

AUSTRALASIA'S LEADING SECURITY RESOURCE FOR BUSINESS AND GOVERNMENT

SECURITY

\$8.95 inc GST
\$9.95 NZ

SOLUTIONS



Buying & Selling *Online* AVOID BEING SWEEPED AWAY IN A SEA OF CRIME

INSIDE

The David Hicks Trial
Was He Really Guilty?

#48
JUL/AUG 2007

ISSN 1833-0215



9 771833 021487

Simon Hensworth

>>> **access**
denied

Security Awareness:

SECURITY IS EVERYONE'S RESPONSIBILITY

Do the people in your organization understand why you have security? Is your organization's security successful? Do your staff support your security systems? Can you be sure your business secrets or sensitive information aren't walking out the door every night? Are you confident that your business is not a ticking time bomb ready to explode into workplace violence? Are your vital computer systems and records safe from theft or sabotage? If you can answer "yes" to all the above questions, your organization is doing well. Many of the above issues can become problems if an organization's people lack security awareness. Security awareness is a crucial element of a successful, integrated security system. Security is everyone's responsibility, and the people within an organization need to understand what security is, why it is important and the consequences if it fails. If staff are aware of some basic security concepts, they can greatly enhance their organization's security as well as their own.

Information Security

Information Security is an element of security that people and organizations can often overlook. Many mistake Information Security for IT security. Whilst Information Security may include security of information technology (IT) systems, Information Security also concerns other forms of information, such as written information, drawings, prototypes, spoken information and human memory.

Most of the information that circulates an organization is probably of little importance.

However, a small fraction may be vitally important because of its sensitivity or value to the organization. Organizations need to identify (and classify) information so that proper protection can be given to secure vital information.

Staff who need to access sensitive/valuable information must be made aware of their responsibilities to protect it and the consequences, if they compromise Information Security.

Information is a tricky asset to protect. Once you lose it, you can never get it back. You can't check staff as they leave the office to see if they are taking vital information with them. It may all be in their memory.

Computer Security

Most people these days work with a computer at some time. Certainly no office is without one. We can often take them for granted and forget how much we depend on them. Losing access to computer systems has the ability to grind some organizations to a halt. However, many simple ways to avoid problems are overlooked due to a lack of awareness. Locking a computer when it is left unattended can help to avoid other staff sabotaging the network anonymously (or masquerading as you!). Using a good password (and not writing it down on a Postit and sticking it to the screen) can also provide protection. Policies, procedures and security awareness can help to avoid staff using each other's computers, the introduction of viruses by removable media (floppy disks and CDs), and theft of portable items such as laptops.

Sabotage, Leaking Information and Workplace Violence

Security awareness can be effective in the prevention of sabotage or leaking of information by staff. It can also be effective in preventing workplace violence. If there is a heightened awareness of security-related issues within an organization, there is a higher likelihood that staff will notice suspicious behaviour/activity of their colleagues and report it. Heightened security awareness within an organization can also act as a deterrent against unwanted behaviours, by increasing the perception of perpetrators of the potential risk that they will be caught or 'found out'.

Staff should be encouraged to be aware of, and report, suspicious behaviour or activity that could present a security issue. However, staff may be concerned about reporting such behaviour/activity for fear of retribution. In order to provide staff with support, organizations may consider setting up a Security Intelligence system.

Security Intelligence

A Security Intelligence system is aimed at monitoring information that might provide an organization with an 'early warning' of an upcoming security issue/incident. It could be run by a Senior Manager, Facility Manager or Security Manager within the organization. Information can be sourced from outside the organization including:

Police, Internet, Government Intelligence organizations, and partnering or similar companies. These outside organizations may provide information about crime trends, known assailants, copycat crimes, targeted individuals, large-scale computer viruses,

access denied

hackers, terrorism and new forms of attack that may suggest a heightened risk to the organization.

Perhaps more importantly, information can be sourced from staff inside the organization. Staff can provide information on issues such as internal theft, internally planned attacks and suspicious behaviour. A Security Intelligence system should encourage and support staff with strategies including: direct lines of communication, anonymity of reporting, and protection from other staff who may suspect a 'whistle blower'.

Acceptance of Security

Security can often be seen as a nuisance. Access Control can slow staff down, CCTV can be intrusive, procedures can be time consuming and annoying, and searches can be embarrassing or humiliating. It can be difficult to get staff to accept security, especially if they do not have an appreciation for why they have it. If staff do not support security, it can compromise the effectiveness of security. People start to 'tailgate' at Access Control points, they might avoid or reposition CCTV, they might skip procedures, and they may openly resent searches and become

“A Security Intelligence system is aimed at monitoring information that might provide an organization with an ‘early warning’ of an upcoming security issue/incident.”

upset or difficult. Security awareness can be an effective way to educate an organization's staff as to why security is important, how it is of benefit to the individual, and to encourage acceptance of security.

End Note

Security awareness is a crucial element of a successful, integrated security system.

The best security system is one that all staff accept and actively support. Without security awareness, staff may not realise that security is everyone's responsibility. ■

Simon is a Senior Security Professional with global engineering consultancy GHD. GHD employs a team of eight Security Professionals in their Perth Operating Centre and 30 specialised Security Professionals Australia-wide. Simon has a Bachelor of Science Degree in Security Science from Edith Cowan University and is an ICA

(International CPTED Association) certified CPTED practitioner (Crime Prevention Through Environmental Design).

Simon has provided security solutions for many clients with major assets in Western Australia including: Australian Customs Service, Department of Justice, Fremantle Ports, Department of Transport, Bunbury Port Authority, State Library of Western Australia, Western Power, the City of Rockingham, the Water Corporation, CSBP, Administrative Appeals Tribunal, WA Police and the Department of Defence.

Simon is involved in all aspects of security, security technologies, promoting security and security awareness.

*Simon Hensworth, BSc (Security Science) (ICCP – Advanced), GHD Pty Ltd
Ph: 61 8 6222 8640
Email: simon.hensworth@ghd.com.au*