
Information Technology Security Management for NSW Public Agencies

Facilitators' Handbook

To accompany the video:

“{I Wish} it wasn't me”

**September
2003**

This publication is available in other formats for the vision impaired. Please advise of format needed, for example large print or as an ASCII file. It is also available in HTML format, at www.icac.nsw.gov.au

Contacting the ICAC

ICAC: Level 21
133 Castlereagh Street
Sydney NSW 2000

Post: GPO Box 500
Sydney NSW 2001

DX: 557
Sydney

Phone: 02 8281 5999

Toll free: 1800 463 909

Facsimilie: 02 9264 5364

Website: www.icac.nsw.gov.au

Email: icac@icac.nsw.gov.au

Business hours: Monday — Friday 9am - 5pm

ISBN 1 920726 01 2

© September 2003 – Copyright in this work is held by the Independent Commission Against Corruption.

Part III, Division 3 of the *Commonwealth Copyright Act 1968* recognises that limited further use of this material can occur for the purposes of 'fair dealing', for example; study, research or criticism etc. However, if you wish to make use of this material other than as permitted by the *Copyright Act 1968*, please write to the Commission at GPO Box 500, Sydney NSW 2001.

Contents

Commissioner’s foreword..... 5

Resource objectives 6

IT security guidelines overview 7

The six steps to creating an IT Security Management Policy..... 9

Step 1: Set Information Security Objectives 9

Step 2: Identify Information Assets..... 11

Step 3: Identify Threats..... 13

Step 4: Assess Risk 17

Step 5: Select Controls 19

Step 6: Implement Controls 21

IT security workshop to accompany ‘[I Wish] It Wasn’t Me’ Video 24

IT security checklist 26

Commissioner's foreword

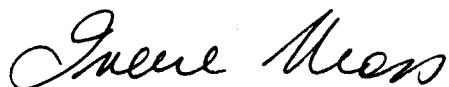
As our reliance on information technology increases, information itself becomes a valuable commodity and a source of new threats. Criminal networks, including terrorists networks, are adapting to the information economy and are finding new ways to exploit government networks for criminal purposes.

Like other counterpart agencies, the ICAC is responding to these new threats by emphasising the need for better information security.

This new resource, a video and support guide [produced in conjunction with the Office of Information Technology], is designed to provide practical advice on the secure handling of government information. The resource emphasises the need to ensure information technology systems are secure and in line with moves to have government departments and agencies comply with the Australian and New Zealand Standard for Information Security Management.

The procedures outlined in the video are simple and easy to implement, but to work, they must become part of your workplace culture. This is because a lapse by a single employee can threaten the security of the entire organisation.

I urge you to ensure that this resource becomes part of your general staff training program and induction process and that your organisation adopts the strategies that we recommend. The ICAC welcomes your feedback on this important topic as we build corruption resistance strategies for a technologically advanced world.



Irene Moss
ICAC Commissioner

Resource objectives

A recent survey¹ has found that changing users' attitudes and behaviour regarding computer security was the most challenging and problematic issue facing IT managers. But with the right education program and a supportive workplace culture, attitudes *can* be changed and risks reduced.

The video '[I wish] it wasn't me' is a staff training video designed to promote desirable practices on how to safeguard electronic information and reduce electronic corruption. 'Electronic corruption' (or e-corruption) is an aspect of information security and can only be addressed as part of a comprehensive IT security strategy.

The objectives of this video and handbook are to:

- Educate users about the importance of information security
- Increase staff knowledge about information security issues
- Give managers the tools to create or revise their IT Security Management Policy
- Educate users about their role in information security management
- Help to build a pervasive information security culture, and
- Build understanding and cooperation between IT units and other business units

¹ Australian Computer Crime and Security Survey, 2003

IT security guidelines overview

Since 1994, the state agency now called the NSW Office of Information Technology (OIT) has published advice and guidelines for the public sector, which sets out in detail the steps managers should take to protect their organisation².

