Learning with Security

Päivi Jokela and Peter Karlsudd
University of Kalmar, Kalmar, Sweden

Paivi.Jokela@hik.se; Peter.Karlsudd@hik.se

Executive Summary

The current higher education, both distance education and traditional campus courses, relies more and more on modern information and communication technologies (ICT). The use of computer systems and networks results in a wide range of security issues that must be dealt with in order to create a safe learning environment. In this work, we study the security status within Swedish Net University, where several universities collaborate in order to offer ICT supported higher education distance courses. The total ICT-security is defined as a combination of computer security and information security, and the focus in this work is on the information security. The four main components of the information security that are used in the study are: confidentiality, integrity, availability and accountability.

The data gathering was made in two steps: first preliminary interviews then the main questionnaire. The interview respondents were a small number of students, teachers and ICT-experts at various universities, and the results of this preliminary study were then used to complete the questionnaire. The main questionnaire was sent to approximately 747 students, 106 lecturers and 40 ICT-pedagogues. The answers were analyzed both quantitatively and qualitatively. However, due to a relatively low response rate, we must point out that the conclusions made are based on these limited results, and are therefore not necessarily generally applicable within the distance education.

The results show that both teachers and students involved in distance education consider that they have relatively good basic competence regarding the use of various ICT-resources. In addition, they consider that the computers and network connections they are using have adequate technical standard. However, the respondents also express a need for more information and training in various areas that are directly connected to information security issues. What is more, both students and teachers require that adequate computer support is constantly available. It is especially important to pay attention to the differences that have been observed between the sexes. The studied material indicates that female students may feel unsure concerning the handling of technical equipment, and that they want more instruction in the use of computers as well as more computer support.

Several respondents have not developed procedures for backing up files on a regular basis. There seems also to be some uncertainty concerning which measures should be taken in order to protect computer systems from viruses and also what should be done if the computer is infected. Many teachers consider that the risk for cheating, especially for plagiarism, is greater in the distance education that in campus courses. These teachers also spend more time to prevent this problem in distance

Editor: Janice Whatley

courses, and may have special procedures in order to detect plagiarism.

Even if several security issues are indicated, most of the respondents consider that the general ICT-security in distance education has a relatively high standard. This may be a sign of some discrepancy between the users' knowledge and their actual behavior when they use the computer systems. However, there is a definite belief in the future when it comes to web-based higher education. Hopefully, reinforced user instruction and computer support can lead to both female and male distance students feeling more confident in modern technology and also to better match between the users' theoretical knowledge and their actions.

Keywords: higher education, distance learning, information security, integrity, availability, confidentiality, accountability

Introduction

Internet-based higher education is characterized by studies that are flexible and to a great extent independent of time and space, but very dependent on a well-functioning and reliable IT infrastructure. The students often work on their own and are expected to take a big responsibility for their own learning. They must also be able to utilize the IT resources in an efficient way in order to handle large quantities of information and to communicate with their instructor and other participants in the course.

The fact that the courses are becoming more and more dependent on IT resources puts high demands on the information security of the education. To create trust between those attending the course and the instructor it is extremely important that the information presented is correct and easily accessible, and that the channels of communication are dependable. It is necessary as well to be able to trace the original source of information, especially when the students´ individual knowledge and skills are to be judged in an examination (Gunnarsson, Lingefjärd, Mekki-Berrada, & Sjöblom, 2002; Jokela & Karlsudd, 2005). If we encourage awareness of the computer security issues, we will contribute to the deployment of an IT- infrastructure designed to minimize the corresponding economic and social risks (Stajano & Anderson, 2002). In light of this it is a matter of some urgency to observe and investigate those areas and factors that concern IT security.

New Way of Learning, New Students

University and college education in Europe and the USA has for some decades been in the focus for change and transformation. A growing number of students are to be educated with the support of less and less resources (Hargreaves, 1994; Trowler, 1998). The combination of inexpensive computers, fast multimedia technology and the Internet has created the conditions needed to increase the number of students, renew learning and open up new possibilities for lifelong learning. Distance education can be ideal for creating a situation in which instruction is teacher-supported instead of teacher-led. (Hjelm & Sandred, 1997; Light & Cox, 2001). But as the supply of distance education increases, the demands for IT security will also grow. In Swedish Net university education, which this investigation covers, over 21,000 students study with the aid of IT-based communication.

When investigating questions of security, it is important to distinguish between computer security and information security. Computer security refers to the technical aspects in connection with unauthorized accessibility and change or different kinds of disturbances in a computer system, while information security includes security problems associated with the handling of information in different activities (Gollman, 1999). In this study, IT security is defined as a combination of computer security and information security, and it is primarily information security that this investigation focuses on. In the net university's courses it is many times a matter of making the cor-

rect and reliable information easily accessible, rather than protecting information from being viewed.

A modern computer-based system of education is supported by strong interactivity between human users and computers, and many researchers consider the human ”soft” part of the system decisive for the total security level of the system (Gali, 1992; Siponen, 2000). Adequate information security demands a well-structured organization with clear guidelines and strategies and reliable technical solutions. At the same time, it is not sufficient that the organizational and technical basis for security exists in case the users of the system apply rules in a careless way. A great sum of constructive information has been published about the concepts of computer security (Bishop, 2003; Pfleeger, 2003; Summers, 1997), but it seems that people have to experience a problem in order to understand it.

It should be pointed out, too, that it is not always easy to combine serviceableness with information security (Allwood, 1998; Brandt & Wennberg, 2004; Siponen, 2000). In the universities and colleges it is especially important that the security measures do not create obstacles to the simplicity and accessibility that is necessary for the activities.

Information Security

Information security can be divided up into four areas: integrity, availability, confidentiality and accountability (Statskontoret, 1997). Integrity refers to protection from unauthorized change and it is a fundamental requirement for information quality. Availability guarantees that the authorized users can utilize resources whenever they are needed, whereas confidentiality means that sensitive information should not be accessed by unauthorized persons. Accountability means that the user cannot deny that he/she has sent or received a message or participated in or caused an action, and it is made possible by authentication of users.

