

INFORMATION TECHNOLOGY - THE NEED FOR SECURITY

(Or, Companies have a responsibility for the information in their keeping)

The rapid growth of information technology (IT) telecommunication networks and computer systems is having a considerable impact on the global economy. The spread of telecommunications companies and networks, through mergers, acquisitions and investment, is not only boosting global economies but also increasing competition, hopefully to the benefit of consumers. Hot on the heels of telephone and facsimile communication systems is access to the Internet and, by definition, access to world-wide databases of information and knowledge.

The idea of an interconnected network was for an 'open' system that allowed, in the beginning, a number of US University computer systems to be connected for the exchange of information and ideas. The Internet, as it became, has now progressed to a system where any individual with a computer anywhere and with the appropriate software, browser and access to telecommunication networks can connect through Internet Service Providers (ISPs) to a wealth of databases and company websites.

However, the fact that it is a public service, that it is freely available and does not have an overall management and control system means that connected computer networks and databases are open to possible security threats and breaches. Indeed as more and more people 'get connected' the possibility of security threats is likely to increase.

However, in stating the obvious, in this knowledge driven age no company can get very far for very long without equipment and systems to store, retrieve and exchange information. Companies and organizations exchange information as part of the business process. It can be something as simple as order forms, advice notes or even confirmatory letters arranging for the supply, delivery or return of materials and resources or, more complex like financial data or project management planning boards, bar charts and information.

Indeed for businesses to survive and by that I mean the difference between profit and loss much depends on having the right information in the right place and at the right time. It does not matter whether it is with a sales person at the point of contact in the office or shop, a salesman in the field, the design, operation or manufacturing processes or financial staff producing balance sheets time is, increasingly, of the essence. And, for customers it not only provides an alternate means of conducting business but an opportunity to speed the process of negotiation and conclusion.

As confidence in the use of the 'net' increases more and more people are looking to conduct electronic transactions with their bank such as paying bills and transferring assets from one account to another. They are also looking to purchase goods and services direct from manufacturers, suppliers or other financial institutions. In some countries and regions they can also deal direct with local and central government to pay bills for such services as television licences, driving licences, motor-car registration and even council taxes, or, in the US, to order personalized number plates and to replace lost identity cards. Whatever the reason for using the Internet, that information is, strictly, a transaction between one company or an individual to another company or individual. But, it must be acknowledged and accepted that not all networks are 'secure' and that information can be obtained from computer databases and networks.

For companies and organizations the Internet is not only an opportunity to expand their business on a global scale and provide better customer services but it is becoming an area of increasing frustration and possible danger because of the security implications.

As computers and networks expand there is an increasing threat from younger people, often very computer literate, who have the knowledge and ability to cobble together viruses to destroy personal and company e-mail addresses and databases. Sometimes this is done for sheer malice and maybe even achieves notoriety and sometimes done to prove a point, perhaps how clever the computer hacker is?

But, because most, if not all, Internet network connections are insecure, and by that I mean they are accessible by a third party bent on disruption, personal information and details can be accessed, deliberately or otherwise, by other people. This information could, inadvertently, end up with a competitor or even in the press. Indeed there have been reported instances in the past few months where a customer has, accidentally, been provided with access to bank and company databases and from there to personal details and information. Further, the ISPs are not responsible for your connection to a network nor are they responsible for the security of your information. Under those circumstances how can individuals and companies have faith in Internet websites to retain confidentiality?

The first point to recognize is that all companies and organizations have a duty of care to protect any and all information kept by them from unauthorised disclosure. This information can be contained on paper in books and in files. It also includes information sent or received by facsimile or the older telex systems, stored internally or externally on computer databases or associated with backup facilities, transmitted across electronic networks or even telephone conversations that may have been taped. This is, clearly, a management challenge and responsibility and accountability for the introduction, working and operation of any and all computer databases and networks must be at the highest level in companies.

So, the question is how does an organization ensure that they have made every reasonable and possible effort to provide security to the information they have within their systems whilst making it accessible to their own staff and other relevant companies?

There are two initial issues at stake. The first is the overall physical security of databases and information contained in hardware and software equipment in a building. The second is the electronic security of information contained in hard and floppy disks.

Apparently we all make appropriate efforts to secure our personal possessions like homes, motorcars and briefcases, through the use of key and combination locks, alarms and immobiliser systems. This same process, of assessing the physical threat and the physical risk and taking appropriate measures, is also applied to items of company property, although laptop briefcases are an obvious item and have become a target for petty thieves and criminals. Nonetheless, most organizations not only have systems of physical access security but valuable items such as desktop computers and laptops in desktop housing are, more often than not, secured to the desk fittings. And, internal systems and connections can be made more secure by the use of a 'Firewall', that is software that monitors the network for any unusual attempts at access. But, what do you do with laptop computers?

Apart from the more obvious cost of replacement of the laptop a more pertinent question must be what is the possible risk from the loss of the information contained in the electronic files? Can the information be used by a competitor, how much business might a company lose and, could this lead to a loss of business because customers lose faith in the integrity and ability of the organization to keep their records secure? What do we do with information stored on disks and in databases, who do we make responsible for such matters, how do we educate employees to recognize the need for security and what do we do and how do we deal with security breaches?