In 2001, the ICAC conducted a comprehensive study of the risks of e-corruption in the NSW public sector³. That study found that executive level awareness of information security issues was low and there were a number of risk areas that were not being effectively addressed.

In addition, the NSW Premier's Department Circular No 2001-46 sets out specific measures to ensure information security. These include:

- Developing information security management policies and plans
- Assigning IT security to a nominated officer
- Ensuring that all staff understand their responsibilities for information security, and
- Having IT systems certified to the national information security management standard AS/NZS 7799 Part 2: 2003.

The most demanding of these measures is Standard 7799. This Standard describes six steps, which managers should use to help create an IT security management policy for their organisation.

The 6 steps are:

1. Establishing information security objectives
2. Defining your organisation's information assets
3. Identifying potential threats to those information needs
4. Assessing the risks
5. Selecting controls to manage the risks, and
6. Implementing controls and evaluating the plan

² OIT's most recent publication is Information Security Guidelines: Part I - Risk Management; Part II - Examples of Threats and Vulnerabilities; and Part III - Baseline Controls (June 2002). This report is available from the OIT website and is recommended reading for IT Managers.

³ eCorruption: eCrime Vulnerabilities in the NSW Public Sector – Summary Report, ICAC, September 2001.

The chart below lists these steps and outlines the main features of each. Each step is explained in detail in the following sections.

The steps to creating an IT Security Management Policy⁴

STEP 1	STEP 2	STEP 3	STEP 4	STEP 5	STEP 6
Set Objectives	Define Assets	Identify Threats	Assess Risk	Select Controls	Implement Controls
Objectives	Assets	Threats	Risk Analysis	Control Types	Specific Controls
Confidentiality Integrity Availability	Databases Work files Infrastructure Brand image	Environmental Accidental Deliberate	Risk Identification Valuation of assets Classification of consequences	Management Physical Operational Technical Continuity Plan	Passwords Viruses Hackers
Requirements	Sensitivity Classification	Human Actions	Risk Matrix	Organisational Roles	Implement Policy
Legal rules Business rules Operational rules	In-confidence Protected Highly protected	Carelessness Corruption Abuse of trust Identity theft Viruses etc	Likelihood v consequences General risks Specific risks	Management IT Management Users	Educate Comply Monitor Evaluate

⁴ Based on OIT Guidelines: Information Security Part 1 – Risk Management, 2002

The six steps to creating an IT Security Management Policy

Step 1: Set Information Security Objectives

Objectives

There are three standard objectives relevant to all discussions of electronic information security:

- Confidentiality
- Integrity
- Availability

These objectives aim to keep information accurate and complete, but also to make it easily available to legitimate users.

When information involves an instruction or an authority to act, two further objectives come into play:

- Authentication and
- Non-repudiation

Authentication means ensuring the identity of the person issuing the instruction or undertaking a transaction. Non-repudiation means ensuring that a person issuing the instruction or undertaking the transaction cannot subsequently deny it.

Access control

Access control is the major issue for security management. It is this issue that makes “User IDs” and user “passwords” a central element of any security policy. While the pressure from users is upon making passwords simple and capable of providing access across multiple systems, security needs may require users to follow a more complicated access control regime.

To solve this problem many organisations are adopting alternative security measures such as biometrics and security cards, which are designed to be both an effective access control device and yet easy for users to apply.

Legal requirements

The legislative requirements within the state privacy regime also have some practical implications for information security. The rules are contained within:

- NSW Privacy & Personal Information Protection Act, 1998
- NSW Health Records Information Privacy Act, 2002
- National Privacy Principles
- NSW Freedom of Information Act, 1989

Want more information?

