Pitching the Policy: implementing IT Security Policy through awareness

James McKay
Version 1.4b
16, July 2003

Abstract

This paper discusses the important process of implementing an IT Security Policy in the workplace. It aims to demonstrate the vital and complimentary role of conducting an awareness program in order to achieve effective implementation of the IT Security Policy, including compliance issues. The context of the paper is the Australian public sector, however much of the material would also relate to private sector organisations. To provide the background setting for this paper, aspects of the standards and legislative environment that focuses and drive IT Security Policy in Australia are described and critical elements that facilitate an effective IT Security Policy are discussed.

Background

The Australian IT Security framework is governed by several key documents (i.e. policies, guidelines, legislation) that define Commonwealth government standards. While the documents exist for Commonwealth public sector agencies, the principles of the standards etc. can be adopted by State and Local governments and other non-government organisations.

Key documents

- Commonwealth Protective Security Manual, 2000 (PSM 2000) [1]
- DSD Australian Communications – Electronic Security Instructions 33 (ACSI 33) [2]
- Standards Australia AS/NZS ISO/IEC 17799:2001 **:** Information technology - Code of practice for information security management [3]
- Various Australian Commonwealth Government Acts including the Privacy Act 1988, Archives Act 1989, Crimes Act 1914 and Freedom of Information Act 1989.

Protective Security Manual

The Commonwealth Protective Security Manual, 2000 (PSM 2000) is the principle guiding document for security arrangements within Commonwealth government agencies. The manual outlines the minimum standards of security to be applied within agencies, including for those external organisations that provide services to the agencies. The PSM is comprehensive, bringing together the many legislative and other policy elements that affect organisational security, including IT security. The PSM is divided into 8 parts that are listed below in Table 1.

Table 1: The eight parts of the PSM (as adapted from the Commonwealth PSM, 2000) [1]

- Part A Protective Security Policy
- Part B Guidelines on Managing Security Risk
- Part C Information Security
- Part D Personnel Security
- Part E Physical Security
- Part F Security Framework for Competitive Tendering and Contracting (CTC)
- Part G Guidelines on Security Incidents and Investigations
- Part H Security Guidelines on Home-based Work

While all parts of the PSM are relevant to IT Security Policy formulation, Part C, Information Security is specifically concerned with computing issues and references Australian Electronic Security Instructions 33 (ACSI-33) provided by Defence Signals Directorate (DSD). DSD provides guidance and advice to Australian Commonwealth Government agencies.

ACSI-33 details comprehensive issues relating to IT Security on particular topics and is intended for security and technical personnel in 14 separate handbooks. In particular Handbook Four relates to security management policy and includes the Australian Standard AS/NZS ISO/IEC 17799:2001 [3] for Information Security Management that defines ten key controls. These controls form the basis of IT Security Policy and awareness needs, and are listed in Table 2 that provides a brief explanation of each.

Table 2: The ten key controls of Information Security Management (as adapted form ACSI 33) [2]

Control	Rational
1. Information Security Policy Document	This control is required to ensure the organisation is clear on the security objectives relevant to the agency, and that endorsement for the policy has been granted by executive management.
2. Allocation of Information Security Responsibilities	Clear statements defining those staff or agencies responsible for security functions need to be agreed and promulgated
3. Information Security Education and Training	One of the most important and effective security countermeasures is education and training of users and managers of the organisation's information infrastructure.
4. Reporting of Security Incidents	It is critical that security incidents be addressed in a timely and thorough manner.
5. Malicious Software Controls	An increase in virus types and infection methods over the years has resulted in an overall increase in the threat likelihood of an information infrastructure being infected with a virus.
6. Business Continuity Management	The process to develop contingency plans needs to be dynamic and owned by the organisation.

