Science and Technology, 7 (2002) 31-43

Information Security Risks on a University Campus

Amer A. Al-Rawas and S. Millmore

Centre for Information Systems, Sultan Qaboos University, Sultanate of Oman.

المخاطر المتعلقة بأمن المعلومات داخل الحرم الجامعي

عامر عوض الرواس و ستيف ميلمور

خلاصة : يتعرض هذا البحث لدراسة الأمن في أنظمة المعلومات داخل الحرم الجامعي , وذلك من خلال الخبرة في إدارة شبكة المعلومـات فـي جامعـة السلطان قابوس وعند دراسة المخاطر والتحديات التي تواجه القائمين على تقديم خدمات المعلومات الإلكترونـية ، يتعين علينا أن نأخذ في الاعتبار عددا من الموضوعات المتداخلة ، وتشمل هذه الموضوعات: أهمية المعلومات للأفـراد داخـل الحرم الجامعي , نوع المعلومات المستخدمة, وأنواع المخاطر التي تتعلق بتقديم خدمات المعلومات الإلكترونية للمجـتمع الجامعـي. وبناء على مناقشة المخاطر في تقديم المعلومات الإلكترونية يقدم البحث عددا من التوصيات لتحسين أمن وسـرية المعلومـات داخل الحرم الجامعي والتي يمكن أن تتبناها المؤسسات التعليمية التي تولي أمن المعلومات أهمية خاصة. ويمكـن تقسـيم هـذه التوصـيات إلـى ثلاث فئات: توصيات عامة للبيئة الجامعية بأسرها, توصيات اجتماعية تتعلق بعادات وأخلاقيات العمل عند أعضاء هيئة التدريس والطلاب ، وتوصيات تقنية تتعلق بالخبرات والتقنيات الواجب توافرها.

ABSTRACT: This paper is concerned with issues relating to security in the provision of information systems (IS) services within a campus environment. It is based on experiences with a specific known environment; namely Sultan Qaboos University. In considering the risks and challenges that face us in the provision of IS services we need to consider a number of interwoven subject areas. These are: the importance of information to campus communities, the types of information utilised, and the risk factors that relate to the provision of IS services. Based on our discussion of the risk factors identified within this paper, we make a number of recommendations for improving security within any environment that wishes to take the matter seriously. These recommendations are classified into three main groups: general, which are applicable to the entire institution; social, aimed at the work attitudes of staff and students; and technical, addressing the skills and technologies required.

KEYWORDS: Security, Information Systems, Campus Environment.

1. Introduction

1.1 Information and The Campus Community

Computers, information systems, communication tools and networks all play an increasingly important part in our lives. They provide a wide variety of services to us, and there has been increasing recognition that they are key and integral to the prosperity of all developed and developing nations. This importance is recognised in some countries (White House, 2000; Hansard, 1998; Attorney General, 1999; Hunter, 2000) that are implementing, or considering implementing, mechanisms to protect them.

General security standard guidelines and policy documents have been developed. Some have a very direct reference to higher education (Joint Information Systems Committee, 2001), others are more general applying to the Internet community as a whole (Fraser, 1997). In the government, commercial and industrial sectors there have also been efforts to formulate standards, on a national/international level (British Standards - BS7799, 1999; International Standards Organisation - ISO 17799). It is unclear if these latter standards have been applied to higher education, so whether they hold lessons for us is not known.

If we consider education, and in particular higher education, specific issues related to information sharing arise. For example, a typical university environment consists of a single overall body (the institution itself) and is divided up into closely-knit communities of different sizes, large and small (faculties, departments, research teams, etc.). Within and between these communities different kinds of information sharing takes place. Thus within a university campus information exchange is, especially in the academic arena, a fact of life.

Universities are institutions that have many different roles in the wider community, however the most fundamental roles are research and education. These are built around information: its acquisition, storage, exchange and application. This means that they are highly dependent upon the utilisation of IS. Many universities have taken on-board the importance of information systems to the fulfillment of their academic responsibilities, and included them in their academic plans (San Francisco State University, undated; University of Leicester, 2000).

The importance of information to universities is, in general, well recognised (Harvard University, 1991). For the efficient and effective operation of the institution this information exchange should be encouraged and developed. Given the signficant growth of IT in the sector, along with the sharing culture, we need to consider the issues of the effective security management and control (Elliot *et. al*., 1991; Hassler, 1998; Stamen, 1986).

