Crisis Management Training Concept

A scenario based training concept for Fortum Corporation

16. Turvallisuusjohdon koulutusohjelma

Development project report

Jarkko Karonen

Fortum Corporation

29.5.2020

Aalto University Professional Development – Aalto PRO

Tiivistelmä

Kriisijohtaminen on moniulotteinen aihe, joka leikkaa läpi organisaation eri tasojen. Tässä työssä kriisijohtaminen nähdään ensisijaisesti kattokäsitteenä, joka pitää sisällään niin ensitoimet, kriisinjohtamisen, liiketoiminnan jatkuvuussuunnittelun, varautumisen, kuin myös toivuttamistoimenpiteetkin. Kriisin määritelmä vaihtelee organisaatiokohtaisesti.

Fortumissa kriisijohtaminen on ensisijaisesti osana linjaorganisaatioiden eli liiketoimintadivisioonien vastuita. Suunnittelua, varautumista ja harjoittelua tehdään organisaatioiden eri tasoilla, mutta sitä ohjataan konsernitason ohjeella. Harjoitusten skaala on aina yksittäisen kohteen poistumisharjoituksesta laajoihin useiden toimijoiden yhteistoimintaharjoituksiin.

Fortumin yritysturvallisuusyksiköllä on yhtiön kriisijohtamisessa selkeä rooli, joka pitää sisällään konserniohjeistusten ylläpidon ja kehittämisen, kriisinjohtamisen koordinoinnin ja kehittämisen konsernitasolla, kriisijohtamistilojen ylläpidon sekä harjoitusten fasilitoinnin tarvittaessa. Kriisitilanteessa yritysturvallisuusyksikkö on osana konsernitasoista kriisiryhmää.

Työn tavoitteena on tunnistaa mitä elementtejä kriisijohtamisen harjoitteluun Fortumissa liittyy ja miten harjoituksia voisi kehittää edelleen monistettavan paketin muotoon. Tämän paketin tai konseptin avulla yritysturvallisuusyksikkö voisi entistä tehokkaammin tarjota liiketoiminnalle tukea harjoitteluun ja jalkauttamiseen.

Abstract

Crisis Management itself is a topic which covers the whole organization in all levels. In this project crisis management is seen as an umbrella term that covers all the elements from rescue operations, crisis management, business continuity planning, preparedness and recovery planning also. The definition of a crisis typically varies between organizations.

In Fortum Corporation crisis management is primarily in the responsibilities of the line organization in business divisions. Planning, preparedness and trainings is done in group, division, business area and site levels. The scale for trainings varies from single site's evacuation training to complex multi stakeholder cooperation trainings.

Fortum Corporate Security Unit has a clear role in company crisis management. It includes managing and developing the group level crisis management instructions, crisis management facilities, coordinating and developing crisis management in the group level and support for facilitating trainings. In crisis situations the Corporate Security unit is a part of the Group Crisis Team.

Purpose of this project is to identify elements that should be part of crisis management trainings in Fortum and develop trainings further to a form of duplicatable package or concept. With this concept the Corporate Security Unit could better support business divisions in training and implementing crisis management.

Sisältö

1 Introduction

1.1 Background for the project

Crisis Management is an important issue for all kinds of companies but it has an especially crucial role in those companies that are providing critical services or infrastructure like electricity, heating, cooling, telecommunications, internet, water supply etc. For the companies of this field a possible crisis situation is typically very visible and has an immediate effect on both its stakeholders and customers. Company is put to an ultimate test when it faces a real crisis situation. Fortunately – organizations can be trained in order to be prepared in advance.

Recent examples especially from the Nordic region show that a crises can have a dramatic impact on companies. For example the shipping giant A.P. Møller-Maersk faced a cyber-attack during 2017 which in result basically paralyzed company's all operations worldwide and based on the estimates cost the company even up to around 300 million dollars (Greenberg 2018). In this case the crisis was from the very beginning obviously so visible for the whole world that the CEO of the company was very open about the crisis management and all related actions.

Since different kind of crisis can have devastating effects of companies performance it has become something that especially the stock listed companies are stating along with their financial status. For example in case of Fortum Corporation, the topic is covered in the sustainability report under the Corporate Security segment (Fortum Corporation 2020a, 54). Legal frameworks related to the topic differ depending on the country where the company is operating. It is worth mentioning that in some of those countries where Fortum operates, there has been increase in the amount regulation (Fortum Corporation 2020a, 54).

For the stock listed companies crisis management also has another angle – how markets are reacting to the performance in crisis situations. According to a study - a crisis offers a possibility for the company top management to show how well they can manage difficult situations (Knight & Petty 2001, 15). This is in relation with the company reputation and image also. As famous investor Warren Buffet has stated “It takes 20 years to build a reputation and five minutes to ruin it. If you think about that, you'll do things differently” (Berman 2014).

According to studies - companies can be divided roughly to two separate groups – those who are able recover and those how don’t (Knight & Petty 2001, 15). The study (Knight & Petty 2001, 15) suggests that when a company encounters a crisis situation the share value typically starts to lower. After initial shock there are typically two options, if the crisis is handled poorly or this is the overall impression the share value might stay below the level that it was before the crisis. For those companies who handle the crisis well, the share value might quickly rise even to a higher level where it was before the crisis. The basic idea is that if the company could handle a crisis situation, they most likely can perform very well in the normal circumstances also.

In Fortum Corporation the Corporate Security Unit has a clear role in coordinating and developing crisis management on the group level. Those include managing and developing the group level crisis management instructions, crisis management facilities, coordinating crisis management and support for facilitating trainings.

As part of this development project the key stakeholders related to crisis management were interviewed during 2018 and 2019. The interviews were arranged as theme interviews and followed the same structure for all of the interview sessions. All of the 9 stakeholders were interviewed separately. The main input from these interviews was that training is very important and as a topic something that can never be developed too far (Interview memos 1-6 2018 & Interview memos 7-9 2019). Based on the interviews it was quite clear that this project would have a focus on developing the trainings.

1.2 Project scope and aim

Purpose of this project is to identify elements that should be part of crisis management trainings in Fortum and develop trainings further to a form of duplicatable package or concept. The idea is that with this new concept the Corporate Security Unit could better support business divisions in training and implementing crisis management. Project is done for the Corporate Security unit, represented by Juha Härkönen, VP Security.

