

INFORMATION TECHNOLOGY – SECURITY – AN ENIGMATIC PROBLEM

“And you all know, security is mortals’ chiefest enemy.”

(Shakespeare. Macbeth, III. Iv)

Every individual, every organization and every company has information that he or she or it wants to protect and to have control over when considering who to share it with. The information may be of a purely personal nature that might affect the reputation or job and livelihood of an individual or his family. Or it could affect matters of national security, especially when related to government policy or military matters or the information could relate to company security of drawings or plans of products, future strategy on investment, mergers or acquisitions or a list of customers and their requirements. Whatever the information there are various levels of security that are or could be applied in order to restrict unauthorized access by a person or persons who might use, misuse or abuse the information for personal gain or to gain advantage in a professional or commercial sense.

The area that most affects human beings these days, at work and at home, is the use of information technology and particularly computers and the Internet through telecommunication networks. Of course there are, increasingly, loud and annoying conversations from people using mobile phone systems on all forms of public transport particularly trains. However, if we actually were to overhear someone saying, for example, that a particular horse had the best chance of winning a race or that a company had invented an item of equipment that would revolutionize an area of business or that another company had just signed a very large contract to provide goods and services then, given the wherewithal, we might pay more attention and be tempted to gamble. But then most of us tend not to want to listen to supposedly private conversations and pick up information especially when we are most likely to have used computers, telephones, facsimile machines and other forms of communication during the day and are often suffering from information overload.

The Internet, or World-Wide-Web (WWW), is designed and intended to be an open network that allows free access, through Internet Service Providers (ISPs), to information contained in a variety of databases in an electronic format. The system uses any and all telecommunication network operators to provide the ‘electronic string’ that connects company desktop, home-based or portable personal computer to whatever database is available through a unique routing location (URL) message address. The Internet is not and never was intended to provide a secure means of exchanging information between organizations, companies or individuals and that is why it is vulnerable to electronic attack through corrupt programmes or viruses designed to cause chaos and disruption.

And, that is why most, if not all, large and medium-sized companies have introduced a ‘firewall’ in their electronic communication systems to prevent files and databases being accessed by unwanted third parties or corrupted or destroyed. A ‘firewall’ is a gateway of hardware equipment and software programmes through which all electronic traffic must pass and it is designed to enforce corporate security policy. The major threat to these systems is the fact that ‘hackers’ are becoming increasingly sophisticated in the viruses that they design and it is important to keep such firewall systems up to date to ensure the security of data contained therein.

Which leads into the next point and that is the need for company's to conduct a threat assessment of all their electronic means of communication and to determine how vulnerable they are to security threats and what the fall-back position is should the primary method of communication be disrupted by whatever means.

Of course, the degree of security provided in individual computers and on internal local area networks (LANs) and external wide area networks (WANs) depends entirely on how important senior management believes their IT, databases and telecommunication networks and services are. Increasingly companies are being encouraged to site their equipment in purpose-built 'IT Hotels' where most aspects of security, physical and electronic, have been installed to prevent loss of service. This concept is sold on the premise that precautions have been taken to maintain systems and equipment through back-up services and that there is on-site support 24 hours a day and 365 days a year.

However, there are no absolute guarantees that one system, one building or one network is totally and completely secure simply because whilst IT and telecommunication network designers are working to improve the security of their equipment and systems there are others working to gain access. It is extremely difficult to discourage anyone who is determined to access a system, cryptologic, network or database that presents a challenge.

There is another form of threat likely to cause concern and that is one associated with identity theft and that is likely to increase as more and more information is stored in computer systems and as more and more call centre activity is moved, outsourced or off-shored, to other parts of the world, as a way of reducing overheads.

UK companies and organizations who off-shore their call-centre and information technology (IT) services to any other part of the world are still responsible for the security of customer data and other information contained in their computers and databases or passing through their networks. Some companies may not fully appreciate the ramifications of the Data Protection Act with respect to this particular issue.

This threat is particularly relevant to companies in the banking, insurance and other related areas of finance that include electronic access systems for financial and other data transfer transactions and to companies in the travel or information technology sectors who have sited call-centres in other parts of the world. The use of passwords provide only limited security and IT systems can only be secured by the used of cryptographic equipment, which is not a viable proposition.

