Defining Information Security As a Policy

Bachelor Thesis
Software Engineering and Management
IT University of Göteborg

Author: Göran Pettersson
Supervisor: Björn Olsson

Date: 2008-05-26

Abstract

This report is a bachelor thesis created for the Technology Center as a part of the Software Engineering and Management programme at the IT University of Göteborg.

The report deals with the problem of security issues in organizations with wast amounts of data. The question at issue asked what could be done to increase information security for the Technology Center at the IT University of Göteborg.

While solving the problem the report presents the Technology Center and what their IT-resources is and why they should be secured. The author describes the method used to gather data that was used in a risk assessment and analysis.

The next part in the authors struggle to increase information security was to create an information security policy. The policy is a document that all members and users of the Technology Center should read and follow as it has rules and guidelines that can help the organization minimize the risks found in the analysis.

The author recommends that the organization as future research creates more formal supporting policies that focus more on a single subject like network- or user management.

Foreword

First I'm thanking my supervisor Björn Olsson that helped me with the choice of thesis subject and all the advice and support while I struggled. Also I give thanks to the Technology Center at the IT University of Göteborg as without it and it's merry members my thesis would have been empty. My lovely wife that got me to move to Göteborg deserves a great thanks as without her I would not have found the IT University of Göteborg and it's Software Engineering and Management programme.

Lastly I would give thanks to Professor Gene Spafford that coined a phrase that has nested deep inside of me: "The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards—and even then I have my doubts."

1 Introduction

One thing that is often overlooked in companies and organization is clear rules and guidelines for how their information resources and data should be secured. If data is lost due to user error or neglect that could most certainly have been avoided if the user would have had education or a set of rules to follow while processing data. Even a simple thing as leaving a cable on the floor could mean system downtime or loss of network access if someone trips and unintentionally unplugs the cable. If data then gets corrupt and no recent backup exist the company or organization could be in big trouble. These threat examples and more can be reduced or eliminated by risk analysis and the implementation of countermeasures.

1.1 Background

The organization that the author is going to help design an information security policy for is the Technology Center at the IT University of Gothenburg, hereafter shortened to the TechCenter. The TechCenter will host several virtual environments and databases for students to aid them in school related activities, for instance learning and managing an Oracle SQL database.

1.2 The Problem

As the TechCenter is a fairly new institution[1] it lacks guidelines and policies including an information security policy. The lack of policies compromises data security and integrity together with plans to handle crises such as theft or fire. Also the users lacks a document that informs them about how to handle their accounts and passwords.

1.2.1 Problem Formulation

A common mistake when someone thinks about information security their focus will be on the external threats, like intrusions or DoS[2] attacks. Information security should also include internal threats. By internal the author includes staff and the users of the TechCenter. A user mustn't be aware that they are handling data, like their user account wrongfully, in fact it is common that the user errors are accidents that could have been avoided if the user had rules to follow.

[1] The TechCenter was formed 2005

[2] Short for Denial of service. When a server gets hit with a massive amount of outside requests so legit request gets denied access.

1.2.2 Question at Issue

The question at issue that the author will answer in this report is: “What can be done to increase information security for the Technology Center?”

1.3 Method

Applied constructive research is the research model the author uses as he tries to solve a problem and improve on the organizational process. The method chosen to use for information collecting is the Qualitative method with a ethnographical research method as the data is gathered from documents, participant observation and interviews.[3]

This method was chosen as the author found a direct approach from the inside of the TechCenter organization could give him a good source of information. He also gathered information from literature that have been written about information security policies and subjects close to it.

As the TechCenter is such a new institution, written information was lacking. Data was therefore gathered during weekly meetings that the TechCenter members had and with meetings with a key member from the faculty.

1.4 Purpose

The purpose for choosing this subject was to get a deeper knowledge of information security and to create an information security policy that the TechCenter could use to help it secure it’s IT-resources.

The author also wanted to enlighten people about the different aspects and areas that information security has and to expose risks that could be potentially damaging to the TechCenter.

1.5 Delimitation

As the author is time limited he can’t follow-up the use of the information security policy so he’s delimiting his work to the creation of the information security policy. Also the organization is so new it hasn’t yet stabilized and matured. This brings both frequent organizational changes and changes to the hardware and software. Therefore he set out to create a more general information security policy that should have smaller and more specific policies connected to it to give it more robustness.

