LAUREA
AMMATTIKORKEAKOULU
Yhdessä enemmän

Business Continuity and Preparedness in a Contact Center

Case: Company X

Sanna Niemi

Laurea-ammattikorkeakoulu

Business Continuity and Preparedness in a Contact Center
Case: Company X

Sanna Niemi
Degree Programme in Security Management
Bachelor´s Thesis
January 2019

Laurea University of applied sciences **Tiivistelmä**
Degree Programme in Security Management
Bachelor of Business Administration (BBA)

Sanna Niemi

Yrityksen jatkuvuus ja varautuminen palvelukeskuksessa. Tapaustutkimus: Yritys X

Vuosi 2019 Sivumäärä 27

Tämän opinnäytetyön tarkoitus on tarkastella riskienhallinnan ja jatkuvuussuunnittelun taustalla olevia tekijöitä ja hyödyntää toimivia käytäntöjä palvelukeskusympäristössä. Työ on laadittu selvityksenä Yritys X:ää varten, ja sen aiheet nousevat yrityksen palvelukeskusyksikön kohtaamista yritysturvallisuuden haasteista ja vaatimuksista. Selvityksessä tarkastellaan työntekijöiden ja työnjohdon toimintaa.

Työn tärkeimpänä tavoitteena on havainnoida yrityksen ulkoisille ja sisäisille vaaroille altistavia riskejä, ja niiden perusteella turvata toiminnan jatkuvuus mahdollisilta keskeytyksiltä. Yrityksen tarkoituksena on varautua erilaisiin häiriötilanteisiin ja luoda palautumissuunnitelma, jotta toipuminen mahdollisista kriisitilanteista olisi sujuvaa. Työn toisena tavoitteena on ohjeistaa työntekijät toimimaan itsenäisesti keskeytystilanteissa ympäri vuorokauden (24/7).

Tutkimusmenetelminä käytettiin teemahaastattelua ja kyselyitä. Teemahaastatteluun osallistui viisi työnjohtajaa ja esimiestä, ja heiltä kysyttiin jatkuvuudenhallintaan, varautumiseen ja yritysturvallisuuteen liittyviä asioita. Toisena menetelmänä käytettiin kyselyä, johon vastasi 18 henkilöstön edustajaa. Kyselyssä pyrittiin selvittämään, kuinka työntekijät selviytyvät nykyisillä työohjeilla ja kuinka he osaavat toimia erilaisissa poikkeustilanteissa. Tutkimusmenetelmien tavoitteena oli kerätä aineistoa yrityksen eri toimijoiden näkökulmista.

Selvityksen tulokset osoittavat, että työnjohtajien ja esimiesten sekä henkilöstön vastaukset ovat yhteneviä. Tuloslöydökset ovat osittain puuttuvia ohjeistuksia sekä toimintamallin uudelleen jäsentelyn tarvetta. Kehittämisehdotuksena on palvelukeskuksen prosessien dokumentointien päivittäminen. Kaikessa toiminnassa korostui tiedon jakaminen kollegoiden kesken, niin että toiminta ei nojaisi yksittäisiin avainhenkilöihin. Tarvittaessa dokumentointia apuna käyttäen voisi avainhenkilöitä sijaistaa myös muut henkilöt mahdollisimman sujuvasti.

Johtopäätöksenä voidaan todeta, että yrityksen ohjeistuksen yhtenäistäminen ja henkilöstön perehdytyksen yhdenmukaistaminen ja lisäkoulutus avainhenkilöille ovat tämän selvityksen mukaan tärkeimpiä kehittämiskohteita. Nykyisten prosessien dokumentointi ja sen hyödyntäminen on merkittävää sovellettaessa käyttöön uusia toimintatapoja tai aloittaessa uusia asiakkuuksia.

Asiasanat: Jatkuvuuden hallinta, jatkuvuussuunnittelu, varautuminen, yritysturvallisuus, palvelukeskus

Laurea University of Applied Sciences **Abstract**
Degree Programme in Security Management
Bachelor of Business Administration (BBA)

Sanna Niemi

Business Continuity and Preparedness in a Contact Center. Case: Company X

Year 2019 Pages 27

The purpose of this thesis is to examine the background factors of risk management and contingency planning and how it is managed in a contact center. The thesis is established for Company X and the topics for it have risen from the demands and challenges in the specific contact center unit. The material is collected as a case study for the company, it includes the views from the employees and the insights of the management team of the unit.

The goal of this study is to find and mitigate risks. And make plans to those risks and make the operations run smoothly without any interruptions. Additionally to give guidelines to the employees how to manage any interruptions whenever they might occur. Furthermore to prepare for the most common interferences and to make a recovery plan to recover any possible crisis.

The data collecting methods included theme interviews and questionnaires from the employees. The aim was to get different perspectives from all kinds of employees as well as the views of the management.

The findings were missing guidelines and a need to re-organize operating model. The documentation of processes have been re-written from the beginning to bring the documentation up to date. The sharing of knowledge was emphasized between colleagues so that the operations would not rely on a key person. In case of an absent key person the colleagues would be more able to substitute his or her work duties as fluently as possible.

