

Risky business

Kevin Fitzgerald says Australian businesses that have inadequate security policies are sitting on liability time bombs.



Executive managers that run comprehensive security strategies should be rewarded with overall reductions in their insurance premiums, as their organisations will be more likely to detect and prevent mistakes, fraud and malicious software attacks as well as being able to keep operating in the event of a disaster.

US insurance companies have been offering incentives to organisations to heighten the status and currency of their security measures since the tragedy of 11 September, 2001.

We should follow suit. We already reward car and home owners, so why not businesses as well? Even having a comprehensive and current corporate security policy document is a step in the right direction that insurers should reward.

How can we move Australian business out of its reactive state in relation to security? Most businesses wait until there is a problem that can no longer be hidden before security improvements appear.

This was a familiar tale in the US until the traumatic shock of 11 September. Following this event, the US Government formed the Department of Homeland Security to coordinate a national policy of defending the country's citizens and infrastructure.

At the recent Homeland Security conference in Sydney, a US presenter explained that one of the consequences of the Homeland Security movement in the US was that insurance companies were offering insurance premium discounts to businesses that had effective security policies in place.

It is hardly surprising that after 11 September the US still feels it is a country under threat. We have followed their lead by establishing approaches to protect our critical infrastructure, but not to the extent of forming a Homeland Department. As a consequence, we have not had the same wave of cooperative enthusiasm from the business world.

Before 11 September, the US business attitude to security was similar to Australia's business attitude today. Now the US attitude has changed, probably forever.

A security culture is emerging and many businesses will follow the lead of the insurance industry and start where they should: with a formal corporate security policy and procedure guidelines document.

Australian insurers should offer the same encouragements to businesses as their US counterparts. This is a powerful start. Security policies signal that management is prepared to formalise its commitment to establishing and enforcing security.

A security policy and procedure guidelines document is a formal statement endorsed by senior management that states the business's position in relation to security from an enterprise-wide viewpoint. It encompasses physical, personnel, and information security. It covers a variety of policies, each one followed by several procedure guidelines.

A corporate security policy should contain the following chapters:

- I** Security policy positioning: risk and vulnerability profiles shall be developed and used to determine the necessary policies, procedures and controls.
- II** Security organisation: management infrastructure roles and responsibilities.
- III** Asset classification and control: guidelines will be provided under 'Public', 'Internal use only', 'Confidential', and 'Highly restricted'.
- IV** Personnel security: job definitions, recruitment, training, segregation of duties, and so on.
- V** Physical and environmental security: perimeter controls, key management, intrusion detection, equipment security and maintenance.
- VI** Communications and operations management:

'So why not businesses as well? A comprehensive and current corporate security policy document is a step in the right direction that insurers should reward'

change control, incident management, system planning and acceptance, malicious software, backup, network management, media handling and disposal.

VII Access control: user access management, administration, user responsibilities, system access, application access, and monitoring access.

VIII Systems development and maintenance: requirements, application security, message authentication and cryptography.

IX Business continuity planning: impacts, strategies, detailed plans, testing and maintenance.

X Compliance: legal, technical and auditing considerations.

Such a document has the power to kick-start the development of a holistic approach to security. When sponsored by the CEO and based upon international standards, it signals the arrival of a change in attitude. Management will know that plugging a few holes here or there is no longer acceptable. This document says the business must manage security seriously. □

KEVIN FITZGERALD is an information security consultant with more than 25 years experience in designing and executing security solutions for large organisations.