Report - Windy Island Power

ROGER LARSEN
Project: IMT 4772 - Risk Analysis 2
Gjovik University College
2011 Fall

Document Classification: RESTRICTED.

Thursday 8th December, 2011

Contents

Chapter 1

Scenario description – Windy Island Power

This chapter describes the company Windy Island Power.

1.1 Terms of reference

Wind power production are a sensitive activity. The Managing Director have recently had a course in risk management and was a bit stressed on behalf of his own organisation. He want to start analysing the organisations risk. Initial he want an risk analysis regarding information security executed before the end of the year.

1.2 Company Objectives

The primary objectives of Windy Island Power are:

- Produce electricity in an effective and efficient manner.
- Produce electricity according to the Norwegian Water Resources and Energy Directorate's recommendations.
- Ensure that the staff are well trained in order to technical and administrative manage the companies production equipment.
- Ensure that the electricity are produced and delivered in a safe and secure manner for the organisations staff.

1.3 Company Performance Indicators

Power production in Windy Island Power are measured by indicators such as

- Amount of electricity delivered for each month, quarter and year.
- Production uptime.
- Number of unwanted events.

1.4 Company Organizational Structure

Windy Island Power is managed by a Board - chaired by the Chairman. The board engage a Managing Director (MD). The MD have a IT Manager, a Business Manager and a Production Manager in his leader group. The IT manager manage both the administrative and production data systems. The IT manager reports to the business manager regarding normal operative IT issues. The IT manager is the emergency preparedness coordinator and in this case he reports to the MD. The IT manager have its own staff. The business manager is responsible of finance and economy in general and have a staff that also do internal and external customer service. The production manager have the technical license to produce and manage the electrical production plant. He have a staff of electrical engineers and installers to guard, operate and maintain the production equipment. The production manager have a 24/7 system control center. The production manager works closely with the IT manager regarding IT equipment.

1.5 The Company's use of Information Technology

Windy Island Power has an IT department which is responsible for both general IT services in-house and computer network and equipment to all wind turbines. They have staff in the customer service team and are always represented in the system control center 24/7. The IT department offers remote connection for some home workers and travellers. This remote connection can give access to both the computer center and all production equipment.

1.5.1 IT Hardware

Windy Island Power has office personal computers (portables), Internet access (via a powerful Juniper Network firewall which also controls the remote access). Access to Internet from internal computers can be both by wireless (offices) and wired. The IT department have a computer room with several servers and network equipment. All employees have smartphones. Each wind turbines have several computerized controls for own use (weather stations, cameras) and for remote monitoring. The company main buildings (main office and production) are supervised by cameras. Telephone central from ALcatel and emergency radio system from Navtron.

1.5.2 IT Software

Windy Island Power use Microsoft Office Suite for general administrating. Microsoft Office Suite includes; Outlook (email client), Visio (drawing), PowerPoint (presentation), Word (word processor) and Excel (spreadsheet). For Internet browsing; Internet Explorer (IE), FireFox and Google Chrome are available. Adobe Reader are used for viewing PDF files. Microsoft Dynamics are used regarding finance, accounting and salary.

IT departments servers are based on Microsoft, Debian Linux and FreeBSD. The IT staff use several other software in their own test lab.

Production department use a lot of more specialised software. Monitoring is based on OpenNMS (open source) and locally adapted. Cables and connections are documented by Telemator (MxData, Norway). Monitor and operate software for the wind turbines are from Vestas (manufacturer).

1.5.3 Security Tools

All computer systems are with antivirus. All personal computers have the local software firewall activated and automatic Microsoft Update. All of these basic functions are centrally managed. For email washing (to avoid unwanted emails) they buy this service at their Internet Service Provider (ISP). The firewall have an advanced intrusion protection system (IDP) in-built. This function can in many situations block possible attacks. If an virus or unwanted behaviour are detected - the actual client(s) are isolated from the normal network connection immediately.

1.6 Physical Access Control

Access control and fire alarm systems are delivered by YIT Installation. All buildings are physically locked by a special locking system. Most buildings have installed a number pad with built-in RFID reader. During normal daytime the office, car houses, tools shop and spare parts stock buildings do not ask for more then an active RFID, but outside normal office time a corresponding code must also be used.

Indoors there are seldom locked offices (except MD's), but system infrastructure rooms are always locked. These infrastructure rooms are the computer room and the system control center. These rooms are not accessible for every employee.

The production/infrastructure buildings that contains electrical hazard environment are only accessible for trained staff.

1.7 The Company Funding

Windy Island Power is producing electricity from wind power plant located in Nordnes municipality in south west of Norway. Windy Island Power is a partly owned private limited company.

The shares of common stock are divided in this manner:

- The former landlords = 40%
- Employees = 10%
- Island Power = 50%

1.8 The Value Chain in Electric Production

1.8.1 Wind to Electricity

Windy Island Power have 12 large wind turbines delivered from Vestas type V80-2.0 MW. These wind turbines are heavy duty constructed to manage high wind speed (they have full capacity from 14 to 25 m/s). The wind turbines are arranged in 3 rows with 4 wind turbines in each row.

1.8.2 Electricity Transport

Windy Island Power have two large electrical cables that makes the produced electricity brought to Island Power. These cables are physically independent of each other - and each of them can manage the amount of produced electricity all by themselves. In this way Windy Island Power have redundancy concerned deliverance.

1.8.3 Infrastructure and Facilities

Windy Island Power have a lot of buildings and electronic equipment to monitor, operate and (if necessary) re-establish any failure situation.

1.8.4 Trained and Experienced Staff

The last but most important link in the value chain is the staff. Several of them have over 20 years of experience running this kind of power plant.

Chapter 2

Assets Valuation

Windy Island Power have a complex mix of tangible and intangible assets regarding information security. They have the internal administrative computer system and they have the process computer system (controlling the wind mills). In this report we focus on information security assets.

2.1 Valuation Method

We have in our assessment valuation chosen a qualitative approach with a mixture of Cost, Marked and Income.

Quantitative methods are very time consuming and often complex – which not was suitable for our Manager Director. When qualitative methods struggle to show a clear picture regarding cost/benefit – quantitative method are normally used in this part.

With the respect to valuation, the initial cost of physical computer equipment normally not high. The cost regarding installation, managing and training is often much higher then initial cost.

Please find our assets valuation in table 2.1.

