Impact of Cyber and Physical Incidents in Finnish Water Utilities

Anni Karinsalo, Heimo Pentikäinen
VTT Technical Research Centre of Finland

Abstract

Critical Infrastructure (CI) companies are facing more and more cyber and other incidents, either by direct attacks or by accident. The result can be unexpected. The cascading of these incidents can also be due to many reasons. In this paper, we study Finnish CI companies' incident resilience and how they estimate or measure the effect of cyber and other incidents on their operation, by interviewing Finnish water utilities. We propose improving methods for the revealed problems and focus especially on factors of impact analysis, cascading effects and dependencies. Our analysis offers significant new information about CI state with relation to cyber risks, benefiting not only water industry, but CI systems in general. Our findings are that companies assess industry-specific security impacts, estimate cascading effects, dependencies between impacts and recognize dependencies to industrial automation providers. However, there is a clear lack of cyber security risk recognition and impact assessment, clear interfaces and responsibilities. One development area is to integrate cyber risk management into automation-related risk management, and increase cyber risk education. In addition, there is a need for systematic situation awareness at national level and locally. Finally, there should be communication-enablers between different actors in Finland and between Nordic and European countries.

1. Introduction

Critical infrastructure (CI) utilities are facing new threats as more and more infrastructures are connected to Internet. Concurrently, cyber criminals have more and more incentive to seek novel ways for finding access to CI facilities and harming them [1]. For instance, the earlier WannaCry outbreak had severe consequences on health services of UK making them inaccessible [2].

Additionally, CI dependencies are causing concern as they are recognized as a key challenge, being a source of cascading effects [3]. Dependency can be unidirectional, whereas interdependency is defined as a "bidirectional relationship between two infrastructures through which the state of each infrastructure influences or is correlated to the state of the other. More generally, two infrastructures are interdependent when each is dependent on the other." [4]

An essential property of CIs is resilience. According to [5], resilience can be defined as "an overarching attribute that reflects the degree of community preparedness and the ability to respond to and recover from a disaster". Water supply is recognized as one of the CIs [6], so the resilience of water utilities and security impacts for them have a huge impact on Finnish society as well. The authors of [7] have studied Finnish CIs such as electricity, telecommunications and rescue services, but the absence of water area motivated us to study water utilities as CI and their place in Finnish society. In the study of [8], water area is included and some dependencies to other CIs are presented, after which a system for gaining situation awareness is presented. From our point of view, we wanted also to analyze what are the factors behind the companies' incident response, and how they consider factors for dependencies and cascading effects of incidents.

In this paper, we present analysis from interview results, in which Finnish water utility company representatives discuss the following themes: companies' resilience (incident preparedness), impact analysis and various types of dependencies of their facilities. We analyze the most important details revealed during the interviews, and factors that affect the themes mentioned above. We discuss the main problems and suggest methods or improvement actions based on the problems. The problem field might be vast, but we aim to examine the subject field from the impact analysis point-of-view, and considering especially cyber security, but also learning from the practices of physical security in water utilities.

This paper is organized in the following way: In section 2, we discuss Finnish water utilities and how regulatory parties set requirements for their risk management. In section 3, the structure of interview questions is presented. In section 4, the interview answers are summarized and in section 5, discussion and future work is provided. Finally, in section 6, the conclusions are presented.

2. Finnish water utilities and regulatory push for risk-based approach

The very first water utility in Finland was established in 1876 and at present, 90 % of Finnish households' water is received using water utilities' water supply systems [9]. Latest update for the legislation regarding Finnish water supply service that is from the year 2014 includes some requirements for risk management, therefore setting the baseline and exigencies for risk-driven approach in water utility companies. First, the legislation emphasizes the preparation for incidents and failures, and second, the legislation sets the obligation for situation awareness, according to which the water supply service is obligated to be aware of the state of their equipment and risks targeting quality or quantity of the raw water [9].

Furthermore, European Union (EU) is also effecting the implementation requirements of water utilities by its Council Directive 98/83/EC, handling quality of water for human consumption [10]. The directive recognizes “use of risk-based approach” as one of the areas with “room for improvement”. However, the directive does not comment on the need for cyber-related risk management approaches or precautions that may or should be implemented.