[3] http://www.qual.auckland.ac.nz/

1.6 Disposition

This report starts with the introduction that describes the background and the problem together with the question at issue that the author set out to answer. In the chapter theoretical background the author focus on his literature study, he also explains the meaning of the definition “Information security”. A general explanation of what a policy is are also present in this chapter together with an explanation of information security policies, threat pictures and the process of risk analysis.

In the chapter named Implementation the author explains how he went about in his search for information and how he created the policy. The next chapter is about the result that he got from this study. The conclusion and discussion chapter discusses if he reached his goals and gave answers to the question at issue. Future research gives some points on his ideas about future improvements to the TechCenter’s information security and it’s policies. Lastly the author has the references used in this report and the added appendix is the finished information security policy.

2 Theoretical Background

The most valuable asset a company or organization possesses is it's information. This can sound strange but if one think about it what would happen to a company if it's secret recipe for a soft-drink would come into a competitors hands? Or if an organization would loose it's system database that contained information assets like customers, invoices and plans?

The above scenarios are good points on why one should be concerned about protecting ones assets. When considering the cost of security breaches it's hard to set a specific cost but Sharon Gaudin from InformationWeek has looked into a recent study written by Khalid Kark from Forrester Research that sets the cost to between $90 and $305 per lost record. This can lead to enormous amounts if the damage is severe. Just think about the cost for a software company that might need to have their programmers redo their work because someone broke into their system and erased their servers and backups.

Another thing that might be overlooked is the loss of reputation that might arise after the breach gets public. This could mean that some companies might cover up a breach to not let their lack of security be known to the public. Shostack and Stewart[4] confirms the authors thoughts as they mention a company that was subject of a security breach and that was keeping the breach secret until a Californian law was founded that demand organizations that lose control of people's personal data to notify the persons affected.

Another interesting but dangerous thing that could happen to organizations is social engineering. Social engineering by definition is about the errors humans can make regarding security like loosing their wallet and it includes manipulating people into for example mentioning their password to their user account to a complete stranger face-to-face or remotely. Some estimate that 80 percent of a corporations information knowledge are present with it's employees.[5] A famous user of social engineering is Kevin Mitnick.[6]

2.1 Information Security

Information security is a term that describes the need to protect information based upon the fact that information is classed as a valuable asset.[7] So what information forms are considered as information that should be protected? Well, any medium that can hold information such as an audio tape, a letter, a compact disc or a webpage is considered but it's the value of the information that sets the level of needed information security work.

Garry Geddes explains another aspect of information security: "*every information security framework is centered on understanding the risks to the organization and managing them to an acceptable level."*[8] This statement is all about the value of risk assessment and this is a vital part of information security. If an organization is unaware of risks or lacks a plan to minimize them their IT-resources are in danger.

---

[4] The New School of Information Security, Adam Shostack, Andrew Stewart, 2008

[5] Threat Analysis, Infosecurity 2008

[6] http://en.wikipedia.org/wiki/Kevin_Mitnick

[7] Handbok i IT-säkerhet, Predrag Mitrovic 2005

[8] Information Security: Design, Implementation, Measurement and Compliance, Timothy P. Layton 2005

So far information is the only thing that has been taken into consideration of a need of protection. But there is more things worth mentioning and those are put together into the term IT-resources. An IT-resource could be an application, hardware, operating systems and the data that these resources manages is a form of information. Information security is a mean to help protect the resources integrity, availability and confidentiality. The IT-resources needs to be protected from alteration, unauthorized access and damage.