The final conclusions consist of standardizing the guidelines and unifying the introduction process of a new employee. In addition provides the needed training for different level key persons. The documentation of current processes also helps tremendously when adapting the services according to the wishes of a new customer and when adapting new operating models.

Keywords: Continuity management, continuity plan, preparedness, corporate security, contact center

Contents

1 Introduction

I used the publication from the ministry of finance translated freely as ”Watch 2, continuity management”, as a baseline for this project. It offers good recommendations, operating models and tools to support continuity management in governmental level, as in other similar organizations. In addition to the guidelines it provides a tool for example Business Impact Analysis (BIA-tool) which can be used to determine critical services, and how to secure the services from interruptions. Vahti 2 (Watch 2) has been written by a division that operates in the governmental level under the IT and the cyber security management board.

The main principles in Vahti 2 are to preempt interruptions and to prepare for interruptions. Its aim is to adapt continuity management as a part of ongoing operations alongside preparedness. Vahti 2 and the guidelines it instructs, can be added to a part of the risk mapping processes. By investing on continuity management, it gives tools to secure the continuity of the services and to recover from occasions of interruption. The main goal is that core processes are planned to run as smoothly as possible without any disturbances.

As it is stated in the document; "The goal is to create a documented system for continuity management that helps to predict any possible threats that might compromise the continuity and to minimize the possibility of interruptions, to prepare for repair them and how to recover from the interruptions.” (Vahti 2, 2016)

Any quotes used in this thesis that are from Vahti 2, are freely translated as it exists only written in Finnish and Swedish language.

2 The Thesis Framework

The project was established from the demands and wishes of this Call Center unit, some concerns have risen up about the lack of guidelines in the interruption scenes and the preparedness of the employees to act on those occasions.

Thus the next step was to figure out the research questions and how to do the research itself. The questions are introduced in the following chapter and the research method was chosen after a consideration what would be the best ways to map out the challenges in the area of continuity management in this particular work environment.

After the research methods comes the theoretical part and how it applies on this case company X. Material from the interviews and the questionnaire follows the theory part.

Additionally the research is followed by the findings, that are introduced including challenges and the final recommendations to improve the situation with the continuity management in case company x.

The research questions

- Is the Call Center unit prepared for the scenes of interruption ?
- Does the personnel know how to operate in case of the interruptions and does it work 24/7 ?

2.1 Research Methods and Conduction

Thesis project consists both qualitative and quantative methods in the process of the research. The main purpose of the research was to gather background info of the current situation and focus on the main challenges.

Quantative research used a survey, since the purpose of the survey is to point out some major findings by statistics. However this method alone would not sufficient if the volume of the survey is not wide enough the accuracy of the statistics is compromised. And since the survey was gathered in this specific unit only they survey covers only a small area of the study. The raised issues appear in many work environments thus it was necessary to look for basic information about risk management, security management and other related topics from literary sources.

Qualitative research became part of the study project when some insights, opinions and reasoning were needed of the field. Interviewees were chosen based on their background information such as former work history and the field of work. They also had a comprehensive overall view of this company and from this unit that was investigated for the study.

During the survey the questions were mostly structured but in the interviews a semi-structured approach worked more fluently as it did not limit the conversation in the way as structured questions would do. More or less the interviews reached a good level of communication and some developmental issues came up more fluently using this method.

A short introduction to the company and the contact center unit

The case company is a large international actor that operates globally in most of the countries. It is originated in Europe, which means that the standards are thoroughly well thought than in those corners of the world that do not operate so strictly in collaboration with the establishing country aka the mother company. Thus they are a daughter company in Finland which mostly runs on its own but it is supported by the original founders company. In practice this means that most of the guidelines in general come from another country. However some minor decisions are mostly left to the units themselves. The company employs thousands of people in Finland. The introduction process is supported with general materials and forms, but the guidelines about the work itself comes from the unit where the employee will be hired. The call center unit operates 24 hours a day, 7 days a week and 365 days in a year and

thus it is crucial that everyone goes through the same training so that all the employees know how to operate at any time or any situation.

The open office holds a work place for about 30 people. There are approximately 20 to 25 people working daily, mostly during the day and a couple of people during evenings and nights as well.

At the moment there are no strict laws or decrees that guide or create demands for call center units, each organization creates their own set of values, rules, and guidelines how to operate a 24/7 environment. When comparing the situation for example to alarm centers in private security companies the reality is a lot different. They operate strictly under certifications and standards. The work is very similar but the main differences are, that on security side, the security guards work in these 24/7 units. In the facility/multiservice side the employees are simply customer servants without any licenses or other complications. Only the Finnish labor law defines the starting and ending times for work shifts alongside collective labor agreement.

Inside the call center and as a part of the services operates the Helpdesk team, it consists of the same employees as the call center employees. However, the main difference is that the services are tailored according to the wishes of the customer. Often the customer is a large company who wants to outsource some of their back office services cost-effectively. Thus Helpdesk should operate as it was part of the Customer´s Company and using the tools and operating models that the customer applies. This increases the stakeholder palette in the company, since the stakeholders might grow up to customer´s customers.