Table 2.1: Asset valuation – Tangible and Intangible information security

#	*Asset*	*Type*	*Imp.*	*Uniq*	*Sub.T.*	*Explanation/Reason*
1	System Operation Centre	T	5	4	5	The system operation centre is monitoring and managing the wind mills. It is not crucial but makes the operation of the windmills easy. There are SCADA systems used.
2	Computer room	T	5	2	4	The computer room hosts many important equipment.
3	Servers	T	4	4	3	The servers runs important databases, but are physically not expensive.
4	Computers, stationary	T	2	2	2	The stationary computers are easy to substitute.
5	Computers, portables	T	3	2	2	The portable computers are medium easy to substitute (rough versions of portable computers).
6	Smartphones	T	5	2	2	The smartphones are easy to substitute, but they play an important role in communication.
7	Network switches	T	4	1	3	We have many places to connect our computers
8	Network boarder routers	T	5	3	4	Important for Internet communication
9	Network firewall	T	5	4	5	Important for controlling external, internal and production network
10	SCADA communication equipment	T	5	3	3	The SCADA equipment monitors and controls the windmills
11	Smartphone's address book	I	5	3	5	Important in daily operational and in emergency situations
12	Monitoring software	I	5	4	5	Important to correlate failure situations
13	Business Plans (Continuation, Emergency)	T	5	5	5	Critical in emergency situations
14	System Knowledge	I	5	4	5	Critical for prompt recovery of failure situations
15	Reputation	I	4	3	4	Important for less noise regarding the windmill power plant.
16	Documentation	T	5	5	5	Important to get access to our procedures and system documentation
17	Local developed computer applications	I	5	5	4	Important to get the alarm system to work smarter (correlation alarms)

Legend:
The asset types are Tangible(T) and Intangible (I).
The scale are as follows: Very Low(1), Low(2),Medium(3), High(4) and Very High(5).

Chapter 3

Risk analysis method requirements

Based on Windy Island Power's challenges regarding information security we will here identify some requirements for a risk analysis. Risk analysis are often time-consuming and boring processes. With good planning that includes motivation and clear goals the next revising – the actual risk assessment may be a much easier tack to execute. It is also crucial that the stakeholders in the actual area are included in the processes.

Requirements for the risk analysis method:

1. Risk assessment
2. Compliance with NVE (Norwegian Water Resources and Energy Directorate)
3. Easy for non technical personnel to participate
4. Easy to audit (controls established)
5. Suitable for our organisation
6. Supporting tools (optional)

3.1 Comments to Choosing Risk Method

We assume that a discover process of our vulnerabilities and threats are not dependent of the risk analysis method. Please remember that the choice of risk method never must force us to follow every detail in the actual risk method. We may act as an adult in the candy store; we only pick what we like and ignore the rest. When the organisation have worked with risk management and (i presume) tried some risk analysis methods, they know what they need. Nevertheless, do not exclude other risk methods as an other reference or as supporting literature.

Chapter 4

Risk Analysis Method Selection

In this chapter we will evaluate what risk analysis method that may fit Windy Island Power's criteria. We use the following risk analysis method in this evaluation of methods:

4.1 Risk Analysis Methods

The following risk analysis methods are evaluated:

- RISK IT FrameWork by ISACA
- ISO-27005 by International Organization for Standardization
- IDART
- SP-800-30 by NIST (National Institute of Standards and Technology)

4.2 Risk Analysis Methods Evaluated

Evaluation of risk analysis methods can be found in table 4.1. We give the following points 1(low), 2(medium) and 3(high).

Table 4.1: Risk analysis method evaluation

Requirements $\Longrightarrow$ **Method** $\Downarrow$	1 - Compliance with legislation (NVE)	2 – Risk assessment	3 - Easy for non technical personnel to participate	4 - Easy to audit (controls established)	5 - Suitable for our organisation?	6 - Supporting tools (database)	7 - Available competence/knowledge (database)	**SUM**
RISK IT FrameWork by ISACA	3	3	3	3	2	2	3	19
ISO-27005	2	3	1	2	1	3	3	15
IDART	1	1	3	1	3	1	1	11
SP-800-30 by NIST	3	3	1	3	2	2	2	16

Please note that NVE = Norwegian Water Resources and Energy Directorate.

4.3 Comments to Risk Method Evaluation

We have now evaluated what risk analysts method to use. The numbers we got in our SUM column show a close race. The goals to train up an employee in this process is a good idea. We may want to use local competence/knowledge but perhaps we need an initial project just to get our plan right? Planning is important ans an stressed managing director may force us doing wrong decisions. Be also aware of that the risk analysis methods are in general based on common sense and best practise and they overlap each other in large degree. A choice of method now does not need to be a lifetime choice!

The risk analysis method we ended on in this evaluation: RISK IT FrameWork from ISACA. They have done a great job in their job in their approach to risk analysis. They offer many tutorial literature and supporting tools in addition to strong knowledge in Norway. There are frequent courses in this method/framework. Their easy approach to technical terms will be of good help in our risk analysis group that consist of several non-technical employees.

Chapter 5

The Stakeholders and Threat Agents

We will here identify relevant stakeholders and threat agents and identify their interests. Please find our result in tables 5.1 5.2.

Table 5.1: Stakeholders.

Stakeholders	**Interests**
Staff	Keep their jobb. Learning and developing job experiences. Have good colleagues. Earn money. Get respected. Get good reputation.
Guardian Staff	Have more challenging jobs. Earn more money. Be looked up to as "rescue staff"
Owners	Earn money. Secure their long term investment.
Electrical consumers	Get stable electrical service. Get electric supply as cheap as possible. Get good conscience because they are users of recyclable energy.

Table 5.2: Threat Agents.

Threat agents	**Interests**
Hackers	Show their skills or just make a mess just for fun (both can destroy companies). Earn money (industrial espionage).
People against windmills	Make problem for windmill companies (so they loose money and reputation etc) and by doing this get published (newspapers/television) so they can "sell in" their case to others.
Dissatisfied staff	Make his/her company suffer in any way which can result in much trouble and loss of money
Stressed staff	They just want to get finished with the job ASAP without following all procedures.
Malware	Malware can alter, destroy files and documents - they are in general evil on behalf of their developers.. Malware are an unpredictable threat agent. Many types of malware changes their properties/behaviour in their lifetime (some have in-built functions (polymorphic)and other get instructions to this (bots))
Rodent animals	Mouses and rats can destroy wiring with they sharp teeth. If they are trapped indoor a building or cabinet they will eat on everything in their desperate need for foot.
Wind	Wind is a natural phenomenon that we can not control, but on the coastal island the statistics for wind are good. Nevertheless storms can destroy buildings and tear down trees including poles with wiring (both electrical and telecommunication). This is just how storms behave - their inherit characteristic. The other alternative; no wind is very bad for electrical production.
Suppliers	Our suppliers need to sell their products. Their main interest is to sell much product for good prices and earn money.
Contractors	The contractors are in general positive to as much as work as possible. If they are specialists they want to exploit this situation for perhaps a long term contract.
Temp staff	Temporary staff are in general interested in doing a very good job, they are in general unemployed. This may also be a place where industrial espionage can take place.

Chapter 6

Vulnerability Discovery

In this chapter we will focus on the vulnerabilities regarding Windy Island Power. We have in this chapter chosen Dataflow Diagram (DFD)[1] as the vulnerability discovery method. We considered using the VAMM (Vulnerability Assessment and Mitigation Method) by RAND[2] – but found the latter to complex and difficult when consulting our non-technical staff.Please find our diagrams at the end of this chapter.

