Security: Reactive or proactive?

SECURITY in the Internet era is more like our famed Hindi film police; they always appear on the scene after the damage has been done. A lot of security in the Net world today is still reactive--attacks are found and security measures are only taken later. The classic examples being the Philipino love virus and most recently the attacks on Microsoft Network. That is acceptable in the short term but in the long run security should be more proactive. Securing systems don't require a great new idea; it needs something that's been around for a while, something that has been tested and most importantly something that has been implemented properly.

There is also the cost factor. Should an all encompassing, highly secure system be implemented or a reasonably secure system that expects the company to accept an element of risk be put in place? The balance is different depending on the application. There is no such thing as a totally secure warehouse or a totally secure bank vault, there are only different degrees and levels depending on the requirement. Most banks are secure enough for the money they maintain and just the same way as they assume risk of default on
credit management, they need to assume a certain amount of risk in building a security system depending on how much one is capable of spending. You obviously wouldn't want to spend more money on a system than it is worth just to make it extra secure. Every application has to balance price-performance ratios while dealing with technologies. It is important for a company buying technology to evaluate the extent to which it can invest in acquiring them. The simple example to illustrate the balancing of technology and cost is email. In an organisation, information needs to be circulated among all employees. Instead of printing and photocopying the information on paper, setting up an Intranet system and sending it through email works out to be a better and cheaper option. That saves money in printing, photocopying and in the physical effort of distributing, not just in a single location but in diverse geographical locations where the company's offices are located and that too in real time.

Since the results of technology implementation cannot be ascertained immediately; a long-term strategic vision is needed. The same is true in case of security as well. Every company would need to secure some critical parts while leaving others out of the high security net or the degree of security may have to be varied across the system. So in any business you always weigh security with cost. No doubt, as a business you want to maximise your returns and manage your risks and security counter measures but including security in your scheme of things is crucial and the balancing of cost and security depending on their application is important. The example of how cost can be a deterrent in the growth of even highly efficient technologies can be seen in the acceptance levels of SSL and SET. Despite its lacunae, SSL has been a widely used security system as it is less expensive and easy to implement than the prohibitively expensive SET systems. Also the element of risk makes the system managers to be on their guard.

So the choice of a proactive and reasonably secure system or a reactive and highly secure system is wide open.

G. P. Vinaybabu
vinayg@mm.strategicnewspapers.com
E-SECURE November 2000