2.2 Contact Center

> "Call Centers are organizations or departments that are specifically dedicated to contacting clients and customers. These can be either a helpdesk, or client service department of an organization, but companies may also have outsourced this to a Call Center company, which handles all client contacts for a variety of organizations. One important distinction is therefore between internal and external Call Centers." (Norman, 2005)

In this thesis the Call Center environment has evolved to a Contact Center during the years. This means that the clients contact the center in other methods beside phone calls as well.

> "A Contact center is a business where the employees mainly handle incoming and/or outgoing phone calls. Typical services with outgoing calls are advertising campaigns, market research and selling by telephone. Examples of activities with incoming calls are customer services, giving information, taking orders and providing helpdesk functions." (Norman, 2005)

In this case, the main focus is especially on incoming calls and taking orders such as service requests. Additionally the facility alarms have become a vast part of the services, so forwarding alarms is a major work assignment in the contact center of this case.

3 Terms and Definitions

In this third chapter, I will introduce theory and terms behind this study that play major role in understanding the background, terms, and definitions that are crucial in this subject. First, the operating environment, a contact center and then business continuity management and some related crucial parts of it. Shortly, some abbrevations are also introduced as they are a part of business continuity management and essential in this study.

3.1 Business Continuity Management

> "The process of developing and maintaining a complete business continuity plan which will ensure the continuity of the business when disruptions occur. BCM covers plan development based on the business impact analysis, the exercising of the plan and the regular updating of the plan to reflect new threats, risks and business circumstances" (Hotchkiss, 2010)

The purpose of continuity planning is to establish actions, which would help to mitigate and shorten the amount and effect of disruptions that harm the normal operations. It consists of spare plans and procedures that minimize the effects of harmful disruptions and it helps the recovery process on those situations. These plans also include operations with details about leaderships, responsibilities and actions so that operations may continue in case of an interruption.

The contingency plan should address all the possible risks and give recommendations how to mitigate them, and if a crisis occurs how to recover from it and return to business as usual.

In risk assessments, it is crucial to recognize and determine any possible disruptions that the operations may face, especially those that are targeted to critical operations of the service center.

> ”Continuity management is based on work orders, job descriptions and the annual clocks procedures. It must be organized as a part of normal operations so that the management responsibility and operating models stay the same in interruption scenes and in abnormal conditions. The top management of the organization accepts and prioritizes the procedures in continuity management in cases if interruptions based on the plans and guidelines of the key personnel in charge of the operations.” (Vahti 2, 2016)

Continuity management is more than a continuity plan, because plans and updating them are easily forgotten. Management consists of the whole process where continuity becomes part of daily routines and monthly meetings and it pushes the employees in charge of the plans to check and update those regularly.

Assets

Depending on the line of business the assets vary between companies and businesses. In most companies however two of the main assets are the personnel of the company and information. Without those two assets, the company would not be able to operate at all.

Nowadays it´s common to protect company's reputation, since it is a critical asset on modern times. Since social media gained its position as a part of rapid media, it is crucial to safeguard the company´s good name. It may be harmful if the trust of the clients is lost, it may even destroy the company, and all its operations.

Prioritizing

An organization has to determine the lowest level of service in order to recognize what is the point when the service is not anymore useful to the clients using the service. Most crucial functions need to be given a standard procedures and solutions that can mitigate the effects of the disruption. When these points and levels have been determined, they create a base for a recovery plan that supports in the process of recovery of the services and to restore the desired service level.

Business Impact Analysis (BIA) is a tool to investigate continuity management and determinating the critical levels secures the successfulness of it.

> "This is the process of determining which areas of the business have potential losses requiring mitigation and what controls are needed. Controls can reduce or occasionally eliminate risk and loss. Controls cost money and, in a BIA, the objective is also to balance the cost of these with risk appetite." (Hotchkiss, 2010)

When categorizing software's few things should be considered such as determining how the disruption effects work duties on the field. Are there any systems or software's that can be used as a plan b ? How long will the operations work without the systems and with the help of spare systems ? How to solve the situation while returning to the standard operations ?

Vahti 2, 2016 defines a few tool tips for prioritizing in continuity management:

- Determine software's and systems by their level of criticality.

- Make a running order between the systems.
- Do not over or underestimate the levels.
- If the system is not critical but somehow important, a reaction claim is sufficient. If the system is critical or very important, it should be addressed with a solution time claim.
- Define Recovery Time Objective (RTO) and Recovery Point Objective (RPO)
- Optimize the costs, too strict estimates can lead to higher cost

Business Impact Analysis (BIA)

> "The purpose of BIA is to determine and to document the effect of different hazards to the business process. BIA can be used to evaluate risks that threat business processes. And to determine dependencies between actions." (Vahti 2, 2016)

The research for BIA is done by interviewing the people in charge of the operations and going through the documentation. The data of the operations is crucial for the BIA. When the operation environment, protected assets, and their core processes and functions are known, they can be categorized into priority classes according to the gathered information. The main goal of BIA is to map all the possible effects of risks to operations and functionalities. Based on Business Impact Analysis it is possible to choose the necessary procedures to maintain continuity and recovery actions that are needed.

Recovery Time Objective (RTO)

> According to Al-Hour (2012):"The RTO is the time objective or goal for restoring the processes/activities. RTO defines what is the needed time in seconds, minutes, and hours or days that the operations should be recovered in case of disruption". (Vahti 2, 2016)

RTO gives framework to identifying the magnitude of disruption scenes and creates guidelines in starting to the process towards recovery.

