BIZCOMMUNITY

Employees are the new line of defence in any cyber security strategy

LONDON, UK: Security awareness means turning your people into your first line of defence, but many organisations are worryingly complacent when it comes to information security assuming that "it won't happen to me," while individuals often tend to think "it is someone else's problem." However, a report from PricewaterhouseCoopers LLP (PwC) explores how organisations should be making employees the first line of defence against damaging security incidents.

Security awareness: Turning your people into your first line of defence suggests that the response of organisations to improving protection and reducing risks has historically been strongly biased towards further investment in technology. In essence, they have been solving what are perceived to be technical issues with technical solutions.

Craig Lunnon, OneSecurity, PricewaterhouseCoopers LLP (PwC), thinks this approach is misguided:

"Technical solutions are too frequently being prescribed for people problems. Although technical defence is vital, systems are inherently vulnerable to both negligent and malicious acts by people. Ignorance, confusion, anger or even curiosity can all give rise to incidents."

The report considers whether information security has currently got the right focus, and is backed up by PwC's 2010 Global State of Information Security Survey, which shows that only 48% of organisations questioned in the UK have an employee security awareness programme, falling behind global leaders - the US (64%) and India and Australia (59%).

Efforts to improve security often create cumbersome processes that get in the way of people doing their jobs. Consequently, they can be tempted to by-pass security controls, so the human element of technical solutions often diminishes the desired effect.

New approach needed

What is required, suggests the report, is a new approach in which an investment in understanding and influencing the behaviours of all those concerned is balanced against continued investment in technology.

The difficulty large organisations often face is that security functions tend to be autonomous, fragmented and isolated while ignorance can provide a false sense of security among a workforce. PwC recommends that better engagement between security teams and the business is needed as well as higher levels of engagement between organisations and employees.

The solution is to invest in people. Make them the first line of defence - rather than the cause - of security incidents. Thus, the return on investment from a strategy that leads people to exhibit new behaviours around information security will exceed misdirected investment in technology-based solutions.

Says Lunnon: "The goal is that all those working for an organisation are alert to risks, will want to act to protect information and will be actively supported in doing so. As the first line of defence, security-aware employees are often best placed to identify a potential breach or weak link. Equally, they can prevent and reduce the impacts of incidents when they do occur."

Investment in security awareness measures pays for itself many times over and can help in:

- Reducing incidents of theft, loss and fraud;
- Avoiding breaches of law and/or regulation;
- Ensuring continuous availability of business-critical information;
- Protecting brand and reducing the potential for reputational risk; and
- Enabling the use of security as a positive marketing differentiator.