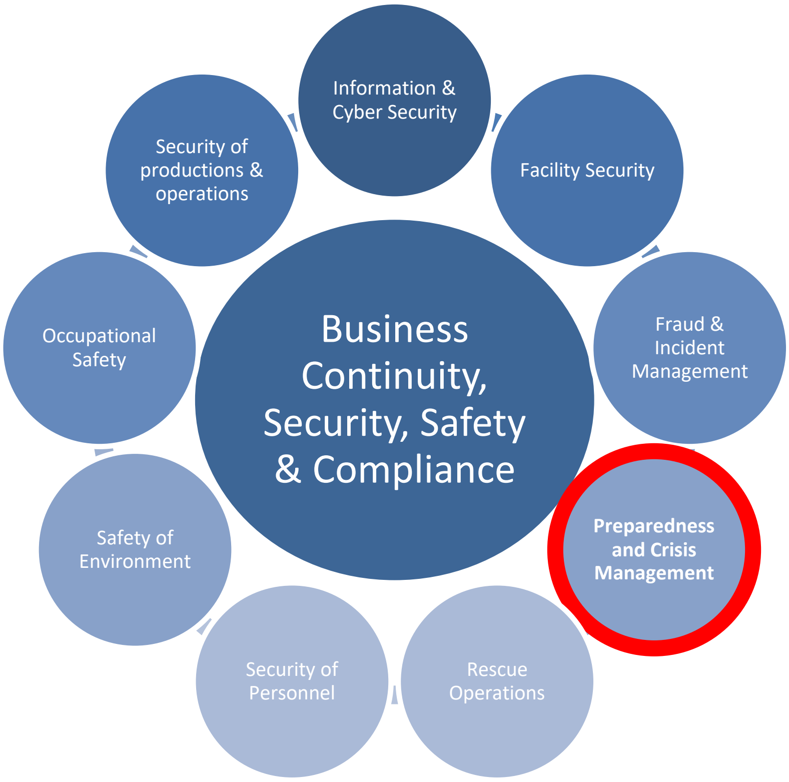
Three questions should be answered based on this project:

1. Holistic view - what are the key elements of crisis management in Fortum?
2. What is the relation of these key elements?
3. What should the crisis management training concept for Fortum be like?

2 Definitions and framework

Corporate Security

Corporate Security is all about securing and keeping safe all the elements of a company. Confederate of Finnish Industries (EK) has created a model which is based on a set of security and safety subcategories. The weight of a specific subcategory itself can vary depending on the company but it is applicable for both domestic and international companies. The subcategories are: (Picture 1) information and cyber security, facility security, fraud and incident management, preparedness and crisis management, rescue operations, security of personnel, environmental safety, occupational safety and security of production and operations. In the very center are business continuity, security, safety and compliance. (Confederation of Finnish Industries EK 2016, 3-4)


Information & Cyber Security
Facility Security
Fraud & Incident Management
Preparedness and Crisis Management
Rescue Operations
Security of Personnel
Safety of Environment
Occupational Safety
Security of productions & operations
Business Continuity, Security, Safety & Compliance

Picture 1 Crisis Management is one element in the EK's holistic model (adapted from Confederation of Finnish Industries EKs. 2016, 4).

Crisis

Crisis is typically defined as “an abnormal and unstable situation that threatens strategic objectives, reputation or viability” (British Standards Institution 2014). What this means in practice depends of course on the organization in question. Companies have different kind of strategies, assets and priorities. Even reputation or how it is valued depends on the company.

In reality it is very hard to predict beforehand all kinds of crisis that could occur to a company. There is also a term ”black swan” that is typically used to describe and phenomenon that deviates from what is expected from a normal situation and would be extremely hard or even impossible to predict (Chappellow 2020).

Crisis Management

There are several different approaches & frameworks to crisis management but a holistic view typically includes the following elements:

1. Efforts that focus on reducing the possibility of different crises

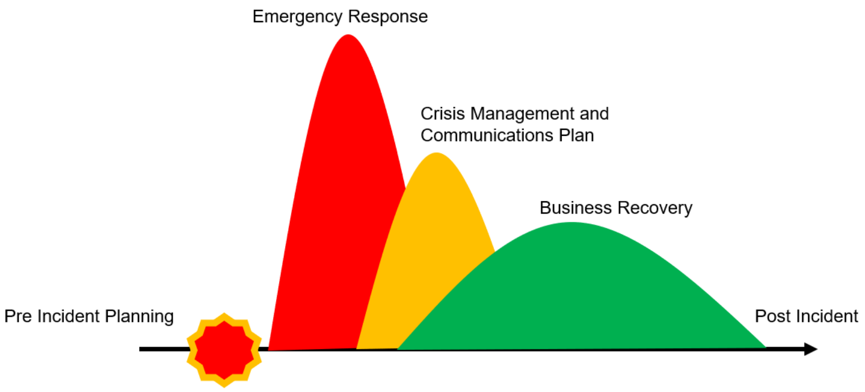
2. Efforts that build and maintain the organizations capability to respond to a crisis

3. Efforts that focus on minimizing the impacts of a crisis when one happens

4. Embracing systematic improvement

(Hinton & Udell 2018).

Crisis Management itself can be seen as a holistic approach that covers all the elements or it can be seen as part of the process itself where it typically fits between those immediate lifesaving actions and business continuity/recovery processes (Picture 2).



Picture 2 An example of a timeline illustrating the phases and their relations in holistic Crisis Management process (adapted from Jaqschies, Westman & Raw 2014)

Crisis Communications

Crisis Communications is typically focused on collecting, coordinating and timely assessing of crisis related information with the idea of protecting the organization facing a public challenge to its brand or reputation (Goh 2019). Communication plays an important role in organizations daily processes but in time of crisis it has even more crucial role. Crisis Communications, as normal communications, must have two dimensions – internal and external and they should be aligned. Communications during an acute incident is typically mostly instructive (The Security Committee. 2017, 34). Crisis communications is not in the scope for this project but it is a fundamental part of crisis management.

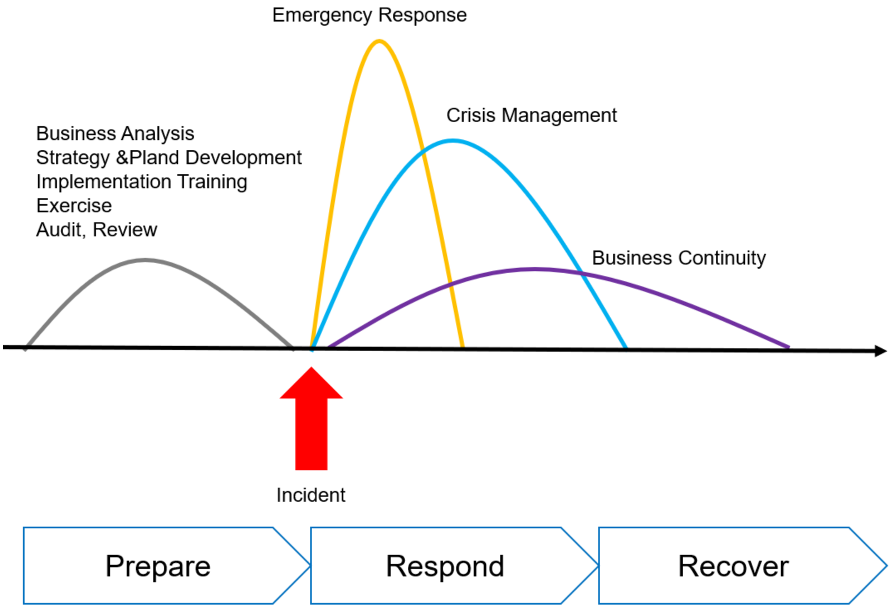
Preparedness Planning

Preparedness planning is typically placed to a national defense context and focuses on protecting the security of supply in emergency conditions (Confederate of Finnish Industries EK 2016, 13). It typically has a strong link to national security and as such is in most cases regulated and this applies especially to security of supply critical companies like e.g. infra providing companies. Regulation for this area varies based on the countries where the company has operations.

