4

Risk Management

Introduction

4.1 This chapter examines the security risks involved in the movement of electronic messages and other data, particularly sensitive data, where unsecured public communication networks – such as the Internet – must be used.

4.2 The Internet is an environment of constant, low-level threat. A computer connected to the Internet faces a potential threat from any of the millions of other computers that make up the so-called World Wide Web. A 'cracker'[1] on any one of these computers can attempt illegal access.

4.3 Most threats are easily defended against. Virus scanners can be kept up to date and vulnerabilities can be closed with the latest software patches. EDS indicated that:

> In the case of the Melissa virus, which first manifested itself in North America, we were able to advise our customers here and close the gateways so that the virus did not have an impact on our customers. The Slammer was actually detected by our team in South Australia, who were responsible for not only informing our customers in this country and isolating the servers that could have been impacted but informing the world of the Slammer virus.[2]

---

1 A cracker is a person who breaks the security on a computer system, usually for malicious or destructive purposes.

2 Ms Whittaker, *Transcript*, 1 April 2003, p. 88.

4.4 In rare cases exploitation may occur before countermeasures are available. The Committee heard that the 'I Love You' virus infiltrated DoFA.[3] In such cases, prompt action will be necessary to temporarily protect the system until a more permanent solution is available.

4.5 The ANAO recommends that agencies adopt a structured approach to the management of Internet security, employing a sound risk management model. It also recommends that agencies ensure that appropriate risk assessments are conducted prior to introducing a new IT system or instituting major changes to an existing system[4].

4.6 Commenting on the need for regular risk assessment in its *Guidelines for the Security of Information Systems and Networks*, the OECD encouraged an active program. It said that risk assessment should be sufficiently broad-based to encompass key internal and external factors, such as technology, physical and human factors, policies and third-party services with security implications:

> Risk assessment will allow determination of the acceptable level of risk and assist the selection of appropriate controls to manage the risk of potential harm to information systems and networks in light of the nature and importance of the information to be protected.[5]

Broad Risk Management

4.7 Risk assessment and management must be applied broadly and continuously and must cover all areas of the computer system. This includes not only the computer hardware and software, but everything that comes into contact with the system.[6]

4.8 Effective risk management is an unending project. Threats to computer systems are constantly evolving, with new vulnerabilities discovered and exploited on an almost daily basis.[7] Even a system that has initially been thoroughly secured can quickly become insecure.

---

3 Mr Nicholson, *Transcript*, 2 June 2003, p. 247.

4 ANAO, *Submission 17*, p. 12; ANAO Audit Report No. 13 2001-2002, *Internet Security within Commonwealth Government Agencies*, p. 23.

5 OECD, *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*, Paris, 2002, p. 11.

6 Check Point Software Technologies (Australia) Pty Ltd, *Submission No. 9*, p. 19.

7 Check Point, *Submission No. 9*, p. 16.

4.9 Check Point Security Technologies (Australia) Pty Ltd recommends that risk management for computer systems be applied to all of the following areas:[8]

- Exterior security – fencing, lighting, building location;
- Secured dumpsters – disposal of confidential information;
- Building security – key-locked doors, biometric authentication, physical guards, cameras;
- Departments - logically broken up, kept secure;
- Passwords – elimination of Post-It notes stuck under a keyboard or on the side of the monitor, with user ID and password;
- Computer / Data Centre – environmental controls, fire and cable management, secure consoles;
- Data Classification – confidential, secret, need-to-know;
- Access groups – assigned by user and / or group;
- Human Resources and IT staff coordination;
- Unauthorised modems; and
- Social Engineering – persons pretending to be an employee or maintenance worker to gain unauthorised access.

4.10 The initial parts of this list, dealing with physical security, were examined in Chapter 2. This chapter concerns itself with the prevention of attempts to access the electronic data itself.

Risk Management Lifecycle

4.11 Continuous risk management can be illustrated by a risk management lifecycle, which proceeds through a series of fixed stages. Immediately it completes the last stage, it reverts to the beginning and restarts. System administrators may start a new instance of the lifecycle for each new threat and need not complete the previous one before restarting.

4.12 There are various ways of approaching the task of applying a risk management lifecycle. Submissions from Check Point and EDS set out detailed steps by which an effective program could be established.[9]

4.13 The common elements of those proposals make up a simple risk management lifecycle of three stages: Analysis, Implementation and Testing. Check Point also proposes additional precautions through an initial stage of Perimeter Protection, performed before the first Risk

8 Check Point, *Submission No. 9,* p. 19.

9 Check Point, *Submission No. 9,* pp. 17-21 and EDS, *Submission No. 6,* p. 7.

Assessment is made and an Intrusion Detection System that operates throughout the lifecycle.

