TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies
TTU IT College

Henry Orlov 179936IVSB

Analysis of the Estonian Automation Company for Breaches in Physical Security

Bachelor's thesis

Supervisor: Mohammad Tariq Meeran
PhD in Information Technology

Tallinn 2020

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond
TTÜ IT Kolledž

Henry Orlov 179936IVSB

Eesti automaatikaettevõtte analüüs füüsilise turvalisuse rikkumiste kohta

Bakalaureusetöö

Supervisor: Mohammad Tariq Meeran
PhD in Information Technology

Tallinn 2020

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Henry Orlov

6/1/2020

Abstract

The aim of current thesis is to analyse the equipment and workspace of the automation company for breaches/problems of physical security, and then aims to propose the possible solutions to the identified vulnerabilities. The work will give an overview of the popular solutions and analysis through real-life implementation to see which solutions will be the optimal ones and to identify the cause of absence of the solutions before implementation. The automation company has breaches in their IT physical security when it comes to implementing new solutions for their business. All those issues will be examined and solved in this thesis. The new solutions proposed by author should fix those security breaches and give the answer to what caused their absence.

During the thesis, the practical analysis will be conducted. Theoretical analysis will examine the IT physical security of the industrial automation company alongside how they were caused the company and under what circumstances they are overlooked. Practical part will consist of developing and applying different solutions to those problems, the further outcome will serve as the main data for subsequent analysis. Then the gathered data will be analysed with the purpose of answering how to ensure that the solutions to the problems are implemented throughout the implementation processes and project life cycles.

The thesis is in English and contains 24 pages of text, 7 chapters, 2 figures and 1 image.

List of abbreviations and terms

CCTV Closed-circuit television

ESD Electrostatic Discharge

GDPR General Data Protection Regulation

IBM International Business Machines

IOT Internet of Things

ISKE Infosüsteemide Kolmeastmelise Etalonturbe Süsteemi.

IT Information Technologies

MMS Multimedia Messaging Service

NAS Network Attached Storage

QR Quick Response Code

RIA Riigi infosüsteemi amet

SIM Subscriber Identification Module

SMS Short Message Service

TUT Tallinn University of Technology

UPS Uninterruptible Power Supply

Table of Contents

Introduction 7
1 Description of the problem and formulation of the assignment 9
1.1 General Overview of The Topic 9
1.2 Limitations and scope 10
1.3 Description of the problem and goals 10
2 Materials 12
2.1 Materials review 12
3 Research methods 13
3.1 Overview of the methods 13
3.2 Overview of the final act of the theoretical part 13
4 Theoretical part 14
4.1 Overview of the security breaches in the office 14
4.2 Overview of the breaches in the manufacturing area. 15
4.3 Overview list of the breaches. 16
4.4 Tips for resolving procedures. 17
5 Practical experience 19
5.1 Finding the base cause 19
5.2 Solving the base causes and issues 21
5.3 Solving the identified issues 24
5.4 Gathering the Data 25
6 Result analysis 27
6.1 Origins of breaches 27
6.2 Majority of breaches 28
6.3 Resolving the breaches 28
6.4 Dealing with post-factor 30
7 Conclusion 32
References 33
Appendix 36
Non-exclusive licence for reproduction and publication of a graduation 36

Introduction

The work deals with analysis and deep examination of the automation company for the physical side of IT security, including finding and analysing breaches and searching for the most efficient way to solve them and finding the outcome in the form of the proposal for specialists who work with such companies across Estonia. The work will give an overview of the implementation of the different procedures and give feedback with thoughts on why those solutions are often not being used in such situations.

The automation company has been working on the Estonian automation market for a long time. The author was hired for the purpose of modernisation of their business, because of their potential growth. The authors responsibility was to find the existing breaches as well as proposing the best way to deal with them to ensure the security of the company information and assets. Due to being a part of a team, the author has been assigned to work only with physical aspects of IT security.

From the start the author identified for himself that there will be 2 different types of breaches: existing breaches, and the breaches that will be uncovered by modernization and solving of the existing breaches.

The importance of the work topic and the need to improve the current situation are related to the author personal experience and opinions of the authors colleagues that work in similar fields.

The results of this work should be universal and applicable to any company or organisation that would like to improve their IT physical security with the purpose of prevention of critical failures, that might lead to material losses or sometimes even lethal outcomes.

The main research questions that the author will answer in this thesis are as follows during the work will be:

1) What are the current most seen and ignored breaches?
2) What are the best solutions that could be used to easily get rid of those problems?

3) Why weren't those breaches solved in time?
4) How to make such issues appear less frequently?

By finding answers to the posed questions the outcome of the work should be the guidelines that the author can suggest in helping to solve similar issues in different situations. This will be the most useful for a scenario where the specialist has the same situation of being in charge of solving IT security breaches in another automation company in Estonia, but it also will be really helpful for companies in other spheres connected to IT.

The additional important requirement for the solutions is that as mentioned before, solutions must be adaptive, not being narrowly oriented to automation, so they can easily be used for companies in other spheres connected to IT, as trending solutions are often being developed with adaptability in mind, so they would work in other environments without the need for further actions.