With private companies the planning is typically done based on the company's own requirements that focus on safeguarding the business but it is also possible that the requirements coming from the customers are setting the guidelines for the planning. Preparedness planning for emergency conditions is out of scope for this project.

Business Continuity Planning

Business Continuity planning focuses an outlining on how business will continue operating while there is an unplanned disruption on service – it typically include strategies for bot short term and long term disruption (IBM Services 2019). There might be different strategies on what should be prioritized or how some parts of the services/business replaced in the meantime. Business continuity focuses on restoring the business to the state where it was before the incident. Business continuity is typically placed after the emergency response and crisis management functions as these are the most critical right after the incident (Picture 3).



Picture 3 Crisis Management Process and different elements presented with timeline to illustrate the dependencies (adopted from Simpson et al 2019).

Disaster Recovery

Disaster recovery or IT Disaster recovery planning focuses on restoring IT/OT services, hardware, applications and data after an incident (Department of Homeland Security 2018). Planning should be linked to the business continuity plan that sets out the business requirements, typically acquired as a results of an impact analysis. Plans typically include elements like back upping, duplicating and restoring the data. It is important that disaster recovery planning is done based on facts not assumptions and that business responsible and IT responsible share the same understanding.

Resilience

By definition resilience means an ability to recover from or adjust easily to misfortune or change (Merriam-Webster 2020). Building organization's resilience is typically presented as a goal for crisis management function or trainings.

3 Fortum & Crisis Management

3.1 Fortum Corporation

Fortum is an energy company based on Espoo Finland. It currently has core operations in 10 countries – Finland, Sweden, Norway, Denmark, Estonia, Latvia, Lithuania Russia, Poland, and India. In addition to these countries - Fortum also supplies different type of expert services globally. The company has around 8000 employees and around 128 hydro power plants, 26 CHP, condensing and nuclear power plants. Heat is being supplied to 22 cities and in addition to those Fortum has five waste treatment facilities. Company has been recently growing also on solar and wind. (Fortum Corporation 2020b)

3.1.1 Business Structure

The business structure has been divided to divisions and corporate functions. Generation division includes nuclear, hydro and thermal power production. It also includes portfolio management and trading as well as expert services globally. City Solutions division includes heating and cooling, waste-to-energy, biomass and circular economy solutions. (Fortum Corporation 2020c)

Consumer Solutions division includes electricity and gas retail business – Fortum has about 2,5 million customers in Nordics and Poland. Russia division comprises power and heat generation and sales in Russia. Corporate Support functions and Business Technology unit provide support and services for the business divisions. (Fortum Corporation 2020c)

3.1.2 Corporate Security Unit

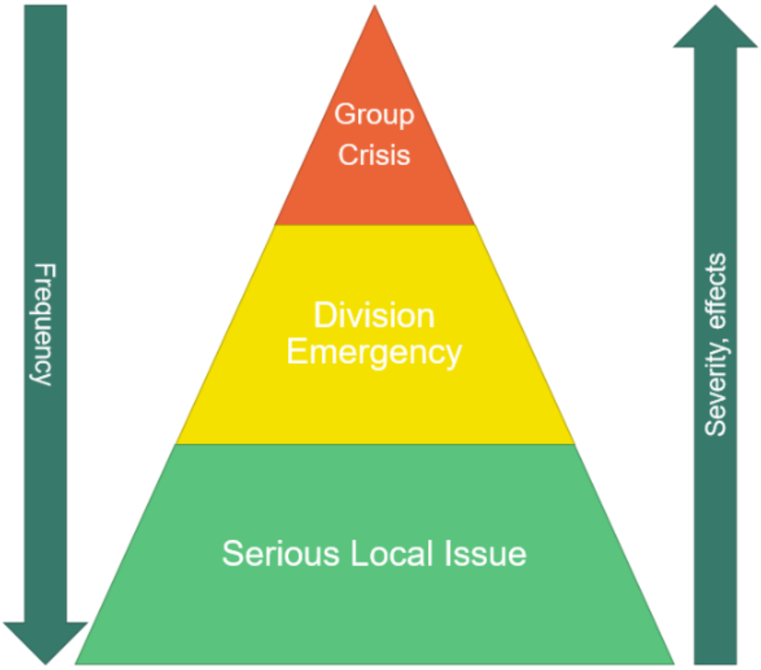
Corporate Security for Fortum means striving to ensure the uninterrupted continuity of business and the safety of people, information, assets and processes in normal and exceptional situations. Corporate Security consists of cyber and physical security experts and is responsible at the group level for cyber, personnel and operational security.

One of the core service areas is Crisis Management. Corporate Security Unit is responsible for group level crisis management development and coordination, e.g., for organizing trainings. The testing and updating of the crisis management and continuity plans are the responsibility of each division and line organization. (Fortum 2020a, 55)

3.2 Crisis Management in Fortum

Fortum Group Crisis Management instructions is policy level document which basically sets the framework for crisis management in Fortum Corporation. It sets out the purpose and objective for crisis management and also definitions how to classify different cases. The document also includes roles, responsibilities and escalation. Latter part of the document is about documentation on the different levels of the organization, training, reporting and monitoring. (Fortum Corporation 2019a)

Fortum uses a three level scale when categorizing incidents (Picture 4) – this way it is easier to keep track on the severity. Sometimes an incident can be quite significant for a single site where it takes place but the overall impact for the group would still be low. The structure follows Fortum business structure (Fortum Corporation 2019a)



Picture 4 Crisis Management in the Group level – not every incident is a crisis and this is why incidents have been categorized to three levels (Fortum Corporation 2019).

3.2.1 Group Crisis Team

Basic principle is that every division and line organization have the responsibility for planning, training and also managing issues and emergencies (Fortum Corporation 2020a, 55). This means that problems should be solved as close to the source as possible and within the normal line organization and structure. However escalation is always possible, from site to business area/division and from division to group.

In case of a crisis affecting the group operations more broadly (Fortum Corporation 2020a, 55), Fortum has established a structure called Group Crisis Team. The team comprises of fixed members and optional members. Fixed members include among others - participants from Corporate Security and Corporate Communications Units (Fortum Corporation 2019a). The full setup of the team depends on the case at hand.