2. Types of Information

As with other educational bodies, a wide variety of information exists and is deployed within the campus. This information may be maintained, stored and communicated in many different ways. Traditionally much is in hard copy i.e. paper format. This might include memoranda, reports, records and so forth. With the development and wide distribution of the ubiquitous PC a great deal of information has migrated from those ledgers onto the hard disks of computers. Whether the minds and attitudes of the custodians of the data have made an equivalent change is another matter and is very relevant to the current issues under discussion.

If we are to consider, in broad terms, the kind of data stored in university campus records, be they paper, or electronic, we can consider them to be of several particular types. These are:

- administrative and infrastructure,
- academic and research.

Within these broad classifications are a wide variety of different types of data. For example, looking at basic administrative data we might find:

- University installations maintenance information,
- Staff, contracts and personnel details,
- Budgetory, financial, procurement and purchasing data,
- Minutes of senior, and not so senior, staff meetings.

The list of broad administrative data recorded and maintained is extensive.

Similarly, if we were to consider the types of data retained under the academic umbrella, we might find:

- Student records, grades, academic plans, and reports,
- Examinations, past, present and future,
- Student project reports,
- Research data, interim programs and draft technical documents and papers,
- Library book holdings.

Again, there is a very wide variety of data and they may be retained in various forms of recording mechanism.

Frequently campus based institutions have close links with other bodies. In these cases other forms of data may be involved. For example when the university has a linked teaching hospital, as has SQU, we should also consider the issue of hospital data. Such data might include:

- Patient information,
- Clinical reports, including test reports,
- Administrative and financial information.

There may also be commercial/business factors to be considered. For example, special contracts and agreements between the institution and external suppliers, sponsorship agreements or even business/academic partnership may exist. Such agreements may imply quite specific needs in terms of confidentiality and integrity of information. The results of a commercially supported academic study program may, for example, be covered by commercial confidentiality agreements and have implication with respect to intellectual property or copyright laws. Such agreements may even give commercial organisations rights with respect to the information security of the institution. Such rights may extend to policies, procedures, audits and inspection.

It is clear then that a wide variety of different types of data are retained in different records. Some of this data may be highly confidential, and should only be seen by a limited number of authorised staff (for example, examination scripts), some may be public information (for example, library holdings), some may have controlled access (for example, collaborative research projects). In all cases there remains the issues of: access and control, information integrity, management, security, confidentiality, copyright, and other legal obligations.

The need for proper maintenance of records, and data, in the correct and appropriate way, has not been changed by the introduction of electronic storage technologies. However, as personal computing and networks have developed the way data has been stored and is transmitted has gone through a revolution. Consider Table 1, Technology and Security Relationships.

Studies have shown that the security issues attached to the use of information systems are real. For example in (University of California, 1998) they discuss the threats and risks to “campus computer and networks ...” along with the “integrity and confidentiality of data ...”. They have identified the needs that should be addressed when considering security (Leach, undated), these needs include:

- Ensuring financial accountability,
- Use of IT to reduce operating costs where possible,
- Prevention of unlawful use of resources,
- Minimising the burden of controls,
- Maintaining the security of academic work,
- Maintaining viability and goodwill.

Our studies are very much in-line with the comments made by these researchers.

Table 1: Technology and security relationships.

Technology	**Data Security Issues**
Centralised host based systems	Closely controlled data, handled by professional staff. Proprietary communications channel with limited general user access.
Personal computer desktop systems	Limited but localised access to data in departments by local staff.
Network based client/server	Controlled server based storage with data carried on a communications channel.
Intranet distributed computing model	Shared distribution of data transmitted over a local communications channel (LAN).
Internet/Extranet distributed computing model.	Shared distribution of data transmitted over a wide area communications channel (WAN).

The need, then, for security become more significant, more urgent, owing to the much wider potential for unauthorised access, misuse, and corruption.

3. Security Issues

When we are considering the issues of information security we have specific objectives. These objectives are to ensure:

- Availability, IS structures are there 100% of the time;
- Accuracy, data is faithfully, fully and correctly reproduced;
- Protected, data is not lost, damaged or corrupted;
- Privacy, information is only revealed to those who should have access.

