School of Mathematics and Systems Engineering

Reports from MSI - Rapporter från MSI

Security of the mobile devices in Växjö Kommun and corporation

Enis Krkusic

November
2009

MSI
Växjö University
SE-351 95 VÄXJÖ

Report 09079
ISSN 1650-2647
ISRN VXU/MSI/DA/E/--09079/--SE

Content List

List of figures

Abbreviations

LAN = A local network that connects a local workplace/school.
WAN = Wide Area Network. Connects two or more LAN:s.
RAS = Remote Access Server. A remote server that can be dialled with modem/ISDN to get access to a network e.g. Internet.
VPN = Virtual Private Network. A virtual private network that establishes a secure connection for confidential communication between companies.

1 Introduction

Mobile devices are a part of everyday life in our society. They are used in our homes, in our schools, in our jobs, and even in our hospitals. Most of them are developed from ordinary old-school devices. Like home phone, you could not take you home phone with you everywhere you go. To solve this developers developed cell phone which you can bring with you everywhere you want to. Take computers instead – first came out laptops but that was not "mobile" enough, then PDAs which can fit in a pocket and have the same functionality as laptops with some limitations.

Most of the mobile devices were designed for some purpose and had only a few functions. Cell phones could only be used as a phone, but nowadays you can use them as cameras, media players, personal calendars, projectors, calculators, clocks, radios and so on. My point is that you forget that it is a phone because of how the development of mobile devices has increased.

As development has increased so has the use of mobile devices increased. The more **cool** and **useful** functions, the better the mobile devices are and the use area increases. The majority of mobile devices today are used in entertainment and business area. Take an ordinary family for example – the father is working as an IT manager in some company. He owns two cell phones, one from work and other is private. At his job he has a business laptop, and at home his private. He uses USB memory sticks and different mobile devices in his job. The mother is a teacher at high school and she also have a cell phone and a laptop and uses memory sticks. She likes to listen to music so she owns an IPod as well. Their children are between 12 and 19 and each of them is using cell phone, some kind of media players, USB memory sticks for school work etc.

What if some of them loses their mobile devices? What if the father loses his laptop or it got stolen? What about information security on all of these mobile devices? Is there any security solution for these devices, and is it strong enough? Well, these are questions that needs to be answered.

Since my education is about security I wanted to do something that is related to security topics. Luckily I got in contact within Växjö municipality and corporations directly owned by the municipality (in this document I will present it as Växjö kommun only) and they were in need of an analysis of security policies and security solutions for all mobile devices used in their area. Since mobile devices are common for Växjö kommun the security level need to be satisfied from information security aspects.

2 Research questions

Växjö kommun and corporation got a new security policy in December 2008. This policy is a total policy referring to all security, including information security. For information security, during spring 2009, it will be specified some guidelines that will result in developing different security instructions.

The biggest vision is that Växjö kommun and corporation will reach to BITS-level[1]. One of the important ”hot topics” about information security is mobile devices, like cell phones and USB-memory sticks. The need of security suggestions is in focus because of the increase in functionality and network connection to internal important systems. At Växjö kommun it is common to use many different mobile devices with different security levels. Some of them are secure enough, and some of them need higher security level. Gathering milestones for policies for those devices is needed.

Questions to be answered in this thesis are:

1. Which security policies, security instructions, milestones etc there are for information security/network security/computers inside Växjö kommun.
2. What is a mobile device and what security solutions there are for those?
3. Go through all mobile devices in Växjö kommun and analyze them.
4. What are the security suggestions for those devices?

[1] Base level for information security defined by MSB-MYNDIGHETEN FÖR SAMHÄLLSSKYDD OCH BEREDSKAP – Society protection and emergency authority.

3 Method

This chapter describe parts in the process of this project. General approaches like questionnaire, interviews and selection of staff involving in this project are discussed.

3.1 Choice of method

To get answers to my questions I am mostly going to use scientific articles about mobile security. The main part is going to be focused on questionnaires and interviews with staff from about 15 different units in Växjö kommun and corporation. Once completed I have a material to work with and analyze.

With questionnaires comes a problem – in my case negative effects to reliability. If questions are not clear enough the answers may be wrong and this leads to misinterpret. To handle this interviews are used to complement the questionnaires since one can discuss unclear questions and reliability increases.

Interviewing specific people is big advantage since those people are in some matter responsible for different IT departments. One disadvantage is that there is competence variation about mobile devices in those different departments.

3.1.1 Questionnaire

The Questionnaire consists of eight simple questions that are related to mobile devices. Since the processing part of this project is focused on those questions, it is important that the questions are as easy as possible to understand for those who are answering them. The first seven questions are related to each type of mobile device used in that part. The last 8th question is general for mobile security and needs to be answered only once for each person answering questionnaire.

The questions were constructed by a person who works at the IT department in Växjö kommun. Since those questions are important to be answered and analyzed I refined them and added a few of my own. Each question has a short introduction and a short example that makes it easier to answer. Developing those questions I thought about what answers would be interesting for to gather. My supervisors at Växjö University and Växjö kommun, both of them got the chance to take a look at the questions and give me a feedback.

3.1.2 Interviews

Interviews are important because I want to get the whole picture. There may be answers that are wrong or questions that are misunderstood, in that case both I get the chance to ask about the answers, and people who are answering the questions get the chance to correct and understand them.

Since the interviews may help me to gather the important information that may not show up with only questionnaires I will go through the old questions and perhaps come up with a revised questions that might be used in the future.

3.2 Selection

Given that there many different people working for Växjö kommun I chose to interview only them that have enough competence about information security. I visited IT-coordinators at following units:

- Care administration
- Work & welfare
- Upper secondary school
- School child care

- Environment and health
- Culture and space-time
- Technical administration
- Town building office
- IT department at municapility, administration part, support, system and strategy part
- VEAB
- Växjöhem
- Hyresbostäder
- Värends räddningstjänst
- VÖFAB
- Vidinge

3.3 Time plan

I got about 10 weeks for working with this project. Approximately once a week I will meet my supervisors Fredrik Ringberg at Växjö kommun and Ola Flygt at School of Mathematics and System Engineering at Växjö University.