Nonetheless, the more important IT systems and telecommunication networks are to the success and future of a company the greater the need to ensure that every precaution is taken to maintain communications under all circumstances and the more time and effort that should be expended on meeting the criteria. Frankly, any company that does not make every effort to secure their network and databases is almost encouraging unauthorized access to its systems and files. As the Irish philosopher Edmund Burke observed,

"Better to be despised for too anxious apprehensions, than ruined by too confident security."

(Edmund Burke (1729 – 1797), Irish philosopher, orator and politician)

With my background in general management, organization and administration of naval and military radio communications and telecommunications networks, systems and manpower it seems to me that the weakness in some companies appears to be the fact that at senior management, board level, there is often little understanding of IT systems and networks and not much knowledge of security issues. Indeed, I suspect that many directors and senior managers have little or no idea about the importance of data systems and the security of systems and networks to prevent loss of disclosure.

The result can be reduced investment in IT systems, necessary to meet the security demands of the company, let alone provide the organization with appropriate means and methods of securing any information they choose to store in their databases. Perhaps some might wake to this fact if they are sued for the loss of personal as well as financial data.

Like many other areas of business there has been considerable expansion in the provision of IT and telecommunication equipment, networks and security systems and equipment over the past decade. Unfortunately not all of it relevant to the demands of every company and not every electronic software system that has been installed is compatible with other systems.

Therefore, there is a need to address the security requirements of your company or organization as a complete package and even a case for implementing a complete package from one vendor. Nonetheless, before proceeding it is imperative that a company or organization conduct its own security threat assessment taking advice, as appropriate, from specialist IT and Telecommunication consultancies. The areas that should be addressed, as part of basic overview to determine an IT Corporate Risk Analysis, are:

- a. Physical Security – how secure is access to the building and how easy is it to get to a computer terminal and access your systems?
- b. Physical Security – how secure are your computer rooms, not just the door but the surrounding walls and areas?
- c. Ventilation systems – all computer and IT equipment need some form of forced air ventilation to keep systems operating at ambient temperatures. How secure are your ventilation ducting and trunking systems?
- d. Water supplies – most forced-air ventilation cooling systems need a water supply to provide the cooling element. How secure is your water supply?
- e. Electricity supply – all IT equipment need electricity to operate. What are your fallback facilities in the event of a loss of main electricity supply? How secure is the supply duct? Is there an alternate electricity route into the building and do you have fail-safe emergency diesel generators available?
- f. Storage – do you store back-up discs and files, with company information, in secure containers in physically secure areas?
- g. Landlines – how physically secure are the telecommunication network cables into your building? Are they easily accessible by telecommunication network operator staff and therefore how easily can a saboteur access them?
- h. Satellite systems – do you use satellite communication uplink and downlink services to effect communications to dispersed sites? If you do then how secure is the roof of the building and how easily could someone do damage to the satellite dishes, the connectivity into the building or the tracking systems?

- i. Electronic eavesdropping – how secure are your telephone systems from unauthorized wire-tapping. It is very easy to lay a cable alongside an uncovered copper cable and pick up information passing through one to the other.
- j. VDU Security - Can someone in an adjacent building see any visual display units (VDUs) in your building and is the information displayed likely to be of any commercial or national interest? Do not forget that all VDUs, like all electronic pieces of equipment, transmit and that it is possible to receive and monitor exactly what is displayed on a terminal screen at a considerable distance.
- k. Basic Access Security - Have you provided, at the very least, basic access security code systems, which require a login name and a password that has to be changed on a regular basis, so that only authorized personnel can access the information and files in your database system?
- l. Personnel – for those organizations that handle information of a sensitive nature then some form of security vetting has to be carried out. This procedure is not necessary for most commercial organizations but it is a fact that sensitive information is sometimes removed internally and therefore, it is paramount that personnel employed in such areas can be trusted.
- m. Cryptographic – for those organizations and companies that deal with highly sensitive materiel they will, as a matter of course, protect their systems and information by the provision of cryptographic equipment and codes and have a much, much higher level of physical, electronic, electrical, ventilation and supply security systems.
For commercial organizations the degree of cryptographic coverage will depend entirely on the information that is being exchanged and how sensitive and important it is to the company, by that I mean how much importance the board places on information security.
- n. Do not introduce new IT equipment and systems without first ensuring that it is interoperable with existing systems, unless it is a replacement for current systems, nor introduce equipment or software unless it meets a specific strategic or operational requirement.
- o. Do consult staff who will be required to use the systems and, if and when appropriate, ensure that they receive relevant and necessary training before the implementation of new equipment.
- p. Appoint an internal programme manager, with support staff, who will be responsible for liaison with the chosen contractor and for the introduction of the system and training courses necessary prior to rollout and after implementation.
- q. Take stock of current systems and do not consider investing in more IT systems unless it is essential and meets the requirements of the business.
- r. Ensure that information contained in laptops and on computer disks are handled in the most appropriate manner that is handled personally and not left for some unauthorized person to access either by stealth, by deception or simply by stealing. Do not leave such items unattended in any circumstances and avoid carrying sensitive data on unencrypted systems.

