation with its own innovation to deal with the cybercrime innovation in order to be successful in the long run. The process of innovation in the best case scenario must outpace crime innovation and investments must be taken proactively rather than when the crisis hits.

The aim was also to raise the awareness on cybercrime and to provide an insight into the exciting world of innovation and the way to look at the cybercrime. A broader understanding of these factors provides new insights in pursuit of understanding innovation in fields other than cybercrime, and generally to give a deeper understanding also on the subject of cyber security.

8.1 Suggestions for the further research

The following thesis can be considered as a starting point in the way how innovation can be perceived from the angle that wasn't thought of earlier to very large extend. So, other works in that field can lead to more in-depth discoveries on parallelism of the cybercrime and innovation and their mutual interdependence. This study is also very relevant to the world that is being in a transition period for organizations worldwide and becomes digitalized more each year and is covering also less developed countries and their increasing number and embracing more participants in a so-called online community that are united by the web.

The thesis has been primarily about a system where different actors influence each other. On behalf of the society, the cybercrime can be considered from both positive and negative sides. Considering a notion of a cybercrime, innovation is often seen dealing with negative consequences and distress of it.

Cybercrime has developed and adapted to the pace of technological development to the extent that it is of a concern for any social or business environment nowadays. Cybercrime is an integral and permanent part of the social environment, and is influenced by technology, innovation, economy and other factors. The novelty of this research is in acknowledgment of a factor that has largely not been recognized in research on innovation drivers earlier. Since, the cybercrime nowadays is an integral part of the society, understanding the phenomenon of it in the business context as an actor in the process of technology and innovation development and all of the aspects that can be affected by this is highly important. Furthermore, some of the outlaw innovations can be prominent themselves, since they are also driven by knowledge. The knowledge on outlaw innovations can also bring a business value to a regular organization.

Practical implications

During in-depth interviews, there were certain points considered in relation to implications for practice. It was discovered that there is a need for increased knowledge sharing between different environments, organizations and institutions working towards cybercrime prevention. In addition, it was mentioned that more attention should be paid to the research on that topic. This will probably be absolutely necessary in order to handle the increasing number of cyber threats and their new sophisticated forms.

Research implications

This thesis has a rather unusual approach to a cybercrime and innovation and their relationship. An understanding of how cybercrime is seen as a contributing factor and driver to innovation was presented with the help of literature and through qualitative comparative case study on innovations within different organizational contexts. Therefore, more research in this area is required. Research in the field of current innovation studies is required also to understand why certain innovations take place and what are the reasons behind their creation. Here the most important aspects are both the need innovation is trying to fulfil and the benefits it brings along.

The aspect of a cybercrime can be further researched on field through a direct contact with those parties who actually more on the side of outlaw innovation. Here anonymity of respondents would certainly be crucial and if the study is done from the perspective of outlaw user the task can be not easy to accomplish. Though, quite possible, since many outlaw actions are developed with the help of programmers or developers who are not directly involved with the crime but only with development of a product. The further research can also be in estimation of the volumes of innovations in certain industries. Categorization and classification of cybercrime and innovation type can also help to define what have been actually caused by a cybercrime, and without it otherwise would not have been implemented. Knowledge of these developments can determine what are the current driving forces that move the technological progress forward, and how it can be managed to a certain extent.

Bibliography

[1] Rahaman, M. (2016). “Cyber crime affects society in different ways”. http://www.thefinancialexpress-bd.com/2016/07/04/36968/Cyber-crime-affects-society-in-different-ways

[2] Deloitte article. (2016). “Cybercrime costs Dutch organisaions 10 billion dollars each year.” https://www2.deloitte.com/nl/nl/pages/over-deloitte/articles/cyber-crime-costs-dutch-organisations-10-billion-euros-each-year.html

[3] Kaplan, J., Sharma, S. and Weinberg, A. (2011). “Meeting the cybersecurity challenge”. McKinsey&Company. https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/meeting-the-cybersecurity-challenge

[4] DutchNews article. (2015) “The Netherlands is popular with cyber criminals”. http://www.dutchnews.nl/news/archives/2015/04/the-netherlands-is-popular-with-cyber-criminals/

[5] Safety monitor by Statistics Netherlands (CBS), (2017). “Three-quarters of cybercrime cases not reported”. https://www.cbs.nl/en-gb/news/2017/39/three-quarters-of-cybercrime-cases-not-reported

[6] Irandoust, K. (2016). “Most innovative Dutch companies in cybersecurity”. Linkit article. https://www.linkit.nl/knowledge-base/231/Most_innovative_Dutch_companies_in_cybersecurity

[7] National Cyber Security Centre (NCSC), (2017). “Cyber security assessment Netherlands 2017: Digital resilience is lagging behind the increasing threat”. https://www.ncsc.nl/english/current-topics/Cyber+Security+Assessment+Netherlands/cyber-security-assessment-netherlands-2017.html