The topic of the thesis has grown out of the author experiences from work during the internship, where the author had to find the IT physical security breaches and solve them in most profitable way for the automation company way.

The thesis will consist of the following chapters:

1) Description of the problem and formulation of the assignment
2) Literature and sources.
3) Research methods
4) Theoretical part
5) Practical part
6) Result analysis
7) Summary and conclusion

1 Description of the problem and formulation of the assignment

1.1 General Overview of The Topic

Currently the Cyber security is most often associated with mostly digital part of its existence, but cybersecurity has a lot of different spheres and subparts that deal with absolutely different issues.

Currently, almost every Estonian marked is closely connected to the IT Sphere and there is always a need to ensure the security by implementing different solutions. Those solutions are mostly been taken from special standards. For example, in the Estonia there is the ISKE (INFOSÜSTEEMIDE KOLMEASTMELISE) standard. The ISKE standard is based on a German information security standard – IT Baseline Protection Manual (IT-Grundschutz in German) – which has been developed to more fit the Estonian situation. [1]

The standards help to find the answers to most IT issues, including different types of security, like data security, systems security, IoT security and etc.

Recently, the sector of automatization in Estonia and other spheres with electronics have been growing fast and there is a major need of IT security because of it, mostly in information and physical security of equipment and work areas.

In the thesis the author will be discussing the physical aspect of the IT security that was implemented in the office and manufacturing area of the automation company.

It was hard do the first steps of the analysis when the work just started. Author had prepared a lot of possible solutions, implementations and assumed a lot of causes of the breaches that had to be solved.

As the author was a junior specialist, the statement about the causes was based at most common issues that were seen on the first look. More specifically, outdated tools and equipment.

1.2 Limitations and scope

As it was stated before there are some limitations that the author had to take into consideration. There is always a connection between different security measurements of the Cyber security and author job was only connected to the physical security measures. There were also some connections to the security of the internal systems but because of the small scope of those issues they will not have any significant effect on the thesis. Also, the author responsibilities were limited only to office and manufacturing area, so that the outer part of the building that needed security measurements in the form, for example, the street CCTV was not under the author's concern.

The solutions can basically be easily applied not only for the automation company but also for the other companies from other spheres of electronics or IT with similar set of issues.

1.3 Description of the problem and goals

Possibly, many of readers will agree that nowadays the most valuable property of any company is Intellectual Property, and today that property is almost fully connected with the IT sphere. Today the administration of almost every company knows that cybersecurity is a risk factor [2] and often leading to intellectual property theft, which is commonly being done from the inside. As ordinary phishing, still being in the top cybersecurity trends of 2020 [3], however there are still a lot of breaches for thieves, and physical security being the second most vulnerable one.

The automation company simply wanted me to do a job in the form of solving the issues with the existing breaches as well as getting rid of the new breaches that may be created upon doing the modernization steps.

Automation company was planning to modernize their cyber structure by replacing their old NAS machine and server with small, new TIER 2 data centre, so simply only a few measures, like Partial redundancy in power and cooling were in need.[4] But from the perspective of the physical security, the new data centre created the need for the new security measures to be implemented.

In general, there were a lot of different existing security breaches, found within analysis of the infrastructure, and firstly, author had noticed that there are few major problems:

1) Absence of the proper invetarisation of information assets
2) Absence of the proper rules for workers
3) Absence of the proper security measurements
4) Absence of the object qualifications (data security classes in ISKE) [5]

2 Materials

2.1 Materials review

The work has been done using a lot of different sources, literature, and documentation.

The good side of this work topic is today cyber security specialists have a huge cluster of standards such as ISKE, ISO 27001[6] or IT-Grundschutz as well as other different security measurements. Again, thanks for the growing interest in the cyber security many EU governments are now pushing a wider adoption and use of open standards. For example, in 2012 United Kingdom government published a list of open standards for data and document formats and software interoperability for the government's IT specifications. [7] Also, the internet as well is filled with a lot of worthy content and articles. Including a lot from trustworthy sources such as big IT companies such as IBM [8] has their list of articles or Microsoft [9] has a blog to read about this topic:

Also, the author had access to different books about that topic. The literature helped the author to prepare for the internship and thesis. [10],[11],[12],[13]

3 Research methods

3.1 Overview of the methods

The main part will be split in to 3 separate categories:

1) Theoretical part (the setup for solving the issue)
2) Practical part (solving the issue)
3) Result analysis (final analyse of the gathered data)

Theoretical part will contain the gathering of the information, search for breaches, inventing the way of dealing with issues(breaches). Practical part will be the implementation of the solution, created on the theoretical part. Result analysis will give the outcome in the form of the information that will be needed to answer the main questions of this work.

These are the aspects of physical security that the author was working with:

1) Ensuring the physical security of the equipment.
2) Ensuring the physical security of the intellectual property
3) Ensuring the physical security of the area

Now to analyse the whole enterprise of the automation company for the breaches. There are 2 fields to work with: is the office and manufacturing area.