Integrity

The concept of integrity comprises personal integrity, system integrity and information quality. Integrity means that the objects to be protected are safeguarded from unauthorized change. The loss of integrity can be the loss of usable data or other IT resources that supply servers, programs and networks. Information quality means that the services and data provided are without fault and have the correct degree of detail. Information that is produced should be correct, of current interest and intelligible (Statskontoret, 1997).

When the students plan their net education they search for information about, e.g., the content of the courses/programs, time schedules and examination forms. If this information is misleading and/or not up-to-date, or if it is presented in a way that is unintelligible, the information quality will become impaired. As the course information often plays a decisive role in the students´ choice of course, poor information quality can influence the application figures for the program in a negative direction. Another serious problem is that incorrect or unclear descriptions of the content of courses and examination requirements can result in students being put at risk of failing.

Availability

Availability means the possibility for authorized users to utilize resources according to their needs and within a desired period of time. If users through, e.g., interruptions of operations and disturbances are prevented from performing functions in the IT system, these are to be considered examples of the loss of availability (Statskontoret, 1997).

Throughout the duration of the course the students must have continual access to course material, programs and systems. If technical problems arise, it is also important that the students have ac-

cess to IT support – in both asynchronous and synchronous form, such as e-mail or telephone. To be able to communicate with the instructor of the course is likewise an important condition for successful study results (Mårald & Westerberg, 2004). Special access problems and the loss of valuable information can arise when handling long documents such as homework, reports and theses if the student does not put into practice the correct routines when handling different versions and back-up copying.

E-mail attachments and downloaded programs and files can be infected with harmful codes (viruses, worms, Trojan horses) and then be spread further via the network. There is also a risk of unauthorized encroachment when hackers get access to IT resources and use them in a harmful way. These security problems can in the worst case lead to loss of information and damages in data systems and networks.

Confidentiality

Confidentiality means that sensitive information should not be revealed to unauthorized persons. All information should be subjected to rules for access and authorization. Loss of confidentiality occurs when an authorized or an unauthorized user gets access to information that this user does not have the right to. Another instance of loss of confidentiality is the unintentional access to sensitive information. This can happen when electronic mail goes to the wrong person due to a fault in the system. Course material in the form of texts and illustrations seldom contains especially sensitive information, and such material can sometimes be accessible on the net in a completely unprotected form. It is important to point out, however, that course material, including the work done by the students, is covered by the Copyright Act (SFS, 2005).

Course material as such may have low priority for security, but confidentiality is important when students want confidential communication with the instructor for the course. Since students and teachers have few opportunities to meet eye to eye, mutual trust must be built up through virtual meetings in a secure environment, which can be more difficult than in a traditional educational program (Light & Cox, 2001).

Accountability

Accountability affords protection from losses of and crimes against security. Accountability means that the user cannot afterwards deny that he/she has sent or received a message. Nor can the user deny that he/she has participated in or caused an action. On the other hand, if accountability is lacking, the user cannot be held responsible for his or her IT activities. The authentication of users makes accountability possible. If there is a possibility to log in under a false identity, then there will be a lack of correct accountability (Statskontoret, 1997).

Authentication in distance education can be described on three levels. The first, the **physical,** is via the IP or MAC address to identify the computer used. The second level, the **legitimate**, is to identify the one personally responsible for the user name and the password that is used to log in. The legitimate level is also valid for digital signatures. The third level, the **personal**, means making sure that what is written and sent is really produced by the person for whom the user name stands, which is many times the most difficult level to check (Figure 1).

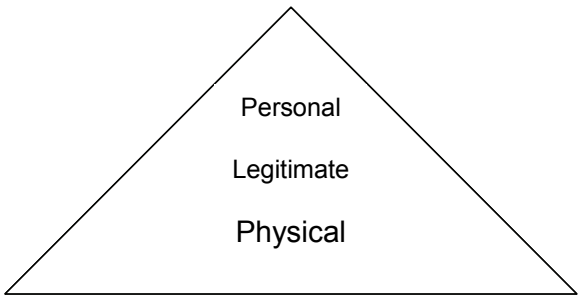

Figure 1: The three levels of authentication

One advantage of having access to the information and communication of the course require logging in with a password is that the activities of the course participants will be traceable, every user will be explicitly responsible for his/her actions. As the course participants cannot remain completely anonymous, the risk for inappropriate behavior should decrease when communicating with teachers and other participants. Course instructors should follow up the students´ level of activity if this is desirable for, e.g., examinations and grading. For the students, accountability means, among other things, a confirmation that work to be handed in and reports have been sent and received by the teacher on time.

Threats and Risks

A threat can be defined as "a possible, undesired event that, should it occur, could have negative consequences" (Statskontoret, 1997, p. 15). Risk can be defined as the probability that a threat will be realized. The most common threats against IT operations are everyday events caused by, e.g., flaws in administrative routines and in the IT activities themselves. Threats of this category are usually called unintentional threats. In addition to these involuntary threats there are also the internal intentional threats (Statskontoret, 1997, p. 15). Internal threats can be difficult to protect against, as they are often made by persons who have access to the computer system (Borg, Lozano, Löfgren, Malmgren, & Palicki, 1997).

Moreover, a large number of organizations are exposed to external threats, often called intentional threats, i.e. some person or organization tries to get hold of certain information or sabotage the whole IT operations. Examples of threats that we must be on the lookout for in distance education are presented in Figure 2.