Analysis

4.14 Analysis is the process of identifying potential threats to a computer system – what the ANAO described as '… formally identifying risks across the range of organisational activity'.[10]

4.15 In order to carry out an effective analysis, a system administrator must know and understand all of the components of the computer system: what they are, how they work and the current threats to those components. System administrators can also supplement this analysis through penetration testing and review.

4.16 Based on this knowledge administrators will then be in a position to proceed by:

> … evaluating the identified risks based on the likelihood that the event will occur and the potential impact on the entity's activities and functions …[11]

System Components

4.17 If system administrators do not know that a particular component is installed on the computer system, then they will not look for reports of vulnerabilities in that component. In this event, even when vulnerabilities have been discovered and corrected by the vendor, the system will remain at risk because the administrators, being unaware of any weakness, will not have implemented the necessary corrective action.

4.18 Similarly, system administrators must know what each component does. If it has functions that they are unaware of, then the system may be vulnerable in a way that they do not guard against. For example, a software program may interact with the Internet without the user or the system administrators being aware of it.

4.19 In relation to risk management, the DSD offered the general advice that '… wireless devices should not be allowed and wireless networks should not be created … [because of] the inherent insecurity.'[12]

4.20 Hardware and software can often be used 'out of the box', using a default configuration. This means that system administrators could set up a

10 ANAO, *Capitalisation of Software*, Audit Report No.54 2002-2003, p. 35.

11 ANAO, *Capitalisation of Software*, Audit Report No.54 2002-2003, p. 35.

12 Mr Burmeister, *Transcript*, 17 October 2003, pp. 389-90.

system, but still not have detailed knowledge about the software and hardware being installed. Such a system may contain components and have functions that the administrators are unaware of. For this reason, the ANAO recommends that agencies avoid default installations of operating systems and web server software[13].

4.21 Even if a system administrator has detailed knowledge of the system, unless that knowledge is committed to writing, it will be lost if that person leaves and a new administrator takes over. The new system administrator may be able to run the system without their predecessor's detailed knowledge, but may be unaware of some of the installed components and so unable to fully protect the system.

4.22 Agencies should avoid these situations by building and maintaining a database of all hardware and software components installed on their computer systems. This would allow a new system administrator to very quickly know which components are installed and what they do. If a weakness is then advised for a particular component, they would know whether or not the system included this component and needed to be protected.

Threat Awareness

4.23 In order to carry out an effective threat analysis, system administrators must learn of newly discovered vulnerabilities as soon as possible. There are many ways that they can be reported by vendors and other interested parties. System administrators need to keep a close watch on all of these sources.

4.24 A number of web sites publish reports on viruses and other computer security threats. These include the *Symantec Security Response* site[14] and the *McAfee Security* site[15]. Threats are reported on these web sites as soon as they become known. Security reports include an assessment of the threat and suggested countermeasures.

4.25 A number of computer system suppliers maintain web sites that report on security threats to their products. These include Microsoft's *Technet Online* site[16], the *Oracle Technology Network Security* site[17], the Sun Microsystems

13 ANAO, *Submission No. 17*, p. 13; ANAO, *Internet Security within Commonwealth Government Agencies*, Audit Report No. 13 2001-2002, p. 23.

14 Symantec Security Response, http://www.symantec.com/avcenter, 28 October 2003.

15 McAfee Security, http://www.mcafee.com/anti-virus/default.asp, 28 October 2003.

16 Technet Online, http://www.microsoft.com/technet/, 28 October 2003.

17 Oracle Technology Network – Security, http://otn.oracle.com/deploy/security/alerts.htm, 28 October 2003.

Security Information site[18] and the *Netscape Security Center* site[19]. These web sites alert users as threats to their products become known and offer fixes and patches to remove vulnerabilities.

4.26 Other resources include user groups, technical discussion forums, journals and books.

4.27 System administrators must consult all of these resources frequently and systematically, in order to keep up with the latest threats to their computer networks and the recommended countermeasures.

4.28 Unfortunately, not all threat reports are genuine; some are hoaxes.[20] Others may be malicious and following their instructions will create a new vulnerability on the computer system.[21] System administrators therefore need to be wary and only heed threat reports that can be corroborated or come from a reputable source.

Incident Reporting

4.29 DSD maintains an incident reporting scheme called ISIDRAS. This scheme collects and analyses information on security incidents as an aid to the protection of Government computer systems.

