Informaatioteknologian tiedekunnan julkaisuja
No. 56/2018

Jouni Pöyhönen

Cyber security in the management of an electricity company

JYVÄSKYLÄN YLIOPISTO

Informaatioteknologian tiedekunnan julkaisuja
No. 56/2018

Editor: Pekka Neittaanmäki
Covers: Petri Vähäkainu ja Matti Savonen

ISBN 978-951-39-7543-2 (verkkoj.)
ISSN 2323-5004

Jyväskylä 2018

Cyber security in the management of an electricity company

2. edition

Jouni Pöyhönen
University of Jyväskylä
jouni.a.poyhonen@jyu.fi

Abstract

The functioning of a modern society is based on the cooperation of several critical infrastructures, whose joint efficiency depends increasingly on a reliable national electric power system. Reliability is based on functional data transmission networks in the organizations that belong to the power system. Furthermore, reliability is linked to the usability, reliability and integrity of system data in the operating environment, whose cyber security risks are continuously augmented by threatening scenarios of the digital world.

In Finland, the production of electricity is in various ways decentralized, which contributes to the reliability of the power system. Finland has about 120 enterprises that produce electricity and about 400 power plants, in which electricity is produced using various production methods. Power system process control is highly automated and networked. This report focuses on the procedures applied to cyber security management in the processes of electricity companies, whereby different standards will also be utilized.

The major contributions of the article are that it integrates cyber security management and risk analysis into the process structures of individual electricity companies and that it utilizes the PDCA (Plan, Do, Check, Act) method in developing a company's cyber security management practices.

In order to put the measures into practice, the leadership of an electricity company must regard trust-enhancing measures related to cyber security as a strategic goal, maintain efficient processes and communicate their implementation with a policy that supports the strategy.

Keywords

Critical infrastructure, Electricity company, Cyber security management, Trust

Paper type

Research paper

1 Introduction

Finland's electric power system – comprising power plants, a nationwide transmission grid, regional networks, distribution networks and electricity consumers – is part of an inter-Nordic power system together with the systems of Sweden, Norway and Eastern Denmark. In addition, there are direct current transmission links to Finland from Russia and Estonia in order to connect the Nordic system to the power systems of Russia and the Baltic countries. The inter-Nordic system is furthermore connected to the system in continental Europe via direct current transmission links. Fingrid Plc. is responsible for balance management, in other words, for maintaining the momentary power balance between power production and consumption in Finland. Monitoring as part of balance management is handled round the clock at the Fingrid Main Grid Control Centre in Helsinki. Within the inter-Nordic system, the main purpose of balance management is to maintain the frequency of the power system, which represents the balance between electricity production and consumption. The better the balance is maintained, the less the frequency varies and the better the quality of electricity is. [3]

Electricity is produced at Finnish power plants in various ways, using several energy sources and production methods. The major sources of energy include nuclear power, hydropower , coal, natural gas, wood fuels and peat. In addition to the sources of energy, production can be classified according to the production method. In Finland there are about 120 enterprises that produce electricity as well as around 400 power plants, over half of them hydroelectric power plants. Nearly a third of the electricity is produced in connection with heat production. Compared with many other European countries, Finland's electricity production is decentralized. A diverse and decentralized electricity production structure increases the security of the national energy supply. [4]

The functioning of a modern society is based on the cooperation of several critical infrastructures, whose joint efficiency depends increasingly on a reliable national electric power system. Crucial in the cyber environment are functional data transmission networks and the usability, reliability and integrity of system data in the operating environment, whose cyber security risks are continuously augmented by threatening scenarios of the digital world. A modern society depends entirely on a cyber environment that provides dynamic services.

In Finland's Cyber Security Strategy, the cyber environment (domain) is defined as an electronic information (data) processing environment that consists of one or more information technology infrastructures. According to the Strategy, cyber security refers to a desired end state in which the cyber environment is reliable and in which its ability to function is ensured. Critical infrastructure, furthermore, refers to the structures and functions that are indispensable for the vital functions of society. They include physical facilities and structures as well as electronic functions and services. [16]

The global threats within the cyber environment have remained at a high level over the past few years, as stated in the annual international business world surveys by the World Economic Forum. They are seen to be among the major global threats based on the probability and impact of their realization. [18]

This finding by the World Economic Forum is supported by continuous news in different media that shake our trust in cyber security. For example, an extensive cyberattack to the power grid caused power failures in Ukraine in December 2015 [8].

The electric power system with all its components belongs to critical national infrastructure: it is vital for the operations of the country and its outage or destruction would weaken national security, the economy, public health and safety as well as make the operations of state administration less effective.

The criticality of the power system is expressed clearly in the seminar presentation 'The power system as a basis for a functioning society' (Sähköjärjestelmä yhteiskunnan toimivuuden perustana) given by the former chief executive officer of the National Emergency Supply Agency. The table below is an extract from the presentation. It describes the effects of a power failure on the operations of society as a function of the duration of the failure. Endangered cyber security has been regarded as one of the most significant threats to the functioning of energy supply and energy networks. [10]

Interruption time	**Consequences**
1 second	Sensitive industrial processes may stop. Data in information systems may be lost.
1 minute	Some industry and hospital processes will stop.
15 minutes	Shops will be closed. The failure may harm people's daily activities and cause traffic delays.
2–3 hours	Industrial processes may undergo significant damage. Mobile phone networks will face problems. Domestic animal production will be disturbed.
12–24 hours	Water supply to homes and offices will stop. Buildings will start to become cold in the winter. Frozen goods will begin to melt.
Several days	The operations of society will be seriously harmed. Industry and services will not function. Workplaces and schools will be closed. Buildings will suffer from frost damage.