Process	
7. Intellectual Property Rights	There are clear legal restrictions on the use of copyrighted material, and these restrictions should be formally observed and promulgated by an organisation.
8. Safeguarding of Organisational Records	In all organisations, regardless of size, there are those records whose high levels of integrity, confidentiality and/or availability are critical to the operations of the organisation.
9. Data Protection and Information Privacy Legislation	The organisation must operate within the requirements of the law, including any relevant data protection and privacy legislation.
10. Compliance with Security Policy	Regular review of compliance with security policy should also be considered as necessary for effective security management.

IT Security Policy Characteristics

Consistent with the ten key controls above, an IT Security Policy should be:

- Relevant, realistic and uncomplicated
- Define who is responsible and why
- Apply a Code of Conduct
    - Describe expected behaviours and values
    - Detail unaccepted usage
- Explain enforcement and outline sanctions
- Provide contact details and be accessible
    - Describe Incident Reporting and Notification Schemes
- Set and manage compliance issues
- Set policy review criteria

Relevant, realistic and uncomplicated

An IT Security Policy is developed according to the security needs and in the context of the organisation, and these may vary across organisations with different business goals. For example, organisations that process extremely sensitive or private information, such as a law enforcement agency or medical provider, would have significantly higher risks than say information registrars or educational institutions where information is intended to be more freely available. Thus IT Security policies need to be designed around the organisation's function and based on the risks faced by the organisation. They should be documented using a sound risk management approach that will give a realistic assessment of priorities and measures. This is turn has implications for the implementation of the IT Security Policy and for user's expectations.

An IT Security Policy should be easy to understand, to the point (i.e. concise) and use consistent terms and plain language. Staff are more likely to read a short policy rather than a lengthy, dry or elaborate document that may also lead to ambiguity and potentially conflicting statements. With this in mind, an objective should be that the key statements of the IT Security Policy should be listed in a one (or two) page handout. Such a brief document would be ideal to issue staff when they first commence work.

An IT Security Policy should also be based on guiding principles rather than attempting to cover all conceivable issues. This is especially pertinent in the case of specific technologies that might require large amendments when that technology changes. Nor should the policy be designed or influenced so as to fit in with existing systems or procedures that might not otherwise meet minium standards or other relevant criteria. Rather, the policy and its related strategies need to be developed to mitigate risks and bring about compliance. The IT Security Policy should remain consistent and be based on best practice principles.

Who is responsible

"It is necessary to establish a culture of security throughout the enterprise; to push security down throughout the rank and file and to have a 100% commitment from management." [4]

Defining responsibilities and explaining under what authority those responsibilities are issued goes a long way to achieving that commitment. The Chief Executive Officer (CEO) or equivalent, is ultimately responsible for the success and overall management of the organisation. However all staff need to understand the various roles involved and take responsibility seriously by following and respecting the IT Security Policy.

Apply a Code of Conduct

Along with the IT Security Policy, developing or applying a Code of Conduct, Code of Ethics, or Acceptable Use Policy that applies to everyone gives a clear set of values and an understanding of what is expected in the workplace.

Define expected behaviours and values

As with policy, the Code of Conduct should be written in clear concise language and without ambiguity. It should also set out the consequences for violations and take into account aspects such as criminal and civil laws. The Code of Conduct should promote fair, efficient, effective and ethical use of IT resources.

Defined unaccepted usage

A Code of Conduct is also an ideal vehicle to outline what is considered unacceptable use with systems (including email and Internet resources). Examples of unacceptable behaviour frequently include:

- Illegal, fraudulent or unlawful activity
- Harassment based on gender, race, disability or beliefs
- Abusive, threatening, slanderous, libellous and or defamatory language
- Offensive, obscene or pornographic content
- Attempting to circumvent security controls

If the organisation has a fair use practice that allows for limited social use of email or other usage such as allowing online banking transactions, it may also not allow these activities in such a way that excessively impacts on the organisation or is defined as unacceptable behaviour.

Providing a well defined list of activities or behaviours that are both acceptable or unacceptable in the one place makes it easy for staff to assess what is an appropriate behaviour. Taking the earlier use of the Internet example, it may be allowable to research web sites for personal interests within prescribed times, but not to download executables, audio or video files without prior authorisation or a business justification.