Idea of the team is that it ensures that the all needed resources from the whole group are usable in case of crisis. Typically – but of course depending on the incident – the whole business can't be put to a standstill but might be continued as limited. There is a famous quote from CEO of General Electric Jeffrey R. Immelt: “"I was Chairman for two days. I had an airplane with my engines, hit a building I insured, was covered by a network I owned and I still have to increase earnings by 11 percent” (Sikich 2008, 50).

3.2.2 Crisis Management Process

Fortum Crisis Management Process in overall can be illustrated with arches that present the level of activity on one axis and then time from the incident in the other axis (Picture 5).

Preparedness - Activities Before an Incident

Activities before an incident include all those preparation tasks and work that have been done in the planning phase e.g. evaluating, risk analyses, scenarios, responsibilities, alarming and mitigation. It also includes documenting, training and rehearsals. As Fortum operates in the critical infrastructure sector – there are also regulation that guide the preparedness phases depending on the country and jurisdiction.

Emergency Response

When an incident occurs – the first priority is always on saving human lives and preventing extra damages. Depending on the incident this might include issuing a local alarm, giving first aid, putting out a fire or isolating a cyber-attack.

Typically the emergency response is made quite close to the source of the incident itself. The duration is typically short but the effort is maximal or close to it. In sites like powerplants – these actions are typically set out in the rescue plan and then executed by the site organization. This area is also typically governed by regulation depending on the operating country.

Crisis Management

When an incident has been reported via line organization and group reporting tool, it will be analyzed by the relevant stakeholders. When an analysis supports the fact that incident isn't just a local issue, if there is possibility that it has wider effects or it is escalated - the crisis management phase kicks in.

Crisis management is all about getting organized, sharing tasks, updating situational awareness and effective crisis communications. As Fortum is a listed stock company - the crisis communications has also an external dimension which comes with strict legislative requirements.

Crisis management is basically used to support the organization to manage something that isn't a local issue or daily business. In Fortum there are pre-prepared crisis management facilities that have been planned so that they'd support group crisis team working. The business divisions are responsible of creating their own crisis management instructions (Fortum Corporation 2020a, 55).

Business Continuity

Right after the crisis management phase allows, the focus should be on business continuity. This will greatly depend on the case in hand and its effects to the certain business area. An example would be that if a certain production site is not functioning normally, there might be for example manual process that could be used or some other smaller sites available that could be used to replace some capacity for example in district heating area.

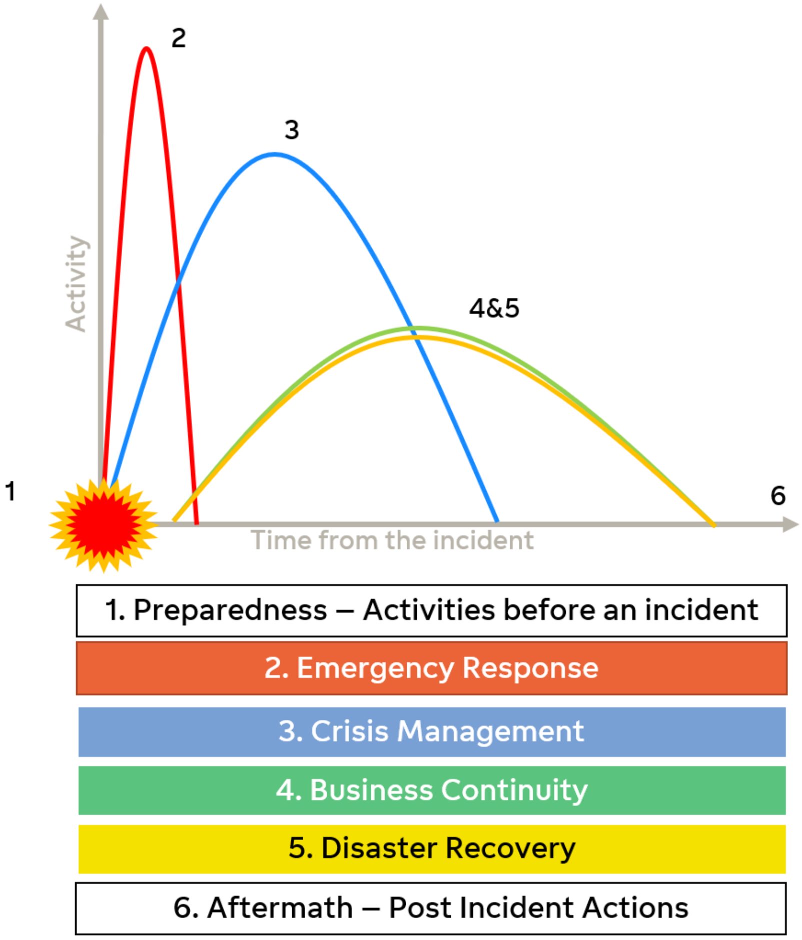
As the business continuity plans are even more business specific than crisis management plans, the responsibility of creating and maintaining those is in the responsibilities of line organization and business units (Fortum 2020a, 55). When business continuity is done properly, the effects of incidents to the customers and other stakeholders should be minimal.

Disaster Recovery

In the era of digitalization Disaster Recovery or IT Disaster Recovery is closely linked to business continuity. Some services are in-house and some are provided by external partners. Business Continuity planning includes identifying and determining which applications and services are critical and what are the SLAs. From crisis management perspective the most important aspect is that Business and IT service providers share the same understanding and expectations and that the mechanisms are tested and proven to work.

Aftermath – Post Incident Actions

There are actions to be done after an incident but those vary a lot depending on the nature of the incident. In some cases the actions would start with a debriefing session for the employees. Investigation and analysis would be done – what is there to learn from the case, how can the instructions and processes be improved – also corrective actions also with a follow up – how to prevent this from happening again. There might also be legal aspects, reporting to authorities, criminal proceedings or for example claims for insurance company.

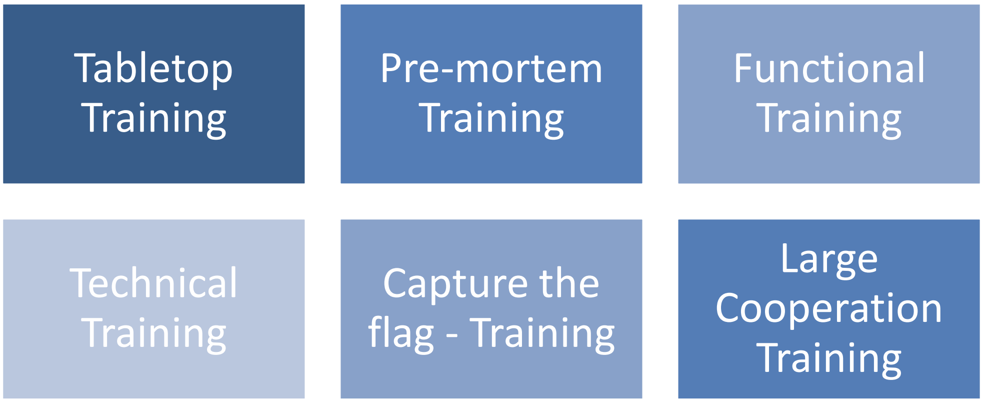


Picture 5 In Fortum the crisis management can be illustrated as a holistic process with different phases and priorities (adopted from Simpson et al 2019)