Table 1. The consequences of power failure [10]

Because the electric power system provides a basis for almost all services in society, its operation must be as uninterrupted as possible. Even short power failures are broadly visible as disturbances in other critical services. Therefore, achieving and maintaining a high availability level in the operation of various processes within the power system is the primary goal of the organizations responsible for them. For this purpose, the continuity of operation must be ensured and recovery from disturbances must be quick. Creating and maintaining situational awareness related to cyber security in individual organizations play a key role in these activities. Controlling process operations and taking coordinated situation-specific decisions call for real-time,

comprehensive situation awareness regarding the organizations' cyber readiness and the factors that affect it in a dynamic operating environment.

A diversified and decentralized power production structure increases the national security of power supply. Considering cyber security in the different parts of the infrastructure further enhances trust in the services of our society.

The national significance of an electric power system is very similar irrespective of the country. For example, in the United States the power system is considered to be a critical infrastructure and a key resource for the functioning of the entire society. The basic structures of the power system are similar to those in Finland. However, in the USA the structural and technical implementation of grid load balance management differs significantly from the corresponding procedure in Finland. Grid management has traditionally been affected by administrative regulation, and an individual electricity company has owned a broad regional production and distribution chain through vertical integration. The electricity company has thus been in charge of power production, transmission and distribution to consumers. The deregulation that has occurred in the past two decades has increased the number of companies in the field, particularly in transmission and distribution, and thus led to the abolishment of vertical integration. As a consequence, competition between enterprises has increased. These events have brought challenges to grid balance management. In the USA the aim is to perform balance management by directing production to consumption in different parts of the grid. This is done by balancing the sums of input and output currents at nodes, in accordance with Kirchoff's circuit law. In the USA it can be seen that the grid represents a technologically highly advanced system entity and that its solutions call for the use of the most demanding technologies. Grid technology and its control procedures constitute the principal areas in examining cyber security. [13]

This article focuses on factors related to cyber security management in an individual electricity company that is part of Finland's power system. We will also examine how these factors are taken into account in the company's process structures while creating trust in its operation within a dynamic cyber environment.

2 An electricity company's cyber environment and its main cyber security threats

2.1 The structure of an electricity company's cyber environment

The transmission network of Finland's power grid is owned by Fingrid Plc. The distribution network consists of dozens of enterprises, and electricity is produced by about 120 enterprises and 400 power plants in different parts of the country. The system structure is thus highly decentralized, and there is no comprehensive vertical integration of ownership in the Finnish power system. Every company is responsible for managing its own working processes. Balance management in the Finnish system, however, is centralized, which also compensates for the benefits of vertical integration in system management and control. From the perspective of the entire power system, the major threats to physical safety and cyber security concern the transmission and distribution networks, switching and transforming substations, and power plants. A decentralized structure limits the potential consequences of these threats in the power system. On the other hand, decentralized electricity production requires good overall management of the system, effective distribution systems in the electricity companies as well as the capability to manage and control power plants. The companies that own power plants must also have a well-functioning logistics control system. The aim is to optimize the size of raw material stocks in each power plant according to their consumption as cost-effectively as possible. Therefore, the correct timing of raw material deliveries plays a significant role for the continuity of production.

The general networks and working processes involved in the operation of an electricity company can be illustrated with a logistics framework that comprises a supplier network, a production process, a client network, and information and material flows that connect them. Information technology (IT) systems are part of a company's infrastructure and thus constitute a significant part of the operations that support a company's core processes. Corporate-level IT systems are related to administration and to the management of information and material flows in the network. The production level includes industrial automation systems (industrial control systems, ICS). Figure 1 presents the structure of a company's logistics framework and common IT and industrial automation systems.