In Directive 2016/1148, handling security of network and information systems [11], “drinking water supply and distribution” is recognized as one of the essential services, to whom this directive “establishes security and notification requirements for operators of essential services and for digital service providers”. The directive will be transposed in national legislation by May 2018 and operators of essential services will have to be identified by November 2018. The effects of the Directive 2016/1148 are further discussed in 5.7.

3. Interviews

Our approach was to conduct interviews for a number of water utility representatives and let them share their view on the questions. Overall, we interviewed six company representatives from five different water utility companies. Due to differences of interviewee background, we gain insight in both detailed as well as broader point-of-view in the matter. Even though the number of interviewees is rather small, we can benefit substantially from the answers to understand current state of water utilities, typical impact analysis and dependencies, as well as possible improvement needs of water utilities in Finland.

3.1. Interview and analysis method

We prepared the interviewees for the interviews by sending questions in advance. The interviews were recorded and conducted remotely. Due to some variation of the interviewees (background, organization size, job description), interview method is semi-structural theme interview, in order to allow free conversation and personal interpretation of questions. The analysis method used for interpreting the answers is qualitative analysis, divided according to the interview questions. We aim at finding common factors and reasons behind actions.

3.2. Interviewees and companies

Interviewees 1 and 2 are quality and environmental control manager and automation manager of a wastewater treatment service provider. Interviewee 3 is a CEO of a water utility company. Interviewee 4 is a CEO of a stock water company. Interviewee 5 is a representative of water service support company. Interviewee 6 is IT manager of a water supply company.

3.3. Interview themes and questions

The questions were formed according to themes, which handle companies’ resilience (incident preparedness), impact analysis and various types of dependencies of their facilities.

1. Risk classification, measuring effects and dependencies

a) Do you have a system to classify risks and their assets?

b) Do you use forecasts when defining risks and otherwise?

c) Do you measure impacts after some (cyber) incident or catastrophe has occurred either in own or in another company? If yes, using which kinds of models? (Notice: Mitigation is not part of impact analysis)

d) Do you measure dependencies between impacts (cascading effects)?

2. Follow-up and communication between other water utilities and other countries

a) Do you follow the state of other water facilities?

b) Is there some kind of information exchange system used for follow-up and communication?

c) Do you have connections to Sweden or other Nordic countries?

3. (Inter)Dependencies between own facility and other companies, dependency on office network

a) How do you see, in general, the dependencies between your own company and others (for example automation providers) in case something critical happens?

b) How is automation dependent on the office network?

4. Factors that can increase the incident effect

a) What kind of factors can increase the effect of the incident in your company (focus is on the cascading effects and dependencies, time horizon and factors that increase or decrease spreading of the incident's effect)?

Copyright © 2017, Infonomics Society

5. Supplementary issues, improvement suggestions

4. Interview results

In the following, we will present some citations (according to interviewee number, see 3.2.) and summary from the interviews according to each question. In order to maintain anonymity of the companies, we could not revel all details. Even though the results are somewhat generalized, they are still valuable in evaluating the current state of water utilities, and benefit general development of all CI field companies.

4.1. Risk classification, measuring effects and dependencies

- Classification of Risk

1. and 2. “There is a standard risk analysis matrix software for recognizing and classifying risks. The risk list updated on a regular basis.”

3. “We classify and recognize risks and their effects using Huovi portal’s risk analysis tools.”

4. “We use several risk-identifying and effect-assessing systems.”

5. “At the national level, there are general security strategies used which describe some general threats but there is not any special, systematic national-level risk analysis system available and the indicators are not fixed. Creating situation awareness of the current situation at national level is difficult, because the field is very heterogeneous: each water utility is a local unit in its county, and each handles risk management for themselves in their own way. Consequently, the threats for each might be different. Regarding impacts, it depends on what kind of impacts are considered; in case of health impacts, the requirements are derived from legislation.”

6. “We utilize ordinary risk management software. Main cyber risks are recognized, but there is a need for cyber risk section as its own subsection. Previously cyber threats have not been thoroughly considered and responsibilities for the matter have been unclear, but now there is strong emphasis on cyber risk management.”

Summary: All companies utilize risk analysis tool(s), either self-developed, or commercial off-the-shelf company-customized risk analysis system, thus the results are not directly comparable with each other. Some cyber risks are recognized, but in general, there is a strong and also acknowledged need to develop cyber risk management and responsibilities further. Not surprisingly, cyber risks have not been relevant for long, because the water utility systems have been relative closed systems. However, risk management and responsibilities directly related to automation are well handled.