Security of information, and information bearing IS infrastructures, can be considered as being composed of a number of different parts. These are:

- Physical infrastructure components, which relate to where and how equipment is installed.
- People, who access and utilise the information,
- Systems which are used to store and retain the accessed information,
- Communication technologies, used to gain access to and transport that information.

In searching for a total security solution we need to address all of these issues.

3.1 Infrastructure: Physical Access Risks

The first issue that must be addressed when looking at security is the physical layer. You must control strictly access to physical infrastructure and related plant and equipment. This means that protection of desktop computers from theft is not just the issue. We also need to carefully protect servers, including file, print, proxy, e-mail, web and related equipment. Careful control over access to communication channels (network, telecommunications, server rooms, control rooms, data closets, cabling systems etc.) also needs to be exercised. For example, if an anti-social citizen gains access to a network control room that person may be able to reconfigure equipment to allow greater access to data resources than would otherwise be allowed. It may be possible to attach unauthorised equipment, monitor data flows, and crash systems.

3.2 People: Social and Geographical Affinities

Universities, just like commerce, business and other elements of human activity, are run on people; even quite modest institutions might have a significant number of staff and large numbers of students. Distance learning institutions might have extremely large student numbers, many accessing the institutions from outside. Unlike organisations in trade and industry a very high percentage of the faculty, staff and the student body of a university will be expect to utilise IS as a significant part of their activities. Therefore higher education is predisposed to have significant numbers of IS literate persons utilising the technology.

People are a product of their culture, background, upbringing and the society in which they live. This means that the attitudes that they bring to important issues are formed by these lifestyles and societal influences. This is very much the case with respect to SQU, since it contains a mix of faculty/staff from many different cultures, as well as students from all regions of Oman.

Faculty, staff and students are brought together and their attitudes and affinities are such that considerable variation may be found in respect to:

- Work ethics,
- Social issues and related customs,
- Professional responsibilities,
- Privacy and security,
- Sharing and collaborative working.

These individuals may have loyalties which are influenced by external factors. These may include:

- Social, tribal or national grouping;
- Research team, department or faculty membership.

Farthermore these loyalties may be stronger and more important to them then those that they have towards the institution as a whole.

In recognition of the importance of these issues many professional organisations have established and published codes governing ethics in the industry (Illinois Institute of Technology, undated).

While these issues are not unique in any way to this institution they are certainly of importance when assessing our IS security needs. For example, within the Arab world there is very much a culture of sharing and openness between social groups, and this means that matters relating to confidentiality and security of system passwords and usernames are relevant. Not to share such knowledge might be considered in some groups to be antisocial, and yet this cannot be permitted since we need to protect sensitive data and vulnerable systems.

When we are considering information systems security, trust is important. There needs to be trust in the custodians of the data, as well as those who administer and utilise that data. If the loyalties of staff are more orientated towards the social groups than towards the institution then this trust will be misplaced. It is therefore important to ensure that these “trust relationships” are established properly.

Along with the issue of trust there is also the matter of what are the acceptable and proper ways that information can be used. Especially when you have many individuals from different cultural/social backgrounds you may find that what might to some be acceptable to others may not be. Similarly, activities like hacking/cracking taking in one frame of reference (for example research), may not be acceptable in others (for example administration). Without clear guidelines as to proper usage we are leaving it to the user to sort out in his, or her, own mind what is the correct way to handle the information that they possess.

Other issues relating to sharing and ownership are the matters of the copying of software products and intellectual copyright. Oman has developed the necessary legislation, but again the culture of sharing means that the copying of software products does still occur, and this represents a number of risks. These include: corporate exposure to legal challenges; the propagation of viruses; the wide dispersal of a variety of incompatible software products (causing maintenance problems); possible security vulnerabilities (due to the use of unsecured or otherwise dangerous products).

This also leads us to consider the matter of a legal framework for the protection of information. As well as the implementation and enforcement of a proper copyright and intellectual property law there is also the matter of security and so forth for personal, corporate, and other types of data. If there is no regulatory framework to define fair use and so forth what should be the guidelines an organisation should implement with respect to its data protection responsibilities.

Risks arise from a wide variety of persons. They may be faculty, staff, students, visitors, contractors, guests, or persons with no reasons for being on site. The reason they have for attempting to gain access may be:

- For academic, political, or economic advantage,
- As an intellectual exercise (it was the challenge!),
- Due to a personal grudge or disagreement (with respect to the institution, or a particular individual).