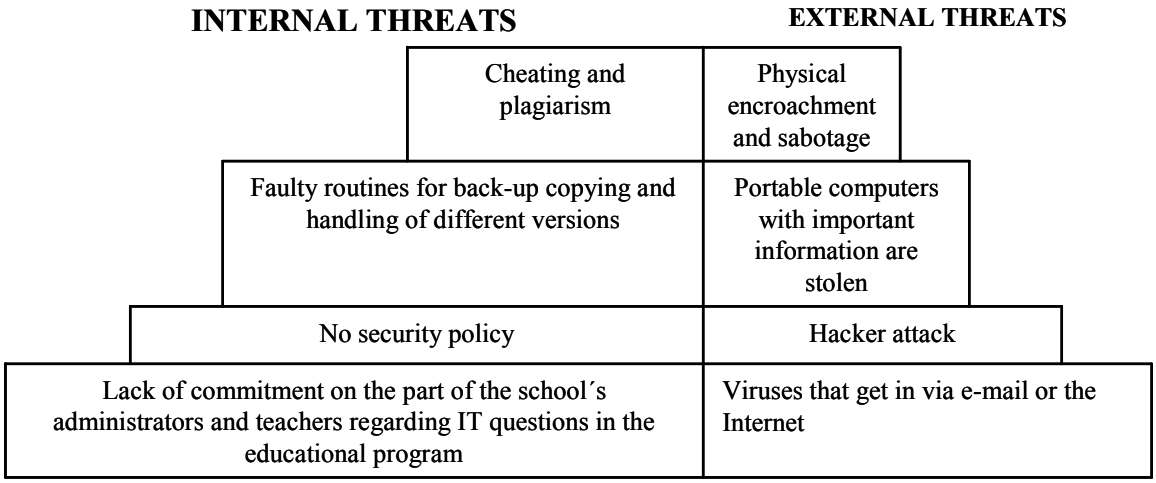

Figure 2: Risk stairway, examples of internal and external threats

According to Gali (1992) the absolutely decisive risks in data security originate with the human factor. Unintentional actions by the school's own personnel are responsible for approx. 65% of the threats and intentional actions on the part of the school's own personnel for approx. 32%. Attacks by individuals from outside of the organization are responsible for only three percent of the threats leveled at the organization.

Cheating

A specific security problem in the educational program in connection with reports to be handed in, essays and examinations is cheating, where the intention is to give the examiner a false picture

of the student's knowledge and skills. It is mainly forbidden collaboration with other persons or the use of plagiarism that is especially associated with net-based instruction. In accordance with the earlier division of information security into four different areas, cheating in the form of forbidden collaboration regarding individual papers handed in, and plagiarism, mainly touch upon the areas of integrity and accountability. If one in a misleading way passes off other individuals´ knowledge as one's own, one has misrepresented information and in doing so considerably impaired the quality of information. Poorer quality of information means impaired reliability, and that can seriously damage the trust between teachers and students and between students who work in the same group. In the long run, impaired quality of information is a considerable threat to the academic credibility of the institute of higher learning (Wiedersheim-Finn, 2005). Cheating and plagiarism also entail problems with accountability, if the work handed in cannot be traced to the right person.

Purpose

In this paper IT security is defined as a combination of computer security and information security. The purpose of the study is to make a survey of knowledge, attitudes, problems and behavior concerning above all information security at selected distance educational programs of Net University. With the student in focus the field is elucidated and discussed in relation to the four main areas, viz. *integrity, availability, confidentiality* and *accountability*.

Method

In order to take in some of the current problems regarding IT security in distance education, interviews were carried out at five universities with teachers, students and IT instructors working in the educational programs of Net University. From the first interviews some interesting security aspects emerged. Reliability and integrity in computer programs, inadequate routines regarding updates and back-up copying, and plagiarism were some of the areas that were taken up. Those that were discussed in the interviews could be imputed to the four areas, *integrity, availability, confidentiality* and *accountability,* and this constituted the basis of how the questions were formulated in the questionnaire.

Construction of the Questionnaire

Based on preliminary interviews, studies in the literature and theoretical standpoints, about 60 questions were formulated with the aid of the model shown in Table 1. In the model a matrix is used where the rows represent the four areas of information security and the columns describe the parts of the process that occurs when a net-based course is completed, here called knowledge/attitudes, actions, technology and check/follow-up.

The four categories – knowledge and attitudes, action, technology as well as control and follow-up – formed the basis of the construction of the questions as well as the processing of the data and the analysis. The questionnaire consisted of background questions, factual questions, attitude questions and open questions.

Table 1: Some examples of how the areas relate to the four main concepts of IT security

	KNOWLEDGE /ATTITUDES	ACTIONS	TECHNOLOGY	CHECK/FOLLOW-UP
INTEGRITY	Can the data and the information be trusted?	What measures are taken when false information is given?	How is the material protected against encroachment and distortion?	Is there a functioning source criticism and checking on the person who supplies the data? Are there tools against plagiarism?
AVAILABIL-ITY	Is the requisite knowledge obtain-able? Are there help func-tions and support?	How are operating interruptions and disturbances han-dled?	What minimum de-mands are made on computer equipment and Internet connec-tion?	Are there routines for back-up copying and handling of different versions?
CONFIDEN-TIALITY	Is there sufficient education in security? What is the attitude to security questions?	How are the pass-words protected?	To what extent is information en-crypted?	How is personal infor-mation handled?
ACCOUNT-ABILITY	What is the attitude toward publishing material in public conferences?	What measures are taken in the case of unauthorized access?	How is authentica-tion guaranteed?	How is cheating on tests dealt with?

Selection and Distribution of the Questionnaire

A total of 747 *students* were given the opportunity to answer a web questionnaire. The respond rate was no more than 39 %. Of the students who responded to the questionnaire, 63% were from the field of medicine and health care, 21% were from the humanities and social sciences and 16% studied the natural sciences and technology.

Of the 106 instructors responsible for courses who were invited to participate in the investigation, 64 respond. Instructors who represented the natural sciences and technology made up 43% of those who answered, 36% worked in the fields of the humanities and social sciences and 21% of the instructors taught in the fields of medicine and health care.

The questionnaire for the *IT instructors and those responsible for security* at the university was responded by 27 and the dropout was estimated at about 50%.

The three questionnaires were distributed and the data was collected during the period of 1st of May to 31st of May 2005.