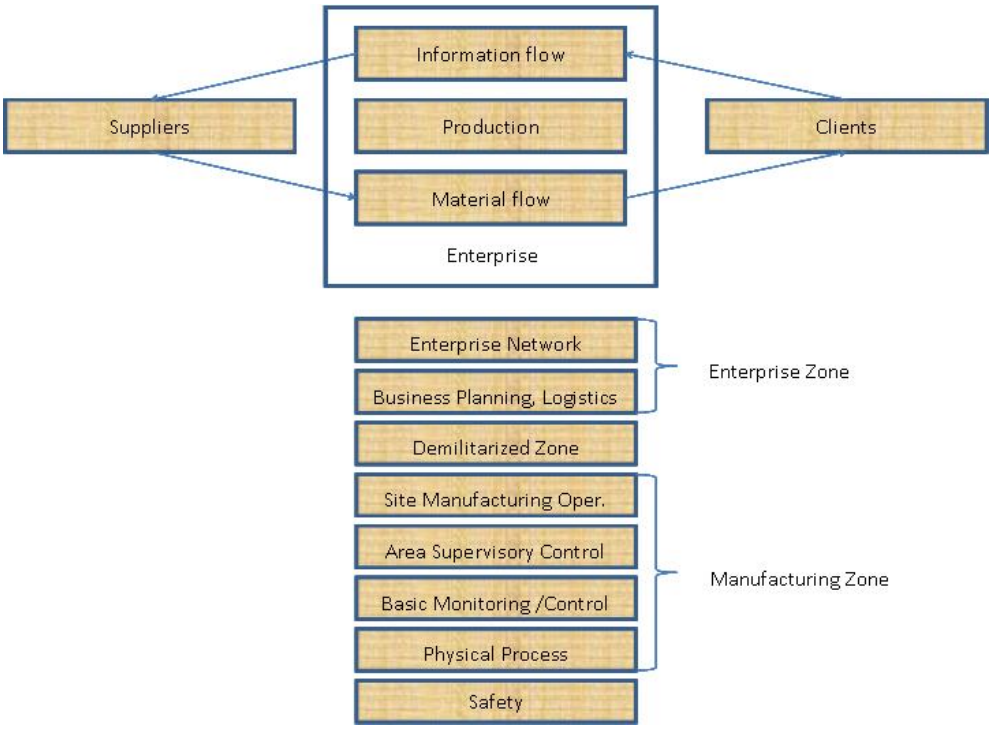

Figure 1. The logistics framework of an electricity company (adapted) and common IT and industrial automation systems [1 adapted; 11]

The highest levels of IT system hierarchy include the general information systems of administration and the enterprise resource planning (ERP) system. The top level of a typical ERP system includes overall process management by, for example, guiding the production volume. It also covers the restocking of raw materials, storing, distribution, payment traffic and human resources. If needed, between ERP software and control rooms there may be a manufacturing execution system (MES), which makes it possible to transfer the information obtained from the control room to the ERP system.

The industrial automation systems of production within an electricity company comprise their own hierarchy levels. Topmost of them is the control room, from which the operation of the entire process is presented to the supervisors in graphic form. Based on the information, process alarms are handled and the operation of the process is monitored and controlled. The next level consists of process stations, which house devices for process control, measuring and regulation. The same level also includes the actions taken to monitor faults and interferences in devices. The lowest level comprises the field equipment used to control and monitor process actuators and to gather measurement data.

2.2 The main threats to cyber security in an electricity company

When evaluating the role of electricity production systems in the cyber world as well as the factors that affect their cyber security, it is of primary importance to be aware of the most central features of the systems. For instance, the distributed industrial automation systems used in controlling production processes can be characterized by saying that their operation is highly established and that their life cycles are long compared with other IT systems in a company. The life cycles of industrial automation systems can even be several decades, as far as the basic systems are concerned. Moreover, the structure of the basic systems is changed infrequently. The changes are mainly carried out as system life-cycle updates in connection with larger maintenance or alteration works. The resources of industrial automation systems are also restricted, which is why it has not been possible to use typical technological information security solutions or cryptographies in them. Their user organizations are properly trained for their tasks and thus familiar with the devices as well as with the operating principles and operating environments of these devices. The data warehouses of industrial automation systems chiefly include process data, whereas administrative IT systems commonly include confidential business information. Unlike in administrative IT systems, no direct connection to the internet is usually needed in industrial automation systems. In the latter systems, IT devices are not used for purposes other than their decentralized tasks within the production process, its measurement and control tasks, and security functions. The monitoring of operations and staff in industrial automation systems is strictly controlled because of, for example, the availability and safety requirements of process operation. [5]

The aforementioned IT and industrial automation systems are part of the common cyber world, in which the primary risks are related to the loss of money, sensitive information and reputation as well as to business hindrance. Security solutions are hereby the key elements in risk management. The vulnerabilities behind the risks can be analysed as insufficient technology in relation to attack technology, insufficient staff competence or inappropriate working methods, deficiencies in the management of organizations, and lacks in operating processes or their technologies. The most common motives of attackers are related to the aim of causing destructive effects on processes, making inquiries about process vulnerabilities, and anarchism or egoism. These attacks can even be carried out by state-level actors, but perhaps most commonly by organized activists, hackers or individuals acting independently. [12]

Harmful measures to the systems of an electricity company can be implemented by foisting mal- and spyware into the systems utilized by the staff; or they can include intruding or network attacks via wireless connections or the internet. The intruders' goals may be related to the prevention of network services, the complete paralyzation of operations, data theft or distortion, and the use of spyware. Components pre-infected with so-called backdoors or the programming of components intentionally for the purposes of attackers is also increasingly common in today's cyber world. [12]

In the USA the security threats to the electric power system concern power plant logistics. They involve interfering and harming raw material supply routes, doing physical damage to transmission and distribution networks as well as to the transformer and switching substations between them, or performing cyberattacks against the control and regulation systems of the power grid. [13]

Protecting the power system against threats implies measures taken based on risk assessment, and they ensure the availability of primarily digital information in the operating processes being examined. The measures are highly significant for the overall availability of the systems that support the processes. Availability plays a key role in achieving business results and promoting the reliability of activities. Further central goals include the reliability and content integrity of information within the processes and used by the processes. Overall trust should be built from these starting points, based on the target organization's realistic idea of its own capabilities to reliably manage the challenges involved in operations within the cyber world. The following section addresses the significance of trust in the cyber environment for the operations of an electricity company. Moreover, trust-enhancing measures applicable to a company will be mapped.

