

INFORMATION MANAGEMENT

Chris Joscelyne

AUSTRALIAN PROJECTS PTY LIMITED
IT Security and Data Protection

Information Management

THE FUTURE LANDSCAPE

“The business environment of the future is likely to be very different from today’s, where boundaries between personal and business computing will blur and everyone and everything will be linked. In order to survive, firms must manage the new risks this environment creates”

**David Lacey
Risk Management Bulletin**

Information Management

THE ENTERPRISE GOAL

The ultimate integration of policies, people, process and technology that will allow us to deliver the right information to the right people at the right time in the right context.

Information Management

THE ENTERPRISE TODAY

“I’m flat out working on my technical responsibilities and I really don’t have the time or resources to get involved with IT security. As long as the network functions smoothly, I’m happy.”

Comment from an enterprise IT manager

Information Management

THE ENTERPRISE TODAY

“I have delegated responsibility for all IT security policy to the people in our IT department. They are the IT technical specialists, so this is their logical role.”

Comment from an enterprise CEO

Information wars

“The 21st Century will be dominated by information wars.”

Alvin Toffler

Futurist

Information security

“Organisations must take reasonable steps to keep information secure. Encryption of data is a basic expectation.”

Australian Federal Privacy Commissioner

Privacy protection

“Our survey indicated that while 67% of companies were addressing the requirements outlined in the Privacy Amendment (Private Sector) Act 2000, 55% did not currently encrypt sensitive personal information.”

Deloitte Touche Tohmatsu

Security problems

- Lack of access control

Unauthorised access

- **70% - internal**
- Inadvertent access
- Office “sticky beaks”
- Employees wishing to steal information or damage the employer’s reputation

- **30% - external**
- Recreational hacker groups
- Protest groups
- Criminals

Source: Market research – Australian Projects 2003

An unfortunate coincidence

- Many organisations require passwords with a minimum of 8 characters
- The word “password” has 8 characters
- In an organisation in Sydney, the password for over 70% of employees was “password”

- A medical centre in Melbourne required passwords with a minimum of 6 characters.
- 100% of doctors had the same password, “doctor”.

Security problems

- Lack of access control
- Unprotected data distribution

Unprotected data distribution

- Unencrypted email messages and attachments inadvertently sent to unauthorised recipients inside or outside the enterprise
- CD-ROMs containing unencrypted confidential data, distributed in unsealed inter-office envelopes or in general mail deliveries

Security problems

- Lack of access control
- Unprotected data distribution
- Unsafe storage of data

Unsafe data storage practices

- Removable media accessible to all employees
- Removable media data content unencrypted
- Critical data stored on premises with no safety copies stored securely elsewhere
- Backup media removed to an unsafe location after hours

Security problems

- Lack of access control
- Unprotected data distribution
- Unsafe data storage practices
- Unsatisfactory perimeter defence

Perimeter defence problems

- Lack of understanding of where enterprise perimeters are located
- Poor or non-existent security policies relating to laptop PCs, PDAs and other memory devices
- No means to prescribe and enforce policies
- Inability to detect any difference between normal and abnormal activity as devices connect
- No response plan should an incident be detected

Security problems

- Lack of access control
- Unprotected data distribution
- Unsafe data storage practices
- Unsatisfactory perimeter defence
- Lost and stolen equipment

Laptops and PDAs are vulnerable to theft

Laptop PC and PDA thefts in New South Wales in 2004

- Over 15,000 devices reported stolen
- Most had no data protection installed

Source: NSW Bureau of Crime statistics

Global trend in laptop computer thefts

- 80% “amateur” opportunistic thefts
 - Of these, 80% resold or given to friends
 - 20% kept for personal use
-
- 20% “professional” thefts
 - Of these, 50% stripped for spare parts or rebirthing
 - 50% sold intact

Source: Oxygen / STOP

Stolen laptops - cost

- Equipment replacement cost
- Lost software
- Lost information
- Time to reinstall software and set up
- Time to re-enter data
- Work interruption

Total cost of replacement of hardware, software and data is generally 3 to 5 times the replacement value of the hardware alone.

Source: Gartner Group "Total cost of stolen laptops"

Laptop & PDA security

Security can be divided into two elements:

- Physical security
- User access control and data encryption

The top priorities are:

- Changing users' attitudes and habits
- Protecting data with encryption

Private ownership of PDAs by employees can pose a highly sensitive challenge for the manager who must enforce security policies in relation to these devices.

IT Security Check List

- Who is responsible for developing and managing IT security policy in your enterprise?
- Does your enterprise perceive it as a “technical” issue or a top-down management responsibility?
- Is IT security policy in clear non-technical language, and is it communicated effectively to staff?
- Do staff adhere to security policies and directives?
- Have you implemented a robust access control infrastructure with appropriate user permissions?
- How safe is stored data and data in transit, including emails and removable media?
- Are your laptop computers & PDA devices encrypted and controlled at enterprise level

Information Management

The solution?

- **Develop policies**
- **Adopt technical solutions to implement and enforce policies**
- **Educate employees in language they can understand**

Chris Joscelyne

chris@apro.com.au

Tel: 02 9652 2600

Fax:02 9652 2700

www.apro.com.au

Reflex – PC Guardian – SecuriKey – Trust Digital – Zondex