Data Processing

The questions with the fixed alternative answers were processed statistically, while the open questions were analyzed qualitatively. The relationship between background variables and selected attitude questions was studied with the aid of the chi-2 test (*X2).* The statistical analysis was used to search for possible significant relationships in the material and thereafter to generate hypotheses in coming investigations. The result can therefore not be generalized to hold for all the programs at Net University. The main reason for this is the relatively large dropout, especially when it comes to the student questionnaire.

Results

The Students at the Net University

The vast majority of those who answered the student questionnaire were women (86%), and this was above all due to the fact that the educational programs dominated by women – medicine and health care – have a high degree of representation in the material. Still another reason for this high percentage could be that the female students were more favorably disposed to participate in the investigation.

The median age of the students was 34 years and 50% of them were within the interval 26-40 years old (inter-quartile range). The home was by far the most frequent place where the computer is used for the studies (84%) and few students (10%) used the computer mainly at the university, institutions of higher learning or at work, and other places (7%). One significant difference was that more women use the computer at home, while the men use it at work.

Most of those who answered the questionnaire were enrolled in educational programs (68%) and the rest (32%) attended separate courses. A high percentage of those who responded (76%) had broadband in their homes, while one-fifth (20%) used an ordinary telephone modem.

The Instructors in Distance Education

The distribution of women (48%) and men (52%) was nearly equal in the questionnaire for teachers. The median age of the instructors was 48 years and 50% of the ages were within the interval 39-56 years old (inter-quartile range). The student's freedom of time and place did not have any effect on the flexibility of the teachers, since their work as distance instructors occurs mainly at the university (91%), and only a few teachers (9%) worked from home.

Most of those who answered the questionnaire (80%) were instructors for separate courses and about half for programs (40%). Some (20%) were thus instructors for both separate courses and for programs. In comparison with the students, somewhat fewer teachers (68%) stated that they had broadband at home. Almost one third (30%) had an ordinary telephone modem in their home.

Persons Responsible for IT and IT Instructors

Of the 27 persons who answered from this group, 11 stated that they worked as IT instructors or had a similar job, and 21 said that they were responsible for IT security in distance education. It was evident from the questionnaire that 12 worked on the central level and 12 on the departmental level. Three who responded worked on both levels.

Knowledge and Attitudes

Judging from the students´ and teachers´ estimates, we can assume that distance teachers and students have a relatively good basic competence when it comes to using computers. 61% of the distance students and 75% of the teachers evaluated their competence as good. Among the students there was a significant difference between women and men in that women admitted that they are somewhat less practiced in working with computers than men, as shown in Table 2. The students in the groups medicine/health care, too, were less practiced in working with computers than the other groups.

Table 2: Statement "My basic competence is good when it comes to using computers" Distribution of students' respond (percent)

	AGREE	NEITHER AGREE OR DISAGREE	DISAGREE	DON'T KNOW
WOMEN	56.7%	29.0%	14.3%	0
MEN	78.2%	20.0%	0	1.8%
TOTAL	60.8%	27.3%	11.5%	0.4%

Almost half (47%) of the students who took part in the questionnaire said that they have acquainted themselves with the university's rules and policy for the use of computers, distance tools and the Internet. 58% of the teachers said that they have been given the information. Those responsible for IT claimed that the students have received information about rules and policy but many had not paid attention to the meaning of the obligation. Obviously the routines needed to check whether the users have taken the information to heart are lacking.

As for knowledge about the rules for publishing, 36% of the students and 25% of the teachers pointed out that this is insufficient.

More than half of the students (52%) and teachers (57%) were relatively certain about what measures to take if their computer gets a virus. In this case there was a significant difference between the sexes in the student group, the women being more uncertain about what measures need to be taken (see Table 3).

27% of the students were not exactly sure where he/she should turn when technical problems occur.

Table 3: Statement "I know what measures must be taken if my computer gets a virus" Distribution of students' respond (percent)

	AGREE	NEITHER AGREE OR DISAGREE	DISAGREE	DON'T KNOW
WOMEN	46.7%	17.3%	28.9%	7.1%
MEN	73.2%	14.3%	12.5%	0
TOTAL	52.0%	16.7%	25.6%	5.7%

Security awareness and trust

Slightly more than half of the students (58%) were aware of the security risks associated with the use of computers for communication. Those responsible for IT and IT instructors evaluated the students´ and teachers´ security awareness as being equal, but considerably lower than the students´ and teachers´ own estimates. When it comes to their fear that material sent by the distance tool will disappear, the students were more troubled than the teachers. 31% of the students and 18% of the teachers expressed apprehension that material sent will not reach the destination in a correct way.

The vast majority of students (67%), teachers (64%) and those responsible for IT and IT instructors (67%) agreed with the assertion that IT security is on the whole good in distance education.

Action

More than three-quarters of the students (78%) believed that they can handle the distance tools used in the course without many difficulties. There was, however, a significant difference between the sexes here, the women finding it somewhat harder to handle these tools, as shown in Table 4. Given the same question, the teachers had a somewhat lower degree of agreement (71%), which may be due to the fact that they have to be able to handle more functions in the system. Judging from their comments, it was mostly asynchronous communication in a text-based forum that was used.

Table 4: Statement "I can handle the distance tools used in the course without a whole lot of problems" Distribution of students' respond (percent)

	AGREE	NEITHER AGREE OR DISAGREE	DISAGREE	DON'T KNOW
WOMEN	74.5%	19.3%	4.0%	2.2%
MEN	94.5%	1.8%	3.6%	0
TOTAL	78.4%	15.9%	3.9%	1.8%

When it comes to dealing with personal information in courses, 78% of the teachers were of the opinion that this is done correctly. Students together with those responsible for IT and IT instructors made a somewhat more negative assessment; 34% of the students and 59% of the IT instructors considered that personal information is dealt with correctly.