As part of your IT strategy you may consider outsourcing your IT services to a reputable company but, be warned, if you really do rely on IT systems and telecommunication networks to conduct your business, and increasingly companies and government organizations do, then you might be wiser to keep IT and telecommunications services and manpower in house so that you can exercise a far greater degree of management and security control especially with possible breaches of physical and electronic security and the loss of information.

That is because, as I have mentioned in previous articles, if something goes drastically wrong with a service and customer data and information is lost it is not the outsourced company that suffers from any reaction from clients and customers but the company providing the product or service and this is particularly relevant to government divisions and organizations that handle personal data of a sensitive nature.

In the past few years some companies have embarked upon the introduction of programme management systems, supply chain management systems and customer relationship management (CRM) systems but they have forgotten about the human element. And, if system security is to be maintained then it is imperative that Chief Executives, directors and senior managers are held to account for any security lapses. Responsibility for ensuring that all such systems are secure and that the information contained in the database or databases must remain at the highest levels within organizations.

An enormous and complicated database programme, designed to provide detailed information to one department, usually the finance department, to enable them to produce yards of statistics as a means of setting targets, is not particularly effective if it is time consuming and creates yet more work for other employees in other sections; and, there is little point having a customer relationship management programme if you are not getting out and about growing the business by selling your products and maintaining close relations with your clients and customers.

You not only have to conduct face-to-face meetings and discussions to understand their needs but you also have to re-assure them that any information about them held in your databases is secure and is not accessible by other companies and organizations and is most certainly not vulnerable to physical or electronic attack.

That is why it is imperative, with an increasingly computer-wise and adept generation, that companies spend time, effort and money in ensuring that details and information contained in their databases is protected not only by password access, firewalls and other security measures but, where essential, with cryptographic equipment.

It is because of the increasing costs of information technology systems and telecommunication networks and database operators why companies, who concentrate more on the 'bottom-line' rather than on security, move their call centre services and activity to another part of the world to reduce overheads. But, they need to give very serious consideration to the sensitivity of the information contained in their databases because of the very real risk of identity and other fraud and theft.

Customers need to be re-assured that their information, their identity and their assets are secure in a company's database, are not wide open to abuse and cannot be accessed by unauthorized, unwanted or unnecessary people and organizations, because if they are not re-assured they will move their custom elsewhere.

Finally, there is no conclusive or irrefutable proof that more and more IT systems have made companies more productive or competitive. Therefore, senior management has to accept that IT systems and equipment are tools and that the introduction of such equipment is to help people carry out their tasks more efficiently and productively such that they can best meet the demands of customers more quickly and effectively.

The introduction of new equipment and different software packages should not be based on the premise that they will, as a matter of course, lead to a reduction in manpower. It is primarily because companies automatically removed manpower with the successive introduction of IT systems that workloads began to increase as did stress levels leading to greater inefficiencies.

In my view, there is a real need for designers and programmers of IT equipment and systems to make sure technology meets the needs of business and people rather than allow IT to continue to drive the work patterns and procedures of people. And, it is paramount that all organizations and companies, and more especially government sections and departments, are acutely aware of the information they are handling and the need to maintain the highest levels of security when handling such information on desk-tops, laptops and anything transferred onto portable data devices. If that is not the case then there is increasing evidence that providing more and more data to companies and organizations can lead to increasing levels of data loss, security breaches and to the compromise of individual information.

(2900 words including quotations)

KENNETH ARMITAGE

29 December 2001