Such persons may be able to achieve their objective by direct access to systems that are not properly secured, or via local LAN or dial in services. There are documented cases of former employees, some in security sensitive positions, being suspected as being the source of sabotage to systems (Texas (State of), undated). Some hackers would have us believe they have a mission to improve society (Garigue, undated).

Campus based institutions, such as those involved in tertiary education and research, face particular vulnerabilities from their student body. The student is, to a certain extent, expected to study, research and develop expertise. There is very much an expectation that they should push both the technology and their expertise. And within the campus community the students will have:

- Spare time to study,
- Available equipment and access,
- Motivation to perform,
- Knowledge available.

Therefore the risk may be higher than in a commercial environment, where availability of all these resources is restricted, or very closely controlled.

Overall then all involved in information systems need to be security aware. They need to know their rights and responsibilities. That is to say that what must be developed is a security culture within the framework of the educational establishment (Cox, 2000).

3.3 Systems: Protecting the Hardware and Software

Personal computers provide an easy to utilise high performance method of storing information. Unfortunately they also present a serious security risk from the standpoint of data protection. There are many risks to personal hardware systems that do not impact those that are centrally managed and controlled (Brook, 2000, Anon, 2000). Some examples of risks that involve personal computers include:

3.3.1 Theft, damage and loss

You may assume that it requires a high degree of technical skill to perform a computer crime. This is not the case, since data in highly portable systems is easy to steal, just take the system. If information is stored on removable media then this is even easier to remove. Someone with a minimal level of technical competence can remove the physical hard disk. If you are not concerned about subtlety, you can easily damage a hard disk and cause the loss of significant quantities of data.

3.3.2 Copying, modification, and corruption

With a somewhat greater degree of technical competence, and open access to an unsecured system, someone can simply copy the data to some other media and take it away. Alternatively, data stored within the system could be modified in any number of ways. Without a proper auditing and policing policy it may be impossible to detect the loss or damage.

3.3.3 Software applications

Good security means close controls over applications. Many different types of "rouge" application may be present in a PC based office system. Some may be user built applications used to augment, or replace, those provided by the data centre. They may be used in preference due to familiarity or simplicity. The problem with them is that they will not be subject to the rigorous development criteria that the data centre would use during development and testing.

Other types of rouge applications may be shareware, freeware and other "fringe" products that should not be used within an administrative or teaching environment. They may be poorly developed, inherently insecure, have backdoors into systems, degrade system performance, waste disk space and otherwise degrade system performance. Such applications may include games and utilities often packaged on magazine covers.

In the case of licenced software illegally mounted, these application may leave the institution open to legal challenge should a software company subject the institute to a software audit.

3.3.4 Viruses, Trojans and the like

Computer viruses are software applications designed to perform some action that is neither expected nor required by the user of a system. A Trojan is an application that allegedly performs some beneficial activity, but in fact performs some other; usually one the operator does not wish for or require.

Unauthorised persons may introduce these into the computer, however they are most likely the result of unsafe working practises. They may utilise a number of different vectors to infect a system. For a stand-alone system this will be via an infected diskette of CD-ROM. For a network connected system it may be via the LAN connection.

3.3.5 System Failure

Computer equipment becomes technologically obsolete very quickly. However it is generally quite reliable and can continue to operate well for some years.

Unfortunately many office based systems now contain important data that is not fully and properly backed up and hard disk systems are particular vulnerable. If you lose your disk you can lose a considerable amount of data. There are protections, of course. Mirroring, RAID, S.M.A.R.T and regular backups all have their parts to play. Nevertheless as a disk gets older failure becomes more likely (Kari, undated).

Our experiences here point to between three and five years as being a good lifetime for a disk, although many do last longer. If you are performing backups remember to ensure that they are usable, by performing recovery tests on a regular basis. Failure to test backups regularly may lead you to have a "false sense of security". If you have remembered to make backups and then find they are not usable you risk serious and catastrophic data loss.

3.3.6 Transient Equipment

When we discuss transient equipment we mean systems that may be utilised within the university campus but also outside. Such equipment will primarily consist of portable (laptop/notebook systems). Such systems may be used by students (in some universities this is almost mandatory), others may be used by staff who choose to work from home, some may be part of test and diagnostic equipment used in the field.