Most of the students (81%) had never felt threatened or attacked in a distance course. The same rate among the teachers is 74%, so that they were basically of the same opinion. However, even if only a small number of students and teachers may have felt threatened or personally attacked in distance courses, it is important to take measures to avoid this kind of problems. Authentication of users makes course participants traceable and explicitly responsible for their actions. This should reduce the risk for inappropriate behavior when communicating with teachers and other participants.

The majority of students (70%) and teachers (66%) believed that they devise their password in accordance with the rules that are recommended. There were not many students (20%) and teachers (21%) who take a new password at least once a semester. This is a fact that many persons responsible for IT and IT instructors accepted, since they consider the alternative – when users write memoranda slips – a greater problem. When it comes to safeguarding the password, more than half of the students (64%) and teachers (63%) considered this to be done in a safe way.

Handling of different versions and back-up copying

More than half of the students (54%) and teachers (60%) said that they seldom have any problems with the handling of different versions. Those responsible for IT and IT instructors were of the opinion that students and teachers have more problems with the handling of different versions than what the estimates of the latter groups would seem to indicate.

Many students (58%) and teachers (59%) took back-up copies of their documents quite often. Nearly all of the students and teachers take some kind of copy, but 25% of the students and 19% of the teachers said that they take back-up copies less often. The students most often save the text on a hard drive (76%) or a diskette (30%). When it comes to the teachers, the most common way of saving a safe copy is on the server or the hard drive of the educational institute (72%). The as-

sessment of those responsible for IT and IT instructors confirmed the action of the students and teachers regarding back-up copying.

Dealing with viruses

67% of the students stated that they update their antivirus programs on a regular basis; the figure for the teachers was a little higher (82%). Quite a few students (5%) indicated that they do not know whether they have antivirus programs or whether these programs are updated. The teachers often have good protection against viruses at their workplace, and this protection is updated automatically from the IT departments.

62% of the students and 66% of the teachers agreed with the statement that he/she doesn't open or use programs that are taken from unknown milieus. Here there was a significant difference in the student group, the men agreed with the statement to a higher degree than the women, as shown in Table 5. The relatively high rate of women who answered *don't know* may also be noted. The assessment that those responsible for IT and the IT instructors make in this question was that the students to a higher degree than the teachers open files that are not checked for viruses.

Table 5: Statement "I do not open or use programs that are taken from unknown milieus" Distribution of students' respond (percent)

	AGREE	NEITHER AGREE OR DISAGREE	DISAGREE	DON'T KNOW
WOMEN	57.0%	16.2%	9.7%	17.1%
MEN	80.0%	5.5%	10.9%	3.6%
TOTAL	61.5%	14.1%	9.9%	14.5%

50% of the students said that they would report regularly to the sender if they were to get a data virus. 34% of the students systematically reported technical faults to IT personnel or course instructors. As for the teachers, they reported technical faults more frequently (75%). One reason for this is surely that IT support is more easily accessible and that the teacher has a special responsibility to reduce various types of interruptions and disturbances in the course.

Technology

When it comes to estimating the technical performance of the computers used in the distance studies, 88% of the students stated that they have adequate computer equipment. The corresponding estimate for the teachers was somewhat lower (75%), and the reason for this may be that the administration of courses puts higher demands on the equipment and the user.

The majority of those responsible for IT claimed that the computers of the distance students have good technical performance (63%) and sufficiently fast connection to the Internet (53%). It should be noted that 20% of the students said that they actually use an ordinary telephone modem.

Antivirus programs and firewalls

88% of the students said that they have an antivirus program installed in their computers and somewhat fewer 70% have a firewall installed. Regarding the question of whether one's home computer has a firewall installed, the proportion of women who answered *don't know* is remarkably high (18%). In the questionnaire for teachers 97% said that they have an antivirus program

installed on their home computer, while 63% said that they have a firewall installed at home. Some students took up the problem that good computer security is often very expensive.

59% of the students agreed with the statement that there are seldom any operating disturbances in the distance tools that are used. There was a significant difference here that is important to note: women felt that technical problems can disturb their studies to a higher degree than men did, see Table 6. The IT personnel/instructors assessed the operating security higher than students and teachers do. The teachers were more bothered by junk e-mail than the students.

Table 6: Statement "Technical problems do not disturb my studies" Distribution of students' respond (percent)

	AGREE	NEITHER AGREE OR DISAGREE	DISAGREE	DON'T KNOW
WOMEN	55.7%	20.42%	20.9%	3.0%
MEN	74.1%	11.1%	13.0%	1.8%
TOTAL	59.1%	18.71%	19.4%	2.8%

68% of the students indicated that they are relatively satisfied with the distance tools used in the educational program. The teachers made a somewhat lower assessment (62%) in their questionnaire. 16% of both students and teachers desired more information about what digital resources are available. The most satisfied group in this respect was the IT personnel/instructors, as only 11% of them considered that more information is needed.

Checking and Follow-up

When it comes to information about the distance tools, 54% of the students, 53% of the teachers and 51% of the IT personnel/instructors agreed with the statement that this is sufficient.

Regarding the instruction in the use of IT, 43% of the students, 52% of the teachers and 51% of the IT personnel/instructors agreed with the statement that the instruction is sufficient. However, in the student group there was a significant difference between the sexes, in that the women experienced greater shortcomings in the education than the men did, see Table 7. Many students have expressed a desire for more instruction in the use of distance tools.

Table 7: Statement "Instruction in the use of distance tools is sufficient" Distribution of students' respond (percent)

	AGREE	NEITHER AGREE OR DISAGREE	DISAGREE	DON'T KNOW
WOMEN	40.4%	27.0%	25.3%	7.3%
MEN	55.5%	27.8%	11.1%	5.6%
TOTAL	43.2%	27.2%	22.6%	7.0%

The computer support given was ranked higher by the teachers in comparison with the students, as 19% of the students and 13% of the teachers thought that they have not received enough help. In this case as well there was a difference between the sexes in the student group, as more women than men claimed that the computer support is not enough, as shown in Table 8. Some students were also critical of the quality and extent of the computer support. It seems to be easier for the teachers to get support, as only 13% of them thought that they have not received enough help.