6.1 Vulnerabilities

The dataflow diagram method gave us the following list of possible vulnerabilities. This list are never complete by several reasons; (i) every organisation are in a continuously change, (ii) information technology changes all the time, and of-course, the first time a risk assessment/analysis are done we seldom manage this.

6.1.1 Remote Access

The remote access are gained by a unit that have several functions; (i) remote access/VPN, (ii) firewall (network traffic filtering), (iii) boarder router and (iv) traffic segregation. This is too many eggs in the same basked.

6.1.2 Windmill Control Server + SCADA system

The Windmill control server serves as a master control unit for all the windmills. The windmills are not depended of this server, but if this server are unavailable - the windmills must be controlled manually with physically presence at each windmill. The actual server are both connected to the production and the administrative computer network. This is not a smart design and may be a compliance breach with the legislations. The communication between the control server and the windmills uses SCADA systems. SCADA systems have few inbuilt security mechanisms.

[1] The dataflow diagram is one of the most commonly used systems-modeling tools.

[2] Anton, Philip S., Robert H. Anderson, Richard Mesic and Michael Scheiern. Finding and Fixing Vulnerabilities in Information Systems: The Vulnerability Assessment and Mitigation Methodology. Santa Monica, CA: RAND Corporation, 2004.

6.1.3 Internal Access

The internal computer network are vulnerable for attack by unwanted/wrongly operations and unsatisfied staff. It is crucial that every employee is well trained in their responsibilities regarding the usage of the internal computer network. The chance of loose sensitive information is very high due to ignorance.

6.1.4 Software errors/bugs

Every piece of equipment that have software loaded is a source of doing errors because of this.

6.1.5 Bad or missing procedures

Incorrect operations are a frequent event in every organisations. People tend to take short cuts as often as they can.

6.1.6 Malware attacks

The Internet is an continuous cyber-war. Any web page, email, electronic document can be infected with malware. This makes any cyber criminal possible of spreading their evil software.

6.1.7 Vandalism

Vandalism from anti-windmill people are not a threat only against physical equipment, but also a threat to the information security area. Fanatic people are a difficult threat to measure and analyse.

6.1.8 Complex communication solution

The complex computer network that makes remote mobile workers connect to the company's remote access and be able to access the windmill monitor and control servers are a challenge. The solution involved many security levels but are again rather complex. Guardian staff do not want to be "stuck" on the production area but rather be at home with their families. This solution may not actually be allowed by the legislation.

6.2 The Dataflow Diagrams

We have drawn the following dataflow diagrams:

1. Windmill Monitor and Control Information Flow 6.1
2. Windmill Monitoring Server – Figure 6.2
3. Windmill Alarm System – Figure 6.3
4. Windmill Guarding Staff – Figure 6.4
5. Windmill Control Server – Figure 6.5
6. Windmill Control Unit – Figure 6.6

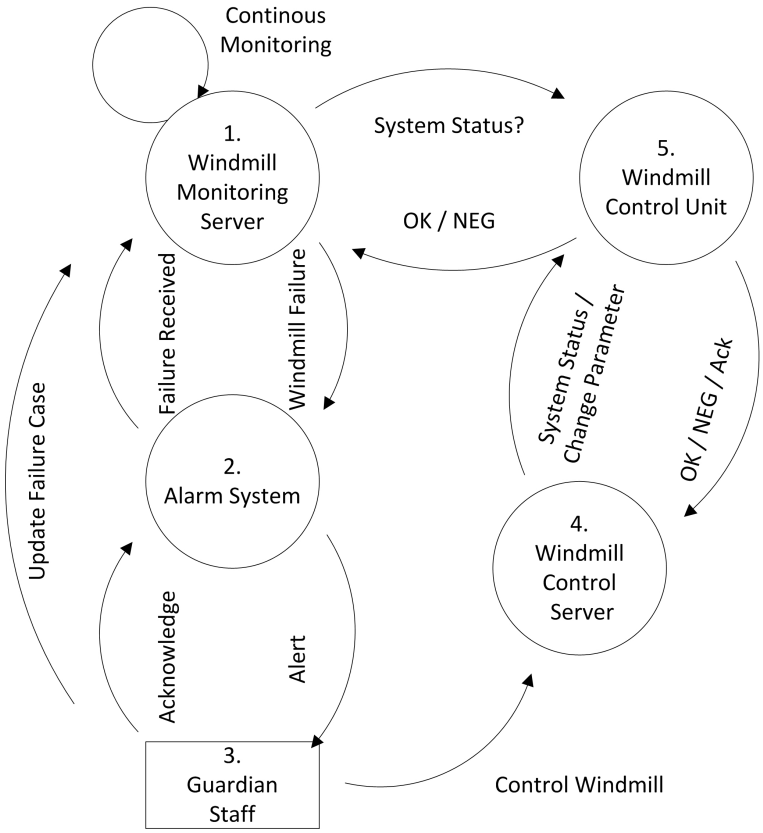

Figure 6.1: Dataflow diagram - Information flow regarding windmill monitor and control.

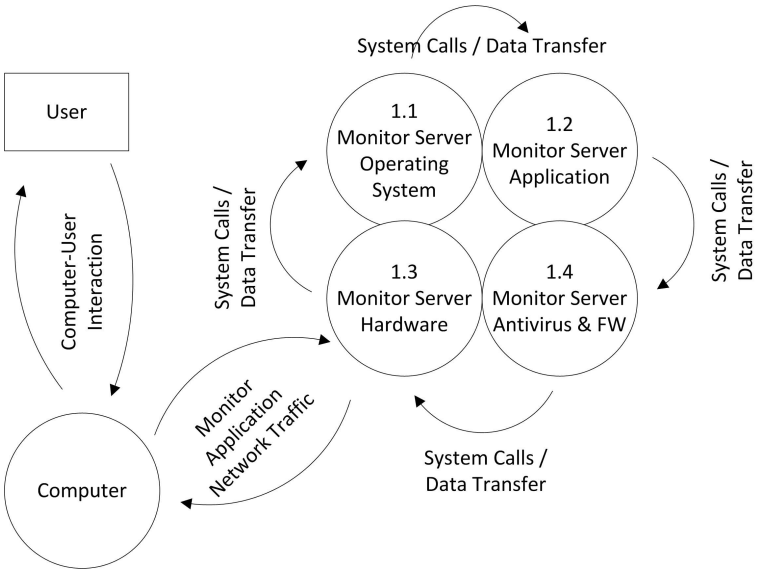

Figure 6.2: Dataflow diagram - information flow regarding windmill monitor server.