3 Trust in an electricity company's cyber security

3.1 The significance of trust for cyber security

Trust in the operation of organizations and its continuous maintenance with effective measures are central factors affecting cyber security. Security is based on trust. Without trust there is no security, and vice versa. It is also good to be conscious of the fact that perfect safety is in general hardly achievable, and this

also applies to the cyber world, which is a dynamic environment difficult to anticipate. Therefore, it is particularly important to understand the great significance of trust in the cyber world and its security. The role of measures enhancing trust is emphasized. When we build operations in the cyber world on a foundation that is as sustainable as possible, we can utilize the diverse opportunities it offers. [15]

Finland's national cyber security strategy highlights the need to increase general cyber trust throughout the entire society. The strategy underlines the role of authorities, but at the same time it notes that in practice most production and service provision with bearing on the national product comes from the private sector. It further states that cooperation between the public and private sectors is an indispensable prerequisite for achieving the goals of the strategy. Citizens' activities also play a key role in enhancing security. An increase in citizens' cyber competences is immediately visible as competence at work and as other daily IT skills. Measures that promote a balanced cyber trust in all sectors of society improve the possibilities for safe operation in an information society, produce shared added value as well as ensure and increase the operational preconditions of both the public sector and the business sector. The strategy emphasises that all actors, from individuals to enterprises and public administration, are responsible for their own preparedness for cyber threats. Education and research also occupy an important role in maintaining and developing cyber security and in disseminating information throughout society. [16]

The ISO 9000 Standard states that an organization achieves success by acquiring and maintaining the trust of clients and other relevant interest groups. Understanding their present and future needs contributes to the organization's continuous success. The standard includes the central concepts of quality management and the principles for building trust. It can be applied by organizations that pursue ongoing success in their operation by utilizing a quality management system of their own. The quality of an organization's products and services is determined by how its clients experience that their needs and expectations are met. Clients also look for guarantees on the organization's ability to systematically produce products and services that correspond with their requirements. The ISO 9000 Standard comprises seven quality management principles, which constitute a commonly accepted basis for applying the standard series. The standard also specifies the benefits to an organization that has adopted the principles in its operation. The seven basic

quality management principles are related to customer focus, leadership, the engagement of staff, a process approach, continuous improvement, evidence-based decision-making, and relationship management. [7]

3.2 Cyber trust and process management

Establishing measures that increase cyber world security and trust in a company is primarily the responsibility of corporate leadership. Integrating the necessary measures with the idea of ensured business activities increases their significance and benefits through better processes for the entire organization, interest groups and society. If security is not considered, risk analysis reveals potential damages as well as their costs and social consequences. The leadership's views and requirements brought out in the analysis play a central role in developing security planning for the operating process. The costs and other resources allocated to the activities are simultaneously specified. [17]

An organization has a management system generally suitable for its business environment when it is managed systematically and at a high level, taking into account customers, the significance of staff, the efficiency and guidance of processes, continuous development of activities, and interest group communication. The management system can also be utilized in managing the processes of the cyber environment.

Process management theory has developed along with industrial production. The development of industrial mass production led to the use of variation theory while developing production process control: to perform control measures, uniform product quality was monitored with statistical methods. Statistical process analysis led to the observation that variation occurs everywhere in nature and in the processes and systems created by humans. After analysing distributions that involved variation, variation was classified into two types according to its causes: variation due to common causes (or the system itself) and variation due to special causes (i.e. named and assignable causes). Systemic variation has random causes and it is therefore, often normally distributed, according to Gaussian distribution. Variation resulting from special causes does not follow any regularities. The common causes of variation are thus constantly present in the process. An individual cause produces only little deviation, but several causes together generate considerable variation. The causes of special variation, on the other hand, are not constantly present in the process. They come from outside of the process and usually

generate more variation in the process than the common causes. In uncontrolled processes, deviation as a result of both types occurs simultaneously. [14]

In principle, Lillrank's theory on the causes of process variation can also be generalized to the processes of an electricity company. The measures taken by corporate leadership can be targeted at reducing variations resulting from both aforementioned types of causes. Proper planning and control of process performance reduce variation generated by random causes. At a general level, it is always recommended to aim at reducing this variation. If corporate leadership, in particular, concentrates too much on process changes resulting from random causes, it can lead to overreactions in process control due to the measures chosen. At its worst, this can lead to loss of control in managing the overall process. The actions of corporate leadership should indeed be targeted primarily at proactively preventing variation generated by special causes. Almost without exception, serious cyber security disturbances occurring in the operating process cause blackouts. They do not represent normal process variation but are deviations resulting from special causes. They are not in the normal range of variation. Taking these special causes into account in planning and proactively implementing managerial activities reduces related risks and improves the overall reliability of the company's operations.