Recovery Point Objective (RPO)

> "RPO means recover point objective, which is a desired point for recovery. It defines the point to where all operations, data or software's should be restored after the interruption. Recovery point is not necessary the same thing as the starting point of a serious interruption in which the operators need to prepare with multiple arrangements." (Vahti 2, 2016)

3.2 Interruption and Disruption

> ”A disruption scene or disruption means in normal conditions a major interruption or serious disruption that can lead to a cease of operations or a major downtime in operation. Disruption does not mean a small interruption or error detection. Usually in service production the international term is Major Incident Management (MIM).”(Vahti 2, 2016)

A mild interruption might happen daily for example in internet-based software's, for example there might be an interruption that lasts a couple of minutes, and then recovers fast from the scene of error. However, MIM is the opposite of a small error, can be defined major interruptions that may shut down the operations for hours or longer. It acquires a well-structured recovery plan, and the knowledge of all the needed steps, and the will to re-act to major incidents as fast as possible.

How to prepare for interruptions and plan continuity so that it supports the business operations? Once the analyzes are done about the current status, the company is able to determine what are the most critical operations and assets to be protected, and how much to invest time in creating a preparedness plan for protecting assets.

The plan for recovery is a crucial part of the continuity plan, without it is only a data about the operations, assets and the risk. Recovery plan gives tools to pull the operations back up in case of interruptions. Time is essential in recovery, depending on the business seconds, minutes and hours may be very costly if immediate actions are not taken towards recovery.

Maximum tolerable outage (MTO)

> "How long things can fail to work before it comes an issue. This is often subjective and a lot of stakeholders will say the maximum is minutes whereas the client might actually tolerate hours. The process of judging this is based upon experience." (Hotchkiss, 2010)

The organization and the environment of operations

> ”An organization must document the operations, services, procedures and the data- and software systems. Dependencies between them should be documented and include as a baseline of the documentation. Continuity management should support the main goals and operations of the organization.” (Vahti 2, 2016)

Preparedness

> "One of the insights derived from the political-economy approach to disasters is that preparedness and response are linked to the development process and related to larger issues of sustainability." (Tierney K, 2001)

4 Risk Management

> "The art of Risk Management is to identify risks specific to an organization and to respond to them in an appropriate way. Risk Management is a formal process that enables the identification, assessment, planning and management of risks." (Merna, Al-Thani, 2008)

Risk management gathers all the possible risks together, categorizes those and divides them into smaller groups based on the likelihood of the risk, and the severity of the consequences from that risk.

Risks are always present in life and work, the word risk itself describes the potential loss or unwanted results that may appear. In businesses, the term is usually linked to the possibility of potential financial losses to the company. The risk can damage for example the building of the company or the company´s reputation. It is something that is not desired unfortunately it is inevitable part of business. Risks and hazards are not the same thing, hazards are all around us, and the fact that it becomes a risk is simply the fact when it can harm the company or its assets. To summarize, risks can be divided into two groups: those that might affect people or those that threaten the material assets. Additionally some events can threaten both of these groups.

In our daily lives we usually tackle risks by our past experiences and knowledge. In corporate field it is not enough, and more effort is needed. Risk management must be based on planning and preparedness instead of fortune.

4.1 Risk Types

> ”Usually all risks threatening the continuity of operations can be organized under these main groups. By preparing for these scenarios recovery can be done in most interruption scenes” (Vahti 2, 2016). Vahti 2 categorizes risk types as following groups (not in any particular order):

1. The facilities of the organization or most part of the facilities are not usable (power shortages, accidents, natural disasters, terrorism, the use of military forces)

2. The personnel of an organization or some of them, top management of key persons are not available (power shortages, accidents, natural disasters, terrorism, the use of

military forces, major interruptions in logistics, major interruptions in distribution of groceries, the disruption in health and well-being of citizens, major accidents.)

3. Data sources, IT-software or serious interruptions in communication systems (power shortages, accidents, natural disasters, terrorism, the use of military forces, cyber threats, systems or software failures, major accidents.)

4. A major service provider is not usable (power shortages, accidents, natural disasters, terrorism, the use of military forces, disruption in the monetary system)

Risk can be divided into categories based on the amount of damaged caused or by the likelihood of the risk occurring.The feeling of safety can be affected by potential risks. If the risks are unlikely, or they do not oppose a threat to anything of value, it does not affect the feeling of safety.