- First weeks are needed for planning and preparations.
- Interviews are going to be during weeks 3-6.
- Week 7 is going to be used for analyses of data.
- Weeks 8 and 9, working on security suggestions.
- Week 10 closing part and presentation for Växjö kommun.

4 Processing

Questionnaires were emailed to participants (different IT-Coordinators) in Växjö kommun and interviews were booked via e-mail or phone and held in participant's office where discussion about questions answers was held.

4.1 Questionnaires

Fredrik Ringberg emailed information to participants that I was going to contact them about this project. I emailed the questionnaire to all participants. In the beginning I did not got any response from participants about questionnaires. I emailed it once again but I got response only by few participants. This problem was solved by Fredrik because he called them and sent one more email.

4.2 Interviews

Since I got replier from the majority of the participants later than expected, I booked as many interviews as possible last weeks in April. At the interviews I informed participants what this project is about and what am I going to use the information for. Since all of them got questionnaires before the interviews the meaning of interview was to go through those questions and for me to gather information about mobile devices. Interviews took about 1 hour.

4.3 Loss of answers

At the beginning I was pretty sure that at least some of 19 participants were not going to participate. But at my surprise all 19 participated. My plan was to interview someone at the IT-department in the Växjö University but unfortunately I could not get so much information because responsibility was divided at different departments in Växjö University. Why I wanted to interview Växjö University was because it is a huge organisation (about 15 000 students) so it would give me an overview of what kind of security solutions they got when mobile devices are involved.

About the questions, some of the participants could only answer for example only about mobile phones, but it was ok because they worked in the same department as some other participants that I interviewed.

5 Result and analyses

This chapter presents result and answer to the research questions in chapter 2. It begins with declaration of security policies in Växjö kommun today, following by definition of mobile device.

5.1 Security policies, instructions, milestones etc inside Växjö kommun?

To understand the architecture of the Växjö kommun's data communication I want to present you how it is built and who is responsible of different area of the network.

The following milestones are decided for Växjö kommun data communication:
(Policy Växjö kommuns datakommunikation 2008-05-27)

- The network consists of mainly three separate networks, called administration network, student network, and public network. On the administration network there is all administrative staff. There is also all administrative servers and systems. Student network is a common network for all schools, from pre-school up to upper secondary school. On the student network there are all students and several teachers. The administration staff for schools is on the administrative network.
  Third and last network, the public network is open for public for example at the library.
- The IT-department is responsible for WAN and LAN communication for those three networks. To get an homogeneous standard, all WAN communication, like fibre, Radio LAN, fixed and phone connections, routers and all LAN-communication like data network, data sockets, switches and other communication equipment is ordered by the IT-department.
- The IT-department is responsible for the communication backbone where all WAN connections are connected together. The backbone-network is placed in the municipality building.
- The IT-department is responsible for the operation of LAN communication on the administrative and the public network, and even for maintaining the standard and security on the student network.
- The school's technicians are responsible for the connection of pc-s and printers on the school's student network.
- The administration network, the student network and the public network are of LAN type. They are sharing the same WAN. Users on the administration network cannot access the student network and students on the student network cannot access the administration network. The public network can only access the Internet.
- The administration, the elementary school and the upper secondary school have their own Internet connection.
- For accessing the administrative servers from the Internet and home, VPN or (Mobility Guard) is used.
- For accessing the administrative resources on the student network the VPN or corresponding technique is used.
- RAS (remote access server) is forbidden. To move or to shut down connections that are ordered by IT-department is also forbidden. Even to change configuration on those connections and to use those connections for other then data connection is forbidden.

- Changes of WAN or connections between WAN and LAN may only be performed by IT-department.
- The IT-department is responsible for supervision of the whole WAN and LAN network in the Växjö municipality.

Policies for the school networks.
A user gets personal login and gets access to computers and personal home directory which is reachable no matter in which school the user is in[3]. A user has to read the rules and sign to accept following rules:

- Not breaking school's rules and laws
- You may not use any information technique during the lecture when your teacher says so. To avoid misunderstanding ask your teacher what is allowed during the actual case and always follow those directions.
- You may not use some other user's user identity, account or read someone else's e-mail.
- You may not give your own account to some other user.
- You may not try to hide your user identity.
- You may not try to access some network resources that you do not have rights to.
- You may not try to disturb or interrupt the intended use of the network.
- You may not obviously waste the resources like storage capacity, equipment or staff.
- You may not make any changes on the computers or it's equipment.
- You may not install or use some other software except preinstalled software only. Games also counts as software.
- You may not try to damage or to destroy the data information or deliberately spread virus. With virus suspicions take contact with someone responsible for advice and help.
- You may not use IT-resources to store or spread pornography, illegal material or copyright protected material like software, music or pictures.
- Responsibility that you have is to change your password often, to backup your own material and to erase not topical material.

Milestones for Växjö kommun:

- **Internet connection and e-mail are tools intended for use on work relate tasks and are owned by the employer. The starting point is that Internet is a tool for making it easier and to increase the efficiency of the work.**

(IT-Säkerhets instruktion Användare, Växjö kommun)

Information security:
Backup
No information is allowed to be saved on the local stationary computer (C:\) or on the computer's "desktop". Each user has an access to its own personal home directory U:\ on the fileserver. The IT-department is responsible for making automatically backup on all common servers. The information that someone is storing on common space that can be reached via Internet is automatically backed up.

You may choose to store on devices, U: or V:

- U: (personal home directory) is your personal unit which you can use for storing personal work material. If you choose U: your co-workers can not access the information.
- V:\Arbete_Valfard\Gemensam_Arbete_och_Valfard is a unit for storing information that all co-workers on the organisation can access.
- Under V:\ "Department" there are folders for each department. The department's folder is a unit for storing information which you and your co-workers on your department can have access to.
- In some cases can even a few unit labels be there.
- If you store information on your local hard drive (C:) you are the one responsible for all backup.