3.3 Measures increasing cyber trust

The following measures related to cyber security management in an electricity company encompass the aforementioned seven principles of quality management.

In order to comprehensively build corporate cyber security, corporate leadership must define and guide actions at the strategic, operational and technological-tactical levels. The strategic level provides answers to 'why' and 'what' questions. The operational and tactical levels answer the 'how' question. The approach guided by questions ensures that the right things are done and that they are done in line with the set goal. The technological-tactical level must implement the goal-oriented activities defined at the strategic level, not create it. The company's organizational capability in implementing the cyber security measures required by the technological-tactical level ultimately determines how the company manages potential disturbance situations. [15]

Building corporate cyber security management begins from the level of vision and strategy work. The visions created by corporate leadership to enhance cyber

trust are translated into strategic goals, operational-level actions, guidelines and a policy. The practical measures derived from the strategy are realized at the technological-tactical level. Organizational capability factors enable the success of the measures.

In this article, creating a vision of cyber security in an electricity company is presented in the context of continuous development and maintenance of cyber trust as part of national critical infrastructure. The strategic choices supporting the creation of visions are primarily related to corporate social responsibility, company reputation, and ensuring business acontinuity nd its economic efficiency. The leadership is expected to make concrete strategic choices as well as support and guide the execution of the chosen measures throughout the organization. It is also important that the leadership ensures sufficient resource allocation to the measures. The chosen measures should be comprehensively communicated to the company's interest groups. [17; 7]

The measures at the operational level promote the strategic goals. Comprehensive measures that increase security and trust call for holistic cyber security management. It must be based on risk assessment and analyses of the measures based on the assessment. It is also important that the company declares and communicates the policy with which the leadership commits to the measures required to develop cyber security management. The declaration of a policy that ensures cyber security and the development of related procedures must be integrated with the organization's general policies. The highest organizational level is responsible for creating a policy that defines acceptable risk levels and the measures used in the reduction of risks [17]. The concrete measures at the operational level must be targeted at ensuring data security solutions and at creating business continuity and recovery plans [6]. The maintenance of situational awareness regarding the cyber environment of the electricity company's processes, furthermore, makes it possible to monitor the effects of the operational measures and, when needed, to react efficiently to events that constitute a threat within the company's operating environment. The aim must be to continuously monitor the availability of processes and to support decision-making in disturbance situations that require analyses and decisions [2].

The tactical corporate level encompasses the systems and processes that comply with the logistics framework. Consistent and predictable results are achieved more efficiently when operations are handled and managed as interrelated processes that function as a coherent system [7]. Cyber security threats set special requirements for these processes in addition to other operational

requirements. At a general level, the performance of processes is determined according to their client-based demands. In an electricity company, uninterrupted production of electricity can be regarded as the most important requirement, and it is achieved through a high availability level of the processes. In the cyber environment, the target can be achieved by defining the processes to be protected, choosing process control mechanisms successfully, and by using expedient technological solutions and services to protect the processes [17]. Successful operation also calls for the adoption of security-oriented values to guide the activities of staff [14]. The aforementioned solutions suitable for the cyber environment constitute an entity that can be called a technological-tactical level.

The continuous improvement of activities related to cyber security as well as the development of staff competence enhance the organization's capability to proactively prevent disturbances and tolerate potential changes in process operation caused by them. Taking the staff into account at all organizational levels, as well as focusing on competence and the possibilities it opens to fully influence in the organization, develops the overall operations of the company [7]. The continuous development of activities and staff competence support the measures taken at the strategic, operational and technological-tactical level.

Sufficient knowledge of the observed process is the starting point for continuous improvement. The measures taken rely on the idea that we observe process variation and reduce it by tackling variation that results from special causes. Addressing this type of variation often requires the use of different basic quality management tools in order to find the causes for deviations. In the context of cyber security development, the continuous improvement of organizational processes can also be seen as a proactive measure and thus as a measure that increases trust in the operating environment. Continuous process improvement is based on the continuous assessment of activities. In an electricity company, the main assessment criterion for an efficient process is its availability. When it comes to cyber security, the main constituent of overall availability is the availability of information in technological systems. High availability is achieved by continuously monitoring process meters and by adopting process performance improvement as an ongoing approach. It is typical that a learning and development-oriented organization is continuously looking for areas in which to improve.

In addition to performance measurement and different quality management tools, the organization can utilize feedback systems and benchmarking for the continuous improvement of processes. Traditional organizational feedback systems – such as internal self-evaluations, audits and reviews as well as external audits and their outcomes – can produce data for the development of operations and continuous improvement also regarding cyber security. For this purpose, cyber security and related trust-enhancing measures must be integrated into the feedback as one of its dimensions. Benchmarking, on the other hand, can be efficiently promoted by, for example, establishing branch-specific user groups among companies and maintaining regular exchange of information between them, particularly on measures that have been effective in solving disturbance situations and recovering from them.