3.2 Overview of the final act of the theoretical part

After finding all the breaches within the physical security they will be organized everything into a table, and under that list will be written all the particular steps of finding the practical answer to resolve each issue one by one. Then the author will move to the practical part of implementing the possible solution.

4 Theoretical part

4.1 Overview of the security breaches in the office

Since the company has constructed a new data centre it is best to start with easily identifiable physical security breaches:

1) The hardware was just standing on ordinary shelves.
2) There was no surveillance system in the data centre.
3) There was no good surveillance in whole office, bad camera locations “lot of blind spots”.
4) The data centre room had only a key lock.
5) Some computers were not password protected.
6) There was a physical list with the passwords of internal devices written on it.
7) The internal documentation was just lying on the desk in front of a non-covered web camera.
8) Near the printer there was an opened bin full of internal confidential documentation.
9) There was a personal mobile device of the worker lying on one of the desks.
10) There was a note that during the last year, company lost 2 devices, but was no information which devices were lost.
11) Following the previous issue, was found that the inventory is very poorly catalogued.
12) Was found that there are not any security measurements done on the almost every company device.

Author must admit that in their opinion the weakest point of the security was the right of workers to bring their own devices because according to the UK Cyber Security Breaches Survey 2019: Statistical release, over four in ten businesses organisations (44%) regularly use a personal device such as a non-work laptop for business purposes. [14]

4.2 Overview of the breaches in the manufacturing area.

After the research was done within the office, next step was the analysis the situation within the production line, since a few of the physical security breaches in the office have already been identified it is logical to first look for the same breaches here:

1) Issues with surveillance systems.
2) Some computers were not password protected.
3) Unauthorized, non-company devices on the desks.
4) The password for the Wi-Fi was just written on the router on the ceiling.
5) Computers that were operating the automated lines did not have security cabinets to prevent unauthorized access.
6) Monitors for the computers that were operating the automated lines did not have any security brackets or locks to prevent them from being moved without authorization.
7) Non licensed software was installed on one of the computers.
8) An inserted flash drive with non-licensed software on one of the company devices.
9) The confidential documentation was just lying in an ordinary bin.
10) There was an opened internet chat on one of the computers.
11) Half of the software was outdated.
12) The password of one of the computers was written on the monitor and was “123456”.

The NCSC's first 'UK cyber survey' published alongside global password risk list. According to the survey, breach analysis finds 23.2 million victim accounts worldwide used 123456 as password. [15]

4.3 Overview list of the breaches.

All the breaches are now listed in one place.

Table 4.3.1 Breaches list (Source: Author created).

Breach number	Breach description.
1	No save(closable) physical storage for hardware in the data centre.
2	Not enough surveillance.
3	No traceable lock for the data centre.
4	Some devices were not password protected.
5	Disclosure of the personal data (password).
6	Disclosure of the internal network logins.
7	No specialized storage for internal documentation and storage devices.
8	No special cover for the build in cameras.
9	Possible to bring unauthorized devices into the work area.
10	Bad inventory of physical assets.
11	Company assets and devices are not properly marked.
12	Company devices are not properly secured.
13	Not enough security measures on computers within the manufacturing area.
14	Not enough security measures against non-licensed software.
15	Not enough security measures against non-authorised storage devices.
16	Outdated software.
17	No basic security hygiene and knowledge among workers.
18	Availability to non-secured internet resources.

After the list was successfully created it can be seen that situation is in a critical condition. Also, because there are much more problems in other spheres, even including the electrical security (for an example: there is no ESD safe covers on some of the workbenches). Now the developments of methods that will be used to resolve those issues can start.

Also. It is important to remember that new issues may occur while we are dealing with these, so we need to keep that in mind.

Before the practical part, it is vital to remember these general suggestions that will help with analysing the situation:

1) Everything that is connected to the internal device usage can be solved by creating the internal rules or rules of conduct.
2) Always check every fact that can point towards to the base cause.
3) Base cause will often point to the other issues.
4) Gathering the data is one of the main goals.
5) The biggest sources of a data breaches are not some unknown or forgotten security bug, it is human error.

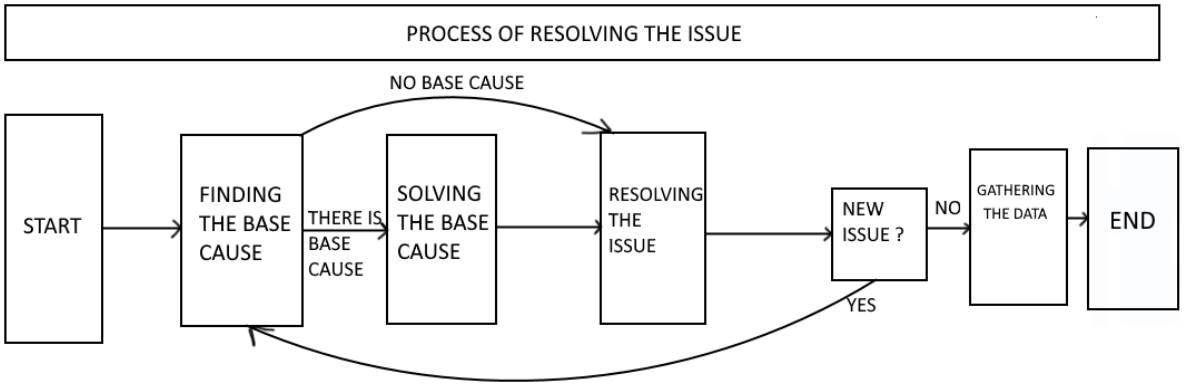
According to the study of over 5,000 businesses around the globe done by Kaspersky Lab and B2B International. The physical loss of mobile devices exposing their company to risk (46%) is the second of top 5 fears of being put at risk. [16]