4 Training Concept

4.1 Training types

There is basically no limits for the types (Picture 6), ways and styles of training but the target group of the trainings should always be kept in mind when planning a training. It is not reasonable trying to train both top management and technical system engineers with exactly the same training – even though both of the mentioned can be part of a complex cooperation training. However the more complex the training – the more planning and coordination it typically requires. (Traficom 2019, 2)



Picture 6 There are many types of trainings but not all trainings are ideal for all target groups and all purposes (Traficom 2019, 2)

In Fortum type of business environment the typical participants for crisis management trainings are management team level persons that represent the crisis teams. The participant level can vary from group, business division, business area to site level management teams. For exercising management teams, tabletop trainings or functional are suitable and good options (Traficom 2019, 6).

Tabletop training

Tabletop trainings are most common type of trainings and also light to arrange – they are good for training and evaluating crisis management, processes, capabilities (Traficom 2019, 7). In utilities area they can also be helpful on generating insights that shape response and prevention strategies (Simonovich 2020, 3). This type of training is also particularly good when the trained group is new or has many new members or they don't have very deep understanding on the scenario. Maybe the scenario itself is totally new or new for specific business area.

Tabletop training can also be useful tool for creating instructions / solutions / processes for a new scenario (Traficom 2019, 7) but in the this case it is recommended to have a dedicated person making notes. As training type is light to arrange – it could even be arranged with a self-learning module with minimal moderation / facilitation.

Functional training

Functional trainings are suitable for training crisis management itself, crisis communications and for cooperation trainings (Traficom 2019, 8). This type of training is more complicated than tabletop training and also has a pressure element as the pace for the training is typically set with various injects that can even be reactive depending on the choices of the participants.

The facilitation of a functional training needs more effort than tabletop training. Typically the setup is built so that there is a separate game center where the training is facilitated and injects sent for the participants (Traficom 2019, 8). Moderating the game center requires good understanding both on the business and the scenario as the participants may lead the training to unexpected direction. This is why typically an "insider" from the business is needed both in planning the training and also facilitating it, possibly in the observer role.

The injects in functional training can vary from incident reports, emails, pictures to phone calls from employees, media, customers. Typically the injects guide the scenario forward piece by piece on the selected path. Whatever the inject is – it is very important to clearly mark them with labels that state that they're only for training purposes to avoid confusion.

Observer is typically needed for functional trainings, making notes and analyzing the performance of the group that is being trained. Typically it adds pressure for the participants if the observer is someone that the training group doesn't know very well. For benchmarking and pressure element purposes it makes sense to ask observers from other companies or important stakeholders like authorities.

4.2 Risks and scenarios

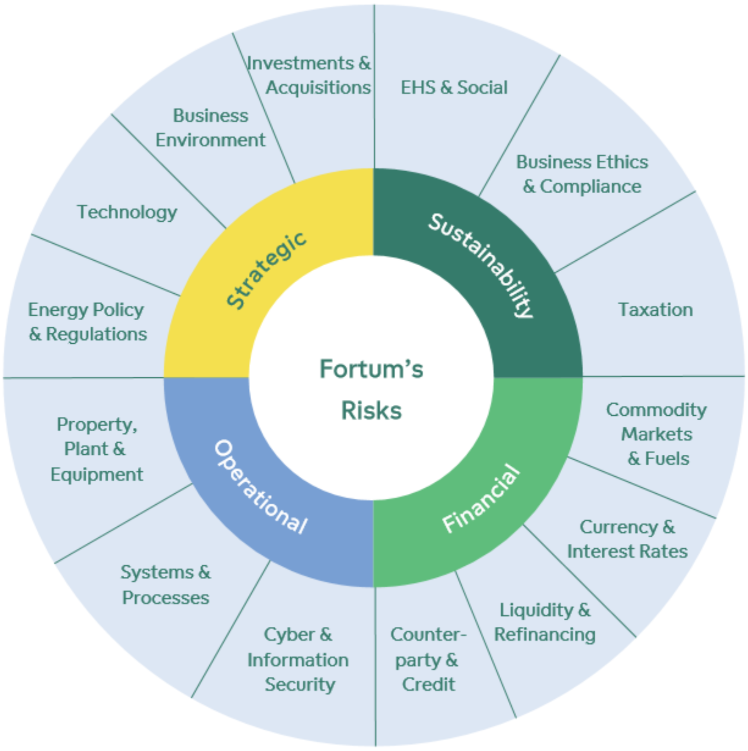
Fortum has a risk policy, group risk instructions and also instructions and analyses for more specific areas (Fortum Corporation 2020d). The risks are categorized in four different domains (Picture 7). Risks for the company and business operations may be related to political situations, terrorism, crime, conflicts and business partners (Fortum Corporation 2020d).

Group crises can of course stem from any of the categories but typically in crisis management the focus is in the operative risks domain. By definition operational risks are unexpected events which can lead to negative monetary, safety, environmental or reputational impacts as a result of inadequate or failed internal processes, systems or equipment, or from external events (Fortum Corporation 2020d, 32).

Scenario-based exercises are a cornerstone for crisis management programs as they ensure that plans are sound but also test the crisis management organization on a simulation of life like case (Schwirian & Udell 2019). Organizations own risk management is a good basis for scenario building – identified risks are turned into different scenarios (Traficom 2019, 20).

In Fortum - scenarios can be built on the basis of more detailed risks analyses. Scenarios typically include short description of the event itself and a few features / boundaries like length and effect in general level.

The scenarios of course vary between different business areas as for some they might be more valid than for others. Scenario could be for example industrial espionage or long term electricity blackout like the Finnish Transport and Communications Agency Traficom's Cyber Security Center has set examples of training scenarios (Traficom 2020a), there typically is a short description of the case itself and then some (technical) boundaries.