- Contact Nigel Evans, Manager Electronic Commerce, OIT on [nigel.evans @dpws.nsw.gov.au](mailto:nigel.evans@dpws.nsw.gov.au). Nigel also convenes the Information Security Management in Government Forum (ISMiG), which is open to public sector employees and will be of special relevance to IT Managers.
- An Information Management & Technology Strategic Plan Template updated in May 2003 is available in Word format on the OIT website
- IT Security Bulletin Number 1, OIT, April 2002
- NSW Government Privacy & Personal Information Protection Guidelines, OIT, 2002
- Information Management – Liability Guideline, OIT, July 2002
- Information Security Guideline for NSW Government – Part 1 Information Security Risk Management, OIT, June 2003
- Information Management & Technology (IM&T) Strategic Guideline, OIT, May 2003

Step 2: Identify Information Assets

Assets defined

The focus of the video and this handbook is on the security of electronic information assets. However when addressing the consequences of misuse of information, you should include all assets that may be affected.

Assets include:

- Information and data
- Documents
- Hardware and software
- Communications and other equipment
- Personnel, and
- The image and reputation of the organisation.

The information held on the electronic system is typically the basis of a system user's work life, making them an important stakeholder in its security. Daily usage can put users in a good position to appreciate the potential vulnerabilities and consequences of large-scale data corruption or theft of information. However daily usage does not appear to ensure a front-of-mind awareness to minimise risk, which creates a problem for managers.

Sensitivity classification

Information can be classified according to its value to an organisation and the risk associated with it being divulged to outsiders. This classification will result in information being treated differently within the organisation with regards to issues like storage systems, access rights, copying rights, and transmission procedures.

There are three generally accepted levels of information sensitivity:

- In confidence
- Protected
- Highly protected

In-confidence information is usually defined by the topic of confidence e.g. 'commercial in confidence' or 'medical in confidence'. Unintended release of in-confidence information can cause: substantial distress; financial loss; commercial damage; damage to agencies and their reputations; facilitation of a crime; impediment of an investigation or policy; and breach of an undertaking or statutory restriction.

Unintended release of protected information can: endanger individuals; impede major policies; substantially damage organisations or economic interests; and, facilitate serious crime.

Unintended release of highly protected information can: threaten life directly; seriously prejudice public order; and substantially damage the State's financial interests.

Want more information?

- Guide to Labelling Sensitive Information, Premier's Circular, 2002
- Information Management Audit Guideline, OIT, May 2002
- Information Management Classification Guideline, OIT, May 2002

Step 3: Identify Threats

The main threats

There are three broad classes of threats:

- Environmental threats: defined as natural disaster and infrastructure failure
- Accidental threats: defined as system failure or human error
- Deliberate threats: defined as attacks by internal or external hackers

These threats can affect specific areas of security concern. For instance, a major storm can cut power or electronic cables, which could disable a computer system and so risk information availability. A virus attack can threaten availability, but also data integrity (if it destroys or modifies files) or accountability if it sends e-mails to names from an organisation's lists.

The management of all potential threats to information assets is the aim of an organisation's information security management policy.

Human actions

Careless use of information systems

Information can be compromised by careless use of information systems e.g. saving files to incorrect drives, failing to save information, and damaging files in the course of accessing them. These problems can be minimised if staff are properly educated about how to use their information systems and are informed as to the negative consequences to the organisation of improper use.

Internal corruption

External attacks are often thought of as the most significant risk, because of publicity given to computer hackers and the viruses released through email. However, internal attacks by staff are almost as frequent, and often are much more damaging.⁵ A person inside the organisation is more likely to have both a motive and the opportunity to misuse the information system. Motives include seeking financial gain, revenge against management for a past action against them, or simple mischief making.

⁵ Australian Computer Crime and Security Survey, 2003

For example, in the case study below from a recent ICAC investigation, the motive is financial advantage:

A motor registry Regional Manager received payments from a middleman who worked with car dealers to “rebirth” stolen prestige cars. He used his employee’s password to gain access and then he overrode the system controls. The override was automatically alerted to him as the Regional Manager, so the fraud went undetected. He also held responsibilities for the registry’s quality control and some audit functions and this assisted him to hide his actions.