4.4 Tips for resolving procedures.

The general process for resolving the issue can be easily described by these steps:

1) If there is any base cause, it must be analysed in case if there are more issues caused by it.
2) Resolving the issue/issues.
3) If there is a new issue/issues that were created upon resolving the original issue, then the base cause is located deeper in the structure.
4) After all the steps the data for the final analysis is gathered.

Figure 1. Process for resolving the issue (Source: Author created)



One of the main points of this profession is to find the base causes of such issues!

5 Practical experience

5.1 Finding the base cause

During the start of the resolving process, it is important to take out every one of the breaches and write down everything that is known about them, for further analysis. Numbers will be used as breach numbers from the overview list of the breaches. (Table 4.3.1) on page 16. After the analysis for each breach will be done, the new table with base causes will be created.

1) If the first breach is a new-born issue that was created upon the modernization of the old workspace into the new one, in the form of a new data centre which spawned the new issues.
2) Surveillance was outdated. There were a lot of unseen corners. After an interview with personnel and administration it revealed that old staff in charge was possibly neglectful or incompetent.
3) The access to the data centre was the part of the facility controls. It was a new-born issue.
4) The physical device policy was in poor condition at the time of the start of this work. As for one of the previous breaches, it was possible that this breach had the same base cause in the form of the poor handling of documentation.
5) Disclosure of the personal data as well as a few next breaches had the same base cause in the form of ignorance for working procedures and absence of IT rules for the personnel who worked with company devices.
6) Improper handling of company device passwords which can easily lead to security breaches.
7) No rules developed by previous staff in charge.
8) Possible security negligence of the old personnel in charge.
9) No rules developed by previous staff in charge.
10) Possible security negligence of the old personnel in charge.
11) FROM 10 up to including 16 has the same cause of breaches.
17) No special rules for cyber hygiene and work on the site for personnel.
18) Possible security negligence of the old personnel in charge.

Now, that everything is written down, it is possible to create a table to see some patterns that will help in next steps of resolving these security breaches. To the surprise of the author, the main base issue was probably the incompetence or simply ignorance of the old personal in charge of the IT department of the automation company. To confirm this theory, author had done an investigation. During the investigation it was completely verified and could not be appealed. Simply there were not any security-oriented specialists at all. It is not yet discovered, if there was opened position or it was the simple disregard towards the security by previous administration of the automation company.

The demand for skilled security professionals was and still is one of the biggest challenges facing the cybersecurity industry today, with 2.93 million positions opened and unfilled around the world in 2019, according to non-profit IT security organization (ISC). [17]

Even according to logs and previous documentation, left by previous IT workers, a lot of work procedures violations were found, such as full absence of supervision of company devices and assets.

All the base causes of breaches are now listed in one place.

Table 5.5.1 Breaches Base causes (Source: Author created).

Breach number	**Base breach cause.**
1	No base cause (New-born issue)
2	Breach caused by disregard towards the security measures.
3	No base cause (New-born issue)
4	Breach caused by disregard towards the security measures.
5	Breach caused by the absence of work security rules for the personnel.
6	Breach caused by disregard towards the security measures.
7	Breach caused by disregard towards the security measures.
8	Breach caused by disregard towards the security measures.
9	Breach caused by the absence of work security rules for the personnel, and disregard towards the security measures.

10	Breach caused by disregard towards the security measures.
11	Breach caused by disregard towards the security measures.
12	Breach caused by disregard towards the security measures.
13	Breach caused by disregard towards the security measures.
14	Breach caused by disregard towards the security measures.
15	Breach caused by disregard towards the security measures.
16	Breach caused by disregard towards the security measures.
17	Breach caused by the absence of work security rules for the personnel.
18	Breach caused by disregard towards the security measures.

Most of the security breaches were caused by the old personal in charge of the IT department negligence towards security procedures, this problem was solved by introduction of new personal in charge of the company's IT department, who put new security measures in place. The only issue that still must be solved is the reinforcement of general IT etiquette and work procedure rules for the other company employees.

5.2 Solving the base causes and issues

Now, before the further steps in solving, some consultations and further analysis must be done. As cooperation between all workers can give more tips and facts for further understanding.

As the only GDPR was a mandatory regulation to follow for the automation company, as a European company,[18] the other specialists are busy solving the newfound to regulation issues, that is why the author is taking help from a employees of the new human resources department and the IT department to create a set of internal policy rules for workers, to safely operate and use the company assets and devices.