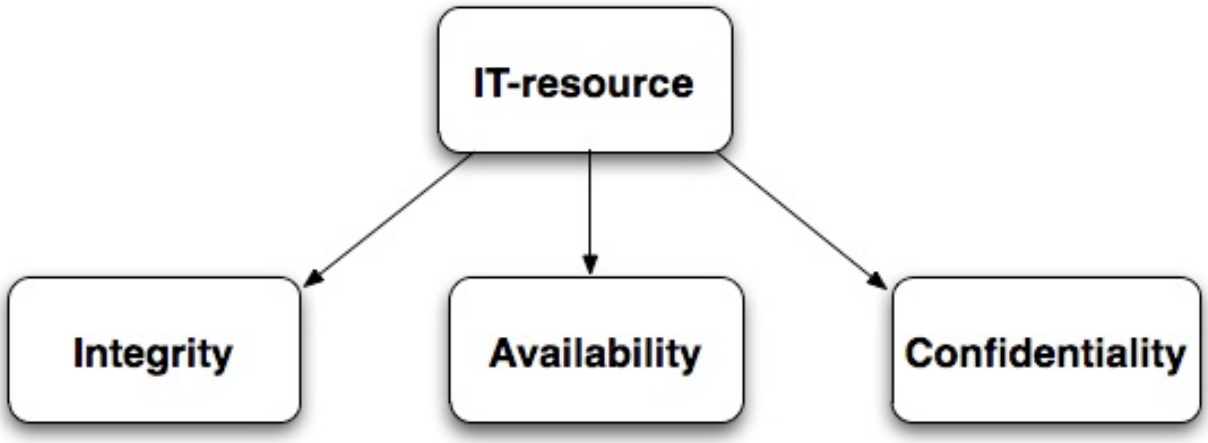

Figure 1: IT-resource diagram

- Integrity of an IT-resource means that the resource changes after an authorized and predetermined procedure. If something differs from this is a risk for the resource.
- Availability describes how an IT-resource is available for the authorized users.
- Confidentiality means that the IT-resources only can be utilized and access by authorized users and services. If something tries to access the resource without the proper authorization the resource should be kept secret.

2.2 Policies

Policies are guides and not rules or laws that governments have enforced. They are however guides that should be viewed as organization rules that need to be followed.

The Sans institute defines policies as: “A policy is typically a document that outlines specific requirements or rules that must be met.”[9]

[9] http://www.sans.org/resources/policies/#name

2.2.1 Information Security Policies

Matt Bishop explains security policies as: “A security policy defines “secure” for a system or a set of systems” in his book “Introduction to Computer Security”[10]. By “secure” he means that one can choose how secure you want your system or organization to be and that you define how the policy should look like. It is important to take into consideration that one can make very strict policies or make them more informal. The policy shouldn’t be to detailed but give a good view of the organizations security work and it should be clear on how to follow it. The author find it a better idea to have smaller more specified policies than one large. For example; a network policy could explain how the network can be used.

To create a good information security policy one must also think about and reference to guidelines and possible standards that might subsist within the organization.

Also when constructing policies and information security policies it is important to take other policies into consideration that exists in the organization. In the TechCenter’s case they have to obey their internet service providers policy, in this case it’s Sunet’s Acceptable Use Policy of Sunet[11].

Updates and revisions to the policy is necessary to keep it up to date with management issues and if new systems or applications are installed.

[10] Introduction to Computer Security, Matt Bishop 2004

[11] http://basun.sunet.se/html_docs/info_sunet/rules.html

2.3 Threat Picture

Predrag Mitrovic states that a definition of a threat picture is: “Threat + Weakness + Vulnerability = Threat Picture” in his book “Handbok i IT-säkerhet” . To understand and have a good information security the author needs to find out which vulnerabilities the TechCenter has, to come up with a good strategy to minimize the threat picture.