4.2 Risk Analysis

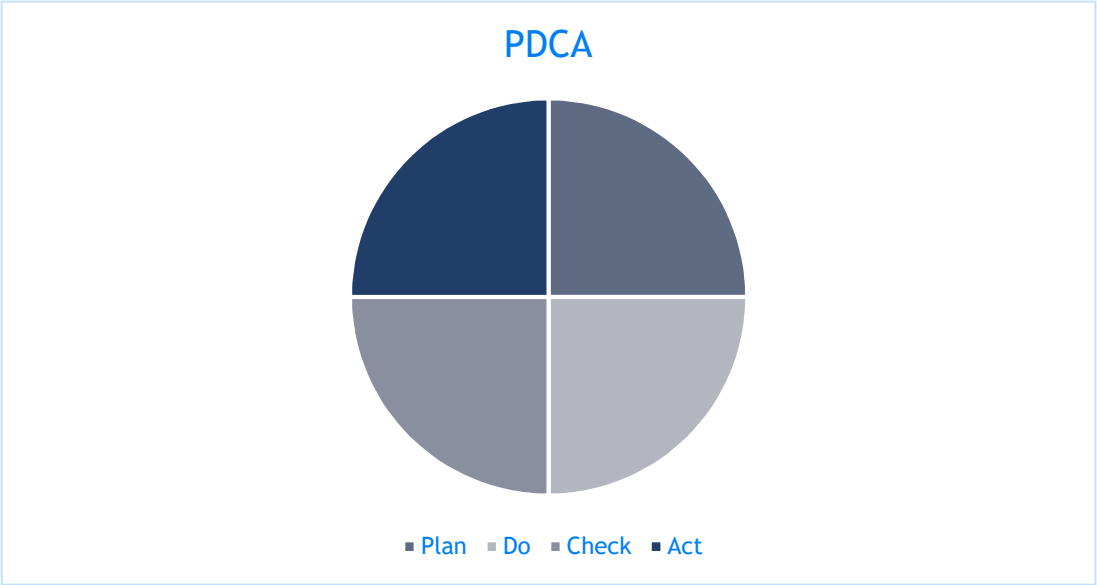
> "Risk Quantification and Analysis involves evaluating risks and risk interactions to assess the range of possible outcomes. It is primarily concerned with determining which risk events warrant a response." (Merna, Al-Thani, 2008)

At first, it is important to identify all the assets that are worth saving, in other words, what parts need to be protected from threats, hazards and all kinds of risks. Next step is to investigate the probability of each of those risks. The analysis altogether is only an estimation, however it gives guidelines to make a risk mitigation plan.

In risk analysis it should be taken into consideration of the work environment and the risks that it may cause. Especially 24/7 operating call center is more prone to have tired employees because of the diverse rhythm during the nightshifts. When we compare the work environment to a general office work (where people work circa 8-16) the risks increase. Shiftwork affects the health of the employees and the health issues must be examined before starting this type of work.

4.3 Plan, Do, Check, Act

PDCA also known as the Deming cycle is an illustrated model of a process when implementing new parts to operations and how to follow its process and development into the entity. Demingin cycle - PDCA (Dale 2003, 145; Lecklin 2006, 49)



Risk evaluation process and choosing the right mitigation tools

> "The process of comparing actual risk levels with previously established risk criteria. As a result of this comparison, risks can be prioritized for further action." (Graham, J et al, 2006)

Risk evaluation maps all the possible risk and then divides those into smaller groups based on the likelihood or the severity of the consequences from that risk. It is also critical to determine what risks are the most crucial to the operations.

Vulnerabilities can be a small issue that weakens the security and safety overall if they occur simultaneously. It can be also a major thing that might shut down the operations for a longer period.

In a facility it is important to manage the people flow (people flow is the coming and going of people) is access control and the presence of a security guard in a lobby. Also the building itself and the perimeters create a safe or unsafe work environment, based on the acquired preparedness level in the facility.

5 Security and Crisis Management

The following chapter consists of key elements in security management such as fire safety risks, information security, safety in a facility and safety culture. Chapter 8 Case Study presents how these elements function in the case company.

Security management consists of different aspects of safety and security. It has to take care of the safety issues related to fire, rescue, and work. Thus the security and safety of a facility. Security management aims to view the whole picture of business operations to evaluate and to manage risks and threats accordingly.

5.1 Fire Safety Risks

Fire only needs some burning material, enough heat and oxygen to start going, hence when these three components are at the same place they create a risk of fire. It all starts with the considering of the materials. Any excess material stored on a wrong place or excessive amounts of material in general, will be the first thing to be considered while taking fire risks into control. The materials that are easily flammable should be stored separately from the source of fire. Facilities should also be planned in a manner that is possible to prevent fire from spreading to the whole facility.

Approximately half of fires are caused in some ways by the actions of humans, it may be an accident or an arson. The second most common reason for fires are equipment malfunctions in fires that happen inside of a building.

5.2 Information Security

> "Cyber threat means a possibility to an act that effects the cyber environment and by doing so jeopardizes an operation that depends on the cyber environment. Threats towards cyber environment are Information security threats that jeopardize the information security system functions in its original purpose." (Vahti 2, 2016)

Cyber threats are now part of our digitalized society. It is common that websites are sometimes out of use because of attacks. Even banks have gotten familiar with these attacks lately, so it is a major issue that needs to be taken into consideration and included into the risk management processes. Since the business relies on various softwares, they may be vulnerable to these kind of attacks.

Information Technology

> "IT provides services for operations, processes and according to the demands by services, and is in charge of documentation and testing of the technical procedures that support continuity management and recovery plans. The role of IT department is to lead and to follow the demands made for the service providers, and to supervise the quality of the technical implementation." (Vahti 2, 2016)

The role of IT can be divided into pieces according to the softwares, because this is the hands-on part that the employees, and the unit sees the part of IT and what it does. IT supports the softwares, but in many cases the reinforcement is outsourced, and challenges and interruptions can not be solved internally in the company.