General rules

- It-system may not be used for storing personal or not work related information like music, pictures, movies or other that is not work related material.
- User information (login name and password) is personal and may not be copied or forwarded.
- Software (via private CD's, other media or downloaded from the Internet) may not be installed without the permission from IT-department.
- USB-sticks is to be used with in case of storing the secrecy material.
- All attempt to hack into Växjö municipality data system is going to be reported to the police.

Example of forbidden usage of the Internet

- Facilitating of drugs or publishing copyrighted material, for example file sharing is forbidden.
- Websites containing illegal material or some kind of offence may not be visited or searched for.
- The Internet may not be used for example videogames, gambling, shopping, personal shopping or participation of chat rums (communities).
- Downloading all kind of software from the Internet is forbidden.

Example of forbidden usage of the E-mail

- Usage of email for illegal activity or for distribution of illegal or offending material, for example agitation against ethnic group, bullying, chainmail or copyrighted material is forbidden.
- Internal e-mail received by mistake is going to be sent to the sender as soon as possible.
- Linking to web pages with the illegal content is forbidden.
- Usage of e-mail for the commercial purposes for example, sale, advertisement, and investigation is forbidden. Växjö kommun has the right to demand damages in case of breaking this rule.
- Gathering, manipulating, publishing, distributing and spreading information that is in the inside, if this is done for the commercial purpose or as link to the commercial activity is forbidden.

- Usage of Växjö municipality network, intranet, e-mail or other resources like distribution channel or contact base for commercial announcement, junk mail, spam or chain letter is forbidden.

(IT-säkerhetsinstruktion – Användare)

The following milestones are particularly for mobile devices

For mobile, laptops, handled computers, telephones etc. you shall be aware of that the information that you are storing on it locally you are also responsible for. This means that:

- You are the one making backup.
- You shall be aware that diskettes, external hard drives or USB-memory sticks are unsecure storage media.
- You shall be aware that others can have undue interest of getting the information.

[5]

Usage of Mobile Computers

Every mobile computer for example laptop, handled computer, mobile phone etc, that is being used outside of the office is a presumptive security risk.
Be aware of:

- The device has to be stored under supervision if it cannot be locked in.
- If you have information on the device that need to have higher security level than normal, you are the one responsible that is it encrypted.
- Always have backup copy at your ordinary office.
- Store devices and sensitive information in a secure way, even at your home.

[5]

5.2 What is a mobile device and what security solutions there are for those?

The word *mobile* has as a meaning to be capable of moving or being moved from place to place. A mobile device is known as a device used for some kind of computing tasks. Typically it has a display screen and some input buttons. There are different types of mobile devices depending on the tasks. Nowadays it is common that it is some kind of touch-screen interface on those devices. For a device to be classified as mobile it has to be some kind of Personal information Manager (PIM), Personal Digital Assistant (PDA), mobile phone, smart phone, camera phone, laptop, tablet personal computer and some kind of removable storage media.

Operating systems among those devices are typically Palm OS, Windows CE, Pocket PC, Smartphone 2002, Symbian, EPOC, and Linux. Among Laptops and Tablet PCs Windows XP, Max OS X and different versions of Linux is more common.[2]

I will present the most common mobile devices and what type of security solutions there is available for those devices.

Smart phones:

- Antivirus software
- Firewall software
- File encryption
- Many different levels of password, like password on the SIM card and device itself.

Laptops:

- Biometric solutions like fingerprint readers for login
- Antivirus and software
- Firewall software
- Encryption of files and discs/drives

USB-memory sticks:

- Password only
- Password and encryption

PDAs:

- Password
- Encryption
- Firewall software
- Antivirus software

Digital Cameras:

- None (but today Smartphones are widely used for taking pictures and they may have some security solution).

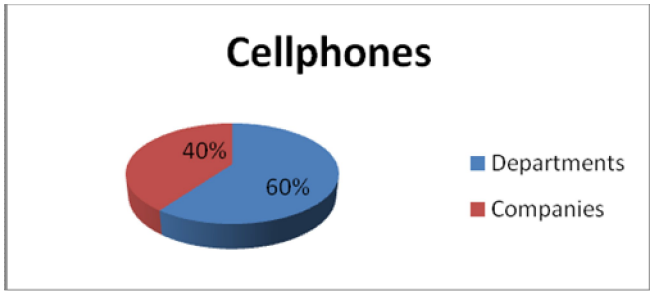
6 Mobile devices in Växjö kommun

This chapter is the result of the interview questions and presents mobile devices used in Växjö kommun following by security suggestions for those devices. I went through all mobile devices in Växjö kommun, 9 different departments, 6 different companies and 19 interviews. The following statistic is based on the answer of the interview questions.

Question 1: **Which types of mobile devices there are?**

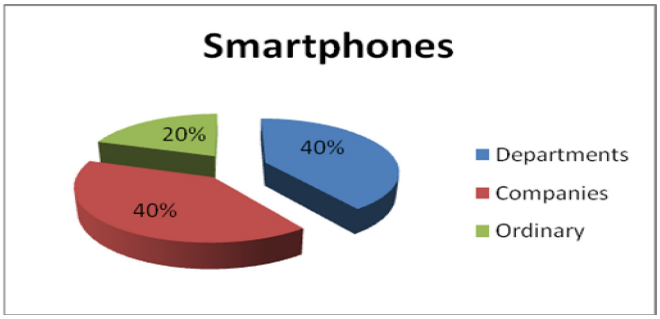
The statistics shows following:

Figure 6.1: Usage of the Cell phones



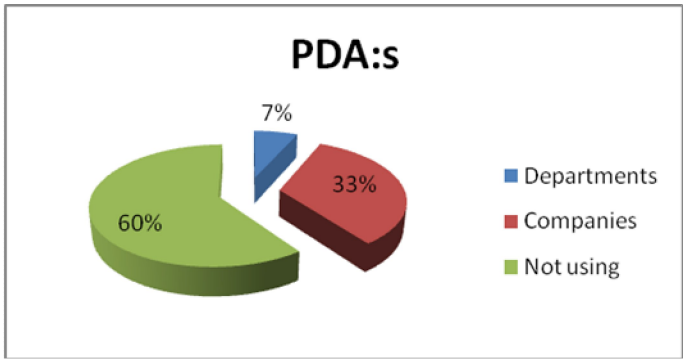
Statistic shows that all 9 Departments and all 6 companies use some kind of cell phones.