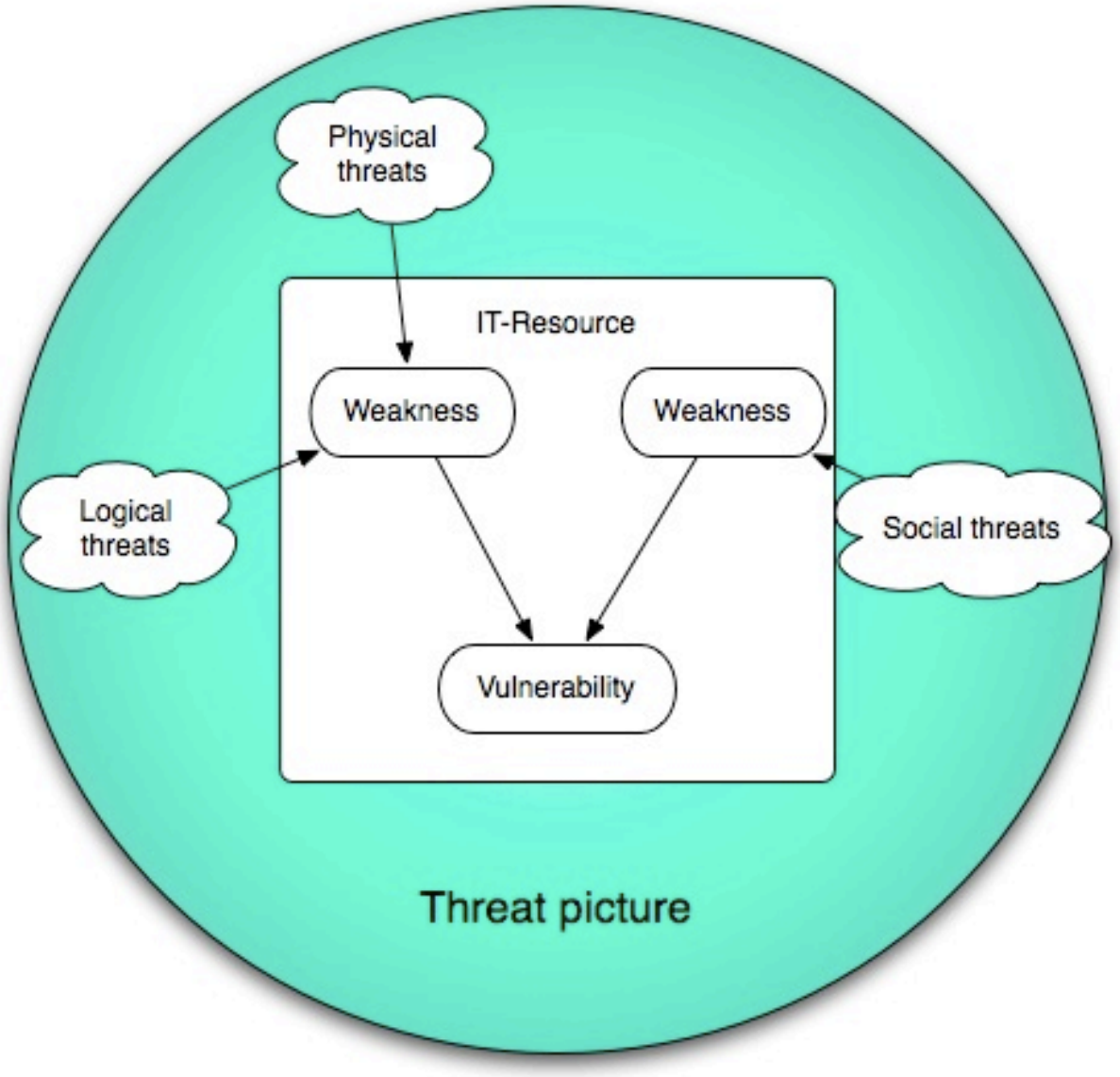

Figure 2: Threat Picture model

Things that could damage IT-resources are defined as threats. The author has chosen this categorization of the threats the most usable as it gives a good real-world picture:

- Logical threats: Bad software, viruses, root-kits, worms, trojans, unauthorized access.
- Physical threats: Faulty hardware, cooling issues, fire, floods and theft.
- Social threats: Lacking or bad system administration, system maintenance, user accounts, lack of system knowledge and social engineering.

Weaknesses are known or unknown faults.

- Software with known or unknown security holes, this includes operating systems.
- Weak password security routines, could be a lack of password cryptography.
- Bad readiness, could be lack of routines to handle upcoming event.

Known and unknown weaknesses and threats combined is what makes up the definition Vulnerability. This includes hardware, software bugs and even misconfigurations that someone with bad intent could misuse.[12]

2.4 Risk Analysis

A risk analysis shall assess and identify everything that could go wrong in an organization, what the odds are of it occurring and and what consequences it might pose. Douglas J. Landoll states: “Within the core of best practices is the security risk assessment.”[13] and this is indeed a good statement when one understands that without the knowledge of the risks one can’t take action against them.