This second case study is very similar:

In January 2003, a former employee of a company used the username and password he held while employed at the company to remotely log into the company’s network and access the accounts data containing customers’ credit card transactions. The offender then changed the customer’s credit card details and proceeded to make refunds to his credit card through the altered accounts. The company only became aware of an anomaly when it noticed an unusual number of refunds were occurring.⁶

In the case study above, the internal security system was by-passed by the corrupt insider to commit the fraud. In the previous case study, a system oversight permitted the corrupt insider to exploit a loophole. Clearly some arrangements will have inherent vulnerabilities unless the risk is anticipated and neutralised. Special care should be taken when staff or management have control over financial or other valuable transactions which can be manipulated by self interested insiders.

Abuse of trust

While we can generally assume that a request for assistance is for a legitimate purpose, corrupt people can abuse this trust for personal gain. A good example is where someone calls an employee at their workspace claiming they are from the Help Desk and asks for ID and log-on details to fix a problem.

⁶ Australian Computer Crime and Security Survey, 2003

In the case studies below, bank account details were sought by e-mail through the use of a “mirror” web site.

Perpetrators created a website that looked identical to that of a prominent Australian bank. Using spam e-mails, the perpetrator sent a fraudulent request to account holders to “re-activate” their accounts by clicking on the website link provided in the e-mail by entering their user name and password. The perpetrator then used this identification to access the accounts electronically transferring funds to their own accounts.⁷

A similar scam used a mirror of the Sydney Opera House website with the slightly different address of www.sydneypopera.com.au (i.e. leaving off the “house”). Patrons would enter the site, find themselves seats on the floor plans provided and pay for them. The problem was that the money went to the perpetrator and the tickets were never sent.⁸

While there are many methods for abusing trust to gain valuable information, the problems noted above could have been avoided if the people concerned carefully checked the credentials of those requesting bank details, and followed the general rule, which is to never disclose passwords to anyone.

Identity theft

Another problem is theft or misuse of personal identities. This strategy is most likely to involve people from inside organisations using the identity of their colleagues – but it can also be used successfully by external hackers to break into an IT system. There are many kinds of identity theft including:

- Sending damaging emails masquerading as another person
- Reading confidential information such as tender proposals
- Changing details within electronic document management systems
- Stealing credit card details
- Issuing permits or licenses in favour of friends or family

Identity theft is made easier when people are careless with their passwords.

⁷ Australian Computer Crime and Security Survey, 2003

⁸ Sydney Morning Herald August 22, 2002

Viruses, worms and trojan infections

IT security systems must take account of external threats from electronic viruses, worms and Trojan infections. Generally speaking, IT Managers are well aware of these risks and adopt various IT systems to eliminate known risks. However, computer users should be aware that they can introduce electronic threats by opening suspicious-looking email files. The general rule is if you are not sure about an e-mail's legitimacy, delete it.

Want more information?

- Information Security Guideline for NSW Government – Part 2 Examples of Threats and Vulnerabilities, OIT, June 2003
- Virus Alerts & Information, OIT website links
- Contracting Out Guideline, OIT, July 2002
- e-Corruption: Exploiting Emerging Technology Corruptly in the NSW Public Sector, ICAC 2001

Step 4: Assess Risk

Risk analysis

A risk is an uncertainty with significant consequences if it occurs. To determine whether a consequence is a significant risk requiring preventative action, you need to conduct a 'risk analysis'.

A risk analysis begins with an identification of the assets, the potential risks to these assets and the consequences that would flow if the risk were to be realised. This involves determining the answers to these questions:

- What are the assets and their value?
- What could happen to them?
- How likely is it that it could happen?
- What would the consequences be?

Analysis of kinds of consequence means identifying the full range of consequences including the cost of:

- Negative impact on the organisation's reputation and image
- Negative impact upon Government as a whole
- Breaching confidentiality
- Violations of legislative requirements, and
- Flow on consequences for stakeholders

A risk assessment is usually conducted at two levels: a general risk assessment and an assessment of specific highly valued information resources.

