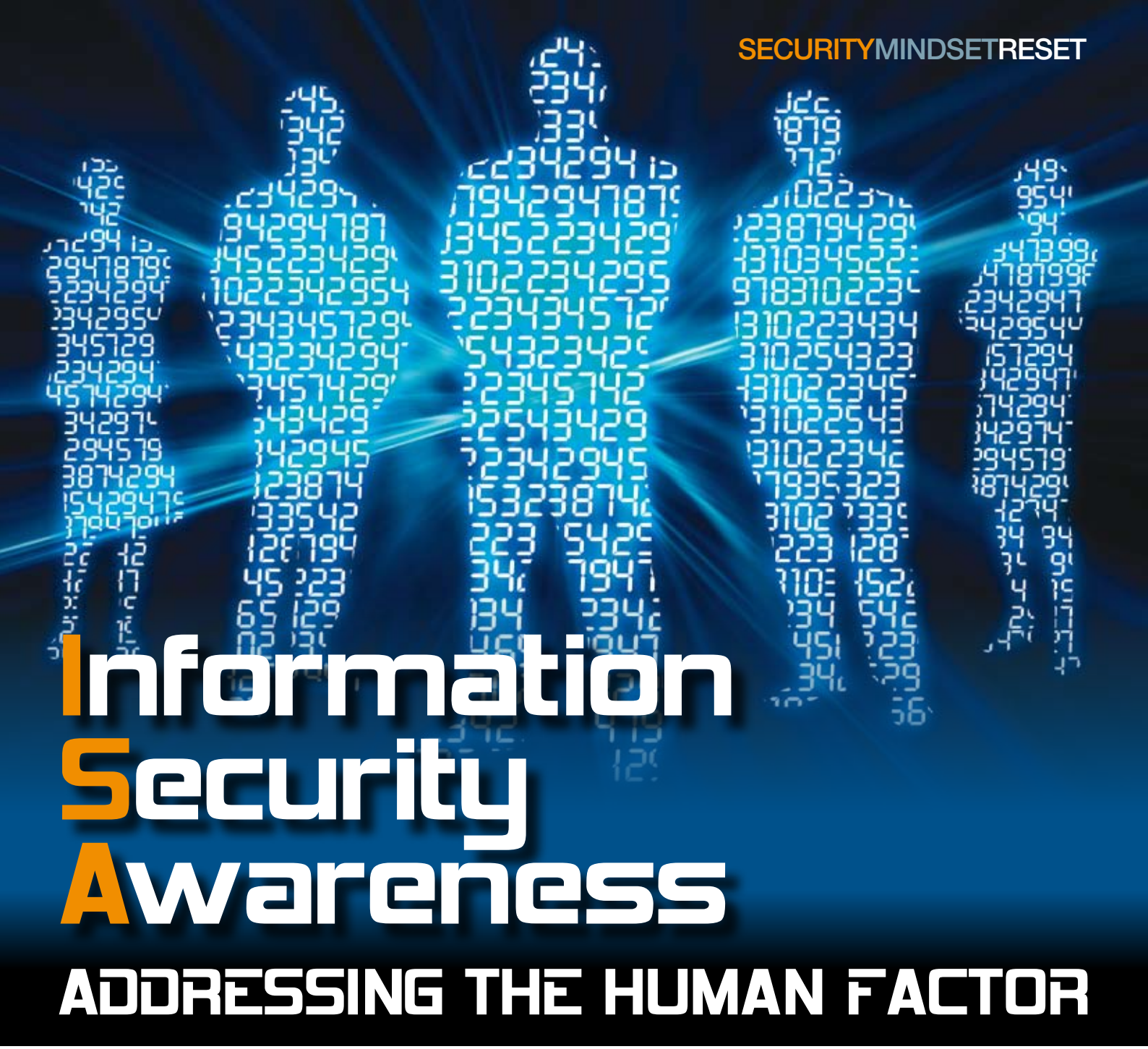
SECURITYMINDSETRESET



Information Security Awareness

ADDRESSING THE HUMAN FACTOR

Effective information security is more than policy and procedures. It's a mindset.

With a surge of reported professional hackers, botnets, industrial espionage and breaches of privacy, there is a call for a new approach to security control and awareness.

Security is not just a technical problem. The human factor (what employees do or don't do) is the single biggest threat to information systems and assets.

Addressing the human factor involves a mindset reset – an ongoing awareness of the basics of information security for everyone who interacts with computer networks and systems.

The ALC Information Security Awareness training programme provides the mindset reset you need to effectively safeguard the information assets of your company.

alc

Call the ALC Team for more information 1300 767 592
or email learn@alc-group.com

www.alc-group.com.au

Information Security Awareness

ADDRESSING THE HUMAN FACTOR

SECURITYMINDSETRESET

The ALC Information Security Awareness training programme gives organisations a straightforward and effective way of addressing security concerns applicable at all levels within an organisation.

Traditionally, information security is seen as a technical issue to be managed by technical experts within the IT department. Although this is largely true, the reality is that all too many security breaches occur almost innocuously at the end-user or non-technical level.

This programme provides organisations with a straightforward, manageable and effective way to ensure that employees have an understanding and knowledge of information security requirements necessary in today's business world.

Objectives

Providing a concise summary of information security responsibilities and threats that all individuals in an organisation need to know and understand.

Structure

The programme is designed for in-house presentation to groups. It is designed to be used both for initial induction and also for periodic security refresher training.

The content is fully customisable and can be tailored to different groups. So, for example, if implemented across the organisation the content would be varied for senior management versus operational staff.

What You Will Learn

The programme addresses:

- Information security – protection of confidentiality, integrity and availability of information
- Physical Security – physical means of safeguarding information
- Personnel Security – identification, authorisation and monitoring of user's access to systems
- Risk Management
- Overarching ISMS Policy

Also Included

- Guides for the use of technology – including password protection and the use of internet, email, social networking, laptops, telephones and portable media.
- Supporting principles – policies and principles to assist in risk management
- Real-world examples – demonstrating the importance of risk

Key Topics Covered

- Email-based viruses, worms and attachments
- Importance of organisation policies and objectives
- Computer viruses: common symptoms & warning signs to watch out for
- Follow organisation policies and objectives
- Staying up-to-date
- "Social Engineering" explained
- The crisis situation: "I need your help!"
- "I'm calling from IT..."
- What to do if you suspect an attack
- Internet Scams and Phishing
- Identity theft: protecting sensitive information
- Online activity while at work: users should have no expectation of privacy
- Passwords are critical for your "electronic signature" – we provide a digital checker for passwords as part of the course work.

Call the ALC Team for more information 1300 767 592
or email learn@alc-group.com

www.alc-group.com.au