Fortum's Risks
Strategic
Sustainability
Financial
Operational
Investments & Acquisitions
EHS & Social
Business Ethics & Compliance
Taxation
Commodity Markets & Fuels
Currency & Interest Rates
Liquidity & Refinancing
Counter-party & Credit
Cyber & Information Security
Systems & Processes
Property, Plant & Equipment
Energy Policy & Regulations
Technology
Business Environment

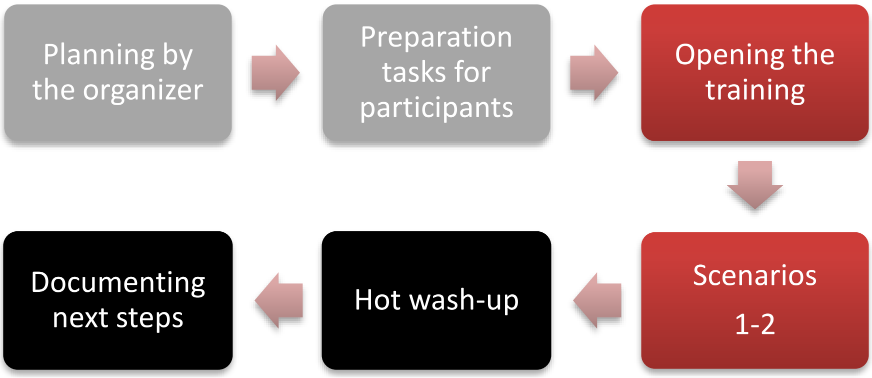
Picture 7 Fortum's Risks presented in a sphere (Fortum Corporation 2020d, 26)

4.3 Light Training Concept

Setup & Scope

From the beginning it was clear that need was for scalable approach – at least two versions. First version would be light and shorter – modification from the tabletop training (Picture 8). It is recommended to be used when participants need to be trained for several scenarios, especially if there are new persons or e.g. new business areas. It has limitations compared to standard one but it has its place and purpose as it is easily duplicated and held for several locations.

For more interaction the training should preferably be face to face session instead of Skype/Teams (or similar video conferencing tool) only. If Teams is allowed then it should actually be Teams only to be fair for all participants. The duration for the training itself could be from 90 to 120 minutes depending on the time at hand. At least 30 minutes should be reserved for the hot wash-up, agreeing and documenting next steps which is an important phase.



Picture 8 Light Training Structure is fairly simple and straight forward

Before the training the participants have to do preparation tasks including:

1. Familiarizing/refreshing themselves with Group Crisis Management Instructions
   a. Group Reporting tool
2. Familiarizing/refreshing with Division/Function level Emergency Instructions
   a. Roles and responsibilities
   b. Risk Analysis
   c. Incidents from past 5 years (from Group Reporting Tool)
   d. Industry incidents
3. With BA/Site level training in question – familiarize themselves with Business Area / Site Level Instructions
   a. Rescue plan or process
   b. Risk Analysis
   c. Incidents from past 5 years (from Group Reporting Tool)

Optionally - if there are many new participants in the team to be trained - the preparation part should be arranged as a short lesson before the training itself.

As the time is fairly limited in this version, it is best to keep the focus on the topic itself, crisis management phase – the scenario itself can begin from the incident/emergency response part which quickly leads the participants to crisis management phase where they need to organize themselves.

Planning & Stakeholders

Planning a light training session is fairly simple as it is based to the tabletop model with a few scenarios. Ideally the planning should be done by someone from the organization to that is to be trained. This way the scenario itself can be fine-tuned to really fit the organization and will also have more realistic look and feel.

The scenario or 1-2 scenarios can be selected from scenario bank or to be created from scratch preferably based from risk analysis on the specific business area and added to the scenario catalogue afterwards. It is typically good to use something that the organization can recognize e.g. real pictures or system names.

Organizer needs to find a time and date for the trainees and organize facilities where the training is held. For best commitment it is recommended to arrange management team level sponsor for the exercise. The homework should be stated clearly in the invitation message with links to the materials. This way the participants are already in the right mindset when the training is about to start.

As communications is crucial part of the crisis management – division or group level communications should always be involved to either participate or as a subject matter expert.

It is recommended to nominate one person to make notes / observing as typically the discussion might get quite intensive and as the ones participating are not in the best position to be making notes of their own behavior.

Training session & elements

Training session should start with a short intro where the purpose and goals of the training are shortly explained. This is also the part where the rules are agreed. After that the first scenario is given to the training group and they have time to think/discuss how they would handle it. After some time there would be an extra element for the scenario – a two tier approach.

Elements to be observed or pushed depending on the participants:

- Who took the lead? How was the group organized?
- Situational Awareness – How was it formed?
- Priorities – Clear first steps?
- Instructions – Was there any for this scenario and were they followed?
- Incident report & Escalation (Group Reporting Tool) – Was it done?
- Crisis Communications aspect –What and for whom?

Feedback & Development

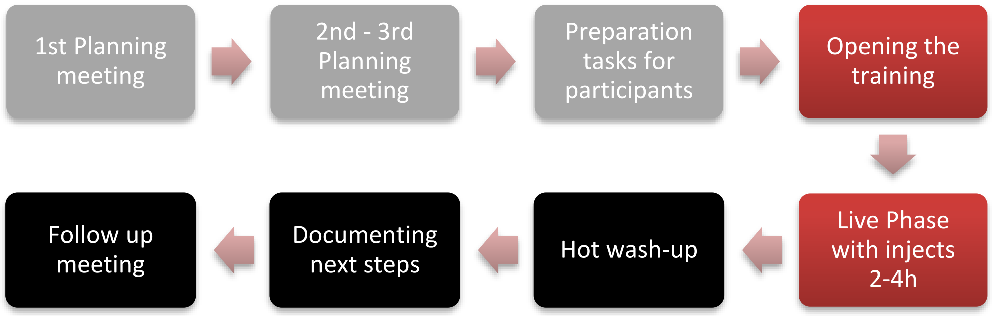
After working with one or two scenarios (around 30-40 mins each) there should be a short technical break and after that the group gathers for hot wash-up. It is typically good to start first with a few minutes roundtable for all participants and after that the organizer/observer can give his/her feedback.

Finally comes the important part where documentation should be done with responsibilities and deadlines so that the process/instructions can be developed even further. In this part it is typically needed to challenge the group on that what could have they done better.

4.4 Standard Training Concept

Setup & Scope

Standard training is modification from functional training (Picture 9). To get the most from the participants and for interaction - the training should preferably be face to face session instead of Skype/Teams only. The duration for the training itself could be from 2-4 hours depending on the time at hand. At least 45 minutes should be reserved for the hot wash-up, agreeing and documenting next steps.



Picture 9 The standard training requires effort from the organizer both before and during the training.

Planning & Stakeholders

Before the training the participants have to do preparation tasks including:

1. Familiarizing/refreshing themselves with Group Crisis Management Instructions
   a. Group Reporting tool
2. Familiarizing/refreshing with Division/Function Emergency Instructions
   a. Roles and responsibilities
   b. Risk Analysis
   c. Incidents from past 5 years (from Group Reporting tool)
   d. Industry incidents / trends
3. With BA/Site level training in question – familiarize themselves with Business Area / Site Level Instructions
   a. Rescue plan or process
   b. Risk Analysis
   c. Incidents from past 5 years (from Group Reporting tool)

Optionally if there are many new participants in the team to be trained - the preparation part should be arranged as separate session before the training itself.