Risk matrix

General risk assessment

A useful method for rating the general risk to an asset is to use a risk matrix (see the table below) where the horizontal axis represents the consequences of risk, and the vertical axis, represents the likelihood of occurrence. The risk rating is described as 'low', 'moderate', 'high' and 'extreme' dependant upon the likelihood of occurrence measured against the consequence. Identifying where a particular asset sits within the risk matrix will alert you to the level of protection you should give to that asset.

Matrix for determining the level of risk⁹

		Consequence of Risk				
		Insignificant	Minor	Moderate	Major	Catastrophic
Likelihood of Occurrence	Certain	High	High	Extreme	Extreme	Extreme
	Likely	Moderate	High	High	Extreme	Extreme
	Moderate	Low	Moderate	High	Extreme	Extreme
	Unlikely	Low	Low	Moderate	High	Extreme
	Rare	Low	Low	Moderate	High	High

Assessing the risk to particular information assets

The assessment of risk to highly valued and business critical assets involves an identification of the specific threats that are likely to occur to that asset. For example, with deliberate human attacks, the assessment should include who is likely to make an attack, for what purpose, and with what effects.

Want more information?

- Information Security Guideline Part 1 – Risk Management, OIT, 2002
- Project Risk Management Guideline, OIT, July 2002

⁹ Information Security Guideline Part 1 – Risk Management, OIT, 2002

Step 5: Select Controls

Types of control

The range of IT security controls include:

- Management
- Physical
- Operational
- Technical
- Continuity Planning

Each of these controls contain a number of specific measures, which may determine how your organisation treats information. The controls are defined below.

Management controls include all of an organisation's arrangements that influence the achievement of information security. Documents dealing with controls may include:

- Information security policy
- Personnel policies
- IT security training for staff
- Outsourcing contracts
- System audit manuals
- Incident handling manuals
- Risk management manuals

Physical controls relate to limiting access to information sources – e.g. locking doors and cabinets. It can also mean eliminating from view potentially sensitive material. A method of encouraging this to occur is for an organisation to adopt a clear desk policy which requires staff to lock away valuable documents and to shred sensitive waste material.

Operational controls are those controls inherent in the design and use of IT systems and planning. They include:

- Systems planning
- Systems configuration
- Email protection
- Virus protection
- Firewalls
- Security of information in transit

Technical controls involve restricting access to information systems, particularly by using passwords and other means to verify identification and authentication. They also include monitoring system usage through audit trails and logs.

Continuity planning controls concern how to 'backup' infrastructure systems, information and databases if the primary system fails. The choice of backup option reflects an organisation's functions and the priority given to continuous operation. Back-up systems can be provided in 'cold', 'warm' or 'hot' sites:

- Cold sites can be set up with equipment and data to operate within a week or two
- Warm sites house IT equipment and can operate within a day or two
- Hot sites have duplicate infrastructure, system and links and can take over operations within a few minutes.

Organisational roles

The level to which we observe the need for IT security controls is largely dependant upon our role within an organisation and the degree to which the IT security policy is publicised and enforced by management.

For instance, senior management will be more aware of risk management issues in a general sense as they have a big picture perspective, and are ultimately responsible for any breaches. However, IT Managers will be more aware of specific electronic risks when compared with the rest of an organisation.

When it comes to explaining the risk to the general staff, IT Managers require the support of other management and in particular HR Managers to ensure that all staff hear the message and make the necessary behavioural changes to implement the IT security policy. In this regard, it is important that there is a good communication channel between the IT Managers and other management.

It is also important to identify who will police the IT security policy and what will happen to offenders. Generally speaking, this is a role for supervisors and HR Managers, relying upon directions from IT Management and senior management.

Want more information?