This is probably due to better contact with and proximity to the IT personnel. The IT personnel/instructors´ assessment of the extent of the computer support corresponded well with the estimates of the students and the teachers.

Table 8: Statement "Computer support is sufficient"
Distribution of students' respond (percent)

	AGREE	NEITHER AGREE OR DISAGREE	DISAGREE	DON'T KNOW
WOMEN	39.7%	28.0%	21.8%	10.5%
MEN	58.2%	14.5%	9.1%	18.2%
TOTAL	43.3%	25.3%	19.4%	12.0%

Authentication

61% of the students and 73% of the teachers can always identify the users who send messages and documents in the courses. It is important to point out that this identification can only be a question of the legitimate authentication. To reach the third level, the personal authentication, requires good familiarity with the person or the taking of other measures.

Cheating

68% of the students didn't think that the risk of cheating is higher in distance studies compared with a traditional campus education. Here 24% of the teachers indicated that the risk of cheating is greater in distance studies. 21% of the teachers took special measures to counteract cheating, but it is not possible to tell from the answers if these differ from those in traditional education. Almost equally many teachers devoted more time to the prevention of cheating in distance education in comparison with a campus education. If one interprets the answers of those who think the risk of cheating is greater in distance studies, there is reason to believe that their examination system is based on traditional tests. Since writing essays and take-home tests do not require a person to be present on a particular time and place, and if the tasks in their structure do not pose questions on the level of details, there ought not to be any significant difference between campus and distance education when it comes to the possibility of cheating. It is possible that the explanation for the fact that some teachers found it more time-consuming to try to stop the students from cheating is that they must choose examination formats that require more time from the teacher and that traditional tests, which are perhaps watched over and corrected by other personnel, cannot be used in the same way.

Discussion

The basis and point of departure for the investigation has been to consider the problem field mainly from the standpoint of four sub-areas, viz .integrity, availability, confidentiality and accountability. This relatively broad approach to the field has most likely not been taken to heart by all respondents, as many associate IT security with purely technical measures. This can be discerned in the answers that the respondents give to certain questions.

Despite obvious inadequacies in several areas, students and teachers say that IT security is good. There seems to be a discrepancy between the respondents´ knowledge/attitudes and their actions in real situations; some examples of this are the handling of personal information and publishing

on the net. This can be partly explained by insufficient knowledge of the laws in force; in other words, there can be security problems in these areas that students and teachers are not aware of. If the problems remain hidden it also happens that the respondents as a rule consider their knowledge good, while independent observers, such as IT personnel and instructors, can differ in their views.

Integrity

To know the rules and policy for using computers, distance tools and the Internet is vital for integrity. Here there are shortcomings among students as well as teachers. Many have received the information, most often in written form, but have not taken it to heart. Another area that is important for integrity is knowledge of the rules for electronic publishing, which also influences confidentiality. Here students and teachers are definitely unsure of how to handle the new manner of publication.

When the handling of different versions is not done properly, this is also a threat to integrity. A significant number of students and teachers say that they have problems keeping the different versions they have saved in good order.

Downloading programs and documents from unsafe sites poses a threat to integrity and thus risks the quality of education, and according to the answers in the questionnaire this occurs fairly often. This area is closely tied to the problems related to cheating. There are obviously a number of teachers who find it difficult to check the integrity of tasks and tests in distance studies.

Availability

That the computers used in the distance studies have good technical performance is vital for availability. It is also important that the broadband is sufficient. Most of the respondents are satisfied with both the technical performance and the broadband.

As for computer support and getting help quickly, these, too, are important factors for good accessibility. Almost a fifth of the students feel that they have not gotten enough help. In this case, too, there is a difference between the sexes; the women feel that the computer support is not sufficient to a greater extent than the men do.

When it comes to information regarding the distance tools, the students, teachers and IT personnel/instructors all agree that this must get better. More information about how to handle the tools is one of the measures that will boost accessibility. One important aspect of accessibility is the user-friendliness of the distance tools that are utilized. This is assessed by all respondents as good, but there is a significant difference between the sexes; women feel that it is more difficult to handle these tools.

Familiarity with the computer is important for accessibility and it is considered to be good by students as well as teachers. Women feel that they are less familiar with computers than men, and the students from the subject group medicine/health care assess their familiarity of computers as somewhat lower than the other groups.

Quite a few are not sure what to do when they suspect that their computer has been infected by a virus, which affects accessibility. Should this occur, it is important to be able to quickly reach support and help regarding technical problems for which the students do not exactly have clear routines and channels. Help with updating antivirus programs and the installation and updating of firewalls are also measures that are in demand.

Accessibility and back-up copying are concepts that are closely related to one another. There is good reason here to encourage measures that stimulate more frequent back-up copying and a better choice of storage media.

Confidentiality

There are a number of students as well as teachers who worry that their material will be read by unauthorized persons. The students, especially, express fear that material sent will not reach the destination in a correct way. If this fear is based on real flaws in confidentiality that have arisen, it is not evident from the results. This lack of trust is most likely due to ignorance about how the system works.

When it comes to handling personal information in courses, most of the teachers think this is done in a correct way. Students and IT personnel/instructors do not exactly share that view. There are examples in the material that point to mistakes that were made.

Safeguarding user identity with passwords is an important confidentiality issue that functions relatively well. Here there is a double message from the IT personnel: one explicit – ”get a new password every three months”, and one implicit – if the change of password requires a note to remember it, it is better to do without. It could therefore be a good idea to give way a little as regards changing passwords every three months.

Accountability

A significant number of students do not report regularly if their computers have been infected by viruses. Still more students do not report technical problems to the IT personnel or the instructor of the course. These routines fall under the heading of accountability and improving them would boost the possibilities of accountability.

When it comes to identifying the user, many agree that one can always see who sends a contribution to a web conference. This accountability can mainly be placed on the level of legitimate authentication.