This equipment is at specific risk for several reasons. It may be lost, stolen or damaged. Confidential information may be moved to an uncontrolled and unsecured environment. Lastly, these systems may be connected to a public network with the attendent risks of being infected by viruses or remotely accessed by hackers. It is interesting to observe that many companies, including PC hardware suppliers, now offer notebook security products.

3.4 Networks: Communication Risks

Your LAN is probably one of the most important part of your IS structures. It is also an area where security is critical (Quinn-Andry and Haller, 1998). This type of communication network possesses many advantages for the institution in terms of the cooperative sharing of information in both academic and administrative areas. Unfortunately it also presents us with a number of serious exposures from the security standpoint.

To ensure a well secured network your design needs to consider the issues of (Quinn-Andry and Haller, 1998):

- Authentication (identifying the user),
- Authorisation (what the user is allowed to do),
- Integrity (protecting the data in transit from amendment/corruption),
- Encryption (to prevent data in transit being transmitted "in clear" text).

The regular basic Ethernet TCP/IP network utilising IPv4 provides little in the way of security controls over access, or mechanisms to prevent misuse of that access. To effectively secure such networks additional measures need to be put in place. These measures would control access, and ensure that data being passed "over the wire" was not easily accessed. There are many mechanisms that can be used to address these issues and these include one-time passwords, card access, digital certificates, secure protocols and so on. A useful discussion is contained in (Read), undated) and while that document specifically applies to isues relating to Internet much of the discussion is just as relevant from the standpoint of the local intranet.

In implementing security controls over access to information systems through network access a balance needs to be struck. This balance needs to consider:

- How much security do we require,
- What are we prepared to pay for that security (that is to say what value do we place on our data),
- The degree of convenience (more like inconvenience) will our faculty, staff and students tolerate.

We should not make security so tight that it actively discourages the use of the resources provided. As with other institutions of this type the university has a developed an expanding LAN network interconnecting into the Internet, due to its internal structure protocols and this connection there are clear security exposures. These exposures can be classified as coming from:

- Outside the university LAN via the Internet,
- By dial-in service,
- By the attachment of unauthorised equipment,

- From within the university LAN,
- Through the use of broadcast technologies.

The Internet can provide a means of gaining access to a campus based system without the particular individual being physically present on the campus. This means that the border controls between the Internet and your LAN have to be carefully and strictly managed. If they are not fully and carefully managed then vulnerabilities may exist. Commercial environments frequently configure their firewalls to block all but a few required services, the so-called "deny all" option. Owing to the open nature of university operations in academic institutions the opposite view is often taken, with free access being the norm, the so-called "allow all" option. In the case of SQU we tend to follow the safer commercial model.

Dial-in services are potential sources of security risks. With these the user may be within your campus or without. Even those institutions with limited internal dial-in facilities may be at risk since internal phone lines may be set-up to reroute external calls to internal dial-in modem services. The location of remote access servers with respect to the LAN, therefore, needs to be carefully considered since placement within the firewall presents definite security risks (since it will permit firewall controls to be circumvented with a simple phone call). Placement outside the firewall presents a more complex access regime, so may be more secure. Once the internal LAN has been accessed by dial-in the security risks are the same as access via a local workstation.

The LAN attachment of unauthourised systems and other equipment can be a major vulnerability. Network enabled Windows and Unix like products are now the norm. It is simple quick and easy to attach such equipment to a LAN. Should the newly attached equipment be misconfigured then it can predjudice the entire LAN operation. For example if a PC is attached with the same IP address as your regular DHCP server then the packets may be misdirected to the wrong system. Since dynamically assigned IP addresses which come from your DHCP service have a specific lease, or timeout period, the problem may not be noticed immediately but could degrade network performance over a period of several days.

Similarly users may, for their own convenience, create remote access servers (using a PC and modem) and attach these into the internal phone network. This would permit them to dial-in to their office number and access the LAN remotely. However, since the remote access server is within the LAN, and not routed through any firewall or other access control mechanism it represents a fundemental risk. Should the user "publish" such a service to his/her department then the risk would grow significantly.

Since the vast majority of university PCs are interconnected into LANs, each represents a potential risk from the standpoint of security. Systems in computer laboratories are generally controlled quite loosely, since the intention is to provide quick, easy, free and open access.