- Information Security Guideline for NSW Government – Part 3 Information Security Baseline Controls, OIT, June 2003
- Premier's Department Circular C2003-02: Electronic Information Security – Business Continuity Planning
- Biometrics, Fact Sheet 19, OIT, June 2003
- Authentication – Digital Signatures Guidelines, OIT, May 2002

Step 6: Implement Controls

Specific controls

Here we consider three important areas where staff can adopt simple procedures as effective IT security controls:

- Protecting passwords
- Avoiding viruses
- Avoiding hackers

Protecting passwords

Passwords identify individual users and their access level to the system. Passwords also certify what you've done as your work. You should take care to create a password that is difficult to crack. Tips for making a strong password include:

- Don't use any of the following information for your password: your own name, your address, phone number, children's names, pets' names, or your car number plate, and especially, don't make it the same as your Username.
- Make sure your password isn't so simple or obvious that it can be easily guessed or cracked. You'd be surprised how many people use "password" or "123456" or ordinary dictionary words as their password.
- Use a combination of numbers, upper and lower case letters, and special characters
- Use a password you can easily remember somehow, but that's meaningful only to you
- Don't write your password down anywhere in any form, or, if you really must write it down, hide it amongst a long string of numbers and letters
- Absolutely never give anyone your password. No one ever has any legitimate reason to ask for it, including IT staff. An exception is "generic passwords" which are used in certain circumstances, like emergency wards

Avoiding viruses

Most organisations have anti-virus IT systems but staff acting carelessly can undermine these systems. For instance:

- Email messages may contain virus infected file extensions which when opened, can spread causing damage to the whole organisation. The general rule is that if you are not certain of the source of an email or all of its contents, delete it, or at least, check with the sender as to its legitimacy

-
- Staff working at home who save their work on a disk and download it at work rather than by emailing it to their computer, will by-pass the organisation's firewall. They can then introduce a virus to the IT system if their own computer does not have up-to-date virus recognition and protection systems

Avoiding hackers

Hackers can steal online identities such as email addresses, to acquire access into an organisation's IT system. Tips for avoiding hackers include:

- When sending email to a group, place the addresses in the 'bcc' field. Each recipient will see only their own address and there's no temptation for hackers
- Always check email addresses before sending. This rule also applies to phone numbers when sending faxes and addresses on traditional mail
- Do not sign on-line petitions. If you want to save the world, write to your local member
- Make sure all your portable devices are pin or password-protected
- For highly sensitive information, use encryption
- Be as careful when you log on as you are at an ATM. Look out for shoulder surfers
- Lock your desktop before you leave your workstation for more than a couple of minutes - and definitely when you go for a longer break or when you've finished work for the day
- Always save your work onto the network server rather than your hard drive and when you've finished, delete any drafts from your hard drive. The document on the server will always be accessible and since it's not on your hard drive it's more difficult to hack into

Implementing IT security policies

Implementation of the IT security policy is normally the role of HR and IT Managers working in partnership with staff supervisors. The policy needs to be explained to all staff as part of their general induction process and revisited on an ongoing basis to keep the policy 'front of mind' and relevant in a constantly changing IT risk environment.

Expressed simply, the IT security implementation process is to:

- Educate the organisation as to the threats and risk minimisation policies
- Ensure compliance with the policies
- Monitor the effectiveness of the control systems in the light of staff behaviour
- Evaluate the policy to ensure that it meets its objectives and remains valid in the light of new threats.

Positive staff behaviour

There are several things an individual can do to improve their organisation's IT security levels including:

- Gain an overview of your organisation's information security policy and procedures
- Understand and follow all of the applicable system controls
- Understand the basic configuration of your organisation's IT system so that you know where to save things and how to access different parts of the system as appropriate
- Encourage sound security practices in your workplace by reminding colleagues of their duties
- Become a knowledgeable IT security resource person and assist others when the need arises

Want more information?