Measures to prevent cheating are of the greatest importance for accountability. About a quarter of the teachers are of the opinion that it can be more difficult to detect cheating in distance education in comparison with campus education. Apparently a number of teachers feel the need to reinforce recognition on the personal level of authentication.

Pedagogical implications

In the material collected clear differences have been found in how men and women assess their familiarity with computers. The knowledge and technical skills that both groups have at their disposal seem to be fairly good, considering the demands made in the courses, where often simple asynchronous text systems are used. Using “simple” technology has been a formula for success, according to many distance instructors (Karlsudd, 2003). As more and more users have both sufficient knowledge and the technological prerequisites, it is perhaps appropriate to go one step further and start using sound and images to a greater extent. Research findings (Söderström, 2004) demonstrate that the communication will be more continuous if multimedia is used synchronously and asynchronously.

Support and help

Many desire an increase in support for IT use. Many researchers, including Holmberg (1998) and Marklund (2002), have pointed out that this is of vital importance for maintaining high quality,

and they stress the need for supporting structures so that the IT education can be successful. These structures comprise technical support and instruction.

In distance education the teacher is often alone in the task of helping the student in data communication and technical questions. Much of the instruction and the support included are the individual teacher's task, problem and challenge (Sherer, Shea, & Kristensen,, 2003). The teachers will in all probability also in the future have to be prepared to give simple support and technical guidance, but can also be relieved in this by personnel working centrally.

Training

Many in the investigation are of the opinion that IT security in distance education is good, but want greater efforts to reinforce it. One way to increase the confidence in technology is in the first phase of the course to use the course tools in simple and frequent achievement exercises. To concentrate more on introductory courses in technology would be a good idea, and Westerberg and Mårald (2004) have also proposed this in a report. All forms of user-training should have a positive effect on IT security (Conti, Hill, Alford, & Ragsdale, 2003; Schumacher & Welch, 2002). If the university or college has competent instructors employed, and if the students are used to utilizing IT resources, this will reduce the risk of mishaps (Karlsudd, 2001). Adequate user-training might be especially important in net-based distance courses for several reasons. These courses are to a high degree dependent on well-functioning IT resources, and frequent security problems can thus affect the study results in a very negative way. Some common problems are associated with inadequate routines in back-up copying and handling of different versions and these troubles can easily be avoided by the relevant instruction. To better inform and help the students in the installation and handling of programs there are a few urgent measures that can be taken. On the computers where the university is responsible for the operation, the antivirus protection apparently functions well and many times is upgraded automatically. A relatively simple web-based course in security with a test at the end could be a way to better determine who has taken security information to heart and what possible threats there are because of insufficient knowledge.

At most universities and colleges in this country there is adequate information regarding security on the net. One measure that would most likely raise the quality of the information efforts being made would be to assemble those responsible for the education where they could discuss their experiences and share with others the information material that was produced. Another measure that can reinforce the work still more is to appoint a head person at every department to be responsible for information about and training in IT security.

Measures against cheating

Some of the teachers think they spend more time guarding against cheating in distance education and then they take measures that they would not do in campus education. What is problematical is most likely to make sure that it is the student who has answered the question - personal authentication, a matter that is a problem even when it comes to take-home tests and essays in campus education. Maybe the teachers believe they have a better picture of the student after meeting him/her in person. Marklund (2002) is of the opinion that the technical aspects should not involve any problems for exams. Perhaps the problem could be to a higher degree related to the examiner (Martin, 2004; Westerberg & Mårald, 2004). With a continual and formative system of examination the risk of cheating will most likely be reduced (Gunnarsson et al., 2002). Following the whole working process as a teacher can be a way to guard against cheating. The students can, e.g., write a process diary, making it easier for the teacher to follow the progress of their work. It is also important to try to formulate the tasks in such a way that it is hard to find ready solutions on the net, e.g., by consistently choosing problems that require one's own analysis and avoiding problems that invite reproduction.

Conclusion

It is especially important to pay attention to the differences that have been observed between the sexes and that have also been reflected in the subject areas where the proportion of female students is higher. The material that has been collected indicates that female students may feel more unsure when it comes to the handling of technical equipment, and that they want more instruction in the use of computers as well as more computer support. Similar experience have been confirmed in Venkatesh and Morris (2000) and Venkatesh Morris, and Ackerman (2000) research. It would therefore be of great interest to do a more detailed study about how reinforced user instruction and computer support can lead to female distance students feeling more confident in technology and – which is even more important – having confidence in their own knowledge and skills.

There is a definite belief in the future when it comes to web-based education, and in all probability there will be an increase of IT in higher education. Hopefully, support for development and research will increase at the same pace.

References

Allwood, C. M. (1998). *Människa-datorinteraktion: Ett psykologiskt perspektiv*. [Human-computer interaction: A psychological perspective.] Lund: Studentlitteratur.

Borg, T., Lozano, A., Löfgren, T., Malmgren, S.& Palicki, J.(1997). *IT-säkerhet för ditt företag*. [IT security for your company.] Uddevalla: Bonnier DataMedia.

Brandt, P.& Wennberg, L.(2004). *Informatisk forskning om riskanalysprocess applicerad på Apoteket AB:s kundcenterverksamhet.*[Informatics research concerning the process of risk analysis applied on the call centre activity of Swedish Pharmacy AB.] *(Licentiate Dissertation Series No 2004:09).* Karlskrona: Blekinge Tekniska Högskola.

Bishop, M. (2003). *Computer Security*. Boston, MA: Addison-Wesley.

Conti, G., Hill, J., Alford, K. & Ragsdale, D. (2003). *A comprehensive undergraduate information assurance program*. In C. Irvine & H. Armstrong (Eds.), Security Education and Critical Infrastructures IFIP TC11/WG11.8 Third Annual World Conference on Information Security Education (WISE3), (pp 243-260), Monterey, California. Kluwer Academic Publishers.

Gali, P.(1992). *Informationssäkerhet: Hur du skyddar data, text, ljud och bild.* [Information security: How to protect data, text, sound and images.] Linköping: Affärslitteratur.