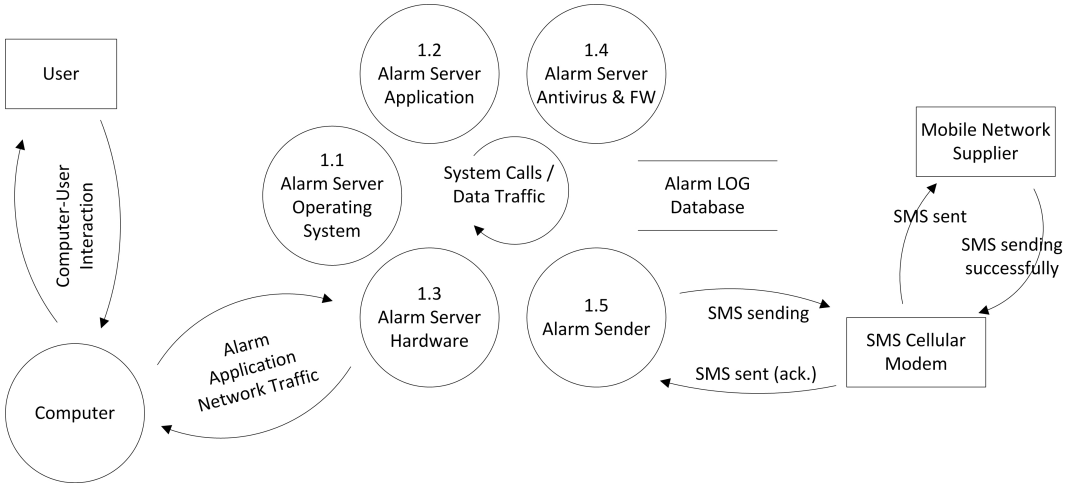

Figure 6.3: Dataflow diagram - information flow regarding windmill alarm system.

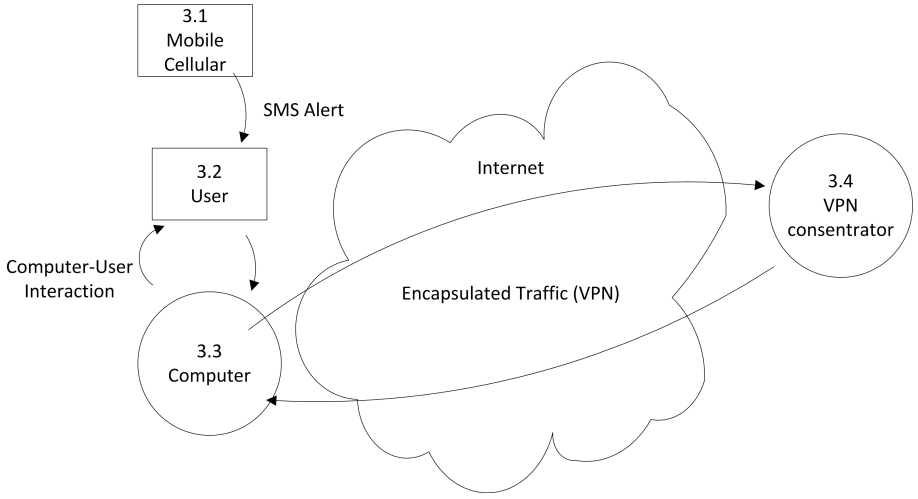

Figure 6.4: Dataflow diagram - information flow regarding the guarding staff.

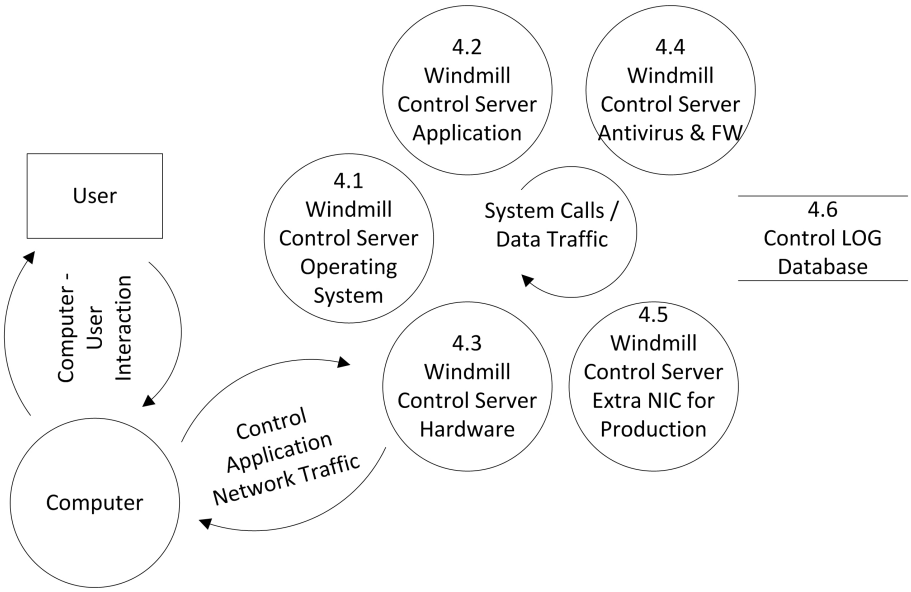

Figure 6.5: Dataflow Diagram - Information regarding the windmill control server.

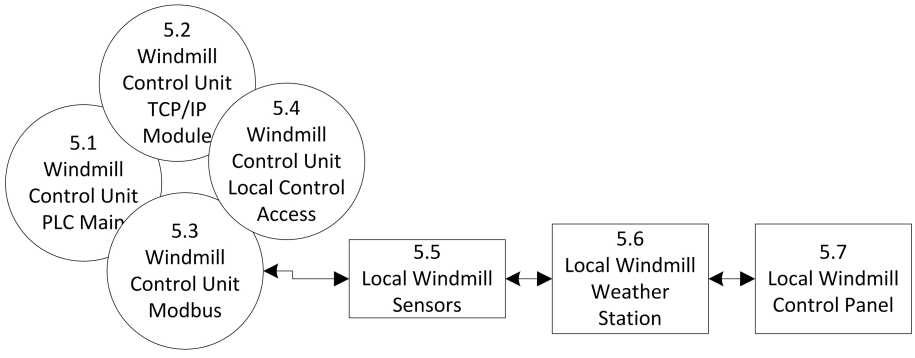

Figure 6.6: Dataflow Diagram - information flow regarding the windmill control unit.

Chapter 7

Threat Identification

In this chapter we will identify threats to some of our vulnerabilities identified in chapter 6.

7.1 Threats to Remote Access

The following subsections show possible threats to the company's remote access:

External Attack - Starvation by DoS Equipments connected directly to Internet are in danger of being a victim of DoS attacks. This kind of attacks are difficult to resist. This kind of attack may both knock out outgoing Internet traffic and incoming connections (mobile workers).

External Attack - Unauthorised Access Equipments connected directly to Internet are in a constant war zone. Software errors and/or weak security level can give unauthorised personnel access to the network.

System Unavailable/Lockout Unauthorised personnel can lock out authorised personnel and blackmail the company.

Software errors/bugs Software errors/bugs in firewall or routers may result in lack of remote access. This kind of errors may occur randomly.

Electrical Power Failure Every electronic equipment that needs power to function are normally very sensitive regarding the quality to this.