Information on a desktop or laptop is of two types. Firstly, there is the information displayed on the screen, on which we may be working, which is short-term memory and consists of usually a few megabytes. Records and other information that we need to retrieve as and when required are stored on a hard disk with a capacity of Gigabytes. Access to information in the hard disk is, usually, partially secured through the use of 'User Identity' or 'Login Name' and password procedures, but that does not provide total security. More secure systems tend to use encryption options and removable hard disks that can be transported separately to reduce the risk and avoid the loss of information.

The third issue over which we do not have a great deal of control is a combination of physical and electronic security and that is using desktop and laptop computers to access electronic websites to exchange personal financial information to purchase goods or services. In this case the possible threat and risk is at least doubled. Not only do we have to consider the security of our own system and software but we have to take into consideration the physical and electronic security of the telecommunication connection between your machine and the chosen host machine and also the physical and electronic security of the computer systems and database of the receiving system.

Having had operational responsibility, in the past, for naval and military global telecommunication networks and strategic broadcast systems I know that the only way to provide security of information exchange is by using cryptographic equipment and codes at either end of a circuit and accessible only by intended recipients. Also, that part of the process of information technology security involves more than a degree of physical and personnel security. However, that throws up a whole new ball game and that is the ability of governments, and government organizations, to know what information is contained in messages presumably in the interests of national and public security and safety. And, since the Internet is designed to provide open access such real-time and full-time systems cannot be used.

So, we need to be re-assured that the information we are providing into a pro forma on a computer screen is, firstly, only going to the intended site and not being re-broadcast or distributed to other sites. Internet sites that have some form of encryption between transmitting and receiving sites have a small icon in the bottom left or bottom right of the screen and usually in the shape of an open padlock. When we connect to and access a site with basic encryption the padlock icon, apparently, closes.

Second, having accessed a site we want to be re-assured that it is not possible for a third party to gain access to unauthorised information either because of a poorly designed system or procedures or through too simple access codes. There have been a number of reported incidents where poor security measures and codes have allowed customers to access personal information on other customers held in databases.

One scheme to increase the reliability of internet shopping such that customers are protected, to some degree with the exchange of credit card details is the 'Which? Web Trader Scheme'. Companies that apply to belong to this Internet scheme have to undergo site checks and once approved are indicated by a round red 'Which' logo on the website page. It is based on companies agreeing to abide by a code of practice and involves initial and random site checks by staff employed by the 'Which' organization.

If, for any reason, the credit card information you supply to such an approved site is compromised and misused the Which organization will, allegedly, reimburse the first £50 of your loss and, legally, the credit card company is required to pay the rest; 'Which' also indicate that they include the necessary legal back up if and when it is needed. Additional information and advice on electronic shopping over the Internet can be obtained from the UK Office of Fair Trading.

Nonetheless, as far as individual companies and organizations are concerned clear direction on information security is paramount. To begin with we need an overall company policy to cover such matters. Not only must the production of such a policy have the obvious support of the most senior management but also it should include involvement in the drafting and endorsement of security guidelines.

That is because inadequate systems or procedures lead to breaches and costly, and some might say unnecessary and time-consuming, investigations depending on the severity of the breach. Rules and guidance on internal physical and electronic security must be made available and be understood by all employees.

Even more importantly the threat of the loss of telecommunication connectivity or access to information or the corruption of data and files through deliberate terrorist attack has increased as cases of 'hacking' are brought to light. If it is possible for disgruntled individuals, technology 'geeks' and even school children to access networks and systems that were deemed to be secure think how much damage can be wreaked by a determined group of terrorists.

One area already addressed by many organizations is the introduction of software programmes to constantly monitor the e-mails and Internet access sites of their employees. This is because companies can be held legally responsible for information sent from their electronic systems to other addresses. According to the American Management Association (AMA) some 70 per cent or more of major US firms record and monitor their employee's telephone, e-mail and Internet connections. Problem appears to be that very few have informed their employees of this action prompting, allegedly, the drafting of appropriate legislation in the US Senate to require employers to notify employees when this practice is happening. Perhaps it is already happening in your organization?

For those companies and organizations that believe, and I am really addressing CEOs and directors here, that there is a need to co-ordinate all matters of physical and electronic security relating to the use of computers, databases and telecommunication networks. As a way of improving both physical and electronic security of such systems they might consider employing some of the hundreds of former naval and military officers, warrant officers and communication operators who have a background specialisation in radio communications and telecommunications and who have knowledge and experience of managing defence communication facilities in a variety of scenarios and who will, probably, have managed a defence communication centre. During their career they are likely to have handled much more sensitive information than what is contained in company databases.

However, there are specialist companies that provide advice and guidance on information technology security. In the first instance organizations might make a start to address information security issues by reading British Standard BS7799: A Code of Practice for Information Security. Many well known companies, consultancy firms and financial organizations were involved in drafting this Standard and have gone further by implementing the procedures as part of their code of practice. If it is good enough for them it may well help to resolve some of your difficulties in this area and provide sufficient advice to improve the security of information contained in your company databases.

(2430 words)

KENNETH ARMITAGE

2001