For most organizations the media is important to give a good picture about the organization, but it could lead to bad press if a story leaks out about the organizations possible lack of security. More things to take into consideration is the possibility of loss of data and the costs to bring it back and fix the security issue. One must look at the possibility of the risk happening and the value of the IT-resources that is involved. A corporation might find that a good backup system is an IT-resource that is prioritized high and more of the budget might be spent on a backup system than on cable ties due to the higher priority.

Rebecca Herold states: “Prevention is much less expensive than response and recovery” in the book “Information Security Management Handbook”.[14] This statement summarizes the thoughts behind risk analysis and information security.

A good tool to use while analyzing the threats and risks to an organization is to look at the tables on the next page. The security levels should also be taken into consideration.

[12] The Best Damn IT Security Managament Book Period, Syngress 2007

[13] The Security Risk Assessment Handbook, Douglas J. Landoll 2006

[14] Information Security Management Handbook Sixth Edition, 2008

Physical threats to IT-resources

	Availability	Integrity	Confidentiality
Hardware faults	X	X	
Environmental hazards like fire or floods	X	X	
Theft	X	X	X
Unauthorized access, physical	X	X	X

Table 1. IT-resources physical threats.

Logical threats to IT-resources

	Availability	Integrity	Confidentiality
Lack of logging		X	
DoS attack	X		
Viruses, worms or other harmful code	X	X	X
Unauthorized access, logical	X	X	X
Software bugs	X	X	X

Table 2. IT-resources logical threats.

Social threats to IT-resources

	Availability	Integrity	Confidentiality
Lack of clear organizational roles	X	X	X
Lack of administration	X	X	X
No event logging	X	X	X

Table 3. IT-resources social threats

Mitrovic[15] states that by looking at these tables one can see that the social threats are the ones that can bring the most harm to the organization. The author disagrees, one can't just

[15] Handbok i IT-säkerhet, Predrag Mitrovic 2005

look at these tables and look at the table that has the most “X” and think that it is always like this. He thinks that a mix of these tables are the most dangerous and in reality is what can cause the most harm. You can have a great administration with clear rules and roles but still, theft and bugs might afloat. A good start is to look into the social aspect but one must not forget about the other areas.

3 Implementation

The author started his ethnographical research by coming into contact with one of the IT University's faculty members that was strongly involved with the TechCenter. He gathered information from him and analyzed it to get a feel of the organizational needs. This helped him while conducting the ethnographical research as he had gained a knowledge foundation about how their organization looked like.

3.1 The Organization Today

From the TechCenter meetings he attended, a lacking of administrational structure was evident. Surely they have two leaders which are faculty members but no set guidelines, rules or policies exist inside the TechCenter organization. This can be understood when one take the organizational youth into consideration. The process of building up the administration together with member and hardware gathering has only just begun.

So no crisis plans exists and no internal policies exists whatsoever. This made the author wanting to conduct a risk analysis from an information security point of view. To make this possible he needed to know what their IT-resources was and who were going to use them and how. As the TechCenter is much an Ad-hoc organization still in it's early phase this is a tricky thing to do as not all IT-resources are known and they change and grow constantly. After the analysis he started making the information security policy.

3.2 Risk Analysis

To make an information security policy the author must know what IT-resources exists inside the organization. If he don't know that it would be impossible to conduct a risk analysis as it is the IT-resources that he will analyze.

He took the users, members and systems into consideration and made risk estimates on what possible could happen and what impact it would have to the organization. Costs was not considered as the organization is not paying it's members and most of the hardware is donated by different companies. Also most of the countermeasures in the risk analysis are free, they are strictly involving the management which the members could address themselves without the involvement of a third party. The risk that the author saw that had the highest risk and with that the highest priority was the backup system.

3.3 The Information Security Policy

As the author's risk analysis was completed the work with crafting of the information security policy started. The organization is small and this lead him to create a more general policy that can grow with more specific policies that goes more deeply in on their subjects, like a network policy or a user policy. There was no other policies to look at that belonged to the TechCenter so the author based it completely on his risk analysis that was conducted using ethnographical research.

4 The Result

The author completed his research and analysis which lead to the creation of the information security policy. It needs to be approved by the TechCenter managers before it is set into use. The organization must remember to update it as changes occur that could have an impact to the policy. The policy will be presented to existing and new members of the TechCenter as a way to increase the security knowledge and minimize risks.