- Forecasts

1. and 2. “We use Finnish Communications Regulatory Authority's Annual Report and it includes a yearly forecast. We have developed for example education and procedures against social engineering using the Annual Report as a guideline. In addition, there is a yearly provision training via Finnish Water Utilities Association (FIWA). Naturally, weather forecasts are utilized.”

3. “We utilize obvious forecasts, such as weather forecasts and calculate predictions, which may cause a need for additional duties and advanced operations. Finance is predicted, network renovation is also based on forecasts and statistics. We regularly review/update contingency plan: if something happens here or somewhere else, we assess how we should or would have acted.”

4. “Concerning the factors that affect functioning of the facility, (for example nature conditions), we assess situations that could occur and estimate values for these situations. Also, we use actual forecasts, to control the process.”

5. “Forecasts are not systematically used at national level. Some are used, for example by Ministry of Agriculture and Forestry, but they do not cover whole water utility branch.”

6. “There is not *regular* use of forecasts.”

Summary: Various forecasts are used: Finnish Communications Regulatory Authority's Annual Report, training via FIWA, weather forecasts, finance-related predictions, network renovation - affecting forecasts and statistics, as well as models of the production to control the process. Some forecasts are used at national level, e.g. from Ministry of Agriculture and Forestry.

- Impact analysis

1. and 2. “Cyber security impacts are not used as such. But security impacts we do assess, not directly measure. We use harmonized and customized standard, risk collection (matrix) from management risks to production risks.”

3. “Our aim is that we have to get things right in the process, so we do not generally calculate impacts. Financial impacts are calculated, such as costs of unscheduled water supply, but these kinds of impacts are marginal. We also recognize critical events and risks, which handle health and security/safety issues. Thus, we have normal risk assessment and critical target risk assessment.”

4. “We have certain statistics and effects calculated based on impacts. Based on statistics, we have calculated risks and risk management actions valued according to probability and financial effect, and decided, which risks should be minimized.”

5. “There is not any special impact analysis at national level.”

6. “Some scenarios are considered, but in general impacts are analyzed otherwise. Office network is separated from the production, so Denial of Service would not *directly* be a problem for production, but it would be a problem for email and reporting functions, therefore email is critical. In general, if network is unavailable, it is more of a reputation risk than production risk.”

Summary: Implied by [12], "impact analysis is the activity of identifying what needs to be modified in order to make a change, or to determine the consequences on the system if the change is implemented." One method to execute impact analysis is by making scenarios. According to the interviews, impact analysis is executed in each company, but the method is very dependent on the company itself. Some companies have considered cyber-threat related impacts, but mostly other kind of threat related impacts. In general, most impacts that are estimated are valued according to their probability and financial value. There is not any regular national-level impact analysis. In every facility, the automation network is separated from office network.

- Dependencies Between Impacts

1. and 2. “We set risk probability on one axis and risk influence on another. We assess the whole chain of risk effects and damages. The process is updated regularly, for example whether the minimization of the risk has progressed.”

3. “Things can occur simultaneously, even if there is no dependency. It can be a positive dependency, such as in case of ultimate power failure, there is no need for water except toilet and drinking. As we are physically attached to other communes, we need to think ourselves as a part of an operating sequence: if water is contaminated in one commune, all the other communes need to be informed. Social media can spread panic even if there is nothing wrong with our water. We exchange quality results of water between communes by email and we inform stock water company about problems and it informs other companies.”

4. “Dependencies are considered very thoroughly and they are most essential for production implementation and especially water supply to succeed. Risks can be cumulated which can have effect on functions outside company. We consider dependency issues also during co-operation events organized by National Emergency Supply Agency together with other parties.”

5. “At national level it is acknowledged that the dependencies should be recognized in end-to-end water supply chain. Some situation awareness is built. General resolutions for the possible threats have been sought and recommendations for the water companies are given.”

6. “Probabilities of the dependencies have not been calculated.”

Summary: Companies recognize the importance for defining dependencies between impacts locally and also within national water supply chain. Some situation awareness is gained and some general resolutions as well as recommendations for the possible threats have been sought.

4.2. Follow-up and communication between other utilities and other countries

- Other Water Utilities in Finland

1. and 2. “Some follow-up with other companies exists, such as education, seminars, networking opportunities and visits. Maybe FIWA could be even more active in organizing events and enabling communication.”