[8] Cybersecurity Ventures, (2017). “Cybersecurity market report”. https://cybersecurityventures.com/cybersecurity-market-report/

[9] Cybersecurity Ventures, (2017). “Cybersecurity 500: Meet the hot cybersecurity companies to watch in 2017”. http://cybersecurityventures.com/cybersecurity-500/

[10] Smith, M. (2016) “Huge rise in hack attacks as cyber criminals target small businesses”. Guardian article. https://www.theguardian.com/small-business-network/2016/feb/08/huge-rise-hack-attacks-cyber-criminals-target-small-businesses

[11] Tidd, J. and Bessant, J. (2009). “Managing Innovation: Integrating Technological, Market and Organizational Change”. John Wiley & Sons Inc., 4 ed.

[12] Lange, T., Ottens M. and Taylor A. (2000). “SMEs & Barriers to Skills Development: A Scottish Perspective.” Journal of European Industrial Training. 24 (1).

[13] Allison, I. and Strangwick, C. (2008). “Privacy Through Security: Policy and Practice in a Small-Medium Enterprise.” IRM Press.

[14] Anderson, R. (2006). “The Economics of Information Security.” Science , 314.

[15] Kolodgy, C. (2002). “Meeting the Grwoing Security Needs of Small & Medium sized Enterprises: SME Security Solutions”. IDC.

[16] Gov.uk press release (2015) “Government urges business to take action as cost of cyber security breaches doubles”. Department for Business, Innovation and Skills. https://www.gov.uk/government/news/government-urges-business-to-take-action-as-cost-of-cyber-security-breaches-doubles

[17] Deloitte request report (2017). “Cyber Value at Risk in The Netherlands 2017”. https://view.deloitte.nl/RISK-201707-CyberRiskQuantification2017.RISK-201707CRQ2017OfficialLaunch_Registerpage.html

[18] Dictionary. http://www.dictionary.com/browse/driving-force

[19] Grant, M. (2013). “Towards a knowledge-based theory of the firm.” Strategic management journal.

[20] Hippel, E. (1994), "'Sticky Information' and the Locus of Problem Solving: Implications for Innovation". Management Science 40 (4)

[21] Ekvall, G. (1996). “Organizational climate for creativity and innovation”. European journal of work and organizational psychology.

[22] Ekvall, G. And Isaksen, S. (2010). “Managing for innovation: The two faces of tension in creative climates”. Creativity and innovation management.

[23] Nussbaum, B. (2013). “Creative intelligence: harassing the power to create, connect and inspire.” Harper Business.

[24] Burt, R. (2004). “Structural holes and good ideas.” American journal of sociology.

[25] Ahmed, P. (1998). “Culture and climate for innovation.” European journal of innovation management.

[26] Terblanche, F. And Martins, L. (2003). “Building organizational culture that stimulates creativity and innovation.” European journal of innovation management.

[27] Absolutereports. (2016). “Cyber security market opportunities and forecasts 2016-2022”. https://www.slideshare.net/RuchikaShinde2/cyber-security-market-opportunities-and-forecasts-2016-20221

[28] Global Smart Grid Cyber Security Market report. (2014). https://www.technavio.com/report/global-smart-grid-cyber-security-market-2014-2018

[29] Slideshare report summary. (2012). “Market research report: Cyber security growth in India 2012”. https://www.slideshare.net/ResearchOnIndia/cyber-security-market-in-india-2012-sample

[30] Allied Market Research. (2016). “Cyber Security Market report”. https://www.slideshare.net/kpriya5/cyber-security-market-by-2022-analysis-growth-drivers-restraint-trend-and-forecast

[31] Imaa institute (2011). “Cyber security M&A: Decoding deals in the global cyber security industry”. https://imaa-institute.org/cyber-security-ma-decoding-deals-in-the-global-cyber-security-industry/

[32] Background paper (2010). “Crimes related to computer networks”. 10th UN Congress on the Prevention of Crime and the Treatment of Offenders.

[33] Marsh. “National oil companies conference 2014: Beyond the horizon – managing the next frontier of risk”. https://www.slideshare.net/ShahSheikh/national-oil-company-conference-2014-evolving-cyber-security-a-wake-up-call

[34] Sinrod, E. J. and Reilly, W. P. (2000). “Cyber-crimes: A practical approach to the application of federal computer crime laws. Santa Clara Computer & High Tech.

[35] Shinder, D. (2011). “What makes cybercrime laws so difficult to enforce “. TechRepublic. http://www.techrepublic.com/blog/it-security/what-makescybercrime-laws-so-difficult-to-enforce/

[36] Wall, D. (2007). “Cybercrime: The Transformation of Crime in the Information Age.” Polity Press.

