

IS Security needs ethics

Prof. Simon Rogerson

**Originally published as ETHicol in the IMIS Journal Volume 12
No 4 (August 2002)**

We need reassurance that our electronic communications are safe from interference and delivered on time to the right people because ICT is not without its problems or its disasters. There continues to be increasing incidents of ICT abuse. For example, the Audit Commission has reported the incidence of ICT abuse within the UK every three years since 1983. The last two reports, Ghost in the Machine (1998) and yourbusiness@risk (2001) report an increase over six years from 34% to 67% of organisations experiencing incidents of ICT abuse. Such surveys suggest that unless positive action is taken the expansion of ICT usage will be matched by an increased level of ICT abuse. The consequences are manifold; business disruption, damaged reputation, financial loss and a loss of confidence in the use of ICT in service delivery.

Clearly computer security must be addressed. If it is to be effective, its objectives must be related to business and be the responsibility of management. Senior management must be seen to support and be committed to the process. All managers and employees must be educated in and convinced of the need for security, and be made fully aware of security policies and standards. There is a dual responsibility regarding ICT abuse. Organisations should minimise the opportunity for ICT abuse whilst individuals have a responsibility to resist such temptations.

Business operations that span the world and comprise multicultural workforces are now commonplace. Organisations frequently use outsourcing in the search for efficiency gains, so important in an increasingly competitive business world. This complex diversity in the workforce both in terms of backgrounds and relationships has added a new twist to the computer security issue. For example, where will the loyalty of the outsourcer lie? Will it be with the client, with the technology, with the outsourcing broker or with another third party? This new twist is particularly so given the increasing dependence of businesses on ICT both in internal operational activities and in the manner in which they interact with customers and suppliers.

Even with the most sophisticated computer security measures successful breaches still occur. It is people's attitude and behaviour that can make that extra difference. In the context of increasing globalisation the moral attitudes and conduct of decision makers, providers, users and consumers of ICT are even more important. Achieving the moral high ground becomes increasingly more difficult in a global context.

People instigate security measures. All those involved in information systems are obliged to be on the look out for computer misuse. We cannot abdicate this collective

responsibility and assume that the computer security professionals will pick up this responsibility.

Computer security is as strong as the weakest link. If a neutral or amoral perspective is adopted then it will be the people who are the weakest link. The best technological security measures will be limited in such cases. Even worse is if an immoral perspective is adopted. Systems security is nonexistent in such cases. This points to the need for a social contract between computer professionals and the society they serve. On the one hand society grants the right to practice as a professional, provides access to needed education, and passes necessary laws. In return the computer professional agrees to practice in a manner that benefits society. This includes ensuring as far as possible information systems are secure.

Consider the example of hacking which is a major security issue. The ethical question is whether or not hacking should be allowed or condoned. In answering this question Mikko Siponen suggests that we should place ourselves under a Rawlsian veil of ignorance where we are ignorant of our status, age, gender and so on. The purpose of this veil is to foster impartiality. Behind this veil ask the question whether we accept that hacking is permissible so that anyone and everyone could break into our systems at any time. Clearly most of us under this veil would not accept hacking and would be vigilant in security enhancement and enforcement. This is because we would be concerned as to whether we are the victims of hacking.

Peter Neumann identifies three gaps that may permit computer misuse. There is a technological gap between what a computer system is actually capable of enforcing and what it is expected to enforce. There is a sociotechnical gap between computer-related policies and social policies. Finally, there is the social gap between social policies and actual human behaviour. Neumann argues that the technological gap can be narrowed through proper development, administration and use of computer systems and networks. The sociotechnical gap can be narrow by creating well-defined and socially enforceable social policies. Finally the social gap can be narrowed by the actions for the other two gaps with additional support from education.

This education process must be twofold. It must include the education of computer professionals in understanding the impact of their actions on us all. This should lead to a realisation of the importance of such things as computer security. The second element of education must be associated with the public. Increasing public awareness of the use and impact of information systems would give the public confidence to question poor system implementation and demand improvement or withdrawal. The overall aim would be to educate people in the social cost and benefits of information systems. It would involve understanding the different levels of security and the need for different levels of security.

A culture of public confidence, trust of individuals and individual responsibility has to be developed, within which secure information communication can take place. There

should be a commitment to training, strong support for good practice and an open management style to reinforce ethical behaviour within the organisation. An appropriate culture should be nurtured that is based upon a code of good practice which is accessible to all staff, visibly supported by senior management and has robust implementation procedures; an objective of enjoying a good reputation in society; and a strong tradition of dealing swiftly and firmly with transgressions. This is because, in the words of Samuel Johnson, "Integrity without knowledge is weak and useless, and knowledge without integrity is dangerous and dreadful".

Please send your views on ethical and social responsibility issues and cases of ethical dilemmas to:

Professor Simon Rogerson
Director
Centre for Computing and Social Responsibility
Faculty of Computing Sciences and Engineering
De Montfort University
The Gateway
Leicester
LE1 9BH
Tel:(+44) 116 257 7475
Fax:(+44) 116 207 8159
Email:<srog@dmu.ac.uk>
Home Page: (<http://www.ccsr.cse.dmu.ac.uk>)