Gollman, D. (1999). *Computer Security*. West Sussex: John Wiley&Sons.

Gunnarsson, M., Lingefjärd, T., Mekki-Berrada, T.& Sjöblom, C-A..(2002). *Flexibelt lärande – lärande examination.* [Flexible learning –examination as a learning opportunity.] *FLEX. UFL-rapport 2002:1.* Göteborg: Göteborgs universitet.

Hargreaves, A. (1994). *Changing teachers, Changing times. Teacher´s Work and Culture in Postmodern Age.* Trowbridge, Wiltshire: Redwood book.

Hjelm, J.& Sandred, J. (1997). *Framtidens utbildare.*[The future educators.] Uddevalla: Bonnier DataMedia.

Holmberg, C. (1998). *På distans – utbildning, undervisning och lärande* [At distance – education, teaching and learning.] SOU: 1998:83.

Jokela, P.& Karlsudd, P. (2005). *Att lära säkert. IT-säkerhet i Nätuniversitetets distansutbildningar* [Learning safely. IT security in the Net University's distance education.] Umeå: UCER – Umeå Centre for Evaluation Research.

Karlsudd, P. (2001). *Att lära på tunna linor och bred(a) band: IT-säkerhet i utbildning baserad på informations- och kommunikationsteknologi.*[Learning on thin wire and broad bands: IT security in

education based on ICT.] Kalmar: Högskolan i Kalmar, Institutionen för hälso- och beteendevetenskap.

Karlsudd, P. (2003). *Att lära på tunna linor och bred(a) band: e-learning: Ambition, mission och vision, en granskning av e-utbildningsföretagens pedagogiska grundsyn.* [Learning on thin wire and broad bands: Ambition, mission and vision, a review of e-learning companies' pedagogical approach.] Kalmar: Högskolan i Kalmar, Institutionen för hälso- och beteendevetenskap.

Light, G. & Cox, R. (2001). *Learning & teaching in higher education – the reflective professional.* London: SAGE Publications.

Marklund, K. (2002). *Högskoleläraren är framtidens hjälte i Borg, C. (red) Vetenskapernas visioner. Elva samtal om framtidens studier och undervisning i högskolan.* [The university teacher is the hero of the future. In Borg C. (red) Vision of science. Eleven conversations about the future studies and university education.] Härnösand: Distum, Rapport: 2002.

Martin, B. (2004). Plagiarism: Policy against cheating or policy for learning. *Nexus, 16* (2), 15-16.

Mårald, G.& Westerberg, P. (2004). *IT-stödd distansutbildning inom medicin och vård höstterminen 2003 – ur studenternas perspektiv. [IT-supported distance education in medicine and health care Autumn 2003- in students' perspective.]* Umeå: UCER – Umeå Centre for Evaluation Research.

Pfleeger, C. (2003). *Security in Computing*, 3rd Edition. Englewood Cliffs, NJ: Prentice Hall.

Schumacher, J. & Welch, D. (2002). Educating leaders in information assurance. *IEEE Transactions on Education, 45* (2), 194-201.

SFS (2005). *Upphovsrättslagen 2005:360. [The Swedish Code of Statutes. The law of copyright.]*

Sherer, P. D., Shea, T. P., & Kristensen, E. (2003). Online Communities of Practice: A Catalyst for Faculty Development. *Innovative Higher Education, 27* (3).

Siponen, M. T. (2000). Critical analysis of different approaches to minimizing user-related faults in information security: implications for research and practice. *Information Management & Computer Security, 8*(5), 197-209.

Statskontoret. (1997). [The Agency for Administrative Development]. *Handbok i IT-säkerhet. Del III. Skyddsåtgärder: Volume 29* [Handbook in IT security part III. Security actions.]. Stockholm: Statskontoret.

Stajano, F. & Anderson, R. (2002). The Resurrecting Duckling: Security Issues for Ubiquitous Computing. *Security&Privacy Suplement to IEEE Computer Society, 35* (1), 22-25.

Summers, R. (1997). *Secure Computing: Threats and Safeguards*. New York, NY: McGraw Hill.

Söderström, T. (2004). *Studenternas uppfattningar om datorkommunikation inom Nätuniversitetets medicin- och vårdutbildningar.*[Students' opinion on the subject of computer communication in the Net University's medicine and health care education.] Umeå: UCER – Umeå Centre for Evaluation Research.

Trowler, P. R. (1998). *Academics responding to change: new higher education frameworks and academic culture.* Buckingham: Society for Research into Higher Education & Open University Press.

Venkatesh, V. & Morris, M.G. (2000): Why don't men ever stop to ask for directions? Gender, social influence, and their role in technology acceptance and usage behaviour. *MIS Quarterly, 24* (1), 115–140.

Venkatesh, V., Morris, M.G. & Ackerman, P.A. (2000): A longitudinal field investigation of gender differences in individual technology adoption decision making processes. *Organizational Behaviour and Human Decision Processes, 83* (1), 33–60.

Westerberg, P. & Mårald, G. (2004). *Nätuniversitet och IT-stödd distansutbildning – Attityder och erfarenheter hos prefekter, kursansvariga och studenter*.[Net University and IT supported distance education - Attitudes and experiences among heads of department, course leaders and students.] Umeå: UCER – Umeå Centre for Evaluation Research.

Wiedersheim-Finn, F. (2005). *Plagiathandbok.[Handbook in plagiarism.*] Uppsala: Uppsala universitet, Företagsekonomiska institutionen.

Biographies

Dr. **Päivi Jokela** is an Assistant Professor in Informatics and Assistant Professor in Physical Chemistry at the University of Kalmar, Sweden. Her main research interest in computer science is evaluation based on systems framework.

Dr. **Peter Karlsudd** is an Assistant Professor in Pedagogic and Assistant Professor in Informatics at the University of Kalmar, Sweden. His research area is special education and flexible learning. He is instructor/tutor for university teachers' pedagogical improvement.