THE HUMAN FACTOR IN INFORMATION SECURITY

The human factor receives too little attention in IT security issues, says Zach Anucha.

The main goal of any IT infrastructure management is to achieve the triad of availability, integrity and confidentiality. This is usually done by information security implementations and management.

Information security is concerned with three components, which are physical, logical (technical) and administrative.

The first two are the most popular, although the physical aspect is more or less taken for granted - a company acquires an office building complete and installed with lockable gates, doors and windows.

The third component - administrative security, which involves policies, procedures and guidelines - is where the problems lie. This component deals with the human factor, the soft factor.

Human beings are involved in every aspect IT. We manufacture hardware components and assemble them to build bare bone systems, write codes and compile them to make software programs, and install and configure software to create fully functioning systems.

We also link the systems together with communication devices to form SOHO, LAN and WAN networks and then implement logical security for the systems and the network.

As part of logical security, we set the access control parameters on the systems to stratify the access privileges of users to the networked resources.

We then use, maintain, review, update and manage the entire networked infrastructure to deliver services to benefit ourselves.

The entire IT infrastructure is the creation of human beings and people are the only intelligent, reasoning and sociable components who also have rights that need to be protected. Any wonder, then, that cybercrime, viruses, spam and all manner of vulnerabilities plague computer users?

Of course, by virtue of our human attributes we are also trusting, imperfect, and prone to errors and omissions. We are naïve and can easily be compromised.

This accounts for not only programming bugs (deliberate and accidental) and vulnerabilities but also the effectiveness of social engineering.
Yet, the human piece of the puzzle, the soft factor, receives the least attention and investment. How often in an IT project do you hear about human vulnerabilities requirements?

Not often. It is not usual for systems integration projects to include the aspect of user training that could enable users to manage their own inherent vulnerabilities.

There is a need for a balance of emphasis and priorities between the physical, technical and administrative components of information security.

Traditionally, this balance has been very difficult to achieve. I suggest the factors as being responsible for this difficulty as:

- Hardware and software makers generally lead the way in defining what the user community tends to emphasize. They produce devices and software to address specific aspects of business needs and then sell the benefits of their products to users.

- The user community, based on the recommendations of vendors, buy products to solve their specific problems. It is still not a common practice among the user community to conduct a thorough investigation into their business, taking into account the physical, logical and administrative aspects of security and then search for products with features and functionalities that best meet their business needs. It is more usual for users to look for technical solutions and not be bothered about the attitudes, behaviours or misbehaviour of users – an issue we can describe as the soft factor vulnerabilities.

- Even now that the user community is aware that the human factors account for more than 50 per cent of information security problems, information security professionals will probably agree that the administrative aspects of security consumes the most resources and require more ongoing attention. It deals with the unknown, intangible and unpredictable and investment into it is more difficult to justify. It is also an endless loop of plan, do, check and act.

- Many companies bought servers and PCs, hubs and switches and routers etc, linked these together into a LAN in order to enable its staff to perform their job tasks and provide services. No serious information security considerations were built into the design of the network from the outset. Along with physical growth, these organizations have also developed a unique culture that has now become well-embedded and resistant to change. But as threats and vulnerabilities rapidly emerge and multiply, they introduce technical security solutions - firewalls, intrusion detections systems, network monitoring tools. These are the usual, easy and quick fix solutions. What is not so easy for the companies is the introduction of security policies, standards, procedures and guidelines. To start with, these are initiated and supported by the highest level of management who should also ensure that they are robustly enforced, monitored, reviewed and updated. But senior management does not usually see the need for investment and pain of change (change of attitude, organization culture and the way people work)
which the implementation of administrative security will introduce.

- Some organizations that were set up in the last three or four years have tended to adopt the same utilitarian approach. Although they install firewalls and monitoring tools they are making no concerted effort to manage information security through the endless cycle of plan, do, check and act. Some of these companies, having invested in technical solutions, lack the resources to pursue such additional requirements. They justify themselves by adopting the belief that it is all about managing an intangible and that the risks may not be as devastating as the vendors and security professionals would have them believe.

What is the way forward then? As an IT professional specializing in information security I recognize that a lot is involved in creating a secure environment. However, I do not believe that it is an impossible task. And it need not involve unaffordable investment of money, as hardware and software costs are steadily lowering.

The main area of concern is skill: it is costly to hire an IT professional with adequate skills to build and configure a relatively secure system.

The difficulty increases when you want to hire an IT professional who can both build secure operating systems and properly configure and manage firewalls, intrusion detection systems and monitoring tools.

This is the preserve of specialist consulting firms and independent consultants and these are not affordable to small and some medium companies.

Additionally employers who, instead of training their internal IT staff, use the services of the consultants, are compounding the problem. It is rather costly for ambitious network and systems administrators to finance their own training on these skills.

Shortage of skills therefore continues. The government and private sector need to cooperate to tackle this problem and software and hardware vendors need to participate more actively in addressing it.

The final bit of the puzzle, the human factor, is the most critical and requires the attention of all. The security of any organization's IT infrastructure is as good as the commitment of its leaders to the implementation of administrative security.

Common sense calls for a balance of approach, which accords equal consideration to each of the three components of security from the outset through to the implementation and usage of systems.

Beyond this, some additional investment is needed to maintain the cycle of plan, do, check and act in the ongoing life of the organization. There is no other option for operating a relatively secure IT infrastructure.

**Zach Anucha MBCS is a senior analyst for a major UK children's charity.**

*in a nutshell*
• The human piece of the IT security puzzle, the soft factor, receives the least attention and investment.
• Users tend to look for technical solutions and not be bothered about the attitudes, behaviours or misbehaviour of other users.
• The main area of concern is skill: it is costly to hire an IT professional with adequate skills.
• The security of any organization's IT infrastructure is as good as the commitment of its leaders to the implementation of administrative security.

This article first appeared in July 2005 ITNOWextra.