In this version there is more time so while the focus should be on the topic itself, crisis management phase – the scenario itself can begin from the incident/emergency response part which leads the participants to crisis management phase where they need to organize themselves. It is also recommended that the training in the end touches also the business continuity part at least on a strategic / tactical level. This way it can be identified / verified that what is the status in that area also concerning the very scenario at hand.

Training session & Elements

Training session can start with a short intro where the purpose and goals of the training are shortly explained or with straight with a first inject. In the latter option it is very important that rules are agreed beforehand and sent for the participants with an email + calendar invite.

After the first inject is given to the training group – the training is in the live phase. The trainees act/think/discuss like they would do in the real situation. The organizer and/or the game command center continues giving new injects based on pre-defined schedule or training groups behavior/choices. The pre-defined schedule or so called playbook is a good tool for simulating the expected outcome and to ensure that right elements are being exercised.

It is recommended to have one major scenario but there can be several side scenarios or injects that have nothing to do with the major scenario. This will add up pressure for the participants but also test their ability to prioritize. Some injects can be used for challenge them to focus on what is important – they can be just extra noise.

Elements to be observed or pushed depending on the group and performance:

- Who took the lead? How was the group organized and tasks shared during the way?
- Situational Picture
    - How was that formed?
    - Was there timeouts during the training where the situational picture was updated?
    - Was the picture correct?
- Priorities
- Decisions made
- Instructions – Was there any and were they followed?
- Incident report (Group reporting tool) – Was it done?
- Escalation
- Crisis Communications aspect – Who and what?

Development & Documenting Next Steps

After the live phase is ready it is good to have a technical break and after that the group gathers for hot wash-up. It is good to start first with a roundtable for all participants and after that the organizer/observer can give his/her feedback. After that the “war journal” or log should be reviewed in order to go through group performance. In this part it is typically needed to challenge the group on that what could have they done better.

Documenting the next steps is a valuable phase as it is used for systematic development. Issues noticed during the training must be clearly documented and for all action points a responsible and deadline must be defined. The idea is to develop process/instructions even further. The participants must be able to influence the action point list as it increases commitment for the actions.

Follow up meeting

As standard training session is relatively big effort from the group that has been trained (multiple persons for half a day) it makes sense to ensure that agreed development actions are going forward and all the value from the training is extracted. Depending on the action points – how much time has been given for their implementation – a follow up meeting should be agreed on 2-4 months from the training.

In the follow up session the action point list should be reviewed in order to see what actions are already done and which might be behind schedule. In this meeting the training calendar should also be checked in order the schedule coming trainings and to discuss the agenda of those.

4.5 Field test results

First Exercise – Standard, Site Management level

First exercise was arranged at 26.11.2019, there were 10 participants, some from site management team and few stakeholders from the business division. Training was facilitated by Corporate Security unit and arranged according to Standard Training model. The selected scenario was cyber related so in the planning face an IT specialist from the business area itself was interviewed in order to make the scenario itself realistic as possible.

There was a theory/awareness lesson before the live phase. The exercise itself consisted of pre-defined injects that were tailor made for the specific site in question. The injects guided the participants through the exercise - participants were active. Live phase took around three hours including breaks and schedule was followed. Hot wash-up was arranged immediately after the exercise and action points we're identified and defined together with stakeholders. Follow up session was arranged with key stakeholders to go through the actions. Feedback was collected from the participants and it was positive (Feedback Survey 2019a).

Second Exercise – Standard, Site Management level

Second exercise was arranged 3.12.2019 and it also very similar to first exercise. There were the 10 participants were from site management team and few stakeholders from the business division. Training was facilitated by Corporate Security unit and arranged according to Standard Training model like the previous one. The selected scenario was cyber related so also in the planning face of this exercise an IT specialist from the business area itself was interviewed to ensure realism.

There was a theory/awareness lesson before the live phase. The exercise itself consisted of pre-defined injects that were tailor made for the specific site in question, the material from the previous exercise was fine tuned to fit the site at hand. The live phase took around 3 hours including breaks, schedule was followed. Hot wash-up was arranged immediately after the exercise and action points we're identified and defined together with stakeholders. Follow up session was arranged with key stakeholders to go through the actions. Feedback was collected from the participants and it was positive (Feedback Survey 2019a).

Third Exercise – Light, Division Management Team level

Third exercise was arranged at 13.12.2019 with the 10 participants were from division management team level and key stakeholders. Training was facilitated by Corporate Security unit and arranged according to Light Training model because of the fairly limited time in hand. The selected scenario was cyber related including two tiers (first phase escalates further). Once again there was careful pre planning with an IT experts from the business itself to ensure realism in the scenario.

There was a limited theory/awareness lesson before the live phase. The exercise itself consisted of one scenario that was divided in two tiers. In total 90 min (2x 45 min slots) were reserved for the playing itself. Hot wash-up was arranged immediately after the exercise and action points we're identified and defined together with stakeholders. Follow up session was arranged with key stakeholders to go through the actions and also a new training scheduled, this time it would be Standard Concept. Feedback was collected from the participants and it was positive (Feedback Survey 2019b).

Fourth Exercise – Light, Business Area Management level

Fourth exercise was arranged at 23.3.2020 with 11 participants from business area management team level. Training was facilitated by Corporate Security unit and arranged according to Light Training model because of the fairly limited time in hand. This time the COVID-19 situation was already on, restrictions valid and the training was decided to be arranged Teams videoconferencing solution only. There were three scenarios selected based on the risk analysis made by the business area. Once again there was careful pre-planning with experts from the business itself to ensure realism in all of the scenarios.

There was a limited theory/awareness lesson before the live phase. The exercise itself consisted of three individual scenarios. There were 3x30min slots reserved for the playing itself. Hot wash-up was arranged immediately after the exercise and action points we're identified and defined together with stakeholders.

Follow up session was scheduled with key stakeholders to go through the actions. Feedback given by the participants in the Hot wash-up phase was positive. Videoconferencing only actually worked pretty well in the training and most likely better than if there would have been a hybrid where some are physically present and some are connected with video.

The time reserved for each scenario was very limited, probably as limited as it can be. In the other hand it added pressure for the participants and also made it possible to cover a variety of aspects in single training session. The downside was that there really was no time for functional parts that are included in the standard concept.

5 Conclusion

In general - successful management requires clear responsibilities and roles, situational awareness, crisis communications, information sharing, operational continuity and cooperation (The Security Committee 2017, 15). Exactly the same principles apply for crises management as such.

Crisis is a situation that forces the organization to get organized beyond the business as usual in order to deal with it and that makes the roles and responsibilities crucial. It might be difficult to prioritize and see the relations - reviewing the situational picture from time to time helps to clear the fog. There are many topics that must be considered carefully before the crisis situation (Simonovich 2020, 1). Existing and tested plans/instructions/processes may not be 100% identical for the situation at hand but most likely they can work as the foundation in the crisis situation.