How the policy is enforced

The IT Security Policy should outline the possible sanctions for breaching the policy. Depending on the seriousness of violations some elements may require criminal charges and others can be managed progressively by first issuing warnings, then providing counselling before considering dismissal or other options. If user monitoring takes place for enforcement, then details of how this is conducted are required to be described with emphasis given to staff privacy considerations.

Be accessible and provide contact details

The IT Security Policy should be available to all users and readily accessible. On commencement staff should have a copy provided of either the policy or a summary key statements handout with links to the policy. Details on how, who and under what circumstances to contact security staff also needs to be provided.

Describe Incident Reporting and Notification

One of the many crucial roles of IT Security management is the coordination of potential or real security events. Only identified staff such as the Chief Information Officer (CIO), Help Desk manager or IT Security Manager should send information relating to IT security issues. The message should be in a predefined format and have a readily identifiable subject heading and section, much like a CERT advisory [5] notice and include:

- Meaningful and identifiable subject
  - e.g. IT Security Alert: Increase in virus XXX reported.
- Description of the issue
- Action taken or needed to be taken by staff
- Sending authority

Contact details should be always provided in all communications and products including designated positions, contact numbers, email and physical location.

Set and manage compliance issues

Details of how compliance issues will be conducted need to be explained. Compliance criteria should be drawn from the IT Security Policy. Sometimes there are situations or events that require an exemption from the IT Security Policy. Examples could include be an odd but vital legacy system that can't be replaced yet, or the need to approve the connection of specialised equipment to the network. While it might be tempting to change the policy there is usually a range of measures that can be taken. Other issues might be that the particular policy statement was narrowly defined or that a new or emerging solution, like wireless LANs, now needs consideration. If the situation absolutely requires an exemption to the IT Security Policy, the reasons why should be documented, ownership identified and a time frame set for resolution. In these cases it is important not to ignore the problem but rather to clearly identify the issues and provide realistic measures using a risk management approach. The longer-term aim of any exemption however, should be to change the situation or circumstances to more acceptable levels.

Set policy review criteria

It is important to build in a review process that includes criteria and how policy issues are logged. For example, there may be updates to laws (legislation) that affect the use of some technologies, such as road laws that make it illegal to use hand held mobile telephones when driving. Other events need to be considered such as:

- If the organisation's function changes
- changed names or restructuring of the organisation with other entities
- major revision of underpinning standards occurs.

From Policy to Implementation

"One of the themes the 2002 Australian Computer Crime and Security Survey was that technology is most effective when it is supported by sound information systems security polices, practices and procedures." [6]

Once an IT Security Policy has been developed for a particular workplace (or updated) it needs to be accessible and comprehensible to staff. The best way to achieve this is to develop an awareness program to complement the introduction of the new or revised policy. Staff need to be made aware of the importance and benefits of the IT Security Policy and their role in adherence to the policy.

Audiences

Within the workplace there are different target groups or audiences that require different messages to ensure drawing attention to, and understanding of, the IT Security Policy. These audiences need to be identified prior to the development of an awareness program. All groups however will share a common basis and need understanding of fundamental aspects of the policy such as a Code of Conduct that is required of everyone. It may be more practical to deliver a standard pitch that covers material relevant to all audiences and to extend specific issues, or hold additional briefings for those audiences with particular roles. Potential target groups include:

- Executive/Senior Management
- IT Staff (e.g. systems administrators/managers, developers, help desk and support staff)

- Internal Users
- External Users

Executive/Senior Management

Essential to any successful policy is not only the endorsement by executive and senior management, but also that they lead by example. It is vital to sell the importance of the IT Security Policy and playing out scenarios of the risks identified in risk assessments can do this. Because Executives often look to see what other organisations do, consider having a professional presenter or experienced senior colleague from another organisation co-present. In order for management to gain an understanding, create dilemmas and role reversal situations that front-line staff contend with. Are the responses suitable or do they conflict with the policy? Is that how senior executives operate in the real environment, or are the rules bent? The objective is not to catch individuals out, but rather to stimulate thinking. An IT Security Policy that is not supported or followed by the Executive will also reduce overall effectiveness. For a more detailed approach on Executive awareness, see Creating an IT Security Awareness Program for Senior Management. [7]