5 Conclusion And Discussion

The question at issue that this report would bring an answer to was: “What can be done to increase information security for the Technology Center?”

Organizations are dependent on information, it is a dependency that grows day by day. Therefore if find it important to secure it and keep it available to the users that are authorized to use it. Also plans on how to deal with incidents and crises is crucial to help minimize damages and to keep information available.

During the authors research he found that having documented rules and guidelines helps with the above and it can also keep costs for maintaining the security to a minimum. These organizational rules and guidelines would in the end form a document called information security policy.

His work with this report and finally the creation of the policy was a great way for the author to both help out the TechCenter with their security issues but also give him a more hands on experience with information security. The author had also before he started this report participated in an information security course so this had spawned his interest for organizational security.

The author read many interesting articles about this subject and found many complete information security policies from different areas such as universities and corporations. The choice fell on free accessible literature and policies as he had no funding and he found that they were well written with good guidelines. Surely the author could have bought a well established security framework from an organization but he found it interesting to look at others work and think for him self while he created the policy. The author could also have been more specific in the policy but that would have required time and resources that he didn’t posses, together with the constant changes in the server park it felt as a good choice to create a more general information security policy.

6 Future Research

As the information security policy leans towards the more general direction the author suggest that it should be broadened with more specific connected policies. A suggestion would be for instance a network management policy and a user management policy.

The faculty members that are responsible for the management and the enforcement of the policy should review the policy as changes occur within or outside of the TechCenter which could have an impact on the organization.

7. References

Literature

Introduction to Computer Security, Matt Bishop 2004

Information Security Management Handbook, Sixth Edition, 2008

Handbok i IT-Säkerhet, Predrag Mitrovic 2005

The New School of Information Security, Adam Shostack, Andrew Swewart, 2008

Threat Analysis, Infosecurity 2008

The Best Damn IT Security Managament Book Period, Syngress 2007

The Security Risk Assessment Handbook, Douglas J. Landoll 2006

Internet

http://www.informationweek.com/news/security/showArticle.jhtml?articleID=199000222

http://www.sans.org/resources/policies/#name

http://www.obfs.uillinois.edu/manual/central_p/sec19-5.html

http://basun.sunet.se/html_docs/info_sunet/rules.html

http://www.qual.auckland.ac.nz/

http://en.wikipedia.org/wiki/Kevin_Mitnick

Appendix

Appendix A: Information Security Policy

Information Security Policy

TechCenter IT University of Gothenburg

Date: 2008-05-26
Approved:

Introduction

As the purpose of the TechCenter is to aid the students with operating system virtualization, database access and storage capabilities appropriate security measures are needed. Once one takes into account that data will be transfered both inside the University and external via network it is understandable we can't overlook the risk factor.

There are many different groups of users and their needs are different and this Information Security Policy understands that their use of data could differ. This policy is not intended to limit the use of the TechCenter but merely secure it's IT-resources.

Purpose of This Policy

IT-resources includes operating systems, applications, hardware and the data that these resources handles. Information security is a mean to help protect the resources integrity, availability and confidentiality. The IT-resources needs to be protected from alteration, unauthorized access and damage.

- Integrity of an IT-resource means that the resource changes after an authorized and predetermined procedure. If something differs from this is a risk for the resource.
- Availability describes how an IT-resource is available for the authorized users.
- Confidentiality means that the IT-resources only can be utilized and access by authorized users and services. If something tries to access the resource without the proper authorization the resource should be kept secret.

The purpose of the information security policy is:

- To create a firm approach to information security for the TechCenter.
- To help analyze and propose countermeasures to risks. That includes the misuse of applications, network, computer systems and the data.

Threat Picture

The definition of a threat picture is: Threat + Weakness + Vulnerability = Threat Picture. To understand and have a good information security the TechCenter administrators needs to find out which vulnerabilities the TechCenter has, to come up with a good strategy to minimize the threat picture.

Threats are things that could damage the TechCenter's IT-resources. They are split up into different categories:

- Logical threats includes: Bad software, viruses, root-kits, worms, trojans, unauthorized access.
- Physical threats include: Faulty hardware, cooling issues, fire, floods and theft.
- Social threats include: Lacking system administration, system maintenance, user accounts, TechCenter member responsibility administration and lack of system knowledge.