As there is a lot of aspects that are not part of the physical IT security in general, only everything connected to the work topic will be analysed and written in this work.

Also, as the author mentioned before, the possibility of the creation of new issues while solving was inevitably.

As for first rules there was a lot of information about the company intellectual property and etc. And after 1 or 2 pages the author measures are starting to appear. Firstly, author is taking care of the issue in the form of disclosed password by applying the rule about the prohibition of the personal information and assets to employees. Author took as example the new rule about the personnel ID pass belongings.

After some time, the new measures are being created, the regulation about the workers devises and other IT connected belongings. Since now, every company worker will have their own storage out of the office and production area to store their belongings, and they will not be able to bring the unsanctioned devices on the work site.

New rules about the device usage were added, including that possessed company devices were specially marked and assigned to specific employees internally. Also, there is some new rules about prohibition of non-licensed software usage. The ability to bringing employees own storage devices, such as flash drives is also being prohibited according to new rules.

There are new rules about internet usage and available resources and etc.

Also, there is new rule about the usage of company phones and their numbers. Only company issued Mobile phones and SIM Cards may be used on the work site. Company phones can only be used for calling other company phones and company associates and there are some major restrictions for phones, for example no SMS, MMS sending.

New rules about internal mail usage are proposed since phishing was and is still most dangerous and popular way of attacking company security.

According to the RIA 2020 yearly book, Incidents registered by CERT-EE, in 2019 infections with robot networks accounted for the largest share. Alongside them, however, the number of phishing incidents doubled compared to last year and was **18.5%**. [19]

The new measures about the utilization of the internal, confidential documentation are added to the rules. Also, those rules are closely connected to the utilisation of IT storage devices and equipment such as automation company flash drives or compact discs and etc. The new, closed recycle bins will ensure the security of the discarded information and will save it from issues like dumpster diving.

Next step is cooperation with the security department to ensure the security of the whole object and connected to this work areas (office and production areas).

As all new the security measurements for the company are being under construction, the security department is also making their contribution in safe of the electronics devices by installing the metallic arcs on the exits of the enterprise. The security department is instructed about the necessary changes that must be done to the data centre as well as office and manufacturing area.

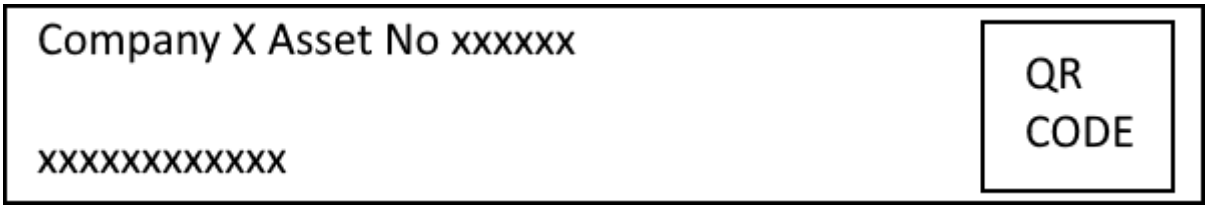
They ensure the author that new CCTV systems will be installed properly according to the instructions given to them.

What about the final touches to the data centre, new company IT Department and the standard ISO/IEC 27001 will easily guide them in securing the new data centre and getting rid of a few next issues from the list. Cabinets are really good solution, because the cabinets house the racks inside the computer room also need to be protected to avoid any costly data breach. In case of any breach in the perimeter monitoring, the second layer of defence restricts access. It is an access control system using card swipes or biometrics.

IT Department had added the special lock for monitors within the production area as well as protected cabinets for the computers operating the production lines.

The IT Department and Storage/Resource Departments are working hard on implementing the invetarisation of whole enterprise. Now, absolutely every company asset, including every type of devices will have special marking in the form of stickers with data on it (including the company own internal QR code).

Image 1. “Marking sticker early design” (Source: Automation Company).



The marking will definitely help the company to follow the ISKE standard for the Cyber security but also will ensure the security of every other asset, because even if intellectual property is really valuable there is a still, big percentage in physical property theft.

Employee theft of employer property is a major issue for organizations. Even though the general scope of the problem seems apparent, exact numbers of employee theft are difficult to obtain. That always was a huge issue, even in year of 2017. [20]

Also, the ordinary company issued stickers and covers were added to desktop mono computers with build in cameras and phones.

5.3 Solving the identified issues

As it was stated previously, solving the base causes and breaches uncovered new but not so critical issues.

After successful creation of the new rules and policies for workers, it is important for us to be sure that all the current and future personnel will understand and follow them. To improve the situation with the personnel understanding, the author and the human resource department are developing the new conduct and study programmes of the IT hygiene and usage of the enterprise electronical devices on the site of the automation company.

Those studies include the improvement of basic skills, knowledge, and control of electronic devices.

The HR department is doing some research among the IT department workers to ensure that there is enough qualification for them to continue working for the company, no issues were found.

The tests conducted for new personnel showed that every expected skill set is confirmed. The test conducted among ordinary workers (non-IT personnel) showed a good understanding too.