Data may be compromised not only by gaining unauthorised access to systems across the LAN, but also by monitoring of data traffic within the network. This is generally a simple process utilising a software application called a packet sniffer. Such sniffers are available on the Internet. More sophisticated users may be able to detect unencrypted confidential data, including usernames and passwords being passed around the LAN. They may modify the content of data packets themselves or disguise themselves as other machines (using a process known as spoofing). Particularly knowledgeable users may be able to send unattributable e-mail, or become a general nuisance, through routing mail through slot facilities (on the Internet) or through misconfigured sendmail hosts.

Wireless networks are another area where security concerns have been raised. While these LANS are not strictly new, until recently they have not been extensively deployed at SQU owing to the absence of internationally ratified standards, low performance and high cost. They have often been proposed as possible solutions to providing connectivity both within and between buildings. Many of the objections to them have now been addressed, although even IEEE 802.11 based equipment operating at 11 Mb/sec cannot, at present, approach the 100 to 1000 Mb/sec that we deploy on our regular hard wired networks. Nevertheless they are becoming more common.

Security is an issue in wireless LANs due to the ability of hackers to gain access to the campus LAN without any physical contact. The possibility of casual passers by being able to tap into the LAN with a notebook computer and a wireless access card has been raised (Ross, 2000; Fisher and Nobel, 2001 ; Leyden, 2001). Should the security encryption technology built into the wireless equipment be inadequate then access could be gained and security compromised. Specific doubts have been raised as to flaws in the Wired Equivalent Privacy (WEP) algorithm (Borisov *et. al*., undated), which is part of the IEEE 802.11 standard.

Similarly LAN connected systems are at risk from hacker/cracker attack. The objective is normally to gain system administrator status (root privilege in Unix machines). Often such access is facilitated by incorrectly configured systems, systems with unsecured user accounts, or unpatched systems where the OS contains known vulnerabilities.

There is an extensive range of hacker/cracker/ network administrator tools and resources available in the Internet and via print publications (Anon, 1998). Frequently these tools are designed for relatively unskilled and unsophisticated users. This has given rise to the so-called "script kiddie"; someone without the extensive skills of the true hacker and, we are lead to believe, without the sense of social responsibility (Garigue, undated).

Unauthorised access is not the only system vulnerability that we need to be aware of. Probably the most well known secondary vulnerability is to the operational system availability and this is known as the denial of service attack. Put bluntly, the intention is to make your system/LAN unusable. Again there are a wide variety of tools available on the Internet for this purpose. Thus we are not talking about anything that requires an extensive amount of technical competence.

The final system vulnerability is the injection of unauthorised applications into your system. Sometimes viruses and Trojans may secure a foothold in your system through regular user activities such as e-mail and so forth. In some cases once they have secured such access they can utilise this as a stepping stone into other systems thereby propagating their activities. An example of this is the (in) famous ILOVEYOU virus. Which relies on firewalls not blocking e-mail attachments, and users being less than careful in their use of E-mail software.

4. Solution Strategies

You need to attack a number of different areas when attempting to reduce security risks to your IS structures. These may be considered as being:

- General, which may be applied throughout the whole institutions,
- Social, which are aimed at changing the work attitudes of faculty, staff and students,
- Technical, which ensure you have the correct skills and technologies to address the challenges.

To reduce risks we need to ensure that IS systems are secure, policed, recoverable. The following lists define a number of strategies that you may choose to consider when attempting this. While they may well not be definitive they are all well worth considering. Let's address the general issues first:

- Committee with full academic/administrative representation (security is the responsibility of all)
- Security officer/team in IS centre (someone has to be responsible),
- Security responsibilities in colleges/centres (responsible not just in the centre, also in all parts of the institution)
- Security reporting and feedback hotline (to ensure security issues are communicated effectively),
- Consider more effective authentication schemes (the basic username/password strategy is not very secure),
- Buy in from executive and management (support is required at the highest levels),

- Ensure all infrastructure installed in secure areas (keep doors to offices, control rooms locked),
- Limit access to secured areas to those with need (can you trust your maintenance and cleaning staff?).

4.1 Social issues

- Develop a security minded culture (everyone should think security – not just the IS centre),
- Code of practice/acceptable use policy (written policy, signed off by users, reminders on screens – so people know what is and is not allowed),
- Education with respect to proper policies and procedures (people may not read the policies, they should be reminded from time to time),
- Pay attention to legal and administrative framework (an institution must conform to the national laws, its IS structures need to be compliant with institutional regulations also),
- Full, fair and effective enforcement (a policy is no good unless it is properly enforced, and seen to be so).