IT Staff

IT Staff are likely to be already involved with security activities and be familiar with technical and procedural security concepts of how the organisation is run. IT Staff are more often faced with considerable decisions that are not always clearly identified, and they may need support and vindication for actions that are often made in high pressure situations. As with the Executive group, if the IT Staff in the organisation do not follow or perceive that the policy exists for other users, then this may not only disenfranchise those users but the example set is likely to be followed.

Internal Users

Internal Users are more concerned with how IT Security Policy will impact on their job and working conditions. Experience and awareness is likely to be more varied between experienced staff and those new to the job. To keep interest up, involve the group with questions and give the opportunity for discussion on experiences, or have participants walk through scenarios of common issues in small teams. Topics could include:

- Being asked by a colleague to disclose a password
- Management pressure to bypass a integrity process
- Responding to a potential virus
- Coming across evidence of a major fraud
- Discovering a colleague accessing email accounts and private data holdings without authorisation.

External Users

External Users often require alternative solutions because they are not as accessible as management, staff or business partners. There should be terms and conditions related to the use of systems that require acceptance before access is granted and a reminder for each time they log in. Terms and conditions should be linked from the entry point with relevant security update links made available; for example, vulnerabilities relating to particular web browsers.

Delivering Awareness Programs

Having senior management accept overall accountability gives creditability and also gains the support needed to implement the awareness program. [8] There is value in using different approaches and messages to reach audiences and these can include:

- Awareness Briefings
- Surveys
- Competitions and Give-aways
- Supporting Information resources
- Newsletter Articles and Emails

Awareness briefings

Awareness briefings should be the principle method of raising IT Security Awareness. Unfortunately, according to the 2002 Security Awareness Index Report most workers show a poor score when it comes to security awareness, and nearly half have not read all the security policies that apply to them in the past year.[9] The report goes on to conclude that organisations throughout the world are doing a poor job of making their employees aware of security issues and consequences. Often awareness briefings are the type of event that staff 'eventually get around to', or the awareness briefings are held infrequently after the initial implement of the IT Security Policy. In particular, after initial implementation of the policy, briefings may only occur as part of a general induction program. As many staff attend such induction programs after being with the organisation for extended periods, this may create an important gap in awareness related to IT Security. Therefore the Executive should require all staff attend to attend an awareness session within a set period after commencement with the organisation.

The awareness briefings should provide a background of why the policy exists, under what authority it exists, who is responsible, and any specific roles. Staff should go away with a Plan of Action and consider implications of the IT Security Policy for themselves and their particular work area.

Competitions and Give-aways

An enjoyable way to engage staff in an awareness session is by running a competition to solve a cryptic puzzle (crossword books or movie tickets make great prizes). If you have a theme associated with your awareness program, or the IT Security Policy is a new initiative, then give-aways could be included. Have items that are likely to be visible on desks such as calendars, stickers, or something that serves a useful purpose such as pencils or rulers. They should always provide contact details or useful links to information such as Intranet page locations.

Surveys

After the IT Security Policy has been introduced and staff have attended awareness briefings, rather than having staff redo the same course every year, refreshers could be done by other methods such as via surveys or questionnaires. There are professional online surveys that can be used to measure and evaluate awareness [9]; the AusCERT and CSI/FBI security surveys also provides a broader perspective [6, 10]. For example, the 2003 AusCERT survey found that a quarter of respondents highlighted insider abuse of Internet and email access and computer systems resources. [6] In contrast, the US, CSI/FBI survey found that 80% of respondents cited insider abuse of Internet access [10].