7.2 Threat to Internal Access

Internal Attack - Unauthorised Access Malware and/or unsatisfied staff may get unauthorised access from the internal network. Unauthorised personnel can destroy important production systems and/or control the windmills so that they brake down (e.g. force them to run in high wind speed).

Sensitive Information Leakage and/or Altering Unauthorised personnel can get access to the company's internal network, the chance of loosing sensitive information is large. The can also leave malware that periodically sends information back to these hackers/cyber criminals.

7.3 Threats to Windmill Control Server + SCADA system

Unauthorised Access Unauthorised personnel can control the windmills and make great loss in electric production.

Production Failure because of Incorrect Operation Stressed, displeased and/or untrained personnel can destroy important production systems and/or control the windmills so that they brake down (e.g. force them to run in high wind speed).

Chapter 8

Identification of Potential Assets Loss

We will in this chapter identify the assets consequence and potential loss due to the vulnerabilities found in chapter 6. We will both use qualitative and quantitative approach. Please note that NOK in the table 8.1 and 8.2 are Norwegian kroner.

Table 8.1: Possible asset loss due to our vulnerabilities. Part 1.

Vulnerability	**Asset affected and potential loss**
Remote Access	*Affected assets:* Staff, firewall, routers, servers, internal documents etc. *Possible scenario:* Internet access from internal network and mobile workers access to the company's network can be lost for hours and days. Internal servers can be attacked and we may loose sensitive data. Unauthorised user access. *Potential loss:* <10.000.000 NOK (very high).
Windmill Control Server + SCADA system	*Affected assets:* Firewall,control server, routers, switches, production computer network, windmills, windmills control units. *Possible scenario:* The electrical production may stop for hours or days (e.g. windmill disconnected from electrical generator, deletion of control programs). *Possible loss:* external unauthorised users can access and control the windmills and stop productions for hours and/or days. *Potential loss:* Several millions NOK or even bankrupt (very high).
Bad or missing procedures	*Affected assets:* Staff, UPS, servers, routers, switches, control units, windmills. *Possible scenario:* Incorrect maintenance of uninterruptible power supply (UPS) may switch off all servers in power supply breakdown, which may lead to corrupt data. *Potential loss:* <1.000.000 NOK (high).

Table 8.2: Possible asset loss due to our vulnerabilities. Part 2.

Vulnerability	**Asset affected and potential loss**
Malware attacks	*Affected assets:* Computers, servers, documents, windmill control system, windmills. *Possible scenario:* Stuxnet is an advanced new virus that attacks industrial equipment with SCADA system (mainly Siemens PLC's). This makes the windmill control system malfunction. *Potential loss:* <5.000.000 NOK (high).
Vandalism	*Affected assets:* Computers, servers, routers, switches, buildings, documents, windmill control system, windmills, facilities (cars, tools etc.). *Possible scenario:* People or group of people may sabotage the companies production equipment or needed assets. *Potential loss:* <10.000.000 NOK (very high).
Complex communication solution	*Affected assets:* Computers, servers, firewall, routers, switches, documents, windmill control system, windmills. *Possible scenario:* Incorrect maintenance of software in routers, firewalls and/or control units. This makes the actual system vulnerability to existing, known threats. *Potential loss:* <1.000.000 NOK (high).

Chapter 9

Likelihood Measure Alternatives

We will in this chapter discuss alternative measures of likelihood/probability for each of the vulnerability/threat pairs.

9.1 General comments

In every situation where we are challenged to start up the time machine and go forward in time we are forced to use both quantitative and qualitative approach. We must in these situations gather all empirical and historical data that exists about the actual case. In information security field we are really challenged because of the continuous changes. Nevertheless – existing data/statistics/logs and security experts gives us important guidelines in how to determine the probability in these cases. In many cases we can not set the probability right, but a qualified guess is better then nothing! Please bear in mind that any event with very low probability may occur any second!

9.2 Remote Access

9.2.1 Threat = External Attack - starvation by DoS

Powerfull external DoS attacks occurs rare fortunately, and the weaker ones are normally easy to handle by firewalls. BUT, they do happens – and may cause trouble for the company. This kind of attack are not really the most likely attack to the company. Their web pages are not business critical and the guardian staff may travel to production site to get their job done.

Measurements for Likelihood regarding DoS attacks can be one or several of the following; (i) Logs in firewall, (ii) in-house honeypot statistics, (iii) statistics from security companies or (iv) statistics from similar kind of company. The political and/or media picture of windmills may be an trigger for higher activity.

9.2.2 Threat = External Attack - Unauthorised Access

This kind of attacks happens continuously 24/7/365 – but fortunately seldom with success. The company may be an interesting target for this kind of attack. An successful unauthorised access

to the company's internal network are very critical.

Measurements for Likelihood regarding unauthorised access attack can be one or several of the following; (i) Logs in firewall, (ii) in-house honeypot statistics, (iii) statistics from security companies or (iv) statistics from similar kind of company. The political and/or media picture of windmills may be an trigger for higher activity.

Chapter 10

Likelihood Assignment

10.1 External Threat

10.1.1 Remote Access - starvation by DoS

External DoS attacks occurs rare fortunately, and are normally easy to handle by firewalls. BUT, they do happens – and may cause trouble for the company. This kind of attack are not really the most likely attack to the company. Their web pages are not business critical and the guardian staff may travel to production site to get their job done.

Measurements for Likelihood regarding DoS attacks can be one or several of the following; (i) Logs in firewall, (ii) in-house honeypot statistics, (iii) statistics from security companies or (iv) statistics from similar kind of company. The political and/or media picture of windmills may be an trigger for higher activity.

Estimated Likelihood: 1 time each 2 year (0.50 times a year).

10.1.2 Remote Access - Unauthorised Access

This kind of attacks happens continuously 24/7/365 – but fortunately seldom with success. The company may be an interesting target for this kind of attack. An successful unauthorised access to the company's internal network are very critical.

Measurements for Likelihood regarding unauthorised access attack can be one or several of the following; (i) Logs in firewall, (ii) in-house honeypot statistics, (iii) statistics from security companies or (iv) statistics from similar kind of company. The political and/or media picture of windmills may be an trigger for higher activity.

Estimated Likelihood: 1 time each 5 year (0.20 times a year).

10.1.3 Remote Access - Software Failure/Bugs

Software failure/weakness are an continuous battle. We update software and end up getting some bugs fixed and other new present. We consider here only serious software bugs that may

sacrifice and/or shut down our network.

Measurements for Likelihood Consult information security forums, subscribe on newsletters/alerts from suppliers and/or vendors. Consult expert groups.

Estimated Likelihood: 1 time each 1 year (1.0 times a year).

10.2 Internal Threat

10.2.1 Internal equipment - Operational Failure

Operational failure happens unfortunately too often, we humans are experts in taking short cuts when we are stressed.

Measurements for Likelihood statistics (unwanted events), empirical data and expert knowledge.

Estimated Likelihood: 10 time each 1 year (10.0 times a year).