3. “We do not have any especial follow-up or communication with other facilities.”

4. “Because our systems in production chain in general are very different compared to others, it is quite difficult to generalize the results, enabling cases to be utilized in other systems. However, we do stay in touch with other actors.”

5. “We have some co-operation with other companies within benchmarking duties.”

6. “There is no special information exchange between ICT units. We have acknowledged the need for this lately, ICT communication should be increased between cities. Production sections communicate a couple of times per year.”

- Nordic Countries

1. and 2. “Some communication to Sweden and other Nordic countries exists, such as visits, but there is nothing regular. There could be more communication, for example some forum. FIWA gathers information and communicates to its members. Projects such as UPC/IVAMO gather 20 sewage handling facilities as a Baltic sea area forum.”

3. “We communicate via FIWA: it communicates to Sweden and us, otherwise it would be impossible for us. There used to be more active communication to Estonia and Baltic countries before. In Finland

Swedish-speaking cities are more active because of the language."

4. "We do not have much co-operation with Sweden, but a bit more with other Nordic countries."

5. "In a pool level there is co-operation with Sweden."

6. "There is not regular communication between Nordic countries and Finland, except yearly common meetings. There is no alarms information exchange. It must be noted, that water industry, compared to electricity industry, has just awaken to realize that these things have to be considered. There is definitely a need also for increased communication between European facilities and Finland."

Summary: Surprisingly, more communication seems to exist between Finnish companies and Sweden or other Nordic countries, than between companies in Finland. Co-operation seems to require some kind of facilitator, forum, possibly tools enabling information flow. Naturally, there is an issue of how much potentially company-vulnerable information should be revealed - especially in case of incidents. Nevertheless, cyber threats will increase and there is definitely a need for systems enabling communication, but also trust between companies.

4.3. Dependencies between own facility and other companies (e.g. automation providers), dependency on office network

1. and 2. "We are very dependent on industrial automation providers, our whole logic concerning maintenance is based on this. Agreements define response times for critical or normal response. Automation and office network are separate, but we are of course dependent on telecommunications equipment that make up our networks."

3. "Everything is mechanic, there is not much automation. We can work by hand at the location. We keep spare parts available, availability is critical because we do not produce spare parts. We can bypass automation if necessary. There is no dependency on the office network."

4. "Dependency to automation providers is very essential factor and we constantly develop connections. Automation and data connections have been doubled and backed up by emergency power supply. Because we have geographically vast function area and small personnel unit, automation is very critical. Office network is separated, we can check automation history database from it but cannot make any changes through it."

5. "At national level some dependencies are covered, but there is no systematic covering follow-up."

6. "There are quite a few dependencies. In this field, one risk is that automation providers have remote communication, including remote supervision to facilities and these communications are not properly reviewed (they can be according to automation provider's terms). Our aim is to define conditions for remote connections in our agreements. Furthermore, there should be stronger cyber security -related requirements and practices for IT providers. IT providers are a potential risk as well, as we are dependent for example on our firewall provider for the public network. Similarly, data connection provider is a dependency, but the critical points are backed up by other operators."

Summary: Depending on the facility, there are dependencies of automation providers from high level to none. The remote communication that automation providers use is recognized as a risk, as many functions and supervision can be used via it. Therefore, Service Level Agreements and responsibility division in agreements have an important role of how great a risk the dependency possesses. However, it is not always a case that agreements are up to date, in some of the respondent companies the agreements should have been written more in detail. It must be noted that critical communications' dependency on communication provider however is in all cases considered and managed properly.

4.4. Factors that can increase the incident effect

1. and 2. "Communication can add to the damage effect of incident, for example in case of an environmental or person-related incident. If false information goes out, there can be substantial damage to image and managing this is a challenge. Communication with service providers can be critical, as they are in charge of the maintenance. If communication breakdown should occur, it may add to the incident effect, in case there is obscurity concerning the state of the process. Internal and external communication are both critical."