Information Resources

Instead of producing separate policies for issues that involve multiple policies or administration within the organisation (for example classification guidelines, or requesting non-standard software) it may be more effective to provide additional resources that link policy statements. Maintain an Intranet page that includes the IT Security Policy and other information resources that can include:

- FAQ's that can be provided on a Intranet page for common questions. (A questionnaire can be created based on the FAQ's to check understanding for staff unavailable to make briefing presentations).
- Guidelines or Brochures – On topics including links to other organisational policy, for example:
    - Physical laptop security,
    - How to classify and secure information,
    - Remote access
    - Sending All Staff emails
- Hints pages and posters can describe the Do's and Don'ts on issues like:
    - Password Management
    - Software Piracy and copyright
    - How to avoiding SPAM email
    - Risk Management process
    - Home computer security
    - Reporting security incidents

Newsletter Articles and Emails

If you have a circumstance that still requires clarification then news articles (i.e. in internal publications) or emails are appropriate methods to give advice and can serve as reminders of aspects of the IT Security Policy. Information resources can also be linked or presented in news articles for internal publications.

Overcoming barriers

With any process that relates to change there are likely to be barriers that need solutions. Possible barriers to the implementation of an IT Security Policy could involve/include:

- Staff availability
    - Incentives
    - Remote or short-term staff

- Perceived lack of benefit
- Resistance to change
  - Loss of autonomy or individuality
  - Existing practices and views
- Privacy and Monitoring Concerns

Staff Availability

Staff may not be available to attend awareness briefings because of competing priorities or other events. Ensure briefings don't clash with other major initiatives within the organisation. Consult widely and give plenty of notice. If you are attempting to introduce a new IT Security Policy when significant upheaval is occurring elsewhere, the messages and impact will be reduced.

If no prior IT Security Policy or awareness exists, or major revision occurs, the CEO should mandate that all staff attend IT Security Awareness briefings within a set time frame. Attendance lists should be kept, with attendees required to sign or register. These can provide statistics that can be reported on to the Executive.

Incentives

Availability of audience is critical and staff may need incentives to attend awareness briefings:

- Some sweeteners may be needed - literally give out chocolates
- Ask inductees to display the must have desk accessory
- Run a lucky door prize for giving up their valuable time - hopefully word should spread faster than a speeding a worm or virus.
- Alternatively use the grapevine to create some intrigue by asking attendees to maintain a 'code of silence' about the presentation with whilst talking incessantly about the messages.
- Use humour and fun to point out common pitfalls and give war stories, but remember not to subvert any of the messages you want the audience to go away with, and don't target any individuals personally.

Even if staff believe that they could do well enough without going to the session, or consider they already know it all, attendance still serves to reinforce security behaviours and needs to be encouraged. If people avoid attending ask why they haven't and when they will.

Performance Review (Assessment) schemes can include a statement in support of the IT Security Policy and be assessed periodically.

Remote or short term Staff

Staff in remote locations or on short-term contracts should either be individually briefed by IT Security or management staff, or have access to the awareness program material. Making the material available online is helpful for such situations, as staff are unlikely to have the opportunity to attend awareness presentations. Staff can be asked to demonstrate their understanding by submitting an email or signing a statement or questionnaire after viewing the presentation.

Perceived lack of benefit

IT Security could be perceived as a cost with little tangible return on investment. Therefore it is essential that all IT Security initiatives considered provide identifiable benefits and be measurable. Some benefits can be represented in financial terms, other aspects may not be less tangible and harder to gauge, such as possible damage to organisation's reputation. If implementing a regime where Internet activity is to be closely monitored, or a content filtering solution implemented, the cost of the activity should have some measurable benefit for the organisation. This might include:

- Measured decreases in downloads for a set period
- Increased bandwidth and performance
- Reduction of unauthorised software recorded during periodic audits.

Resistance to change

Despite the increasing frequency of change to the modern workplace, staff may often be resistant to and wary of change, unless the reasons for the change are clearly demonstrated. The introduction and implementation of an IT Security Policy represents such a change. This behavioural tendency for resistance again highlights the importance of a having a complementary, well-developed awareness program to communicate the benefits of and rationale behind the new policy.