10.2.2 Internal equipment - Unit Failure, Firewall

Unit failures are difficult to predict, but fortunately relatively new equipment can be stable for many years. The environment are electronic equipments worst enemy; operational temperature, stable electrical power, humidity, vibrations etc.

Measurements for Likelihood for unit failures are statistics, mean time between failure (MTBF) numbers from fabric, empirical data and expert knowledge.

Estimated Likelihood: 1 time each 5 year (0.20 times a year).

Chapter 11

Knowledge Distribution

In this chapter we will identify what knowledge stakeholders and threat agents need to possess. Please find our results in tables 11.1 5.2.

11.1 Type of knowledge

We have here categorised knowledge in the company. Please find our discussion regarding knowledge in general later in this chapter.

Type of knowledge in Windy Island Power:

Public Knowledge This kind of knowledge are public available (web pages, public reports, press release, media articles etc.)

Staff Basic Knowledge This kind of knowledge can everyone employee access. Much of this is written in the personnel handbook and describe the company's personnel policy, practical information and non-disclosure agreements etc.

Work Area Knowledge This kind of knowledge are given staff working in their department and other with special needs.

Advanced System Documentation This kind of knowledge are for section/department leaders and other with special needs.

Strategy/Finances/Business Plans This kind of knowledge are for board, managing director and finance section/department leader and other with special needs.

Secret Information This kind of knowledge are for security manager and other with special needs.

11.2 Knowledge in company - a discussion

11.2.1 The challenge - secrecy versus function

It is obvious that a company's knowledge must be spread on the organisation and on several staff members regards their job function. If one individual person holds information that no

Table 11.1: Stakeholders knowledge.

Stakeholders	**Knowledge**
Staff	Knowledge in staff are divided as shown in section above: *11.1 Type of Knowledge*
Guardian Staff	Knowledge level = Work Area Knowledge + Advanced System Documentation. This group of staff have more knowledge then the general employee. They need access to areas and systems affected by their guarding instruction. If necessary they can have access to other knowledge.
Owners	Knowledge level = Public + Staff Basic + Strategy/Financial and Business Plans. Other knowledge as needed.
Electrical consumers	Electrical consumers have only access to public knowledge

Table 11.2: Threat Agents Knowledge.

Threat agents	**Knowledge**
Hackers	Knowledge level = Public.
People against windmills	Knowledge level = Public.
Dissatisfied staff	Varying. There can be a lot of knowledge here...
Stressed staff	Varying. There can be a lot of knowledge here, but in this case he/she will hopefully tell his/her surroundings relatively immediately after an unwanted event
Malware	Not applicable.
Rodent animals	Not applicable.
Wind	Not applicable.
Suppliers	Varying. There can be a lot of knowledge regarding products, buildings and employee roles.
Contractors	Varying. There can be a lot of knowledge here...
Temp staff	Varying. There can be a lot of knowledge here...

other knows, the company have a unwanted situation. People tend to get sic or injured/killed in accidents etc. In the same time, we need to filter/hide some company knowledge for some employees. From the information security manager the challenge may be huge.

11.2.2 Do we trust our employees?

How much should we trust a member of staff? How much knowledge should individual persons hold? The challenge is to get a functional organisation without being naive to what knowledge the company hold. Leaders need to stress every employee regarding the company's policy regarding information/knowledge. A organisation with good loyalty and trusted employees takes time to build. Many organisations works perfectly without military level of security regarding knowledge – but they may not know if they loose important knowledge...

11.2.3 Do we manage a rigid and high security level?

With the usage of a complex and rigid security system we also add more risks by using this. The efficient and effectiveness of this kind of complex information systems must be evaluated (cost/benefit). People tend to take short cuts when possible, and a rigid security system may in some cases be to much to handle. In the same time we can actually monitor and audit the employees activity. This model gives us much more control to see who accesses what kind of information. We actually have track of our employees activity and can find unwanted activity prompt. Please note that a extensive monitoring of employees may go against some legislation (The Right to Privacy Act).

11.2.4 Knowledge administration in general

In information security it is a best practise approach to handle information/knowledge on a "need to know basis". A lot of information in a company may from an employee point of view be seen on as public - but this may not be the case. Social engineering is very effective in getting more information then necessary. Even the company's owners need to be limited in their knowledge. When fewer people know business critical information the possible leakage are in general analogous (e.g. lower chance of leakage). Nevertheless, it is important to spread critical knowledge over several individuals to avoid loss in knowledge when people quit etc.

11.2.5 Examples of "need to know knowledge"

Technical details about the controls of the company's windmills may give anti-windmill people just what they need to destroy the actual windmill's critical functions.

Technical details about the company's computer equipment may give an external attacker (hacker) an easier task just because he/she know what equipment they are facing.

A technical failure regarding the buildings access control alarms are not critical until the matching threat agents know this.

Chapter 12

Game Theoretic Formulation

In this chapter we will use game theoretic nature of the attack-defence scenario. We will simulate an attack from on of our threat agents.

12.1 Anti Windmill People Attack - The Scenario

12.1.1 Background information

Windmills in Norwegian untouched landscape have in many project been a problematic battle - this case was not different.

Access and usage of the island

The island where the company's windmills are places was earlier a much used recreation area for a a smaller number of people (in average 10 different people throughout each year). They had to use their private boats to travel to the island. The island had no proper harbour/key, so they could only visit the island in the summer period when the weather was calm. This situation was not that often, so many times the visitors could not access the island.

Former estate owners

Initial the island was owned by a local fisherman. The earlier owners had died and 14 relatives had inherited the island. This made the buying process a challenge.

From a good idea to media storm - the price was high

The windmill project was problematic from the first day the media got information about it. This may because of bad planning (bad risk analysis) or the way media handled the case. The company Windy Island Power had to pay a large price in the end to get all 14 estate owners willing to sell. The agreement included a recreation key for visitors and lifelong maintenance of a track that goes all around the island.

The "battle" goes on

The local media and people that used to visit the island made problem all the way during the building process of the windmills. Windy Island Power ended up calling the police several time during the building process. Several of the local anti-windmill people got penalty during this time. These people are especially a threat further...

12.1.2 New attacks expected

Recent rumours have reached Windy Island Power; there are reason to believe that an new attack from anti-windmill people are coming soon. Monitoring of underground forum online and rumours in the local community can not be ignored.

12.1.3 Game Theory Approach

Definitions

We define here the players and their utility/payoff in table 12.1

Table 12.1: Players and their utility/payoff.

Players	**Utility/Payoff**
Windmill Attackers	Make trouble for company, make them loose money and/or reputation.
Guardian Staff	Keep production as normal, stop windmill attachers from executing their sabotage plans.

Players strategies

We add the players strategy in table 12.2.

Table 12.2: Players strategies.

Players	**Strategies**
Windmill Attackers	1 - Destroy control cables to windmills 2 - Attack remote access to company 3 - Use Social engineering via an employee
Guardian Staff	1 - Avoid but identify windmill attackers 2 - Identify windmill attachers 3 - Identify and imprison windmill attachers

Possible outcome of the game

The following table 12.3 shows the utility/payoff for the players of this game scenario.