- Premier's Department Circular C2003-03: Procedures for Reporting Security Incidents
- Incident Reporting, Defence Signals Directorate (www.dsd.gov.au)

IT security workshop to accompany '[I Wish] It Wasn't Me' Video

Workshop format

While the video '[I Wish] it wasn't me' outlines the important issues that staff should be aware of regarding IT security risks and procedures, the messages within the video will be more powerfully expressed if the video is used as a discussion starter within an interactive workshop environment.

It is recommended that the workshop be conducted within a 1-2 hour time frame and be lead by the IT Manager and/or the HR Manager. To encourage active participation in the discussion it is best to break into smaller groups of three to four people to discuss questions posed to the group, and then have representatives from each group report back to the whole group with the points noted on a whiteboard.

Suggested workshop plan

1. Introduction & explanation of goals

Often users see information security as a separate and unimportant add-on to their everyday operations – something that is perceived as the responsibility of the IT department only. Explain to the group that the aim of showing the video is to ensure staff see information security as an integral part of their everyday work practices.

Explain that the workshop goals are to:

- Encourage staff awareness of the potential risks to their organisation
- Give staff a better understanding of the information security process and your organisation's information security policies
- Have staff identify, and seek to resolve, shortcomings in their current security practices
- Draw on staff knowledge of strengths and weaknesses in the information systems they use
- Encourage staff to see themselves as being involved in a partnership with IT and management to monitor and minimise IT security risks

2. Investigating the topics for discussion

Ask the group to break into small teams to briefly discuss the following issues and record their answers on a whiteboard for comparison later:

- What information assets do you use in your every day work and what is the value of these assets to your organisation?
- What IT security practices do you follow in your everyday work?

-
- What are the vulnerabilities of your organisation's information assets?
 - How may an outsider misuse the information to their advantage and to the detriment of your organisation and its stakeholders?

3. Show the video (The video runs for 22 minutes)

4. Ask for questions and provide clarification as required

- Ideally the IT Manager or at least an IT representative will be present to answer technical questions
- Try to avoid getting bogged down in unnecessary IT jargon or procedures as this may create the impression that everyday staff IT security risk management strategies are complex when they can be simple

5. Evaluate your organisation's IT security practices

- Have your IT representative or management representative explain in general terms your organisation's IT security practices and the role staff play in mitigating risk
- Show the organisation's IT security policy and HR policy as it relates to staff responsibilities for mitigating IT security risks. Remember to include what happens if the policies are breached
- Ask the group what would they do if faced with a variety of risky situations e.g. an unaccompanied stranger is seen walking around the office; a colleague asks them for their password to access a file
- Ask staff to consider whether they know of flaws in your organisation's IT security practices and how these flaws may be remedied to better protect your organisation's data
- Remind staff that they have an ongoing responsibility to follow the procedures when it comes to IT security and that they should alert managers if they consider a security risk exists. Give them the *IT Security Checklist* for future reference.

IT security checklist

Understand your IT system and security policy

- Have a mental map of the IT system and the drives you use
- Save your work to the assigned network drive, not to your PC
- Follow authorised procedures to access and modify databases

Look after your password: it's your personal signature

- Don't leave it around to be seen
- Don't tell it to others
- Don't make it easy to guess

An open computer is an open door to information assets

- Use password-protected screen savers (time-outs) when not using your PC
- Log off when you leave your desk

Be trusting, but not too trusting: protect against people hackers

- Don't open unusual e-mails, especially attachments
- If people ask for something find out why
- Requests from Help Desk must have appropriate authorisation
- Escort visitors, and watch out for shoulder surfers
- Don't leave faxes on the machine, or sensitive papers on your desk
- Report suspicious activities

Mobile electronics can be lost or stolen

- Save valuable laptop files to disks or network drives
- Protect (hide and secure) your laptop so that it can't be stolen
- Password protect your PDAs (palm held devices), organisers and mobile phones

Protect your IT system's security controls

- Use email to send files from home (disks can carry viruses)
- Only use agency-approved software and hardware
- Never attach a modem to your computer without IT approval as this provides open access to hackers