Existing practices and views

If the organisation has previously taken a relaxed approach to IT Security, staff may consider new changes introduced by the IT Security Policy to be oppressive. Often security is seen as being associated with impositions, or viewed as a restriction on freedoms. Where security does impose inconveniences or restrictions, the reasons for the decisions needs to be explained, understood and accepted. Again the best method to achieve this is via a complementary awareness program.

Loss of autonomy and Individuality

Staff increasingly interact with a dedicated computer (i.e. desktop) and adapt and personalise its environments to preferences that work best for them (this also gives a sense of ownership). Making personalised changes such as the display colour, resolution, and switching mouse button functions, are usually fine and acceptable. However, other configurable changes such as downloading unauthorised software (e.g. peer-to-peer software) can inadvertently expose the organisation to unnecessary risks. Such unauthorised changes could also lead to increased costs by affecting productivity or stability, or by requiring the standard operating environment to be reimaged. While initially this approach may seem harsh, explaining the implications to users often clarifies and justifies the situation.

Privacy and monitoring concerns

Another major barrier to the acceptance of an IT Security Policy may relate to privacy issues. The Australian Office of the Federal Privacy Commissioner has provided advice about guidelines on workplace email, web browsing and privacy.[11]

Email and Internet access provides many advantages for both the organisation and staff and has the potential for personal use. In this respect staff may consider these activities as private, particularly as password controls are often associated with them. "An organisation has a responsibility for its computer systems and networks, it has the right to make directions as to its use." [11] Effectively the workplace organisation owns the emails generated at work and they have the right to log them.

Furthermore, "some organisations impose a policy that staff may only use e-mail and web browsing solely for work related purposes, and that all access will be logged for compliance with this position." Therefore, "If staff were not made aware of the logging of their network activities then this could be considered to be unfair. Therefore, network users should be made aware of the logging practices of the organisation." [11]

Factors that influence Implementation

There are many factors that influence implementation and how the IT Security Policy is received. Some strategies to consider in addressing these issues are:

- Giving an avenue for feedback
- Being accessible
- Ceasing Opportunity
- Giving and Getting support
- Measuring performance
- Reporting to the Executive

Give an avenue for feedback

Because IT Security Policy is likely to affect everyone, it is vital that staff have a means of giving feedback. After running awareness briefings, evaluations and feedback should be sought. Provide a facility where staff can discuss security policy issues, ask questions, and prompt discussion.

Being accessible

The IT Security area should always be accessible and approachable for any staff. Some ways to encourage this are:

- Allowing for formal and informal meetings
- Put on a morning or afternoon tea for other areas and ask about their challenges, concerns and triumphs
- Sponsor or create social events.

Create a culture where people are comfortable about asking questions and where security issues are not seen wholly as criticisms. Information gathered can also be valuable for developing FAQ's.

Ceasing Opportunity

There may be other initiatives or circumstances taking place within the organisation that can be leveraged. For example, when the organisation decides to upgrade the desktop operating system or is redeveloping a legacy system, assess and review the security controls available against the IT Security Policy.

Giving and getting support

Collaborate and form strategic alliances that standardise processes with other functions such as Human Resources (HR), Physical Security, or Financial groups for constant improvement. Opportunities include:

- Using the same categories of prioritisation systems as Service Management or Disaster Recovery areas
- Information Management standards may exist that can be used to classify the sensitivity of information and the systems that hold and transmit data
- Standardisation of risk management terms can be extended where used in other areas such as change management control and fraud control
- Collaborating with the Inventory management area for ensuring software licensing compliance and system ownership is identified
- Including Security requirements in Project Management mandates and System Development and testing Methodologies
- Develop a stream lined form and process for new staff and cessations covering HR, building access and computer account removal and reduce red tape for staff, managers and the actioning groups.