Cyber security management calls for the constant maintenance of staff competence and consideration of their training needs. Staff competence is a crucial factor that determines the level of the entire company's activities. The capacity of human resources can be increased by developing employees' knowledge and skills related to cyber security and thus developing the company's capabilities. Challenges related to capabilities grow when an enterprise's cyber environment becomes more complex along with globalization and technological development. Investment in staff competence can transform the enterprise's capability into core competence, which can be used to pursue competitive advantage through trust. This will provide unique added value to both the company and its customers. In the case of an electricity company, successful cyber activity development and maintenance through staff competence can ideally lead to long-lasting added value, in spite of rapid changes in the operating environment. Valuable capabilities are helpful in a company's threat and risk management and can consequently facilitate, in particular, the utilization of profitable opportunities.

Figure 2 summarizes the aforementioned measures taken to increase an electricity company's cyber trust.

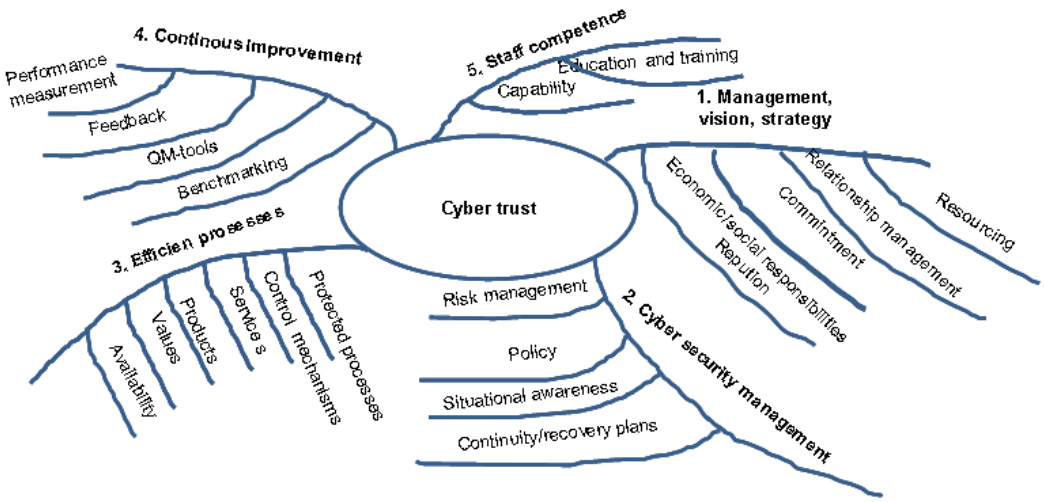

Figure 2. Measures increasing an electricity company's cyber trust

4 Implementing the measures that enhance cyber trust

4.1 An integrated management system and its components

When management in an organization is performed systematically, we talk about the organization's management system. A management system can comprise various control systems that comply with different standards, such as a quality management system, an information security management system and an environmental management system. In order to put into practice principles that comply with different standards, an organization may describe the required measures in its integrated management system (IMS). The IMS is a description of the procedures everyone should apply in the organization. With the help of guidelines and operations models jointly defined by the leadership and staff, the aim is to purposefully maintain a high level of activities and to develop the activities with an eye on set goals as well as the needs of clients and interest groups. The integrated management system compiles process descriptions, guidelines, recordings, indicators, tasks and feedback into a functional whole, which guides and supports the organization's mission and vision as well as the actions taken to realize them.

Management and the necessary measures related to cyber security in electricity production, including their objectives, must be documented in, for example, an organization's quality manual for the entire staff to see.

4.2 Trust-enhancing measures based on risk analysis

The vision for achieving a company's goals is the point of departure for trust-enhancing measures. The definition of strategy derived from the vision guides the actions taken in order to achieve the goals. At the first stage, it is most practical to facilitate the definition of strategy by performing risk analysis on cyber threats. When examining an electricity company, the targets of risk analysis are determined by the company's logistics framework and its IT processes. An electricity company's systems include a fuel logistic and feed system, a production system and its support processes, and the electricity distribution system. Because all the aforementioned components are needed in the operation of an electricity company, their mutual dependence as well as operations management and monitoring are crucial for the success of overall production. In managing cyber security, the different functions of the logistics framework must be treated as subjects of equal value.

If an organization is familiar with the factors affecting the operation of processes, their most vulnerable points in the cyber world and the cyberattack methods most probably threatening the processes, it possesses the most relevant information for creating protective plans for potential threats. Vulnerability analysis against attack methods is a systematic tool for identifying and assessing risks related to process operation as well as for choosing the most suitable measures to enhance cyber security trust. The analysis provides a comprehensive overall picture of the needs to develop the processes.

The risk management standard ISO27005 of the ISO27000 standard family includes the risk management process presented in Figure 3, which can be utilized in analysing the risks involved in the electricity production process.