4.30 The information collected by ISIDRAS is used to compile Security Advisory reports, which are available to all agencies and members of the public on DSD's *Computer Security Advisories* web page.[22] However, not all agencies are reporting incidents to ISIDRAS. For example, Centrelink told the Committee that it only reports the most serious of incidents[23], while CSIRO does not report to ISIDRAS at all because of the volume of information that it handles.[24]

4.31 DSD classifies incidents into four categories:

- Category 1: events not definitely identified as an attack;
- Category 2: unsuccessful attacks;

---

18 Security Information, http://sunsolve.sun.com/pub-cgi/show.pl?target=security/sec, 28 October 2003.

19 Netscape Security Center, http://wp.netscape.com/security/index.html, 28 October 2003.

20 e.g. Symantec Security Response - Jdbgmgr.exe file hoax, http://www.symantec.com/avcenter/venc/data/jdbgmgr.exe.file.hoax.html, 28 October 2003.

21 e.g. Symantec Security Response - SubSeven 2.0 Server, http://www.symantec.com/avcenter/venc/data/sub.seven.20.html, 28 October 2003.

22 Computer Security Advisories, http://www.dsd.gov.au/advisories/advisories.html.

23 Ms Treadwell, *Transcript*, 31 March 2003, p. 30.

24 Mr Morrison, *Transcript, 1 April 2003,* p. 129.

- Category 3: successful attempts to breach security but with only minor effects on system operations; and
- Category 4: Successful attempts with major consequences.

4.32 Of the four Categories, reporting to ISIDRAS is only mandatory for Categories 3 and 4. DSD acknowledges that if all incidents were reported the system would be overwhelmed:

> It is very much the view of the people in our network vulnerability team that if you move to a mandatory reporting regime for all levels of incidents we would be swamped with information which would not really give us any additional insights.[25]

4.33 DSD commented that one of the problems they encountered is that agencies often do not prepare all of the documentation needed to fully explain their network:

> When we work with departments to give advice on how they should set up IT infrastructure, there is a general set of documents that they ought to produce that we would then review. That includes security plans, architectural and network diagrams – things that we can help them develop. … there are certainly a number of documents that we would expect every agency to have so that they completely understand the nature of their networks.[26]

4.34 When asked by the Committee whether agencies, in practice, had that documentation, DSD responded:

> … I think you would probably find that the answer is no.
>
> When we do work with agencies and do security audits with them, our experience is that often the documentation is not complete or is out-of-date.[27]

4.35 In discussing the losses of IT equipment examined by the Committee, DSD commented:

> For the purposes of ISIDRAS, we would consider physical loss of equipment to be probably a level 3 incident. So it really is a mandatory reportable incident – and a number of people have been surprised when we have said that.[28]

4.36 DSD said that the reports that are being received from agencies '… give us an overview of the level of sophistication of attacks that people will

---

25 Mr Merchant, *Transcript, 16 June 2003,* p. *262.*

26 Mr Burmeister, *Transcript*, 17 October 2003, p.393.

27 Mr Burmeister, *Transcript*, 17 October 2003, p.393.

28 Mr Burmeister, *Transcript*, 17 October 2003, p. 392.

experience over the public network.'[29] It added that whereas previously agencies which notified incidents received very little feedback or direct assistance:

> We are now providing a response capability to agencies. If they do have a problem and report it to us, we can help them fix the problem, identify it and make sure it does not happen again for them. So there are now people at the end of the line who will be able to work with them to fix any problems they identify.[30]

4.37 The Committee noted that ISIDRAS is the only scheme for reporting IT security incidents and potential security breaches, which operates throughout Commonwealth agencies. DSD indicated, however, that the system was not widely known, nor were the reporting requirements well understood:

> … I have to say that we do actually have a fairly proactive line with incident reporting. If we hear about something and a department has not told us, we will go and seek a report. Often it turns out that they are not aware of the scheme – which is one of the things we are trying to improve. If they are aware of the scheme they are not necessarily aware of what each of the levels means and which incidents they need to report to us.[31]

Recommendation 5

4.38 **The Australian Government Information Management Office, in consultation with the Defence Signals Directorate, reiterate to all Commonwealth agencies their responsibility to comply with the reporting requirements of the Information Security Incident Detection, Reporting and Analysis Scheme particularly the mandatory reporting of category 3 and category 4 incidents.**

Penetration Testing

4.39 Penetration testing is a controlled attempt to gain unauthorised access to the computer system. If it succeeds, then it has identified a vulnerability in the system. This method is an effective test of the internal and external

29 Mr Burmeister, *Transcript*, 16 June 2003, p. 262.

30 Mr Burmeister, *Transcript*, 16 June 2003, p. 263.

31 Mr Burmeister, *Transcript*, 17 October 2003, p. 392.

security of the computer system.[32] Centrelink carries out penetration testing as an established part of its security measures.[33]