Weaknesses defines IT-resources known or unknown faults.

- Software with known or unknown security holes.
- Weak password security routines, could be a lack of password cryptography.
- Bad readiness, could be lack of routines to handle upcoming event.

Vulnerability explains how much an IT-resource is vulnerable by known and probable weaknesses and threats.

Countermeasures

The way to handle the information and the IT-resources are done by assessing countermeasures and coming up with effective countermeasures. One must also take into account the cost and resources needed to reach the countermeasure goals. The types of countermeasures are split up into three categories:

- Logical countermeasures: Firewall with intrusion detection, unison user administration and virus protection.
- Physical countermeasures: Fire alarm, temperature monitor, secured server room door, backups and an identical server ready incase of server failure to prevent downtime.
- Social countermeasures: Have clear roles, organization, user education and rules.

Responsibility

Two faculty members are the Managers of the TechCenter with full organizational responsibility.

The User Administrators should be responsible for the creation and management of the user accounts.

The System Administrators are responsible for the system management and maintenance.

The Network Administrators are responsible for the management of the TechCenters webpage, irc and shell accounts. This also includes the firewall setup and other network applications.

All users are responsible to follow the set policies, rules and guidelines that apply to them.

All severe events and alarms should be reported to the Managers.

General Policy

- The IT-resources shall be identified together with the possible threats and risks to them.
- Information security should be brought up on all major TechCenter meetings.
- Monitoring and security reviews of firewalls, routers and servers must be done on a regular basis. Access logs and results of intrusion detection software shall be included.
- User education is vital so that they understand how to keep the systems protected. This policy shall also be distributed to the users. The form and scope of the education shall be matched to the different types of users, i.e. Network Administrator, System Administrator and normal users.
- The roles of the people involved with the TechCenter should be clearly specified.
- Periodical vulnerability and risk assessment tests of external network connections are enforced. Twice per term is a good practice to follow, of course, it could be done more often or when new software or hardware is installed.
- A plan for the event of a crisis shall exist and should be updated when necessary.

Finances

All costs from information security measures should be covered in the budget for the TechCenter.

Consequences

If a user breaks the user rules they shall be reported to the User Administrator and access to the systems within the TechCenter shall be restricted.

System Security

- All systems shall be updated to the latest versions with the latest security patches.
- Users logging on to a system inside the TechCenter should be reminded about following this policy.
- The system shall ask the user to change password after 4 weeks.
- Daily backup of the systems and databases shall be performed.

System Maintenance and Management

Maintenance

The System Administrator shall perform these checks daily so that the systems performs as they should:

- That the daily backup is done correctly.
- That the systems and disks temperatures keeps under critical levels.
- That cables and systems are well mounted to keep accidents to a minimum.
- That all system warnings are attended to.
- That the network communication works as planned.

Management

The Managers shall enforce and oversee these things:

- A plan including all hardware, applications and services shall exist and be updated when changes are made. Also a plan over the network shall exist.
- An UPS should be connected to the most important systems to allow time for correct shutdown of the systems to prevent loss of data. The UPS also keeps the connected systems protected from common power problems such as voltage spikes.
- The TechCenter server room shall be locked and access should only be allowed for authorized persons.
- Servers and hardware should be theft marked to help prevent theft.
- All work that has been done in the server room should be written down in a log to increase traceability. Examples of what counts as work are installations, patches, firewall settings, system updates and hardware changes.

Account Management and Passwords

User accounts for the TechCenter is handled by the Account Administrators. It is important to give the account the right type and access rights to keep the systems from harm. Different systems could mean that different accounts are needed.

- The accounts are personal and should be treated as such. Do not let another person borrow your account.
- Trying to gain more access than your account allows is prohibited.
- A good password shall consist of a minimum of 8 characters, symbols, digits and letters. To increase the password strength use both upper and lower case letters. Do not use names, real words or simple keyboard key combinations. A strong password example is: D7rW!k6P
- Your password is personal and shall be kept secret.
- When a TechCenter member or user leaves the IT University his or hers TechCenter accounts shall be removed to minimize the risk of account misuse.

Follow Up

If the TechCenter encounters changes in it’s management or systems this policy shall be looked into and be updated accordingly.

Supporting Policies

- Acceptable Use Policy of Sunet