Safety in a facility

The owner of a facility (e.g. an office building) has obligation to protect the facility from outside threats. The aim is to secure the building so that those working inside it are not at any risk that may arise from the working environment itself. Basically, this means that the facility must be maintained and cared in a manner that everything is working as it should be. Common dangers in a facility are for example slippery (ice, snow) yards, and roads that lead to the premises. Thus, windows and doors must be repaired if there are any damages to those.

A facility can be protected with structional safeguards, such as walls, fences or a gate around the property. Furthermore, a good addition to that is alarm control systems for intruders. Alarm systems can consists of CCTV also known as video surveillance, alarm sensor on doors and windows, access control.

5.3 Safety Culture

> "The Safety Culture Pyramid simply asserts that values, strategies, climate and behavior are linked." (Sabin et al, 2012)

Figure 1.1 The Safety Culture Pyramid

> "Simply stated, safety culture is about 'why we do what we do'."(Sabin et al, 2012)

Safety culture consist not only what the personnel does but also how they operate. You can either do things automatically without paying any attention or you can do things while giving a thought to what and how it affects the daily duties. By giving time and attention to the personnel creates more commitment and motivation. Since the employees can affect in safety issues with their own actions.

Safety as a part of organizational culture

Safety in organizational culture is created during the introduction process, when a new employee is familiarized with the company and its operating models, values and safety issues. During the first days, the employee creates his/her vision about how colleagues react to safety, for example do they wear id-tags and is the attitude serious towards the safety issues. Alongside id-tags and access cards, the access control also tells about the attitude towards safety in a facility: are doors locked, are access cards restricted to a certain area, these for example are the factors that tell about the attitude towards safety. If anybody can walk through the facility in any time of the day with/without the access card, it shows the lack of understanding and caring towards safety.

Auditions also express about the level of commitment to safety issues. If no one independent outside the organization ever measures and audits the safety issues it shows a lack of commitment towards the safety.

The obligations for an employer and an employee

An employer has an obligation to take care of the risks and hazards that may occur at a workplace and to make a plan to mitigate the risks and secure the work environment. An employer has to investigate the most common hazardous situations and how to prevent those from occurring. It is also required for the employer to follow the work safety issues on the business field, for any upgrades and news that might affect the company. These obligations do not apply to conditions that could not be predicted or managed with the safety and security measures applied to the company. If the research of risks and hazards are done in an inadequate way, it does not exonerate the employer from their obligations.

Updating crisis plan regularly is imperative and it requires testing to prove that it works in a real life scenario. Focusing on crisis communication is one method to protect the stakeholders. Training and simulations help the employees to fill their roles according to the plan. The training reveals if there are any weaknesses in the plan. It should be written so that anyone can refresh a memory by going through the plan annually or whenever needed. As in work life in crisis too, the employers are the key resource in making things happen. If the employees of the company are not fully adapted to the process everything will seize to work in case of a crisis. It is important not to complicate the message, it should be short and straightforward so that there will be no room for misinterpretation.

5.4 Crisis Communication

A company should always have a crisis communication plan. When the crisis has emerged, it is already too late to start on building the plan. The number of internet users is growing all the time, internet has taken news into an advanced level, and because of the fast speed it can

spread any information. There is also more room for errors, the news and articles can be written by anyone, which means it may not be that professional type of writing always and not bidden by journalist ethics either. A rapid response is critical while operating with social media on internet. It requires some preparation in advance to not sound unprofessional.

Choosing a spokesperson for the company is the next important step. Thus, training of him/her how to answer to any kind of questions by the media is crucial. Additionally he/she has to be assuring and giving out the right kind of information.

6 Case Study: Company X

This chapter introduces the case study and the security issues and features related to the Contact Center environment in general. After the environment related issues it concentrates on the recovery process, thus the last chapter describes more on the findings, challenges and the conclusion with recommendations.

Risk analysis is a part of the risk management, in other words to investigate and define what are the most severe risk and the ones that occur most likely.

Technical interruptions

Major threat to the operations in a call center is when a system or a software is in error mode. Furthermore the loss of electricity or Internet will cause severe problems in a very short time.

Uninterrupted Power Supply (UPS)

> Equipment that offers short-term protection against power surges and failures. UPS typically allows enough power for critical systems to be powered down plus a degree of supply to emergency lighting, and for transition to a long-term back-up power supply such as a generator if available." (Graham et al, 2006)

The Key personnel

When most of the processes rely on the key personnel, the employees have no other means to find solutions than going through guidelines. If some guidelines are missing, the whole process might depend on a key person.

The Human resources

The human resources can be either a good or a bad influence in a company. It is a crucial element in keeping the operations running, however it can be a risk that can ultimately tore the operations down. For example, an employee may cause significant harm to the company.

Nonetheless, it can be intended or an accident, the outcomes can affect operations remarkably.