3. "If the worst happens outside working hours or during holidays, there may be only one person on duty, who has a huge responsibility in assessing the situation. Web pages or email can be down, phone lines can be stuck, it might be impossible to update the web pages ourselves because they are city-owned, so we have to contact someone from the city at first to get the front page updated. Social media helps, Facebook and Twitter have had huge effects. The problem is still how to manage the coordination of the incident handling and communication chain, especially with the authorities, at the same time. Additionally, in case of understaffing, it is difficult to gain situation awareness, especially if the certain

required expert is not at work. Incorrect communication and canards make lots of damage and correcting it takes a lot of time that is away from correcting the actual issue. Media expects information fast, and the person responsible for the communication has to be convincing to the media. Reputation and credibility are difficult to restore."

4. "If there are more serious disturbances to water supply, operations model can be easily identified, however, because our operations area is very vast, there are interfaces not operated by us. Information flow is a very essential factor. Even if we had clear instructions for reporting and communicating out, there can always be disinformation occurring along the communication path. Because of the vastness and distribution of the operation area (dependency on other actors), handling of incidents can be challenging. Nevertheless, we can easily verify what kind of damage concerns our own system. Still, during incidents, deep and accurate communication between neighboring counties is required, in order not to actually increase the damage."

5. "Most of all the incidents depend on time factor. In other words, when does the incident occur."

6. "Internal communication is critical. If there are changes to data systems in one department, does the information about changes reach other departments? These kinds of issues may threaten cyber security especially in larger organizations. There may occur coincidences that emphasize this, this is why cascading effects and dependencies should be recognized."

Summary: Some factors are repeated in all answers. Communication, both internal and external, is very critical. It plays a big part of how much the incident has effect on the company. It is important that information about changes that affect security is reaching everyone in the company. Larger facilities are especially threatened by the information shortages. Coincidences emphasize the threat. Because of these kinds of interconnections, that may affect the incident in an unexpected and magnifying manner, it is crucial to recognize and define possible dependencies and cascading effects. Lacking or incorrect communication can increase the damage effect, for example via reputation loss.

4.5. Additional issues, improvement suggestions

1. and 2. "Incidents may often cause severe damage, therefore we aim at strong risk mitigation and short recovery time."

3. "We rarely assess costs of repair, rather, we estimate how many are without water and its effect. Otherwise, cyber security is less assessed, health impact is the most important impact."

4. "We aim to improve and clarify interfaces near the customer, and clarify responsibilities of the interfaces."

5. "There is a need for system that builds systematic situation awareness nationally, but this is very challenging. Internationally, it would be good to share information about practices in case of an incident and best practices in general."

6. "Officials could set even more requirements, because this is what usually motivates to improve cyber security, in all areas. Internal requirements do not necessarily cause such motivation. Proactive action is better than active.

Summary: One detail revealed in the interviews is, that often the triggering factor for improvement actions, for example for cyber security awareness and protection, becomes ultimately from officials - there is no motivation to improve things until compulsory. On the other hand, definers of cyber security requirements for the organization should take into account that implementation of the cyber security related requirements is not often done by security professionals. Importance of clear interfaces and responsibilities for strong risk mitigation and short recovery time was emphasized, as there are several actors in the production chain.

5. Discussion

In the future, the five major challenges concerning Finnish water supply services will consist of 1) aging infrastructure, 2) vulnerability and risk management, 3) human resources and maintaining knowledge, 4) research and 5) education [9]. From our interviewees' point of view, the problems were somewhat similar. In the following, we summarize the most important findings of the interviews. We also try to resolve possible methods for the problem fields mentioned in the interviews, in the light of the major challenges.

5.1. Summary of the most important findings

The main findings of the interviews are that in general, companies assess security impacts properly, but there is a clear lack of cyber security impact assessment. Companies estimate cascading effects and dependencies between impacts, and they also recognize dependencies to subcontractors, such as industrial automation providers. In order to diminish the impact of the incident, there is a great need for clear and unambiguous communication and reporting, both internally and externally. The importance of clear interfaces and responsibilities is also emphasized, especially during incident, because there can be several actors in production and supply chain. Cyber risks are not considered thoroughly. One development area is to integrate cyber risk management into recently very well managed automation-related risk management.

In addition, there is a need for system, methods or tools that build systematic situation awareness at national level and locally. Finally, companies recognize that there should be more communication between different actors in Finland especially regarding ICT section, and generally between Nordic and European countries.