Figure 2. Graph of computer skills of ordinary workers (Source: Company X).

MICROSOFT WINDOWS SKILLS:	114	45	13
MICROSOFT OFFICE SKILLS:	92	70	20
MICROSOFT EXCEL SKILLS:	60	23	11

Since the fast-growing e-side of Estonia, more and more people get more experience and knowledge in electronical devices and even those small business created tests confirmed that there is a major jump even among the people who are distant from the IT. [21]

5.4 Gathering the Data

Since the outcome data is the most valuable part of this work, it must be clearly divided and defined.

The Data must be the key to the answering the base questions of the work.

1) What are the current most seen and ignored breaches?
2) What are the best solutions that could be used to easily get rid of those problems?
3) Why weren't those breaches solved in time?
4) How to make such issues appear less frequently?

Since the author is working for a company with intellectual property there is a few restrictions that however will not cause any issues for the work.

The automation company administration was informed of the authors intentions and will use gathered data for the thesis. Automation company asked author not to disclose any confidential information that is not allowed and ensures that the thesis will not loss any valuable to the topic information.

Every other departments of the automation company were helping the author by providing all the information needed and requested by author that is connected to this work.

The company also gave the author an access to the archives and old information regarding previous administration, workers, and procedure for further analysis. The

author promised and agreed to use all the provided information will be used only for studying and thesis purposes. Also, all the information about different people (including their names, positions and etc.) will not be disclosed in this work.

Three periods of time major for the analysis:

1) Information about the company before the new administration and modernization done by new workers and author.
2) Information about the company during the changes.
3) Information of the outcome of changes for the company.

All the data that is major for the analysis:

1) Old company documentation
2) Old company logs
3) Interviews with old workers
4) Practical experience
5) Knowledge of the administration
6) Authors previous experience
7) Authors colleagues experience
8) Standards and developed solutions for such issues
9) Cyber security trends

6 Result analysis

6.1 Origins of breaches

Why weren't those breaches solved in time?

The final result of the research showed that the most issues were created because of the incompetence of the previous workers and ignorance from the previous administration. 8 out of 10 issues on the whole enterprise were the ones and caused by the ordinary human factor.

The simple fulfilment of the standards as well as some development of the ordinary procedures for the previous personal would save the situation before it was too late.

If the measures were taken in time, the company would not suffer critical losses and the staff would not have been let go and later replaced.

According to the information gathered from old archives, the company administration as well as IT department showed critical lack of action when it came to solving new issues on time.

Also, according to documentation, administration did not act at all, even in some critical events, like previously mentioned, the loss of 2 company phones. Normally administration would consider such a case as a wild offense against the company guidelines, but in this example no further actions were taken.

The absence of the proper documentation in IT Department as well as some gathered information from the bookkeeping department shows that there was a possible mishandlings of company assets.

Some information from old workers suggest that there was a connection between administration and specialist who was in charge of the equipment.

To sum up the majorities of the causes and all the investigation that has been done in department it can be proposed that the general origin of those causes was the simple human factor.

6.2 Majority of breaches

As judging from the perspective of specialist dealing with physical IT breaches, the majority of breaches are based on the absence of basic security measures and lack of training among staff members.

Also, author notices and highlights that most breaches can be solved easily if following general ISKE, or ISO procedures.

What about the breaches in general, if physical breaches such as the absence of the right invetarisation can be easily solved, the issue such as lack of understanding among the staff can be quite challenging.

Sometimes the personnel simply do not understand or do not want to understand the core principles of the security and that points out that the main breaches are often caused by the human factor.

What are the current most seen and ignored breaches?

Sometimes, as well as it was in this work situation, the most dangerous issues are the most noticed ones. Even if there was highly developed internal network, there would still be the more dangerous problem that probably would forfeit all the effort done from the side of the admins and developers just by allowing the ordinary physical access to the assets. By this statement, the author means that the main threat to the organization comes from employees: reusable passwords, attacks of social engineering and the inability to implement multifactor authentication are the most likely threats than remotely installed software or any cyber-attacks.

6.3 Resolving the breaches

What are the best solutions that could be used to easily get rid of those problems?

Risk analysis, including their assessment, management, and discussion, is not new, but not everyone agrees with the term "risk-based." In large-scale systems, three components are present in the definition of risk: a description of what can go wrong, the probability of such an event and its consequences.

Risk analysis requires that it be quantified for each component of the system and associated uncertainties. The purpose of the quantification is to determine the contribution of each component to the overall risk, thereby identifying components at significantly higher risk than the rest. Such components form the basis for the development of quantitative benchmarks that de facto become risk-based standards.

Quantitative risk assessment lays the foundation for routine risk assessment. However, in cyberspace, threats change too quickly, and opponents try to respond as quickly as possible, so existing methods for quantifying risks and determining their parameters do not meet the scale, complexity, and dynamism of cybersecurity. Ultimately, risk-based standards should help to make informed decisions based on existing threats and their consequences. The inclusion of the word "based" in the term indicates the need to go beyond traditional risk analysis, with the possibility of developing guidelines on effective risk reduction based not only on the physical state of the world, but also on the preferences and values of interested users of the system.