The Equipment and facilities

A call center is located in a facility that is built to support the services with equipments, softwares, as well as the facility itself. If the premises are compromised somehow the operations are forced to evacuate into another spare facility. In cost-wise it is not relevant to supply two spaces similar way, since the chances of needing the spare space is quite minimum. For example, during the last six years or so there has only been one incident that has led to evacuation, and even then the operations were re-build within the same day to its original location. Thus the unit has responded to the demand by procuring laptops and mobiles as a back-up system, which allows the operations to move quite easily to another space if needed.

The recovery plan for company x

A recovery plan is always required for the critical operations and softwares, such as telephones. The current software for telephone line has been added with a back-up system in mobile phones according the telephone line groups. Since there were lines between 50-100, these had to be divided in three main groups in order to make the telephone calls run smoothly during any technical interruptions on the telephone software.

Internet connections are one major aspect in the unit, since almost all the softwares need access to internet. For a short period of time, a backup “excel” can be used, but for interruptions that could last for hours, a steadier system was essential to develop to support the main work besides phone calls. Fortunately, one of the new systems (a form) provide aid in this situation, although it was created to shorten the answer times of a call center.

7 Qualitative Research Conduction and Results

Interview consisted of three different roles in the organization: team leader, service supervisor and specialist. They all have slightly different area of responsibility, so each of them analyzed the issues in question from their own perspective, and thought about how it affects their team.

7.1 Theme Interviews

In this chapter, Team Leaders interview results are presented. One team relied on a key person in some duties but they also had a good knowledge about guidelines and the common knowledge how to operate in case of some interruptions. They got inspiration from this interview, and realized there is a real need to update the guidelines for the introduction process. The guidelines did not have any mention about interruptions although the team leader thought that their common knowledge and operation models work in those circumstances.

Prioritizing duties is not part of the guidelines, so that could be implemented as well, so it would not vary depending on the person on duty, and they would have more common understanding about how to prioritize. Some duties are only in the hands of one key person, but since they are not critical issues, it generally would not cause a problem. However, perhaps improving the sharing of information could be done just in case. Mostly the team was in progress of updating the guidelines, and making documentation about their duties and processes.

In this chapter, The Service Supervisor interview results are presented. He or she is in charge of a larger team in the unit. Although the documentation process had started well, plans were needed for disconnection in the Internet connections or electricity shortage situations. Protecting the guideline data from any breach through internet The Service Supervisor thought that a non-internet using lap-top might be one option for storing the valuable data. It would make the data accessible in the facility, even during disconnections with the Internet connection.

One new feature, a form was also recently introduced to the daily operations that would simplify things in case of some disruptions. It helps to customer servants to write down the service requests by using a minimum amount of softwares while taking in phone calls.

A question about other possible defects was asked and he replied: “Collaboration between Maintenance operations on the field and customer service center should help with this. So mostly what we are missing are the guidelines from the operative field, where the janitors and cleaners work. This is a problem in a big company, not everyone know what other people do, but they assume others know what they do. And thus do not understand the need for the detailed guidelines.”

In this chapter, the Specialist interview results are presented. Checklists are created to guide the work, and in case of acute interruption most people rely on the Service Supervisor. The back office-team receives inquiries about what to do with problems related to the new systems. In general there are good guidelines, but the Specialist is not aware of all instructions, because they are not part of his/hers daily duties. Usually in case of system failures and interruptions people tend to shout it in the open office so that the specialist can hear it and react to it as well if needed.

Documentation is in progress, but the back-up systems have a few issues that could be developed further such as hands-free-system for the back-up phones. Additionally the employees hoped for the possibility to read the facility’s rescue plan electronically, and to have a safety walk in the premises.

A few additions from the specialist came at the end of the interview: “We have started the unifying of guidelines, so that each Helpdesk has their own “What to do in case of system failure etc.” section, which tells who to contact when a system fails. So it removes the need for a key person or the operating management to be present. Most of these interruptions are short, but it is crucial that the personnel know where to report if something ceases to work, because often, it might shorten the time of repair as well.”

In this chapter the Service Managers interview results are presented. The guidelines are needed in the case of system breakdown, and also an update for the evacuation plan is required. All current acquisitions have been made keeping in mind the evacuation process, this means that the computers are laptops. The most needed tools are available even in an evacuation situation, if the facility becomes unsafe for some reason.

One vital step is to determine the wishes of the unit concerning the recovery time objectives of systems and softwares. A process has been iniated to prioritize the most critical services, and to count the needed personnel to run it. In addition documentation processes are running alongside it, since many guidelines are required to be documented in case of a missing key person for someone to run his/hers duties instead. This is one of the reasons why the process about the job description is essential as well. The replacement for SharePoint (which is used as a data archive for guidelines) is in progress.

7.2 A Questionnaire for the Employees on Security Culture and Guidelines

The questionnaire was created for the employees to fill out a form. It consists of questions about guidelines related to security and cases of interruptions. The answer percentage was approximately 50% but since there are a lot of employees that work part-time, it is valid to mention that the percentage among those that work full-time on the unit are closer to 80%.

Some of the questions were about an online course of safety and security provided by the company. The guidelines in the course do not react to the challenges of a specific unit but are merely general safety guidelines.

Many people were uninformed about the safety plan of the facility, simply because it is not readable on the SharePoint page where most of the other guidelines can be found. This means that the employee has to walk to the reception desk and read it there.