Figure 6.2: Usage of the Smartphones



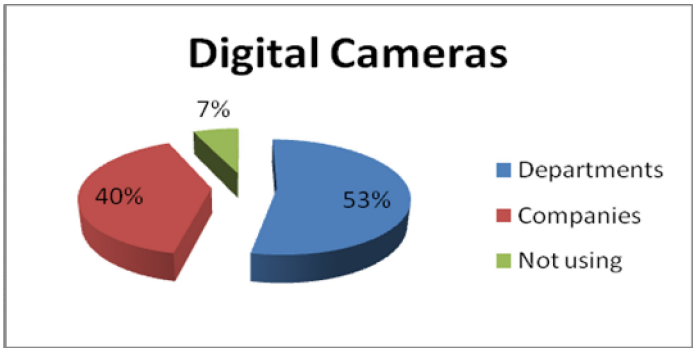
But 80% (6 companies and 6 departments) used some kind of Smartphone. Common types are Sony Ericsson, Nokia, Samsung and HTC with Windows Mobile as operating system.

Figure 6.3: Usage of PDA:s



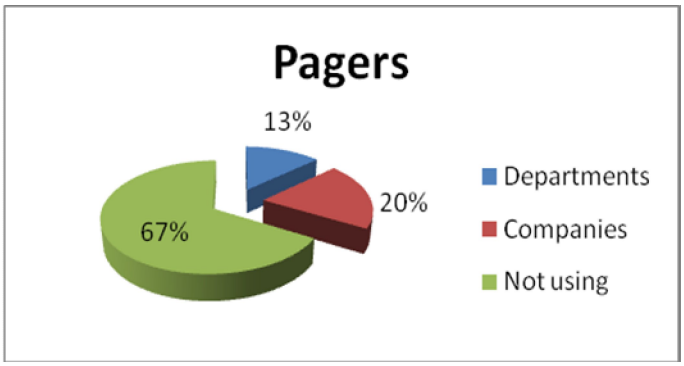
PDA:s are used by 40% (1 departments and 5 companies)only. Again Windows mobile is the most common operating system.

Figure 6.4: Usage of Digital Cameras



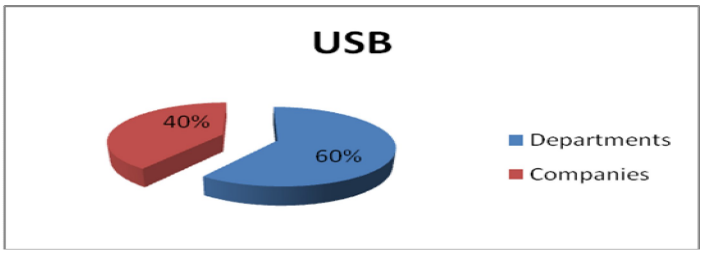
Digital photo cameras are used by every company and almost every department. Those cameras are mostly a few ones, so everyone has access and can borrow them.

Figure 6.5: Usage of Pagers



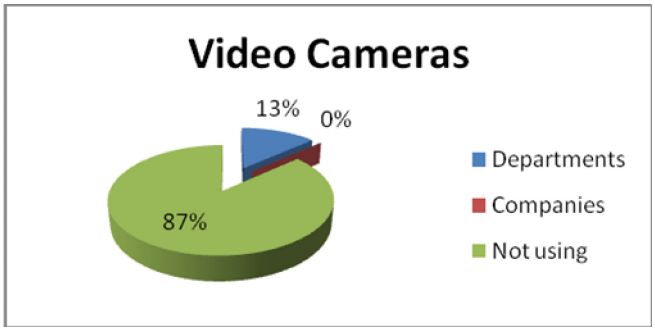
Pagers are no so popular, but there are a few ones that are used by preparedness. Staff that has to be available at all time in case of some emergency.

Figure 6.6: Usage of USB-Memory Stick



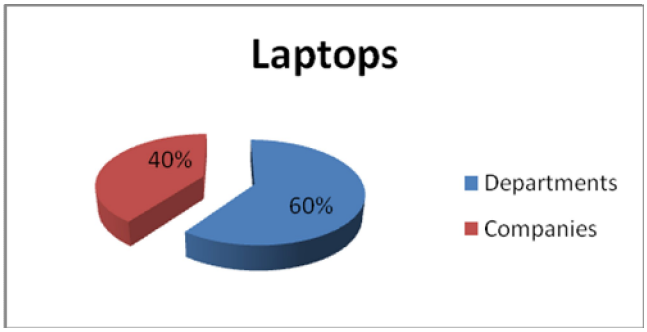
USB memory-sticks are used by everyone.

Figure 6. 7: Usage of Video Cameras



Only some departments used Video cameras, and none of the companies uses it.

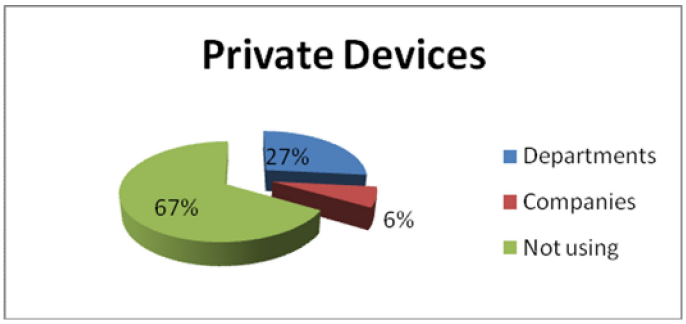
Figure 6.8: Usage of Laptops



Everyone is also using laptops.