4.2 Technical

- Trained technical staff with up-to-date hacker/cracker knowledge (staff should know what the vulnerabilities are before they become problems, not after a problem arises – be proactive),
- Monitor hacker sites to ensure that the latest exploits are known,
- Ensure equipment running at latest service releases with applied patches as required (all systems contain vulnerabilities, close known holes as soon as you can),
- Properly configured systems with good user/password security (don't assume default configurations are secure, always change default passwords),
- Approved software use policy (limit range of software allowed to reduce licence violations, as well as support and other vulnerabilities from unknown products)
- Security probes on key and critical systems (check that your systems are secure, don't assume they are),
- Effective monitoring and assessment of traffic (you're unlikely to fix a problem you don't know about – how do you know you've been hacked?),
- Maintain anti-virus software at latest release (to keep up with the latest development in "virusware"),
- Maintenance and backups of all key systems (if you lose your data you need to be able to get it back, if you've been hacked how can you trust your information),
- Storage of critical data on secured servers, not desktop systems (the knowledge of the institution is too valuable to keep on a desktop system that may not be adequately protected),
- Test backup systems on a regular basis to ensure that information is recoverable.

5. Summary and Conclusions

Information sharing is well recognised as being important to the academic activities of institutions like the SQU. In commercial organisations this isn't usually the case, and it would be difficult for an academic institution to adopt a typical corporate model.

A wide variety of information is stored and utilised within the IS structures of any academic institutions. Some may be primarily administrative, but a significant amount will relate to the primary responsibilities of the organisation: education and research.

Information systems used within academic communities need to be developed to facilitate information exchange but also ensure the security and integrity of the data being handled. Owing to the basic nature of information exchange within the academic community some risks are unavoidable.

To ensure the security of IS we must consider a number of factors. There are technical issues such as hardware, software, networking and physical infrastructure. Similarly there are cultural and social issues, these are important not only with reference to the individual but also on an institutional basis (the organisational ethos).

Many of the risk factors may be addressed by the proper application of a number of user policies. The guidelines and procedures should be applied, on an institutional basis, to the custodians of IS systems as well as the users of systems and data. Users should be educated as to their responsibilities through the establishment of proper training programs. Technical issues should be handled by an experienced and capable technical team.

References

ANON, 1998, *Maximum Security, Second Edition*, SAMS Publishing.

ANON, 2000, Computer Fundamentals and Applications (Course Syllabus), Chapter 8, Computer Security and Risks, www.pentaq.co.nz/Columns/ComputerFunctionality.html.

ATTORNEY GENERAL (Australia), 1999, 26th August, Protecting Australia's Information Infrastructure, News Release law.gov.au/aghome/agnews/1999newsag/601_99.htm.

BORISOV, N., GOLDBERG, I. and WAGNER, D. Undated, Security of the WEP algorithm, University of California at Berkley, www.isaac.cs.berkeley.edu/isaac/wep-faq.html.

BRITISH STANDARDAS INSTITUTE, 1999, Information Security Management, Specification for Information Security Management System, BS7799-2.

BROOK, J. 2000, Computer Reliability Checklist – Revised, www.pentaq.co.nz/Columns /ComputerFunctionality.html.

COX, A., 24th November 2000, Report on Creating a Security Culture in HE and FE Conference, University of Glasgow, litc.sbu.ac.uk/jcalt/conference/confreport.htm.

ELLIOT, R., YOUNG, M.O., COLLINS, V.D., FRAWLEY, D. and EMARES, M.L. 1991, Information Security in Higher Education*, Cause - The Association for the Management of Information Technology in Higher Education*, Professional Paper Series #5.

FISHER, D. and NOBEL, C., February 9, 2001, Wireless LAN Security Holes Exposed, eWeek News, www.zdnet.com/eweek/stories/general/0,11011, 2684262,00.html.

FRASER, B. (Ed), September 1997, Site Security Handbook, RFC2196, The Internet Engineering Task Force, Network Working Group, www.ietf.org/rfc/rfc2196.txt?number=2196.