5.2. Cyber security risk management

Cyber incidents are increasing. Channels that the malicious software use for contamination of and spreading between systems are more and more imaginative. CIs are the backbone of the society and they need to act proactive when security of their system is concerned. In order to help manage cyber security of a water utility, there are several administrative and technical models. One such a model is cross-organizational cyber incident management for national CIs [13]. In order to help recognizing high priority protection areas in CIs, one can use for example listings such as of [14]: governance and security management, secure network architectures, self-healing, modeling and simulation, wide-area situational awareness, forensics and learning, and trust management and privacy. These can be of guidance when analyzing how to improve the state of a CI.

There are several methods available in literature, but the problem is that these are often lacking concrete results and proven effects. An ideal method would combine cyber and physical risk and threat analysis, and would incorporate automation personnel together with cyber security professionals, utilizing both groups' expertize. The process would rather be iterative, in so that when yielding results, these results would act as input when producing a new iteration.

5.3. Security from a cyber-physical system point-of-view

Water utilities are cyber-physical systems. "*Cyber-Physical Systems* (CPS) are integrations of computation with physical processes. Embedded computers and networks monitor and control the physical processes, usually with feedback loops where physical processes affect computations and vice versa." [15] As there is a need for the beneficial combination of handling both physical and cyber threats, it is worthwhile to discover the approaches that combine both worlds, that is, *cyber-physical security*. An interesting method towards cyber-physical threats is presented in [16]. Despite this work handles threats targeting smart grids, which are (yet) relatively more digitalized systems than water ecosystems, we can still use it as a motivation for improving security of water utility industry, especially considering future, more digitalized water ecosystems. The idea is that neither the cyber security precautions nor system theory approaches are enough, when trying to accomplish total security of the system, but there is a need to combine both analysis. The reason behind this requirement is to achieve as encompassing security as possible. Cyber security cannot provide analysis of the possible consequences of the attacks on physical systems, whereas system theory, concerned with performance, stability and safety of physicals systems, cannot provide complete modeling of the IT infrastructure. [17] Some approaches are concentrated to study the cyber-physical aspect of water ecosystems. One lesson learned is that the water industry would benefit from the use of remote, ubiquitous sensing combined with data analysis, thus enabling decision-making when responding to cyber threats [18]. A different point-of-view, a modeling framework for characterizing the effect of cyber-physical attacks on the hydraulic behavior of water distribution systems, is presented on [19].

5.4. Dependencies management

Dependencies management refers mainly to management of subcontractor agreements and the lifecycle of that agreement implementation. Dependencies are also technical interfaces to other systems, which also have to be well managed. An administrative approach to dependencies management is that apart from devising SLAs that are more concrete with subcontractors, one solution could be to demand certificates or compliance to qualitative standards. A technical approach to dependencies management could be to audit system against technical standards such as Common Criteria [19].

A dedicated method for dependencies management is presented in [20], in which the dependence of different critical infrastructure areas on each other is studied by quantifying the effects. The authors note that it is crucial for critical infrastructure operators to recognize the failure periods after which the effects of the dependencies become significant. Quantifying the dependencies over time would enable eventually finding these time limits.

5.5. Lack of situation awareness

The study of [7] have analyzed critical infrastructure situation awareness, concentrating on electricity distribution, telecommunications area and rescue services. The challenges they have recognized for situation awareness for all aforementioned areas are contingency management, provision of critical situations, prioritizing and synchronization of actions with co-operative directions. We have discovered similar findings in our interviews. It is crucial to define the term “situation awareness” and its meaning for the water utility. In practice, what is the timeframe between “snapshots” that is required to achieve a proper understanding of the system state. If the timeframe is too narrow, there is a risk of losing essential data within all data mass. Considering cyber risk awareness, for example a yearly larger revision consisting of asset management, along with some smaller, more often occurring check-ups is one option. For building situation awareness, there are also methods such as [21].

5.6. Unclear reporting and ambiguous communication

One part of functioning (cyber) security reporting and communication, both internally and outside the company, is that information is correct and up-to-date. To have a seamless and well-defined processes help in defining responsibilities and actions. The processes should also define cyber security -related responsibilities of all the interest groups. For instance, company should require subcontractor that manages the network to report short summary of occurred incidents on a regular basis (monthly), and make a larger conclusion less frequently (annually). Regarding the technical aspect, communication enabling and decision supporting tools could help in the communication process inside and between organizations. Naturally, all the solutions that help in clarifying and visualizing cyber security issues are beneficial.