Is there any private devices used for work related tasks?

Figure 6.9: Usage of Private Devices for work related tasks



33% is using some kind of private devices and 27 % of them are departments and 6% companies.

Question 2: **Who are using those devices?**
Use is very different and it depends on the department and company but generally it is like this:

- Cell phones: Almost everyone. Managers (mostly using Smartphones), and ordinary employees different kind of cell phone depending on their work task. In e.g. the IT department almost everyone have some kind of Smartphone, in social services they use simpler cell phone.
- PDA:s are used by people responsible for some kind of area. They are mostly used by people working whit real estates, like janitors, plant engineers, hosts etc.
- Digital cameras can be used by everyone because they are commonly used by everyone. Here are some answers for this question: hosts, plant engineers, everyone, web editors, investigators.
- Pagers are used by people working whit emergency tasks.
- USB memory sticks are used by everyone more or less. By administrators, managers, rectors, teachers, office-holders, civil servants and so on.
- Video Cameras are used by social services and there it can be all used by people working there. It can also be used by investigators.
- Laptops are used by people working in the office but also people working with some kind of administration like system administrator. Rectors, teachers, "inside employees", managers are mostly using them but there are laptops that can be used by any employee for e.g. presentation.
- Other devices like mp3 players, dictaphones, different measuring instruments and so on are mostly used by some kind of special employee. For example dictaphone and mp3 player is used by remedial teacher, and special measuring instruments by people in construction.

Question 3: **Where are those devices used?**
Simply answered it is everyone everywhere, except GPS that you have to be outside for to use. Cell phones, PDA:s, laptops, USB memory-sticks are used both inside and outside of the office, even at home. Cameras are sometimes used outside and sometimes inside depending of the work task.

Question 4: **Is there any device used for unobvious task?**
This question was interesting to know the answer of, take Smartphone for example – one forget that its main purpose is to call because of the many features.
Here are the answers that I got about this question:

- Cell phone as: GPS and SOS alarm, digital camera, calendar, only for data transfer, as part of the VPN solution, documentation.
  Cell phone is even used for scanning IAN codes, server administration.
- PDA:s for inspection. For example if the inspection of apartments is approved.

Question 5: **What type of solution is used for information secrecy?**
No strong security solution is used except following:

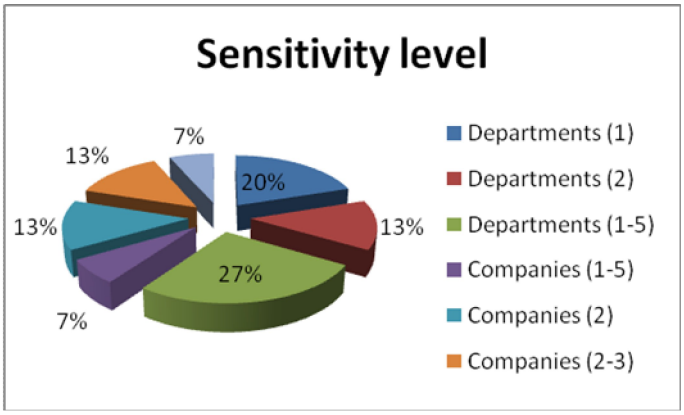
- Remote reset for Smartphones. This resets the Smartphone to factory defaults and files are erased.
- Pin code for cell phones and PDA:s.
- Login and password for laptops.

Question 6: **Is there any backup system for mobile devices?**
Answer is clearly no. This is because the synchronization is used for the important data

information. Other data stored on the mobile device is always a copy of the original one. But there may be exception. For example someone that is working on its laptop and stores the information locally and not on the file server. Since policy says that the employees are the one responsible for this kind of backup it is an obvious answer.

Question 7: **Sensitivity level (1-5)?**
Sensitivity level varies a lot. Depending on the department, device and information stored. Picture below shows the sensitivity level. Numbers between the brackets shows the sensitivity level, 5 beeing most sensitive.

Figure 6.10: Sensitivity level of the information stored on the mobile devices



Question 8: **Do you think that there is a need of resources for improving information security for mobile devices?**
This question got me a few discussions with the ones participating on the interviews. One fact was clear – the need of education and clear policy was the two resources mostly wanted.

Here are some answers for this question:

- It would be better with more information and suggestions for handling mobile devices from the IT-department.
- Routines and more staff working on information security.
- Education connected to usage of the system, and platform independent systems.

These are the eight questions that got answered. By them I got a picture of how the situation is in the Växjö kommun and companies in corporation.

7 What are the security suggestions for those devices?

This chapter describes security suggestions for mobile devices used in Växjö kommun. Suggestions are in form of simple milestones for a security policy for mobile devices or options built in mobile devices (or can be installed) that increases security.

7.1 Suggestions

Coming up with the security suggestion is one of the less simple things to do. Take the security police for example that says "use only encryptable "USB – memory sticks. One must think of different variables in this process. One is that perhaps staff that is using those devices need some kind of education how to handle the interface for encryption. Other one if it is efficient? How much time does it take to encrypt the 16 GB memory stick? Third one can be if it is really necessary to encrypt the information that we are currently having on this memory stick. Do not forget the economic part – how much does it cost to maintain this system?

I am going to present security suggestions for each mobile device found in Växjö kommun. Suggestions are technical solutions and/or milestones for security policy that improves security aspects for the mobile device.
But the most important thing according to Benjamin Halpert, is that organizations have some kind of mobile device policy that all employees are familiar with. [2]

Mobile telephones
There are two types of mobile telephones. Advanced Smartphones and simple ones where one can only call and use SMS.