There are various approaches and theories when it comes to training people. The most important thing is to ensure frequent trainings with training calendar and to keep the participant group in mind when planning the trainings. For best results someone inside the group to be trained should be part of the planning and not playing but observing in the exercise. It is important that the scenario is valid and realistic for the participant group.

Exercises can be planned and executed with maximal resources but it is possible to reach good results with simple scenarios and injects. Focus should also be in identifying and documenting the agreed action points. Implementing those ensures systematic development of processes, instructions and systems.

Having two options for training concept – a light one and standard one makes it possible to train more often. The light one doesn’t allow going too detailed but in the other hand it gives the possibility to cover more scenarios in the same time. In reality the two concepts can be used as hybrids or modified.

Having concepts also sets the scene for the one ordering and arranging the training and for the ones who are to be trained.

Those who are able to succeed in crisis are most likely able to outperform in normal conditions also. Organization with clear processes, instructions and trained experts is more prepared for also for the unexpected than one with poor preparedness. Only through trainings and exercises organizations can really test and continuously improve their resiliency.

6 References

Published sources

Berman, J. 2014. The Three Essential Warren Buffett Quotes To Live By. [online resource]. [accessed 18.5.2020]. Accessible: https://www.forbes.com/sites/jamesberman/2014/04/20/the-three-essential-warren-buffett-quotes-to-live-by/#5c04e8416543

BS 11200:2014. 2014. Crisis Management. Guidance and Good Practice. British Standards Institution.

Chappellow, J. 2020. Black Swan. [online resource]. [accessed 18.5.2020]. Accessible: https://www.investopedia.com/terms/b/blackswan.asp

Confederation of Finnish Industries. 2016. Elinkeinoelämän yritysturvallisuusmalli. 3-4 [online resource]. [accessed 18.5.2020]. Accessible: https://ek.fi/wp-content/uploads/yritysturvallisuus_2016.pdf

Department of Homeland Security 2018. IT Disaster Recovery Plan. [online resource]. [accessed 18.5.2020]. Accessible: https://www.ready.gov/business/implementation/IT

Fortum Corporation. 2020a. Fortum Sustainability Report 2019, 54. [online resource]. [accessed 18.5.2020]. Accessible: https://www.fortum.com/sites/g/files/rkxjap146/files/investor-documents/fortum_sustainability_2019_2.pdf

Fortum Corporation. 2020b. Fortum worldwide. [online resource]. [accessed 18.5.2020]. Accessible: https://www.fortum.com/about-us/our-company/fortum-worldwide

Fortum Corporation. 2020c. Reporting structure. [online resource]. [accessed 18.5.2020]. Accessible: https://www.fortum.com/about-us/investors/key-facts/reporting-structure

Fortum Corporation. 2020d. Financials 2019. [online resource]. [accessed 18.5.2020]. Accessible: https://www.fortum.com/sites/g/files/rkxjap146/files/investor-documents/fortum_financials2019_3_0.pdf

Goh, M. 2019. What is Crisis Management and Crisis Communication? Are They Similar? [online resource]. [accessed 18.5.2020]. Accessible: https://blog.bcm-institute.org/crisis-communication/what-is-crisis-management-and-crisis-communication-are-they-similar

Greenberg, A. 2018. The Untold Story of NotPetya, the Most Devastating Cyberattack in History [online resource]. [accessed 18.5.2020]. Accessible: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Hinton, M. & Udell, B. 2018. Readiness, Response and Recovery in a new world of crisis. [online resource]. [accessed 18.5.2020]. Accessible: https://www.controlrisks.com/our-thinking/insights/readiness-response-and-recovery-in-a-new-world-of-crisis

IBM Services 2019. Adapt and respond to risks with a business continuity plan (BCP). [online resource]. [accessed 18.5.2020]. Accessible: https://www.ibm.com/services/business-continuity/plan

Jaqschies, G., Westman, D. & Raw, D. 2014. Supply Chain Challenges in the Biopharmaceutical Industry: A Case Study Following the 2011 Tsunami in Japan. [online resource]. [accessed 18.5.2020]. Accessible: https://bioprocessintl.com/upstream-processing/biochemicals-raw-materials/supply-chain-challenges-biopharmaceutical-industry-case-study-following-2011-tsunami-japan/

Knight, R & Pretty, D. 2001, 15. Reputation & Value - the case of corporate catastrophes [online resource]. [accessed 18.5.2020]. Accessible: http://www.oxfordmetrica.com/public/CMS/Files/488/01RepComAIG.pdf

Merriam-Webster.com Dictionary. 2020. [online resource]. [accessed 18.5.2020]. Accessible: https://www.merriam-webster.com/dictionary/resilience.

Schwirian, A. & Udell, B. 2019. 13 common mistakes when building global crisis readiness programs. [online resource]. [accessed 18.5.2020]. Accessible: https://www.controlrisks.com/our-thinking/insights/3r-building-a-global-crisis-readiness-program

Sikich, G. 2008. Protecting your business in a pandemic: plans, tools and advice for maintaining business continuity. USA: Praeger Publishers.

Simonovich, L. 2020. Simulating a Cyberattack on the Energy Industry - a playbook for incident response. [online resource]. [accessed 29.5.2020]. Accessible: https://assets.new.siemens.com/siemens/assets/api/uuid:7ee9587c-dfd3-4f8a-b447-c9fb7302ed96/version:1582144985/cyberattackdigitalr4v2.pdf

Simpson, A., Francesca, V., Lai, I., DoQuang, D., Zambon, M. & Willemse. 2019. International SOS Business Continuity as a Key Driver of the Global Health Security Agenda. [online resource]. [accessed 18.5.2020]. Accessible: https://pandemic.internationalsos.com/-/media/pandemic/files/dandp-pdfs/ghsa-business-continuity_a0-poster_june2019.pdf?la=en

The Security Committee. 2017. The Security Strategy for Society. [online resource]. [accessed 18.5.2020]. Accessible: https://turvallisuuskomitea.fi/wp-content/uploads/2018/02/YTS_2017_suomi.pdf

Traficom (Finnish Transport and Communication Agency) 2019. Kyber-harjoitusohje. [online resource]. [accessed 18.5.2020]. Accessible: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kyber-harjoitusopas.pdf

Traficom (Finnish Transport and Communication Agency) 2020. Kyber-harjoitusskenaariot 2020. [online resource]. [accessed 18.5.2020]. Accessible: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kyberharjoitusskenaariot2020.pdf

Unpublished sources

Interview memos 1-6. 2018. Stakeholder interviews. Individual interviews.

Interview memos 7-10. 2019. Stakeholder interviews. Individual interviews.

Fortum Corporation. 2019. Fortum Group Instructions Crisis Management. 19.2.2019

1. Feedback Survey Memo. 2019a Crisis Management Exercise Feedback Results. 9.12.2019

2. Feedback Survey Memo. 2019b Crisis Management Exercise Feedback Results. 20.12.2019

7