[37] Wall, D. (2005). “The internet as a conduit for criminal activity.” In: Pattavina, A. (Ed.), Information Technology and the Criminal Justice System. Sage Publications.

[38] Casey, T. (2015). “Understaning Cyberthreat Motviations to Improve Defense.” Intel White Paper.

[39] Gandhi, R., Sharma, A. and Mahoney W. (2011). “Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political.” IEEE Technology and Society Magazine, 30(1).

[40] Innovation definition. http://www.businessdictionary.com/definition/innovation.html

[41] SCHUMPETER, J. (1934). “The theory of economic development: an inquiry into profits, capital, credit, interest and the business cycle.” Harvard Economic Studies, Vol. 46, Harvard College.

[42] Everett M. Rogers. (2003). “Diffusion of innovations”. Simon & Schuster; 5th ed.

[43] Eveleens, C. (2015). “Innovation management; a literature review of innovation process models and their implications”.

[44] Tidd, J. and Bessant J. (2011). “Innovation and entrepreneurship”. John Wiley and Sons Ltd.

[45] Albury D. (2005). “Fostering innovation in public services.” Public money and management.

[46] Tushman L. and Anderson P. (1986). “Technological discontinuities and organizational environments.” Adm Sci.

[47] Schumpeter, J.A. (1942). “Capitalism, Socialism and Democracy.” New York: Harper.

[48] Chesbrough H., Appleyard M. (2007). “Open Innovation and Strategy”. California Management Review, 50(1).

[49] Hippel E. (1988). “The Sources of Innovation”. Oxford University Press.

[50] Hippel E., Baldwin C. (2009). “Modeling a Paradigm Shift: From Producer Innovation to User and Open Collaborative Innovation”. Organization Science, vol. 22(6)

[51] Hippel. E. (2005). “Democratizing Innovation.” The MIT Press.

[52] Kolodgy, C. (2002). “Meeting the Grwoing Security Needs of Small & Medium sized Enterprises: SME Security Solutions”. IDC.

[53] Flowers, S. (2006). “Knowledge, Innovation and Competitiveness: Dynamics of firms, networks, regions and institutions.” Freeman Centre, University of Sussex.

[54] UN Manual on the Prevention and Control of Computer-Related Crime. (2001). United Nations publication. http://216.55.97.163/wp-content/themes/bcb/bdf/int_regulations/un/CompCrims_UN_Guide.pdf

[55] Verburg, R., Ortt, R.and Dicke, W. (2006). “Managing Technology and Innovation: An Introduction.” Routledge, 1ed.

[56] Link A., Scott J. (2011). “Public goods, public gains: Calculating the social benefits of public R&D”. Oxford University Press Inc.

[57] Beije, P. (1998). “Technological change in the modern economy: basic topics and new developments.” Cheltenham: Edward Elgar.

[58] Kim B. (2005). “Internationalizing the internet: the co-evolution of influence and technology”. Edward Elgar Pub.

[59] Khosrowpour M. (1999). “Managing information technology resources in organizations in the next millennium”. IGI Global.

[60] Kaplan, D. E. (1999). “On the Literature of the Economics of Technological Change: Science and Technology Policy in South Africa.” The South African Journal of Economics, 67(4).

[61] Hill, C. and Rothaermel, F. (2003). “The performance of incumbent firms in the face of radical technological innovation.” Academy of Management Review, 28(2).

[62] Nelson, R. and Winter, S. (1982). “An evolutionary theory of economic change.” Cambridge: Harvard University Press.

APPENDIX

Questionnaire

1. How would you rate the safeness of the use of technology nowadays?
2. What are the major information (cyber) security concerns within your organization and for organizations in general?
3. What is perceived as the most common forms of attacks? Which are the most dangerous?
4. Have you ever been affected by the cybercrime or any other individual/department within your organization? If yes, what were the risks or consequences? What was the measures undertaken?
5. Have you come up with any new specific innovative solutions/products/methods that have come as a direct or indirect consequence of a cybercrime?
6. What are the financial benefits from using the innovative technology?
7. Are you implementing security solutions as the threat arises or you take a proactive approach?
8. Have you implemented any changes as a consequence of the cybercrime in your operations, processes and procedures?
9. Have these changes occurred on the management level in terms of reorganization lay off, hiring more IT security staff, consulting, shifting of the roles etc.?
10. Have the cybercrime in any way affected or reshaped organizational overall strategy and strategic goals, long-term or short term, new goals formulation or any other changed of a strategic approach to consumer or partnerships, etc.?
11. Do you have security awareness training and learning procedures as well as guidance and a code of conduct? And if yes, has the standard procedures have been changed or improved due to the rise of cyber criminality?