Smartphones - since there is only Pin Code used when using the Smartphone it is easy hacking it since there are programs made for this purpose. I would suggest use of password on the device itself, when using the Smartphone with windows mobile operating system. Windows mobile usually has this option for activating the password of the device itself. It is easy to throw away SIM card and put another in the Smartphone, but as a hacker you still have to know the password of the device itself. The result is one more password to hack – which brings a higher level of security.

The second suggestion is to use some kind of antivirus for the Smartphone. Since Smartphones are more and more like ordinary computers, malicious code is going to be common in a few years and it is better be prepared in time. Since Malware (malicious software) can make Smartphones unusable the cost for fixing or replacing it is unnecessary and high enough.

Here are top 5 windows mobile antivirus:

- BullGuard mobile antivirus – Is a easy to use, and used for both Pocket PC and Smartphones
- F-Secure Mobile Anti-Virus – F-Secure is one of well-known antivirus programs for PC computers. The mobile version offers firewall, antivirus and anti-spyware protection.
- Airscanner Antivirus for Windows Mobile - is the antivirus that is mostly used for the Windows Mobile platform.
- Symatec Mobile AntiVirus for windows mobile – provides comprehensive and easy-to-update virus protection and quarantine.
- Trend Micro Mobile Security - is the antivirus that protects against viruses, SMS text messages spam and other malware attacks.

Some milestones when using Smartphones that I want to suggest are:

- Every Smartphone should have some kind of antivirus.
- Only staff that needs some kind of Smartphone in work related tasks will get it from the IT-Department.
- Do not store any confidential information on a Smartphone, for example some kind of password.
- If you store/get some kind of confidential information on your Smartphone, e.g. trough SMS or email delete it after using it and empty the trashcan immediately.
- Always have your Smartphone with you or lock it in a safe storage.
- The local password of the Smartphone is mandatory.

About "*ordinary* "cell phones just use them with common-sense and think about not storing any sensitive and important information for example in a SMS text message.

USB memory sticks

All most everyone uses USB-memory stick in Växjö kommun and other companies that are the part of this project. What I found surprising is that staff using them does not really use any kind of password. According to them they mainly use it for some kind of presentation etc. There are some that know that there is a password option but they do not use it.

My suggestion is to have memory sticks that are sorted for some kind of categories. For example one category called *for presentation*, other called "*for sensitive material*" and so on. In this case USB memory sticks that are used for presentation do not need to have any kind of protection and simplicity is important in this kind of task. On the other hand, when using the USB for storing the sensitive information passwords and encryption are used. In this case the information is protected.

Here are some examples of USB memory sticks with some kind of protection.

- DataTraveler Vault – is a USB memory stick from Kingston, one of the well-known producers in this area of information technology. It offers 265-AES hardware-based encryption. Price (4GB): about 1200 SEK.
- Iron Key – offers many different products and according to the test made by *Computer World* their USB-stick is the winner in the test made by them. The Iron Key is using AES CBC-mode encryption. Always-On encryption is used which means that all data written on the device is always encrypted. Price (4GB) : About 1700 SEK.
- Imation Pivot Plus – is a memory stick that provides strong data security protection. Since the 256-bit AES hardware encryption is used the password prompt will appear when you plug in device. Price (4GB) : About 359 SEK
- Sandisk Cruzer Professioonal – provides 256-bit AES hardware encryption as well.
  Price (4GB): About 1700 SEK.

Milestones when using USB memory sticks that I want to suggest are:

- Ask IT-department for information and advice when ordering USB memory stick.
- Always classify the sensitivity of the information before storing it on the USB memory stick and then use the suitable security solution for it.

- After using the USB memory stick with the sensitive information do not delete files, format the USB stick instead, in that case the information cannot be restored by third party.
- When using the USB memory stick don't forget to unplug it and put in safe storage area when finishing the task.
- Run virus check automatically when plugging in a UBS-memory stick into computer.

Laptops

Laptops are not the main mobile device but they are heavily used by IT-department and technicians e.g. maintenance of system servers etc. Threats that can come up are if someone stores locally on the device some kind of password for accessing system where sensitive and important information is stored. For example login information for server maintenance. According to information from the interviews no sensitive information is stored by "ordinary" staff because they are not allowed to store it locally. So no higher security level is needed since there is already password login.

About staff that has more important tasks it would be more secure to have some kind of two factor authentication. For example password login and fingerprint recondition or Smartcard. Do not forget users who are taking their laptops at home. Antivirus and firewall at home may not work properly which leads to spreading the virus to the entire system when returning back to the office.

Here are more suggestions that would increase security for laptops:

- Have a secure operating system that offers secure login. For example Windows XP professional.
- Be aware of security flaws when using the laptop at home.
- Do not forget BIOS password. Many computers have easy reset of BIOS but some need to be sent to the manufacture for resetting the BIOS. Both DELL and Lenovo have more secure BIOS protection.
- Mark the laptop in some way. For example engraving the company name, address and phone number. This increases the chance to getting it back in case of forgetting it somewhere.
- Register with the manufacturer. In this case the laptop gets flagged if thief sends it for maintenance.
- Rename the Administrator account. This is not huge security level but it will be harder for hackers and why make it easy for them. Do not use word "Admin" for new Administrator name.
- Antivirus and firewall software should always be activated when using the device.

Since laptops are not used so heavily the policy milestones that I want to suggest are:

- Do not leave your laptop in unlocked area and lock the system before leaving it even if you are only going to be away for couple of minutes.
- If you are temporarily storing sensitive information on your laptop you must use some kind of encryption system on it. Ask IT-department for more information about it.
- If you are using your private laptop for work related tasks you should be aware that you might be not have access for administration rights depending on your task as an employer.

Digital cameras and Video cameras.
The use of digital cameras is more common than the use of video cameras. Someone takes a picture with the digital camera but can even record a video with it. Video cameras are mainly used for video recording but there are cameras that can take a picture as well. Pictures could be very sensitive material for those people that are on them.