GARIGUE, R.J., Undated, Hacking Belief Systems, An Agenda for the Survival of Humanity in Cyber-Society,The Activist Agenda in Cyber-Society superior.carleton.ca/~rgarigue/hack.htm, www.infowar.com/articles/00/cyborg/CYBORG3.htm.

HANSARD (UK Gov), 4 Nov 1998, Official Debate Report, House of Commons *Hansard* for 4 Nov 1998 (pt 52), The Stationery Office Ltd, Department of the Official Report (Hansard), Volume: 318, Part:232, ISBN: 0106232983, www.parliament.the-stationery-office .co.uk/pa/cm199798/ cmhansrd/vo981104/ debtext/81104-52.htm

HARVARD UNIVERSIY, November 1991, Information Security Handbook, Version 2, www.all.net/books/document/harvard.html.

HASSLER, A.A., 1998, Guaranteed Access to Campus Network Resources: Policies and Issues, *Cause/Effect*, **21-No. 2**:10-14, www.educause.edu/ir/library/html/cem9824.html.

HUNTER, B., 14 April, 2000, Information Security: Raising Awareness,Version 1.0, Government of Canada PKI Secretariat, Chief Information Officer Branch,Treasury Board of Canada Secretariat, www.iwar.org.uk/comsec/resources/canada-ia/infosecawareness.htm

ILLINOIS INSTITUTE OF TECHNOLOGY, Undated, Center for Study of Ethics in the Professions, Code of Ethics Online, Computing and Information Systems, csep.iit.edu/codes/computer.html.

INTERNATIONAL STANDARDS OREGANISATION, Information Technology – Code of Practice for Information Security Management, ISO/IEC 17799, (The ISO version of BS7799).

JOINT INFORMATION SYSTEMS COMMITTEE, 27th February 2001, Developing an Information Security Policy, www.jisc.ac.uk/pub01/security_policy.html.

KARI, H.H., Undated, Latent Sector Faults and Reliability of Disk Arrays, Dissertation in Helsinki University of Technology, Espoo, Finland, www.cs.hut.fi/~hhk/phd/chapter3/phd_3.html.

LEACH, J., Undated, Findings from the first stage of the Study into the Requirements for Authentication, Authorisation and Privacy in Higher Education, Joint Information Systems Committee, www.jtap.ac.uk/reports/htm/jtap-015-1.html

LEYDEN, J., 29th March 2001, War Driving: The Latest Hacker Fad,The Register, www.theregister.co.uk/content/archive/17976.html

QUINN-ANDRY, T. and HALLER, K., 1998, *Designing Campus Networks*, Cisco Press, Macmillan Technical Publishing.

READ, J. (Editor), *et. al*., Undated, Working Paper on Secure Internet Issues for the HE Community, Interim Report from JTAP-659, University of Southampton, www.jtap.ac.uk/reports/htm/jtap-032.html.

ROSS, J.B., November 4, 2000, Containing the Wireless LAN Security Risk, SANS Institute, www.sans.org/infosecFAQ/wireless/wireless_LAN.htm.

SAN FRANCISCO STATE UNIVERSITY, Undated, Draft Self-Study for WASC Re-accreditation, Volume I - Implementing the University Strategic Plan, Chapter 14, www.sfsu.edu/~acadplan/wascss14.htm.

STAMEN, E.M., July 1986, Ownership, Privacy, Confidentiality, and Security of Data, *Cause/Effect*, **9-No. 4:** 4-9.

TEXAS (The State of), Donald Gene Burleson (Appellant) vs The State of Texas, State. No. 2-88-301-CR Court of Appeals of Texas, Second District, Fort Worth, 802 S.W.2d 429 rampages.onramp.net/~dgmccown/c-txblsn.htm.

UNIVERSITY OF CALIFORNIA, May 22, 1998, Improving Network and Computer Security at the University of California, Berkley, Report of the ITATF Security Working Group socrates.berkeley.edu:2001/security/itatf_swg_report.html.

UNIVERSITY OF LEICESTER, 27th November 2000, Management Information Systems, Computer Security Policy, Administrative Systems, www.le.ac.uk/mis/html_docs/security.htm.

WHITE HOUSE (The), 2000, Defending America's Cyberspace, National Plan for Information Systems Protection, An Invitation to a Dialogue, Version 1.

Received 11 June 2001
Accepted 4 February 2002