Table 12.3: Matrix showing players choices with possible utility.

Windmill Attackers $\Longrightarrow$ **Company $\Downarrow$**	**Physical Windmill Attack**	**Remote Access Attack**	**Social Engineering**
Attack avoided, ID known	s1{2,-2}	s2{3,-3}	s3{0,-2}
Attack success, ID unknown	s4{-2,2}	s5{-3,3}	s6{-2,2}
Attack success, ID known, attackers imprisoned	s7{-1,-3}	s8{-1,-3}	s9{-1,-3}

s1 **Windmill attackers** was unsuccessfully in their physically attack to destroy some windmill parts; they are not satisfied. In this case they may be identified. This means that they may use a lot of time in dialogue with the police/layers etc.

Company avoided the attack but must use time in dialogue with police/lawyers for a 50/50 chance imprisoning. The attackers may sue the company for harassment/being physically brutal.

s2 **Windmill attackers** was unsuccessfully in their attach against the company's remote access; they are not satisfied. In this case they may be identified. This means that they may use a lot of time in dialogue with the police/layers etc.

Company avoided the attack but must use time in dialogue with police/lawyers for a 50/50 chance imprisoning. The attackers may sue the company for harassment/being physically brutal.

s3 **Windmill attackers** was unsuccessfully in their social engineering attack; they will not be satisfied. In this case they may be identified. This means that they may use a lot of time in dialogue with the police/layers etc.

Company avoided the attack but must use time in dialogue with police/lawyers for a 50/50 chance imprisoning. The attackers may sue the company for harassment/being physically brutal.

s4 **Windmill attackers** manage to physically destroy some windmill parts; they will be satisfied. In this scenario they where not identified.

Company lost money (less production, repair time, spare parts and man hours) and have not identified the attackers.

s5 **Windmill attackers** manager to attack the company's remote access; they will be satisfied. In this scenario they where not identified.

Company lost money (less production, repair time, spare parts and man hours) and have not identified the attackers.

s6 **Windmill attackers** manage to attack using social engineering; they will be satisfied. In this scenario they where not identified.

Company lost money (less production, repair time, spare parts and man hours) and have not identified the attackers.

s7 **Windmill attackers** manage to physically to destroy some windmill parts; they will be satisfied. In this case they are identified and will most likely end up in jail.

Company lost money (less production, repair time, spare parts and man hours) but must use time in dialogue with police/lawyers for a rather safe case.

s8 **Windmill attackers** manager to attack the company's remote access; they will be satisfied. In this case they are identified and will most likely end up in jail.

Company lost money (less production, repair time, spare parts and man hours) but must use time in dialogue with police/lawyers for a rather safe case.

s9 **Windmill attackers** manage to attack the company's remote access; they will be satisfied. In this case they are identified and will most likely end up in jail.

Company lost money (less production, repair time, spare parts and man hours) but must use time in dialogue with police/lawyers for a rather safe case.

12.1.4 Game Theory Conclusion on actual game

The game theoretical approach above includes many premises, which are subject to discussion. The goal for the company are the findings of how an attacker may think. It can often be a good idea to do some role playing during the discovery of utilities/payoffs.

In general - Windy Island Power end up as the loosing part of this game. When people decide to break the law and commit vandalism on other property (either physically or virtual), this is always difficult to handle. Companies in Norway are not allowed to use guns - thank god for that! Nevertheless, this kind of game playing can give much important knowledge in how threat agents think.

Chapter 13

Countermeasure/Control Identification

We will in this chapter identify countermeasures/controls and estimate (or "guesstimate") factors regarding risk.

13.1 Threats – Countermeasures/Control

We have here suggested countermeasures against vulnerabilities and threats identified earlier in this report (chapter 6 and 7).

The evaluation of cost is in thousand Norwegian Kroner (NOK 1000,-).

The evaluation of effekt, reduce risk, retention risk, avoidance risk and transfer risk uses the following scale:0(none), 1(low), 2(medium), 3(high) and 4(very high).

13.1.1 External Threats

Table 13.1: Countermeasure for external threats, DoS. Buy a more powerful firewall.

Countermeasure: Buy a more powerful firewall. A more powerful firewall can resist more powerful attacks					
Cost	**Effect**	**Reduce risk**	**Retention risk**	**Avoidance risk**	**Transfer risk**
100	1	2	0	0	0
Comments: General port scanning and weak DoS attacks can in better degree be dealt with, but the most powerful attacks will still be able to stop/reduce our service.					

Table 13.2: Countermeasure for external threats, DoS. Buy a very powerful firewall.

Countermeasure: Buy a very powerful firewall. A very powerful firewall can resist powerful attacks					
Cost	**Effect**	**Reduce risk**	**Retention risk**	**Avoidance risk**	**Transfer risk**
1000	2	3	0	0	0
Comments: A very powerful firewall can resist DoS attacks in large scales, but still we can not totally be secure about huge DoS attacks (typical the variant DDoS which have knocked out huge companies as Google and PayPal).					

Table 13.3: Countermeasure for external threats, software failure/bugs. Subscribe on experts.

Countermeasure: Subscribe on experts from supplier. Their are updated on weakness and software bugs on actual firewall. They can execute upgrades from remote when necessary.					
Cost	**Effect**	**Reduce risk**	**Retention risk**	**Avoidance risk**	**Transfer risk**
50	3	2	0	0	2
Comments: Software bugs and exploits are discovered every day. This agreement are a god action to be updated all the time - but remember that new software bring new bugs...					

Table 13.4: Countermeasure for external threats, unauthorised access. Increase security level.

Countermeasure: Buy an expert to help increase the remote access security level. Training must be included. Mobile workers computers must be checked. Policy regarding remote access must be updated/rewritten.					
Cost	**Effect**	**Reduce risk**	**Retention risk**	**Avoidance risk**	**Transfer risk**
200	3	3	0	0	0
Comments: Proper remote access security level is important. There are many good solutions.					

13.1.2 Internal Threats

Table 13.5: Countermeasure for internal threats, software failure/bugs. Buy an expert.

Countermeasure: Buy an experts from supplier. Set up an updating server for all internal computers so they get fresh updated software and antivirus etc. at every login.					
Cost	**Effect**	**Reduce risk**	**Retention risk**	**Avoidance risk**	**Transfer risk**
300	3	3	0	0	0
Comments: Software bugs and exploits are discovered every day.					

Table 13.6: Countermeasure for internal threat, unauthorised access. Increase security level and monitoring/auditing.

Countermeasure: Increase security level + increase monitoring/auditing + internal security course.					
Cost	**Effect**	**Reduce risk**	**Retention risk**	**Avoidance risk**	**Transfer risk**
500	3	3	0	0	0
Comments: Users need to know how importance information security is in the organisation.					

Table 13.7: Countermeasure for internal threat; incorrect operation. Improve training, procedures and documentation.