Sensitivity is not as high for cameras as it might be for Smartphones so the security level is well enough but here are some milestones that I want to suggest:

- After using digital camera, always format it if possible.
- After using the digital or video camera lock it in a safe storage.
- If possible format the video camera after using it.
- If you are storing sensitive material on the video or digital camera do not leave it anywhere before you store the material on the safe storage.
- Have some kind of register that tracks who used digital or video camera in case of misuse.

These are main things to consider in the policy when using video or digital camera, but there can be more simple things like stay to one standard type of cameras because it is easier to learn how to handle same type then many different.

PDA:s
PDA is on the way to be less used because Smartphones are more and more used instead. Since the synchronization is used the backup is not necessary but the risk for malwares is not excluded. For example just before synchronization you get a malware and your PDA crashes. It is same as for Smartphones, what if it gets stolen? Throw away SIM card is the classic thing hackers and thief do. One should think of what can we do to protect and destroy. Some of companies already have this service but I would suggest for everyone who is using PDA:s to have it. An example of this kind of software is Remote Wipe for iPhone.[12] Don't forget the antivirus as well.

Suggestions for this type of device are following:

- Have proper antivirus software to protect the device against malware.
- Have some kind of encryption program for data confidentiality.
- Do not leave your PDA in the car, open areas, office desk or at home available for third party. Instead have it with you or lock it in a safe storage.
- Make sure to check that no sensitive information is stored on it, if the information is temporarily stored then use encryption software.

Some software that can be useful for PDA:s are following:

- PocketLock for Pocket PC – is a encryption software for PDA:s. It runs on any Windows based PDA, has options for different levels of encryption.
- F-Secure is maybe more reliable since it is more well-known product. They offer antivirus protection for PDA:s as well.

Even some of the previous suggestion for Smartphones that I mentioned earlier can work for PDA:s

Pagers, Mp3 players, Digital Dictaphones and other.
Since those devices are the ones that are least commonly used and data stored is often simple, I wanted to go through them last and together. Let's begin with pagers, there is no risk for the virus because of simplicity of the device. If someone steals it no sensitive

data can be stored on them, this only leads to economic lost. Mp3 player nowadays can store any kind of data because of the storage set. It can be used as a USB-memory stick. But they are only used for special teaching (in our case) and storing mp3 audio files, some special security solution is not needed.

Dictaphones are also used in some cases, and I am not sure what kind of data is really stored there. E.g. interviews can be very sensitive then precaution is necessary.

About other instruments like measuring instruments used for construction purposes no sensitive data is contained and loss is only economic. In this case no information security precautions are needed.

Milestone suggestions for those devices are:

- Digital Dictaphones can contain sensitive information; lock it in the safe storage if no security solution is offered.
  (Olympus offers many different security solutions a.m. biometric solutions and encryption)
- Do not store anything else except mp3 files on the Mp3 players.
- All other devices used keep in the safe storage for avoiding thieves.

Like I said those devices are not so "smart" and do not contain so much information or do not contain any sensitive and useful information for a third party at all. Use them with common-sense and ask someone responsible for security instructions if something gets misunderstanding.

Table 1 – General security suggestions for mobile devices

Smartphone	PDA	Laptop	USB	Video cameras/Digital cameras	Other
Password	Encryption	Active and up to date antivirus and firewall	Encryption	Format after use if possible.	Store safe
Antivirus	Antivirus		Password	Store safe	Encryption
Not storing confidential information	Storing on safe area		Format after use.		

External hard drives are not used but if they come in use just be aware to manage it as a USB-memory stick because it is almost the same but it has more storage area. Use some kind of encryption software to protect files.

Generally for all kind of devices following milestones are important in a mobile device policy [1]:

- **Power-on authentication** – User is required to enter a password when powering on the device.
- **File/folder encryption** – Files and folders containing company information must be encrypted.
- **Antivirus software** – antivirus software that is running must be up-to-date and running at all times.
- **Lost/stolen/missing device** – Must be immediately reported to the supervisor.
- **Secure wireless transmission** – Wireless network used must be encrypted.
- **Firewalls** – Firewall used must be running and be up-to-date.
- **Passwords** – Strong passwords must be used.[1]

General suggestions

It is not always so easy to know what is needed, but these questions helps deciding what is needed:

- **How smart** is the device?
- **What** kind of information is stored on the mobile device?
- **What kind of security solution** do we have today?
- **How** is this solution used?
- Is it **secure enough?**
- What are the **options**?
- Do we have to adapt new solution **after our system used today**, or do we have to **adapt the system after the new solution**?
- What is the **"best" solution**?
- **Do not be "afraid"** for new solutions.
- Do not forget that **education** is needed for every new solution.

8 Discussion and Conclusion

Reviewing the statistic of the interview data I am not surprised of the results. Cell phones are so commonly used by everyone in the world, both in private and in business. Focusing on the mobile devices I got to know is it as a thought it was when use of different mobile devices is involved. Smartphones are getting smarter every time a new model enters the market. They are simply replacing PDA:s. Laptops are getting cheaper and cheaper and because of its simplicity and flexibility, use of laptops is growing and growing. The use of USB-memory sticks is so obvious is also nothing new. But that passwords are not used on them surprised me a bit. There were some memory sticks that had a password as an option but the password was not used. This is because people forget password and there is no administration system for this kind of incident.

Other mobile devices that are used do not have any kind of security solution. Like digital photo cameras and video cameras. The only solution that is secure enough is to lock it in somewhere. But is it enough? Since no accident has occurred yet it might be enough for now. With the future comes development of every digital device and then solutions used today may not be enough.

The security milestones that I found was quite ok but they covered more use of ordinary computers and not mobile devices so much. In one of the documents I found more like a information then clear policy and nothing about use of mobile devices. This is an area that every company/department should have clear policies about. Make some kind of investigation of what is used, and then work on the security policy covering mobile devices. This is very important for everyone involved since people would then know how to handle any kind of situation when mobile devices are used.