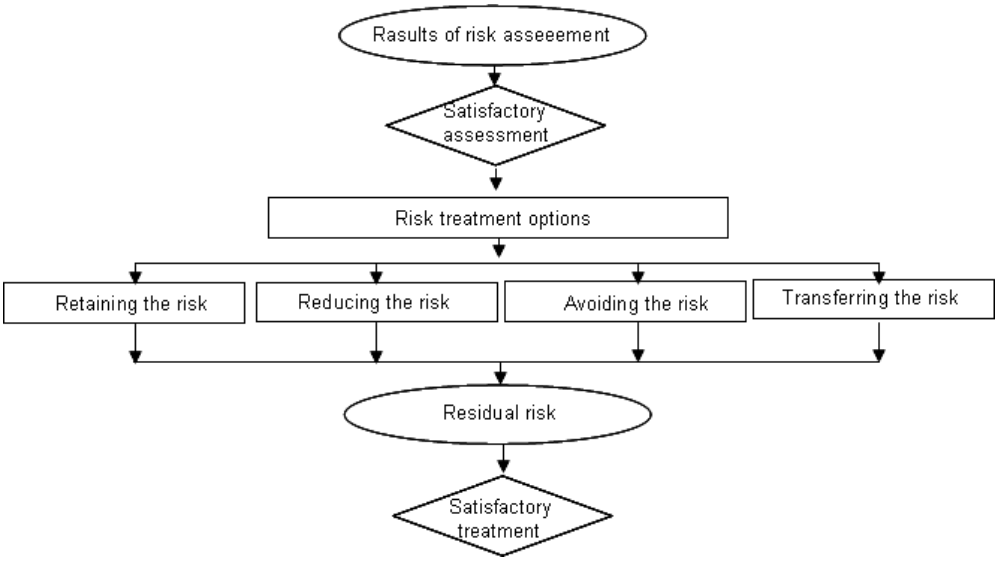

Figure 3. ISO27005: Risk treatment [6]

Risks can be classified in a treatment process according to Figure 3. The aim should be to reduce or completely eliminate the most remarkable risks using different measures. Corporate leadership prioritizes the highest risks to the processes based on risk identification and chooses the measures that best suit risk management and development of proactive measures in the cyber environment. Less significant risks can be retained, aiming to manage them. Risk transfer in the cyber environment of an electricity company can be possible through its logistics network. This means that responsibility questions must be resolved using a clear internal operations model within the network.

4.3 The PDCA method as a tool for developing activities

An organization's policy demonstrates that its leadership is committed to implementing strategic measures. In the business world, general strategic measures are mainly targeted at promoting the business activities, which means that taking cyber security into account as part of the overall strategy supports the business development targets. Cyber security as part of company policy is a way of communicating to staff and interest groups on the necessity and significance of development projects. Operational goals are formed as processes derived from the policy, whereby risk analysis has been considered. In order to create the measures, the organization must have a systematic approach to developing its operations.

The ISO9000 Standard recommends the PDCA (Plan, Do, Check, Act) method for a systematic development of an organization's activities. The method is based on a cycle of four development phases. The first phase (Plan) comprises planning, during which the subject is analysed and alternative measures are created based on the analysis. In the realization (Do) phase, the chosen measures are put into practice. Thereafter the functionality, efficiency and appropriateness of the chosen measures are checked in practice (Check). At the last (Act) phase of the cycle, the chosen measures are improved, if necessary, and established as standard practice. After the cycle has been implemented once, one will return to the first phase and start a new cycle with improvement actions based on a new situation analysis. Development can thus proceed as an endless process, in which a new level of activities is achieved after each cycle. The method is based on the idea of continuous learning and continuous improvement of activities.

The measures during one round of the cycle usually require a lot of planning, so sufficient time should be reserved for them. It is important to select the measures in relation to the resources needed for their implementation. The maturity level of the organization's development activities affects the evaluation of the implemented measures. When developing cyber security, at an initial stage the aim can be to recognize the need for cyber security management and to define cyber security risks for business. Hereby, the PDCA cycle may comprise the administrative actions most necessary according to risk assessment, such as a coherent information security policy in production, practical guidelines for maintaining information security in production, and potential preliminary system-specific cyber security checks. The targets for development must later be chosen according to risk prioritization.

The following is one possible process model for developing cyber security management with the PDCA method:

PLAN, planning phase

1. Choose the target for development based on risk assessment
   - schedule and goal
2. Create a picture of the current situation
   - earlier measures
   - disturbances in the branch resulting from special causes
3. Analyse the problems and define corrective actions
   - identify potential harms caused by the disturbances
   - choose the measures available to anticipate and manage the situation

DO, implementation phase

4. Implement the chosen measures
   - choose the actors responsible for implementation
   - organize information and training for staff

CHECK, checking phase

5. Check the impact of the measures
   - compare the results with the goals
   - return to phase 3 if the goals have not been achieved

ACT; regularize the measures

6. Regularize the chosen development measures
   - update necessary guidelines, technological solutions and services
   - continue staff training
7. Draw conclusions and make plans for the future
   - continue development according to new goals
   - update threat and risk analyses

In this section of the article, we have described one way of launching primary basic solutions related to cyber security management in an electricity company. These first steps provide a basis for later development activities and continuous improvement in a dynamic cyber environment.

5. Conclusion

The national power grid and its electricity production are part of a country's critical infrastructure – the operation of a modern society is based on a reliable electric power system. Ensuring the availability and reliability of processes in electricity companies in all environments is vital for the efficient functioning of critical infrastructure. Therefore, the measures taken in electricity companies in order to manage and control the cyber security of processes are an essential component of the reliability of production.