The practical part proved that the most efficient way to solve such breaches is to fully analyse the situation and trying to create some sort of special workflow. The whole idea of that workflow is to find the cause and connect other issues to it, allowing to easily analyse and understand the whole situation.

Also, the practice could never be so easy if not the cooperation between author and other Departments of the company. The communication is the key to success in the situations like this.

It is, undeniable that it is a famous cliché that those, who work in the IT industry have poor people skills, but while their technical expertise might be second to none, how well are key cyber security messages being communicated throughout the business? It is imperative that security professionals can communicate effectively with employees and administration at all levels. This is especially important in digital businesses, where there may be a high number of vulnerabilities. [22]

6.4 Dealing with post-factor

How to make such issues appear less frequently?

Or simply what to do after everything is settled down?

What about human factor, New employees should be trained in the company's safety standards. It will not be more than once a year to organize a basic seminar on cybersecurity for all workers. In addition, the manager should pay attention to the daily activities of employees, sometimes just watching how security policies are violated.

Knowledge testing is required. This is not about passing the exam, but about checking the actions of employees by imitating a real threat. Regular training will help employees respond correctly to a real threat. Any company has information that requires special protection - confidential data. Employees should understand what data is, know that attacks on such information are carried out purposefully, and remember that the disclosure is punishable. Legally correctly formalize the status of such information and notify employees of this with a signature. This will help to raise the level of responsibility when working with valuable data.

Each employee should know how and to whom they should immediately address in the slightest suspicion that a problematic situation has arisen, or in the case of a cyber incident. The longer the reaction time to the incident, the harder the consequences. If attention is drawn to what is happening at an early stage, damage can be avoided altogether.

Security policies may lose their relevance over time if users believe that their violation will not lead to any consequences, or, worse, if they decide that bypassing will increase productivity. Company standards must be up to date and meet business requirements. Therefore, security policies must be properly implemented and maintained in a connected state. When rules are developed jointly throughout the company, and security issues are part of the corporate culture, violations are extremely rare.

Never, do not underestimate the abilities of one specialist.

A separate specialist responsible for countering insider threats can bring together teams from different departments to quickly detect, investigate, and respond to insider threat incidents when they occur. Such an employee can also help a team become more proactive when choosing the right policies and tools, primarily to prevent insider threats.

What about the digital part, Successful implementation of risk-based standards involves considering cybersecurity at the system level, recognizing the presence in cyberspace of virtual and physical systems and assets.

Security systems based on internationally recognized standards and independent compliance programs protect businesses and consumers from risks in all areas and contribute to the sustainability of company communications networks and systems.

Very importantly those systems must be always protected. It is not enough to react post a security breach, but to prevent it in the first place. Of course, almost no company has the resources to manually check the security of every system, so it is very important to automate daily systems whenever possible to free up employees for other important tasks and to also reduce the human factor. This is especially important for gathering analytical data, that if a breach does happen will quickly let the security specialist assess the situation and find the best and quickest solution.[23]

7 Conclusion

Cybersecurity issues affect everyone today, from IT specialists to the quality control services. At the same time, a large number of cyberspace users increase the rate of changes - along with the complication of protective equipment, the means the attacks are becoming more complicated.

This work was the full analysis of authors first steps as the specialist in this field. The author is really grateful that he had a chance to work with such a great people to prove his skills and knowledge.

The job that Author have done was not so influential for the company as it was for his improvement. There were definitely a lot of new and interesting problems encountered during this work, but the issues, as well as the ever-changing security breaches that can be found in such companies always give a specialist an opportunity to improve.

The Author found new ways of analysing the situations connected to his sphere of work and now he can understand the value of intellectual property.

Also, the big surprise for the author was the discovery of true importance of communication. If not the true communication between different department within a company, the whole job could mean nothing. It was really important for author as a new specialist to gather so much information about how close IT sphere is connected with each part of an ordinary automation company.

Also, Author learned that specialist must never trust their first impression before the analysis. What at first seemed outdated, was absolutely normal and up to date.

The most interesting outcome of this work is definitely about its influence on the author. This work had a big role in the authors past, present and future. The whole point of improving and learning is to always analyse everything that was done even a long time ago. The author is sure that the work that was done during this thesis will still be relevant and even more useful for him as a specialist in the future.

References

[1] Riigi infosüsteemi amet, “Infosüsteemide turvameetmete süsteem ISKE,” 2020. [Online]. Available: https://www.ria.ee/et/kuberturvalisus/infosusteemide-turvameetmete-susteem-iske.html. [Accessed 3 December 2020].

[2] Harward Law School Forum on Corporate Governance, “What Companies are Disclosing About Cybersecurity Risk and Oversight,” 2020. [Online]. Available: https://corpgov.law.harvard.edu/2020/08/25/what-companies-are-disclosing-about-cybersecurity-risk-and-oversight/. [Accessed 3 December 2020].

