

Knowledge Base

Phishing, Fork Bombs, Honeymonkeys and Pings of Death

How do you manage risk?

Information security, like physical security, is more urgent, carries greater risk and is more vulnerable than ever! Paradoxically, it seems that while physical security feels personal, corporate leaders push the protection of their own identities, employee information and customer data far behind other priorities.

According to the Federal Trade Commission, more than 52 million account records were placed in jeopardy because of security breaches in 2005. In 2006, an additional 30 million cases of compromised data, and in 2007, North American corporations are at a loss rate of 6 million/month.

There is some change on the horizon, though. Corporations are increasingly asking the question about how to integrate all of the threats and look at the comprehensive picture of risk. Like barbarians at the gate, your board, customers and employees will go on the offensive the moment you or even one of your competitors experiences a breach that becomes known to the public!

“Many of our clients have consolidated all aspects of security into one senior leader’s accountability, often the Chief Security Officer” says Peter Gordon, Partner, CIO & Technology for Epsen Fuller/IMD International Search Group. “There is a definite blurring of the lines between what is a physical threat vs. an IT threat.”

So the question you should ask yourself is: *who* in the company should be responsible for the comprehensive security of me, my people and our information? Management is recognizing more and more that it is not just an IT issue any longer.

Until senior management recognizes the need to raise the profile of Information Security to the level of strategy, major vulnerabilities of catastrophic losses will continue to grow. Information security is not only a technical issue but a business and governance challenge that involves sufficient risk management, reporting, and accountability. Effective security requires the active involvement of executives at all levels to assess emerging threats and the organizations response to them.

The IT Governance Institute finds that those corporations adhering to strict security measures are lowering financial losses to less than 1% of revenue; whereas other organizations are experiencing loss rates that exceed 5% of revenue.

The procedures that are put in place to secure and protect people, data, systems, facilities, assets and property, not only provide security to your shareholders,

employees, and customers, but help to ensure that your organization has the ability to continue to function and stay in business during or after a catastrophe or disaster.

A key responsibility of a Chief Security Officer is to help determine the areas of weakness within an organization and to correct those weaknesses, which if compromised, can impact the ability of the company to continue essential functions and mission-critical services.

In today's data-centric and information driven world, the challenge of the CSO is to anticipate disaster scenarios - create check-points and redundancies to maintain and safeguard systems and facilities, and develop processes and security measures that protect people and data, including both client and corporate assets and property.

“So what you want to look for is someone who can watch the flanks, understand the threats and drive action where it is needed.” says Gordon. “More often than not, CEO's want one 'go to' person to call.”