5.7. Co-operation enablers

We consider co-operation enablers especially through the role of spreading awareness and educating about incident preparedness by bringing together all necessary parties. Considering the future of water ecosystems, it is utmost important to strengthen cyber incident awareness as well. Openness and co-operation add to trust, and may prevent further damages, such as incident cascading. National-level administrative associations offer information and support co-operation. European-level organizations, such as EurEau, have a significant role in strengthening the co-operation and enabling communication activities and information flow among and between European countries. Thus, European-level organizations should be considered not only as co-actors with, but also as facilitators of national administrative associations.

EU will affect the co-operation enablers with the Directive 2016/1148 [11] by “creating a Cooperation Group in order to support and facilitate strategic cooperation and the exchange of information among Member States“ and “creating a computer security incident response teams network (CSIRT)”. ´The directive will also “lay down obligations for Member States to designate national competent authorities, single points of contact and CSIRTs with tasks related to the security of network and information systems”. This means it can also support implementation and putting into the action the work of the administrative parties. The outcome of their work could be arranging regular meetings or workgroups concentrating to a certain problem. Workgroups could benefit significantly when combining forces with the research community, for example, consulting expertise from the cyber security field.

5.8. Education and tacit knowledge

High quality education is important for the development of water utilities, in a sense that when education is considered attractive, the motivation of future employees will be high [9]. In a next couple of years, a large part of professional employees of water utilities will be retiring in Finland, and a major risk is, that tacit knowledge is lost along these professionals [9]. Maintaining that tacit knowledge is a challenge, but also a great opportunity when the knowhow of these professionals could be utilized properly in education. Similarly, as the working environments of CIs will be even more dependent on the networks in the future, the importance of cyber risk education embedded within the curriculum cannot be deeply enough stressed.

5.9. Future work

Future work consists of applying methods for minimizing the problems that were discovered in the interviews. There are a vast collection of methods and approaches, which could be utilized either one at a time, or combining some of them. The problem is not that much about which method to choose, but rather if the method is applied in a systematic and iterative manner, and whether cross-disciplinary expertize is used where needed.

Managing cyber security is not an easy task. For a facility with a small number of employees, it can be hard or impossible to follow regularly practices required for a good level of cyber security or for detecting incidents. Rather than keeping each to their own, water utilities as a CI need co-operation, openness and awareness.

6. Conclusions

In this paper, we presented results analyzed from the interviews of water utility companies. Themes of the interviews concerned resilience for and dependencies of incidents. Interview themes also included the question of impact analysis, in other words how the companies estimate or measure the effect of cyber and other incidents on their operation. We focused especially on factors of impact analysis, cascading effects and dependencies. The most important conclusions from the interviews were that companies mostly use effective impact analysis method and recognize some dependencies and cascading effects, but there is a need for:

- clear and unambiguous communication and reporting, both internally and externally in order to minimize incident impact,
- unambiguous interfaces and responsibilities for the several actors in production and supply chain,
- methods and tools for situation awareness, both on national level and inside companies, to minimize the cascading of the impacts,
- co-operation locally and internationally - especially regarding ICT section - and enablers for this: facilitator, forums, even a communication system
- clear responsibilities and management in cyber risk area, and
- cyber risk education and awareness

National and European legislation will put more pressure on implementing risk-based approach in critical infrastructure, especially concerning cyber risk management. For water industry, this will mean it has to take new approaches to keep up with requirements, as well as technical risks posed by constantly renewing cyber threats. However, administrative parties are also obligated to help CIs in the process of implementing cyber security. We have proposed several methods and techniques to be implemented in water utilities, enabling to overcome challenges posed by cyber risks. Further work consists on applying one or some of them and analyzing the concrete effect on the company.