Countermeasure: Improve training, procedures and documentation.					
Cost	**Effect**	**Reduce risk**	**Retention risk**	**Avoidance risk**	**Transfer risk**
300	3	3	0	0	0
Comments: Knowledge in operating advanced computer systems are crucial. It staff are insecure, they must find help in documentation/procedures.					

Table 13.8: Countermeasure for internal threats, physical failure - electricity. Buy an UPS.

Countermeasure: Connect important computer equipment to uninterruptible power supply (UPS). A power loss and/or noise/transients in electrical power supply can destroy computer equipment.					
Cost	**Effect**	**Reduce risk**	**Retention risk**	**Avoidance risk**	**Transfer risk**
500	3	3	0	0	0
Comments: Prepare an test procedure and train on power loss.					

Table 13.9: Countermeasure for internal threats, physical failure - electricity. Buy an generator and UPS.

Countermeasure: Connect important computer equipment to uninterruptible power supply (UPS). For longer power failure - buy also an generator. A power loss and/or noise/transients in electrical power supply can destroy computer equipment.					
Cost	**Effect**	**Reduce risk**	**Retention risk**	**Avoidance risk**	**Transfer risk**
1000	4	4	0	0	0
Comments: Prepare an test procedure and train on power loss.					

Table 13.10: Countermeasure for internal threats, physical firewall failure. Subscribe on swap agreement.

Countermeasure: Subscribe on swap agreement. Computer suppliers normally offer so-called swap agreements on special equipment (routers, switches, firewalls).					
Cost	**Effect**	**Reduce risk**	**Retention risk**	**Avoidance risk**	**Transfer risk**
100	1	2	0	0	2
Comments: We do not avoid downtime with this action. The spare parts must be shipped from our supplier.					

Table 13.11: Countermeasure for internal threats, physical firewall failure. Buy a spare unit.

Countermeasure: Buy a spare unit. For expensive equipment this may be a high cost but if the actual unit also are very important we may consider this action.					
Cost	**Effect**	**Reduce risk**	**Retention risk**	**Avoidance risk**	**Transfer risk**
500	4	3	0	0	0
Comments: Spare units must be tested and updated to actually make a functional spare.					

Table 13.12: Countermeasure for internal threat, physical firewall failure. Outsource firewall service.

Countermeasure: Outsource the firewall services. Buy the firewall services from an external company.					
Cost	**Effect**	**Reduce risk**	**Retention risk**	**Avoidance risk**	**Transfer risk**
500	3	4	0	3	4
Comments: Please note that outsourcing also add risk. The cost in this estimate are correlated against our savings of the actual firewall, internal man-hours, training etc.					

Chapter 14

Risk Management Strategies

In this chapter we will use two decision strategies in our struggle for selecting the right countermeasures/controls in our risk management strategies.

14.1 Decision Strategies

14.1.1 General Comments

We have in general 4 different ways of handling our risks:

Reduce risk / Retention / Avoidance / Transfer = RRAT.

In tables below we have merged the the scores of my evaluation of countermeasures/controls regarding RRAT in the way that the highest score end up as the SUM of all the RRAT parameters. This is because if we manage to get a high score on one of them - we are in general happy. The outsider here are the retention (acceptance), this parameter is only used when we have done every action regarding cost/benefit to reduce or avoid actual risk.

The column *magnitude* represents the scale of how this event will influence the company in time and effort.

The column *likelihood* show the likelihood estimated in chapter 10 in this report and are annual estimates.

The column *Sum* are calculated like this: Sum = $\frac{1}{cost}\times$ effect $\times$ RRAT $\times$ $\frac{1}{Likelihood}\times$ Magnitude The cost and likelihood are inverted because they need to be a positive drive in this calculations. The larger the calculated sum are - the better the choice countermeasure/control are. The company want, of course, low costs and high uptime on the firewall service.

14.2 The tables with countermeasures/controls regards firewall service

14.2.1 Subscribe to a swap unit agreement

Table 14.1: Subscribe on swap unit agreement.

Countermeasure: Subscribe on swap agreement. Computer suppliers normally offer so-called swap agreements for this kind of equipment.					
Cost	**Effect**	**RRAT**	**Likelihood**	**Magnitude**	**Sum**
100	1	2	0.2	1	0.1
Comments: We do not avoid downtime with this action. The spare parts must be shipped from our supplier.					

14.2.2 Buy a spare firewall

Table 14.2: Buy a spare unit.

Countermeasure: Buy a spare unit. The firewall are an important asset in the company's infrastructure.					
Cost	**Effect**	**RRAT**	**Likelihood**	**Magnitude**	**Sum**
500	4	3	0.2	2	0.24
Comments: Spare units must be tested and updated to actually make a functional spare.					

14.2.3 Outsource the firewall service

Table 14.3: Outsource firewall service.

Countermeasure: Outsource the firewall services. Buy the firewall services from an external company.					
Cost	**Effect**	**RRAT**	**Likelihood**	**Magnitude**	**Sum**
500	3	4	0.3	3	0.24
Comments: Please note that outsourcing also add risk. The cost in this estimate are correlated against our savings of the actual firewall, internal man-hours, training etc. The probability in this countermeasure are higher because of more systems, people and building involved etc.)					

14.3 Decision dilemma

We have in this section described 3 possible solutions to our struggle in decreasing the risks regarding our edge to Internet; the firewall. The firewall are a very crucial part of both our

internal and external communication needs. When we own and operate it in our own organisation we take the cost of the unit in addition to training etc. When we outsource this service we can avoid these costs, but the risk also rises and the more complex solution gives a higher likelihood regarding downtime. This is of course a very simplified dilemma - but it may also likely be the case.

14.3.1 Maximum Expected Utility (MEU)

The decision strategy using Maximum Expected Utility (MEU) focus on the the best outcome regarding utility and probability/likelihood. In our case the *outsourcing firewall service* action would we chosen. This is because the risk was moved out of the company and we have fully transferred the risk to an other company; the actual ISP/ASP.

14.3.2 Minimize Maximal Regret (minimax regret)

The decision strategy using Minimize Maximal Regret (minimax regret) are focused on that whatever we decide, we will regret as little as possible whatever the result of fail decision will be. In this case we would have to choose the alternative of *buying a spare firewall*. This is mainly because the probability/likelihood was smaller in this alternative.

14.3.3 Decisions must be taken

Decision strategies can most likely end up on different alternatives, as we have shown here in this chapter. There are a lot of historical data to show crucial effects of wrongly made decisions. What angle or drive the leaders/decision makers have are hopefully in harmony with the companies policy. We do not want to make wrong decisions - but we humans do make mistakes.

The important learning in this chapter is obvious; we can take right decisions without proper sustainable evidence with the use of some methods in our mind (decision making under ignorance). We may decide without knowing if it was the right decision – but we must *never* be afraid of changing this decision if we come up with more solid background information. Many leaders unfortunately tend to be very stubborn when it comes to change their opinion/meaning, which is very sad. Easy understandable methods can in this way help them change. Another important element is that people tend to be very creative when they cooperate/work together, and good decisions can often be the fruit of teamwork!