Addressing The Human Factor In The Information Security Dilemma

The main goal of any IT infrastructure management is to achieve availability, integrity and confidentiality. Information security implementations and management are usually put in place to help achieve the triad (availability, integrity and confidentiality). Information security is concerned with three components, which are physical, logical (technical) and administrative. The first two, in the order of logical (technical) and physical security are the most popular, although the second (physical) is more or less taken for granted – a company acquires an office building complete and installed with lockable gates, doors and windows. Where there were not adequate, the organization usually improves upon the basic provisions before it moves into the building.

The third component – administrative security, which involves policies, procedures and guidelines, is where the problems lie. This component of information security triad deals with concepts such as "the human factor", "the human component", "wetware" "systems managers", "users. I will use the concept "the softfactor" in this article to convey the same meaning.

Human beings are involved in every aspect of the information communication technology. Human beings manufacture hardware components and assemble them to build bare bone systems. We write codes and compile them to make software programs. We install and configure software on the 'lifeless boxes' to create fully functioning systems. We 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 (human beings) 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. Among its main components (physical facilities, hardware, software and people) people are the only intelligent, reasoning

and sociable one who also have rights that need to be protected. Information communication technology is our creation and we know how to circumvent it. Any wonder then why cyber crimes, viruses, spam and all the other threats and vulnerabilities plague the world of computer users?

Another point to remember is that human beings are not only the intelligent, social and creative component of IT, we are, by virtue of these attributes, 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 reason for the effectiveness of social engineering.

Yet, the human piece of the puzzle, the "softfactor", receives the least attention and investment from the systems planning stages through to the build, testing, rollout and usage of the infrastructure. How often in an IT project do you heard of 'the gathering of the human factor' or human vulnerabilities requirements? Not often. Instead, you often hear concepts like 'systems specifications', 'systems requirements', 'power and environmental requirements', 'hardware and software security controls, 'access control' and user training and this is usually a basic training on how the user will use the system to perform his or her job tasks. 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 as members of the human species. Equal weight is not usually given to managing and motivating users human 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:

1. Hardware and software makers generally lead the way in defining what the user community tends to emphasise. They produce hardware, firmware, devices and software applications to address specific aspects of business needs and then sell the benefits of their products to users.

2. The user community, (until recently when threats and vulnerabilities have escalated), based on the recommendations of vendors bought 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 research 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 describe here as the 'softfactor' vulnerabilities.

3. Even now that the user community is aware that the human fact account for more than 50% of information security problems, information security professionals will probably agree that the administrative aspects of security is consumes the most resources and require more on-going 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.

4. 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 to their customers. No serious information security considerations were built into the design of the network from the outset. These companies then experienced operational growth and added more systems to their infrastructure. 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 emerged and multiplied, they introduced 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 because of the disconnect between business and IT, 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. It has therefore proved to be the most difficult aspect of information security to implementation.

5. Some organizations that were set up in the last 3 or four years have tended to adopt the same utilitarian approach – that is, implement IT systems in order to enable their staff do their jobs. Although they installed firewalls, intrusion detection systems, and monitoring tools, they are making no concerted effort to manage information security through the endless cycle of plan, do, check and act. In fairness, some of these companies, having invested in technical solutions, lack the resources to pursue such additional requirements. Therefore their firewall and IDS logs are not regularly checked; network traffic is not monitored, neither do they carry out other information security housekeeping. They tend to justify themselves by adopting the belief that it is all about managing an intangible, the unknown, and risks that may not be as devastating as the vendors and security professionals would have them believe. Some think that it is not worth the additional investment and trouble. The burden of Compliance is changing this attitude among big organizations but not so much among the small and medium ones.

What is the way forward then? Well, as an IT professional specialising in information security, especially through my preparation for the CISSP certification, I recognise that a lot is involved in creating a secure environment. However, I do not believe that it is an impossible task and it needs not involve unaffordable investment of money, time and efforts. 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 as well as properly configure and manage firewalls,

intrusion detection systems, and monitoring tools. The average systems administrator may not have such broad combination of skills, rather it 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 to acquire these skills, use the services of the consultants, are compounding the problem. It is rather too 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 co-operate to tackle this problem. Software and hardware vendors need to participate more actively in addressing this problem.

I believe that the final bit of the puzzle – the human or 'softfactor', is the most critical which requires the attention of all. It is now all too familiar that the security of any organization's IT infrastructure is as good as the commitment of its leaders to the implementation of administrative security in addition to physical and technical security. Commonsense calls for a balance of approach, which accords equal consideration to each of these three component of security from the outset through 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 on-going life of the **organization**. There is no other option for operating a relatively secure IT infrastructure.

By Zach Anucha, Cyber Security Subject Matter Expert.