Measure performance

Using the professional online surveys, as mentioned previously, provide benchmarks and data to evaluate security awareness levels among staff. It may be prudent to undertake a comparison with broader surveys once results become available, so that management can see the continuous improvements in performance against accepted benchmarks – aim to be a leader of the pack!

Reporting to the Executive

Regular periodic reports to the Executive should include progress on projects, issues that arise, and highlight positives; for example, the server team exceeding response times to mitigate new vulnerabilities, and other incidents, events or breaches, and survey comparisons.

Conclusion

Human nature is such that people usually require incentives and justification to change behaviours or adapt to new instructions. In order to conduct their work effectively and achieve business goals it is increasingly important that public sector staff are aware of the implications and consequences of IT security risks. The existing governance and guidelines for IT Security in Australia provide a high-level and focused framework in which to develop effective IT Security Policy. The implementation of IT Security Policy also represents an opportunity to educate and inform staff of related security issues. However, surveys and results worldwide have demonstrated that the best way to achieve the effective implementation of security policy is through targeted and continuous awareness raising programs. When complemented by an awareness program, the introduction of an IT Security Policy provides an avenue to bring about change in workplace behaviour while giving staff a clear understanding and rational for the policy in order to translate these requirements into daily workplace practice. It is also clear that there are several approaches available to raise awareness and that identification of target audiences prior to implementation facilitates effective translation of critical messages.

Work Cited

1. Australian Commonwealth Protective Security Manual, Commonwealth Government of Australia, 2000, URL: http://www.ag.gov.au/www/protectivesecurityHome.nsf/AllDocs/3ABEF2858B90B6D3CA256BB3001AE07C?OpenDocument
2. Australian Communications – Electronic Security Instructions 33 (ACSI 33) - Handbook 4, Security Management, Commonwealth Government of Australia, 2000, URL: http://www.dsd.gov.au/infosec/acsi33/HB4.html
3. Standards Australia URL: http://www.standards.com.au/catalogue/script/Details.asp?DocN=AS401174312067
4. Mary P. Kirwan, Friend or foe: Which are your employees?, 2003, URL: http://www.computerworld.com/securitytopics/security/story/0,10801,82134,00.html
5. Computer Emergency Response Team, URL: http://www.cert.org/advisories/
6. AusCert, Australian 2003 Computer Crime and Security Survey, 2003, URL: http://www.auscert.org.au/render.html?it=2001,
7. Robert Nellis, Creating an IT Security Awareness Program for Senior Management, 2003 URL: http://www.sans.org/rr/paper.php?id=992
8. K. Rudolph, CISSP, G Warshawsky, L Numkin, Computer Security Handbook, 4th Edition, Chapter 29, Security Awareness URL: http://nativeintelligence.com/awareness/chap29-4.asp
9. 2002 Security Awareness Index Report, The State of Security Awareness among Organizations Worldwide, 2002,Pentasafe Security Technologies, URL: http://security.ittoolbox.com/documents/document.asp?i=3189
10. Eight Annual 2003 CSI/FBI Computer Crime and Security Survey, Computer Security Institute, 2003, URL: http://www.gocsi.com/forms/fbi/pdf.html
11. Office of the Federal Privacy Commissioner, Guidelines on Workplace E-mail, Web Browsing and Privacy, 30 March 2000, URL: http://www.privacy.gov.au/internet/email/index.html

References

12. Dancho Danchev, Building and Implementing a Successful Information Security Policy, URL: http://www.windowsecurity.com/articles/Building_Implementing_Security_Policy.html

13. Karen Roberts, How to create and maintain a security-aware workplace, 2003, URL: http://www.computerworld.com/securitytopics/security/story/0,10801,81618,00.html
14. Dan Verton, Thwart Insider Abuse, 2003, URL: http://www.computerworld.com/securitytopics/security/story/0,10801,82922,00.html
15. Grant Gross, Study: Human error causes most security breaches, 2003, URL: http://www.computerworld.com/securitytopics/security/story/0,10801,79485,00.html