[3] University of San Diego, “Top Cybersecurity Threats in 2020,” 2020. [Online]. Available: https://onlinedegrees.sandiego.edu/top-cyber-security-threats/. [Accessed 3 December 2020].

[4] Northwestern University, “Use Best Practices to Design Data Center Facilities,” 22 April 2005. [Online]. Available: https://www.it.northwestern.edu/bin/docs/DesignBestPractices_127434.pdf. [Accessed 3 December 2020].

[5] Riigi infosüsteemi amet, “Implementation manual for the THREE-LEVEL BASELINE SECURITY SYSTEM ISKE,” 2017. [Online]. Available: https://www.ria.ee/sites/default/files/content-editors/ISKE/iske-implementation-manual.pdf [Accessed 3 December 2020].

[6] ISO, “ISO/IEC 27001 INFORMATION SECURITY MANAGEMENT,” 2019. [Online]. Available: https://www.iso.org/isoiec-27001-information-security.html [Accessed 3 December 2020].

[7] UK Cabinet Office, “Open Standards Principles – for software interoperability, data, and document formats in government IT specifications,” 2012. [online] Available at: http://ofti.org/wp-content/uploads/2012/12/46907_Open-Standards-Principles-FINAL.pdf [Accessed 3 December 2020].

[8] IBM, “The top ten security articles you need to read,” 2017. [online] Available at: https://www.ibm.com/developerworks/library/se-top-security-articles-you-need-read/index.html [Accessed 3 December 2020].

[9] Microsoft, “Security Blog,” 2020. [Online]. Available: https://www.microsoft.com/security/blog/ [Accessed 3 December 2020].

[10] David L Berger, "Industrial Security 2nd Edition ", August 4, 2011 [Book]

[11] Eric D. Knapp, Joel Thomas Langill, "Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems 2nd Edition ", December 29, 2014 [Book]

[12] Pascal Ackerman, "Industrial Cybersecurity: Efficiently secure critical infrastructure systems, October 18, 2017 [Book]

[13] John M. White, "Security Risk Assessment: Managing Physical and Operational Security 1st Edition ", August 6, 2014. [Book]

[14] Gov.uk, “Cyber Security Breaches Survey 2019,” 2019. [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/875799/Cyber_Security_Breaches_Survey_2019_-_Main_Report_-_revised.pdf [Accessed 3 December 2020].

[15] National Cyber Security Centre, “Most hacked passwords revealed as UK cyber survey exposes gaps in online security,” 2019. [Online]. Available: https://www.ncsc.gov.uk/news/most-hacked-passwords-revealed-as-uk-cyber-survey-exposes-gaps-in-online-security [Accessed 3 December 2020].

[16] Kaspersky Daily, “The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within,” 2017. [Online]. Available: https://github.com/aerokube/ggr. [Accessed 3 December 2020].

[17] ISC, “Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens,” 2019. [Online]. Available: https://www.isc2.org/-/media/ISC2/Research/2018-ISC2-Cybersecurity-Workforce-

Study.ashx?la=en&hash=4E09681D0FB51698D9BA6BF13EEABFA48BD17DB0\h [Accessed 3 December 2020].

[18] Intersoft Consulting, “GENERAL DATA PROTECTION REGULATION (GDPR),” 2020. [Online]. Available: https://gdpr-info.eu/. [Accessed 3 December 2020].

[19] Riigi infosüsteemi amet, “The 2020 yearbook of the INFORMATION SYSTEM AUTHORITY,” 2020. [Online]. Available: https://www.ria.ee/sites/default/files/content-editors/ria_aastaraamat_2020_48lk_eng.pdf [Accessed 3 December 2020].

[20] CNBC, “This crime in the workplace is costing US businesses $50 billion a year,’’ 2017. [Online]. Available: https://www.cnbc.com/2017/09/12/workplace-crime-costs-us-businesses-50-billion-a-year.html [Accessed 3 December 2020].

[21] Riigi infosüsteemi amet, “The 2020 yearbook of the INFORMATION SYSTEM AUTHORITY,” 2020. [Online]. Available: https://www.ria.ee/sites/default/files/content-editors/ria_aastaraamat_2020_48lk_eng.pdf [Accessed 3 December 2020].

[22] Computerweekly.com, “Security Think Tank: Communication is key to cyber security in digital era,” 2016. [Online]. Available: https://www.computerweekly.com/opinion/Security-Think-Tank-Communication-is-key-to-cyber-security-in-digital-era [Accessed 3 December 2020].

[23] DATAINSIDER, “Data Breach Experts Share The Most Important Next Step You Should Take After A Data Breach in 2019 & Beyond,” 2020. [Online]. Available: https://digitalguardian.com/blog/data-breach-experts-share-most-important-next-step-you-should-take-after-data-breach-2014-2015 [Accessed 3 December 2020].

Appendix

Non-exclusive licence for reproduction and publication of a graduation[1]

I Henry Orlov, grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis Analysis of the Estonian Automation Company for Breaches in Physical Security.

Supervised by Mohammad Tariq Meeran,

1.1 to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;

1.2 to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.

2. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

3. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.

06.01.2021