One problem with security solutions is that it costs. I was calculating what it would cost to have 100 secure USB-memory sticks with some kind of administration system and I got a six digit number (about quart of million SEK) every year.[13] This kind of system is definitely hard to justify.

Other problem that I would note is that there are many people I met in my work that would need more education about this area. I mean if IT coordinators need more education, how is then for others ordinary employees? When I asked what kind of resource is needed to improve information security, I got a clear answer that they would need more education and information about this topic. But again, money is involved and time needed for this kind of education, and this pushes unfortunately the priority down.

Use of common devices e.g. cameras and laptops is common in some departments. I am not sure if some kind of booking system is used but it would be good to have for every kind of device that is commonly used. I got an impression that threat from outside is not such a big threat, but do not forget threats from inside. It is easily happened that some employee takes some mobile device at home, what happens there no one knows. Next day the employee comes at the office and accidently spreads some kind of virus on inside system. This kind of accident is unfortunately not so uncommon.

I tried to contact some companies to see what kind of security solutions they got for mobile devices and it was impossible to get any information at all from them since they are busy or do not want to reveal it. Microsoft is very huge company and I found it surprising that there were no one in Sweden that could help me at all.

My conclusion is that Växjö kommun is taking information security very seriously. Since the IT-department in Växjö kommun is working with new milestones and taking the view of mobile devices in those milestones, improvement will be a result of it. Security solutions right now seems to be clear instructions and policies.
One important thing to be aware of is that it helps to visualize information instead of

using lots of text pages. Even to show examples of what went wrong on other organisations and why, can be good part of security education.

8.1 Future analysis

One could wonder what the future brings. What kind of security risk there would be and what kind of security solutions there would be for them. I think that every time some kind of security solution comes up, there would be someone trying to break it and maybe succeed in it. Operating systems that are emerging would provide more security solutions, like encryption. Biometric solutions are getting more and more popular. Fingerprint readers, iris scans, face recognition software and so on are getting better and more reliable. I think we will see more of them but combined for higher security level since there is a way to hack them as well.

The fact we are using digital devices in our everyday life brings the security risk for every device we are using. In this case I think some kind of unique scanning before pass would be a solution. This unique property is not going to be something that one can change and manipulate. It is going to be something that every individual is born with and unique, like DNA.

Something that is invisible for ordinary people today is that social network communities, like Facebook, can be used for some one's life mapping and in that case breaking of passwords. Name of relatives, friends, activities, numbers and so on are often used in passwords by private users, which make it easier for a hacker when he/she maps your social network via e.g. Facebook. There are people making money on this kind of information and Facebook is valuated to 195$ per user. This may sound a bit strange but it is just the way it is.

I did not had a chance to look at the wireless connection used and security solutions for this, but for the future work someone should take a closer look on how to secure it as good as possible.

9 Reference

[1] Green, A. , Information Security Curriculum Development Conference'07, September 28-29, 2007, Kennesaw, Georgia, USA.
[2] Halpert, B. , InfoSecCD Conference'04, October 8, 2004, Kennesaw, GA, USA.

Documents by Växjö kommun:
[3]. Kärnhusets regler,
[4]. Riktlinjer för användning av datorer och internet I Växjö Kommun,
[5]. IT- Säkerhetsinstruktion Användare,
[6]. Policy Växjö kommuns datakommunikation

[7]. http://en.wikipedia.org/wiki/Mobile_device (05-15-09)
[8]. http://www.microsoft.com/sverige/smb/security/sgc/default.mspx (04-14-09)
[9]. http://searchmobilecomputing.techtarget.com/generic/0,295582,sid40_gci1315281,00.html (05-15-09)
[10]. http://searchmobilecomputing.techtarget.com/generic/0,295582,sid40_gci1315281,00.html (05-15-09)
[11] http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1337531,00.html (05-15-09)
[12] http://www.apple.com/mobileme/whats-new/ (19-10-09)
[13] http://www.blockmastersecurity.com/product/secure-usb/ (19-10-09)

Appendix

Questionnaire

1. Mobile devices are becoming increasingly dominant in today's society. Examples of devices are mobile phones, USB keys, laptops, PDAs, digital cameras, pagers, and MP3/MP4 players etc.
- What types of mobile devices and models of those used in the administration / company? I it common to use private devices for work-related tasks, or that contain job-related information? What is it then for the type of device and why are they private?

2. Different types of mobile devices can be used by different types of personnel.
- Who uses the respective mobile device?

3. Use areas may vary depending on the mobile device used. Some examples are in the car, indoor, meeting, etc.. Where is each device used?

4. Many mobile devices have an obvious use. For example, a USB memory used to store information and a cell phone to call. Are there any mobile devices in the management / the company used for any other information that is not immediately obvious? For example, it could be a cell phone that is used to unlock doors, or any device used to track people. If so, give these solutions.

5. Since mobile devices can be easy lost, it entails the risk that unauthorized part can access sensitive information stored on these devices.
Examples are the mailing lists or sensitive documents on USB memory sticks.
- What type out of security solution for information privacy there is in the respective mobile device?

6. Backup of important data is essential. Many uses a backup system. Examples are an ordinary home users who have an external hard drive regularly copy important information from his workstation or a laptop.
- Is there a backup solution for various mobile devices. If yes please describe the solution. Is it centralized or local to each division of administration / company?

7. Loss of sensitive information can be serious. Make an assessment of the sensitivity of the information found on each unit of administration/company. Use a scale of 1-5 where 1 is not sensitive to 5 is at its maximum sensitivity.

8. Right skills and access to a range of resources is important to achieve a desired level of security.
- Do you think there is a need of more resources to improve information security of mobile devices? Please come with your own ideas for what types of resources there is needed. Examples of these may be to have a greater expertise in information security or multiple
technologies.

Matematiska och systemtekniska institutionen
SE-351 95 Växjö

Tel. +46 (0)470 70 80 00, fax +46 (0)470 840 04
http://www.vxu.se/msi/