7. References

[1] J.P. Farwell, and R. Rohozinski, "Stuxnet and the future of cyber war", Survival 53(1), 23–40 (2011), http://dx.doi.org/10.1080/00396338.2011.555586

[2] V. Woollaston, "WannaCry ransomware: what it is and how to protect yourself", http://www.wired.co.uk/article/ wannacry-ransomware-virus-patch (Access Date: 5 December 2017)

[3] E. Luiijf, A. Nieuwenhuijs, M. Klaver, M. van Eeten, and E. Cruz, "Empirical findings on critical infrastructure dependencies in Europe", pp. 302–310. Springer Berlin Heidelberg, Berlin, Heidelberg (2009), http://dx.doi.org/10.1007/978-3-642-03552-4_28

[4] S.M. Rinaldi, J.P. Peerenboom, and T.K. Kelly, "Identifying, understanding, and analyzing critical infrastructure interdependencies", IEEE Control Systems 21(6), 11–25 (Dec 2001)

[5] T.D. O'Rourke, Critical infrastructure, interdependencies, and resilience. BRIDGE-WASHINGTON NATIONAL ACADEMY OF ENGINEERING- 37(1), 22 (2007)

[6] J. Moteff and P. Parfomak, "Critical infrastructure and key assets: Definition and identification", (2004), http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA454016

[7] S. Horsmanheimo, H. Kokkoniemi-Tarkkanen, P. Kuusela, L. Tuomimäki, S. Puuska, and J. Vankka: "Kriittisen infrastruktuurin tilannetietoisuus (critical infrastructure situation awareness)" (in finnish), (2017)

[8] L. Lääperi, L. Rummukainen, and J. Vankka, "Kriittisen infrastruktuurin tilannekuvajärjestelmä" (in finnish), Tiede ja ase 72(1) (2015), https://journal.fi/ta/article/view/50158

[9] P. Silfverberg: Guidelines of water and wastewater services for 2020's (in finnish), Publication series of Finnish Water Utilities Association number 44. Helsinki, 2017.

[10] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the quality of water intended for human consumption (recast) COM/2017/0753 final - 2017/0332 (COD) 1st February 2018.

[11] DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

[12] P. Jönsson, and M. Lindvall, "Impact analysis", pp. 117–142. Springer Berlin Heidelberg, Berlin, Heidelberg (2005), http://dx.doi.org/10.1007/3-540-28244-0_6

[13] G. Settanni, F. Skopik, Y. Shovgenya, R. Fiedler, M. Carolan, D. Conroy, K. Boettinger, M. Gall, G. Brost, C. Ponchel, M. Haustein, H. Kaufmann, K. Theuerkauf, and P. Olli, "A collaborative cyber incident management system for european interconnected critical infrastructures", Journal of Information Security and Applications pp. – (2016), http://www.sciencedirect.com/science/article/pii/.

[14] C. Alcaraz, and S. Zeadally, "Critical infrastructure protection: Requirements and challenges for the 21st century", International Journal of Critical Infrastructure Protection 8, 53 – 66 (2015),

http://www.sciencedirect.com/science/article/pii/S1874548214000791

[15] Lee, E. A. (2008). "Cyber physical systems: Design challenges." 2008 11th IEEE Int. Symp. on Object Oriented Real-Time Distributed Computing (ISORC), IEEE, New York, 363–369.

[16] Y. Mo et al., "Cyber–Physical Security of a Smart Grid Infrastructure," in Proceedings of the IEEE, vol. 100, no. 1, pp. 195-209, Jan. 2012. doi: 10.1109/JPROC.2011.2161428

[17] Z. Wang et al., "Cyber-physical systems for water sustainability: challenges and opportunities," in IEEE Communications Magazine, vol. 53, no. 5, pp. 216-222, May 2015. doi: 10.1109/MCOM.2015.7105668

[18] R. Taormina and S. Galelli and N. O. Tippenhauer and E. Salomons and A. Ostfeld , "Characterizing cyber-physical attacks on water distribution systems", in Journal of Water Resources Planning and Management, vol. 143, no. 5, 2017. doi = {10.1061/(ASCE)WR.1943-5452.0000749

[19] Common Criteria for information technology evaluation. https://www.commoncriteriaportal.org/

[20] A. Laugé, J. Hernantes, and J.M. Sarriegi, "Critical infrastructure dependencies: A holistic, dynamic and quantitative approach", International Journal of Critical Infrastructure Protection 8, 16 – 23 (2015), http://www.sciencedirect.com/science/article/pii/S187454821400081X

[21] G. Settanni, Y. Shovgenya, F. Skopik, R. Graf, M. Wurzenberger, and R. Fiedler, "Correlating cyber incident information to establish situational awareness in critical infrastructures", 2016 14th Annual Conference on Privacy, Security and Trust (PST). pp. 78–81 (Dec 2016)

8. Acknowledgements

The authors would like to thank all the respondents for their contribution, which has been crucial for this work to succeed.