Additionally there were some misunderstandings where to find guidelines in case of interruptions.

The employees hoped to have first aid training, and training about safety and security issues in the unit.

8 Development Ideas and Conclusions

Many operations rely on a key person who has not shared the information about their exact work duties. The work descriptions have changed during the last five to ten years, and new titles and duties have emerged. Many tasks are handled by one single key person, so the colleagues may not have an idea about someone´s responsibilities.

Some guidelines have not been standardized enough or there may be some room for miss-interpretation. The documentation process is still ongoing.

In a large public company, information tends to move slowly within the company. Additionally some guidelines may not apply to each unit specifically, because they have been created as general advises and guidelines. This challenges the unit to make rules and instructions that work under the main rules of the company. The company is also a part of an international consortium therefore, they have to maintain some common grounds to the rules and guidelines as well.

Some people from the management team work on their own, thus sharing their knowledge is crucial whether it is done through documentation or through weekly or monthly meetings with other key persons from the unit.

As part of the process, we mapped out all the current projects relating to continuity management in the unit and defined the status of each project. During this investigation most of the documentation reached a start-up phase. There is a good course in continuing the process of documenting processes systematically. The work descriptions and these mentioned procedures will help anyone that has to replace suddenly a key person to learn the duties and processes of the unit.

Recommendations and turning points

One of the turning points was to standardize the SharePoint pages for each customer ship so that the data would be found in the same place, even if the clients were from a different company of different customer ship.

I recommend that the unit focuses on highlighting and standardizing the place for in case of emergency/interruption guidelines. Already it has helped the employees to find the critical info during interruptions and difficult situations.

The unit also lacks a plan about how all the data and guidelines are archived and handled. When the plan is compiled, it will help to lead the process in developing these detected issues.

The guidelines should be included about continuity and preparedness as a part of introduction process for a new employee. During monthly meetings, the renewed guidelines should be introduced to the personnel. The training and educating of those employees that help and support the new employees in the introduction process must not be forgotten either.

By continuing the documentation project, it will help in the future the new member of management team, whether they are Service Supervisors, Team Leader or Specialists. This will keep the whole unit better in charge of their current situation and of their to do-list for the future.

The continuity management must be kept as a part or monthly meetings because it maintains the topic current and viable for updates and corrections. It is important to gather feedback. It should be done as a continual project, since it brings up any potential missing guidelines and instructions. The feedback will give a good advice as to where the corrections must be made.

Standardizing the operation model in each clientele helps in keeping the information updated. The employees should be able to find the guidelines easily. Unifying the guidelines and the visual appearance of each information page improves the usability.

It is important to measure regularly the capabilities of the current staff and have discussions with the employees. This way the company can detect if there are any issues that should be handled. Forty pairs of eyes may notice more than one so potentially issues may rise up easily from that group.

The plan how to distribute duties evenly is vital and to make sure that there is a plan b for every operation and person b for every duty in case of absence. This alone helps to build up the continuity more since nothing relies solely on one person.

It is critical to pay attention to the documentation. In case of a more severe disruption, anybody that is assigned to the task should be able to continue the operations based on the documentation and guidelines only. This could include for example outsiders who have virtually no experience of the operations of that specific unit (same company, different unit for example).

References

Al Hour, A. 2012. Business continuity management. IT Governance Ltd.

Bernstein, J. 2011. Manager´s guide to crisis management. New York: McGraw-Hill.

Broder, J. & Tucker, E. 2012. Risk analysis and the security survey. USA: Butterworth-Heinemann.

Dale, B. 2003. Managing Quality 4th Edition. Blackwell Publishing.

Graham et al., 2006. A Risk Management Approach to Business Continuity: Aligning Business Continuity with Corporate Governance.

Halibozek, E. & Kovacich, G. 2017. The managers´s handbook for corporate security. USA: Butterworth-Heinemann.

Heinonen et al, 2013. Turvallisuustutkimuksen tekeminen. Helsinki: Tietosanoma Oy.

Hopkin, P. 2010. Fundamentals of Risk Management.Great Britain: Kogan page limited.

Hotchkiss, S. 2010. Business Continuity Management: In practice. British Informatics society limited.

Leppänen, J. 2006. Yritysturvallisuus käytännössä. Helsinki: Talentum Media Oy.

Merna, Tony, Al-Thani, Faisal F. 2008. Corporate Risk Management (2nd Edition). Wiley.

Norman, K. 2005. Linköping University, Sweden. Call Centre Work, 2005. Accessed 3/208. http://www.diva-portal.org/smash/get/diva2:20713/fulltext01

Payant, R. 2016. Emergency management for facility and property managers. New York: McGraw-Hill.

Sabin, E et al, 2012. Safety Culture. Ashgate Publishing.

Tierney, K. 2001. Facing the Unexpected: Disaster Preparedness and Response in the United States. Joseph Press.

Valtiovarainministeriö, 2016. Vahti 2. Accessed 3/2018. http://vm.fi/julkaisut/vahti

Watters, J. 2014. Disaster Recovery, Crisis Response, and Business Continuity: A Management Desk Reference. Apress.

Wong, W. & Shi Jianping, 2014. Business Continuity Management System: A Complete Guide to Implementing ISO 22301. Kogan Page.