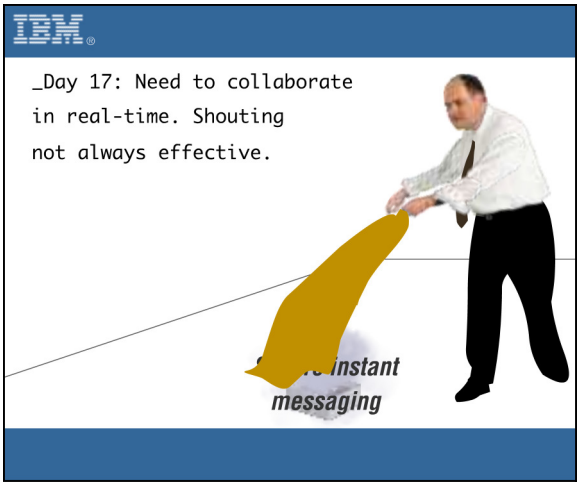
COMPUTERWORLD
THE VOICE OF IT MANAGEMENT

Cyber insurance, what's that?

MICHAEL CRAWFORD AND DARREN PAULI

14/07/2006 13:08:24



Cyber insurance will become as commonplace as car or home or any form of business cover within a decade as a way to mitigate financial losses should a "cyber attack" occur and sensitive data be lost or stolen.

But that's a decade away. Today, very few IT managers are aware of cyber insurance. Even underwriters and insurance agencies have shown little interest in the market despite hundreds of serious breaches in the past two years.

Sydney-based security services provider Sift has released a white paper entitled, The Economic Viability of Cyber Insurance: Seeking Financial Certainty in IT Security. According to Sift associate Bosco Tan, the government needs to educate both the insurance industry and vendors on this issue.

"Both academics and insurance industry professionals forecast that cyber insurance will become as common as traditional brick-and-mortar insurance products within the next decade," Tan said.

"In order for the accelerated development of cyber insurance to occur there is a role for the information security industry, the insurance and reinsurance industry as well as the government to work together."

Tan said the government should be supporting market education as it should be part of an overall risk management strategy.

While cyber liability does exist, Hydrasight research analyst John Brand said enterprises have refused to buy it.

He said there are existing policies relating to disaster recovery, but when it comes to hacking or malicious attacks, few policies exist.

"Insuring data as a result of a malicious penetration is often included in disaster recovery policies, [because] it is something that is easy to protect against. A base level of security technology is shared among most organizations anyway; but information leakage and the damage it can cause to a company is unquantifiable and undetectable," Brand said.

"From a senior IT perspective, it would be difficult to assure the rest of the business is doing the right things, and be able to defend your position in the event of forensic investigation as a result of the claim.

"Once an issue is raised that would result in a claim, most people are worried about fixing the public image and then considering the financial losses; from an audit perspective, breaches are difficult to trace anyway and there is an enormous amount of work to discover what really happened."

Despite the obvious need, most IT managers have not heard of cyber liability insurance.

IT manager for Rigby Cooke Lawyers, Anthony Strangis, said he would rather spend the time that it took to fill in such a policy in better securing his company.

"There is just no point vying for insurance against data breaches when security systems are inadequate and, conversely, if the systems were up to date, why would you want to get insurance?" Cooke queried.

Micheal Axelsen, IT manager for chartered accountancy firm BDO Kendalls, said the problem with such insurance is insurance firms would apply and enforce security standards for clients through a very costly and thorough third-party audit, which may not be feasible.

"The lag between software vendors becoming aware of security vulnerabilities and a patch becoming available is wider than it used to be, and hackers and malicious coders are becoming smarter and exploiting this," Axelsen said.

"Business needs to take a holistic approach to security and a company could invest greatly in electronic data security, yet sensitive data could be left in the back of a taxi."

Cyber insurance: where do you get it?

Zurich Insurance does not offer any policy relating to liability of data breaches.

QBE - professional liability - ICT proposal for hardware and software faults - no mention of data protection or liability.

Allianz Insurance - does not offer any form of cyber insurance relating to households or businesses.

IAG - offers a business liability package but nothing relating directly to hacking, loss of data or cyber liability.

Insurance house Lloyds of London currently offers a "Cyber Insurance" policy through various underwriters in Australia, but according to analysts and IT managers, uptake in Australia has stalled.

The actual policy document, provided by Australian Insurance underwriters Epsilon, is called Esurance and contains nine elements relating strictly to IT that extends as far as liability cover in terms of viruses interrupting business, extortion, intellectual property rights, brand protection cover and even paying the costs of a public relations agency to "minimize the damage to your reputation".

The document also covers system damage in restoring computer records in the event of a hacking incident or virus, lost revenue as a result of network downtime and covers "ransom demands or threats to introduce a virus or hack into computer systems, or to disseminate to third parties the data held on computer systems."

An element of the insurance also covers forensic consultants to repair systems and restore data in the event of an incident.