The major cyber environment risks within the processes of an electricity company require that trust is enhanced and maintained at all levels of business activity. Comprehensive measures to increase cyber trust, together with the development of capabilities related to cyber activity, also improve a company's competitive edge.

The initial measures taken to develop cyber security management and trust in an electricity company can be summarized and prioritized as follows:

1. It is ensured that the company sees cyber security measures as strategic goals and that sufficient resources are allocated to the chosen measures.
2. Risk assessment is performed and the company's policy is updated to meet the requirements of cyber security.
3. The primary trust-enhancing development measures needed based on risk assessment are taken at the first development phase, using the PDCA method.
4. A continuous process is formed of the development actions by choosing the subjects of the next cycle, and the PDCA development cycle is repeated. This procedure will provide the organization with a culture of continuous learning and improvement. The organization's capabilities and competitive advantage are enhanced.
5. The impact of the measures is monitored as part of the company's audit and management procedures (e.g. as part of the ISO 9001 Standard procedures).

Investigations have revealed that the extensive power failure in Ukraine on 23rd of December 2015 was caused by a coordinated cyberattack by an external party to the control systems and data warehouses of three enterprises in charge of power distribution. One potential target of the attack is suspected have been the industrial automation system, which the hackers may have managed to enter via a remote access service. When preparing for cyberattacks against industrial automation systems and trying to improve their resistance, organizations are recommended, in the first place, to introduce the best practices of cyber security management. [9]

The power failure in Ukraine and other international experiences of disturbances in power grids highlight the crucial role of developing trust in electricity company operations as well as the importance of their organizational management in the cyber environment.

References

[1] Bowersox D., Closs D., Jessop D., Jones D., Logistical Management, New York, John Wiley & Sons, Ltd., 1986.

[2] Faber S. Flow Analytics for Cyber Situational Awareness. SEI Blog, 2015. https://insights.sei.cmu.edu/sei_blog/2015/12/flow-analytics-for-cyber-situational-awareness.html

[3] Fingrid Oyj, Voimajärjestelmän yleinen kuvaus. Retrieved on 6 August 2016 from http://www.fingrid.fi/fi/voimajarjestelma

[4] Finnish Energy. Retrieved on 25 October 2015 from http://energia.fi/energia-ja-ymparisto/sahkontuotanto

[5] Finnish Society of Automation. Teollisuusautomaation tietoturva. Verkottumisen riskit ja niiden hallinta. [online document], 2010. www.viestintavirasto.fi/attachments/tietoturva/TeollisuusautomaationTietoturva.pdf

[6] Finnish Standards Association SFS. SFS-käsikirja 327. Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintajärjestelmät. SFS ry, Helsinki, 2012.

[7] Finnish Standards Association SFS. Johdanto laadunhallinnan ISO 9000 -standardeihin. [online document], 2016. www.sfsedu.fi/files/126/ISO_9000_kalvosarja_oppilaitoksille_2016.ppt

[8] Helsingin Sanomat (6 January 2016). Poikkeuksellinen kyberhyökkäys onnistui sammuttamaan ukrainalaisten sähköt. http://www.hs.fi/ulkomaat/a1452053903722

[9] ICS-CERT. Cyber-Attack Against Ukrainian Critical Infrastructure. Retrieved on 23 June 2016 from https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

[10] Kananen I, National Emergency Supply Agency. Sähköjärjestelmä yhteiskunnan toimivuuden perustana. Seminar presentation on 2 December 2013. [online document] http://www.fingrid.fi/fi/asiakkaat/asiakasliitteet/Seminaarit/K%C3%A4ytt%C3%B6varmuusp%C3%A4iv%C3%A4/2013/K%C3%A4ytt%C3%B6varmuusp%C3%A4iv%C3%A4%20021213%20Kananen.pdf

[11] Knowles W., Prince D., Hutchison D., Ferdinand J., Disso P., Jones K. International journal of critical infrastructure protection 9. A survey of cyber security management in industrial control systems, 2015.

[12] Lehto M. Cyber Security: Analytics, Technology and Automation. Springer, 2015.

[13] Lewis T. Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation. Second Edition, 2015.

[14] Lillrank P. Laatuajattelu. Laadun filosofia, tekniikka ja johtaminen tietoyhteiskunnassa. Otavan Kirjapaino Oy, Keuruu, 1998.

[15] Limnell J., Majewski K., Salminen M. Kyberturvallisuus, Docendo Oy, Jyväskylä, 2014.

[16] Secretariat of the Security Committee. Finland's Cyber Security Strategy. [online document], 2013. http://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf

[17] Stouffer K., Falco J., Scarfone K. NIST Special Publication 800-82. Guide to Industrial Control Systems (ICS) Security. Recommendations of the National Institute of Standards and Technology. U.S. Department of Commerce. [online document], 2011. http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf

[18] World Economic Forum. Retrieved on 8 August 2016 from http://reports.weforum.org/global-risks-2015/part-1-global-risks-2015/technological-risks-back-to-the-future/#frame/20ad6

Informaatioteknologian tiedekunnan julkaisuja
No. 56/2018

ISBN 978-951-39-7543-2 (verkkoj.)
ISSN 2323-5004

JYVÄSKYLÄN YLIOPISTO