4.40 Penetration testing must be carried out by a person or organisation with no inside knowledge of the computer system. This reflects the circumstances of a cracker trying to gain unauthorised access to the system.[34]

4.41 It is important that penetration tests be carried out in controlled circumstances. In November 2002, a Commonwealth Government agency received an e-mail survey, purportedly from the ABS. Users who responded would have compromised the security of their agency. This e-mail was part of a penetration test performed by a private security company on behalf of another government agency. Neither the ABS, nor the agency being tested, had known that the name of the ABS would be used in the e-mail.[35]

4.42 Any agency conducting a penetration test must be aware of exactly what is to be done, how it is to be done, any possible consequences that may arise and any recovery or response processes which need to be put in place.[36]

Review

4.43 A review involves examining the computer system in detail. It is a long and laborious process, but can be very thorough in locating vulnerabilities. Each component of the system can be examined separately.

4.44 Hardware and software components can be reviewed by their observed behaviour and by examination of the accompanying documentation.

4.45 Open source software allows system administrators to examine source code and determine the behaviour of software components in the greatest detail. The Committee heard that:

---

32 Check Point Software Technologies (Australia) Pty Ltd, *Submission No. 9*, p. 20.

33 Centrelink, *Submission No. 18*, p. 1.

34 Check Point Software Technologies (Australia) Pty Ltd, *Submission No. 9*, p. 20.

35 Defence Signals Directorate (DSD), Information Security Group Computer Security Advisory DA2002-05, Hoax E-mail, November 2002, http://www.dsd.gov.au/_lib/pdf_doc/advisories/da2002-05hoax.pdf, 28 October 2003.

36 DSD, Information Security Group Computer Security Advisory DA2002-05, Hoax E-mail, November 2002, http://www.dsd.gov.au/_lib/pdf_doc/advisories/da2002-05hoax.pdf, 28 October 2003; DSD, Information Security Group Computer Security Advisory DA 2002-06 IT Security Audit Guidance and more on E-mail Hoax Advice (DA 2002 –05), 26 November 2002, http://www.dsd.gov.au/_lib/pdf_doc/advisories/da2002-06moremailhoax.pdf, 28 October 2003.

> The issue of access to source means that an enormous amount of peer review goes on. Certainly, not everyone who uses an open source system looks at the source code, but the fact that it is available means that it is looked at by a very broad number of people from different educational and cultural backgrounds, and that diversity leads to a lot of out-of-the-box thinking; therefore a lot of problems are found proactively and are fixed.[37]

4.46 In response to this line of criticism, Microsoft Australia informed the Committee that it had launched a Government Security Program which will give key government security agencies access to the source code on its products. [38] Negotiations on the participation of Commonwealth agencies in this program were completed to the satisfaction of DSD in 2003.

4.47 System processes in a network can be reviewed by examination and analysis and by interviews with the people responsible for carrying them out. The practical experience of the users can be used to reveal flaws that are not readily detectable by other methods.

4.48 ANAO recommends that agencies ensure that applications supporting transactions with users be reviewed regularly for secure coding practices.[39] DSD uses a detailed review of the relevant system as part of its accreditation process.

Implementation

4.49 Implementation is the process of modifying the computer system so that it is no longer vulnerable to the threats identified in the Analysis stage. Methods of implementation include applying a patch which eliminates the weakness, or instituting a temporary arrangement to work around the problem until the solution becomes available (known as a 'work around').

Patches

4.50 The simplest way of addressing a software vulnerability is to apply a patch; that is, a piece of software that modifies the system's existing software.

4.51 When a software provider learns of a problem affecting one of its products, it will usually act quickly to develop a patch that removes the

37 Mr Paddon, *Transcript*, 2 April 2003, p. 164.

38 Microsoft Australia, *Submission No. 64*, p. 1.

39 ANAO, *Submission. 17*, p. 13; ANAO, *Internet Security within Commonwealth Government Agencies*, Audit Report No. 13 2001-2002, p. 24.

vulnerability. The patch is then made available to users through the company's web site.

4.52 The ATO has built this requirement into its system processes. The measures applied within its system to protect electronic information during transmission, require it to apply the latest patches to software as soon as they are available.[40]

4.53 Microsoft pointed out that unless IT managers regularly patch their systems, vulnerabilities will continue to exist even when they have been recognised and addressed by the original software developer.[41] To suggestions that a disadvantage of closed source systems is that they require continuous security responses Microsoft responded that the high incidence of attacks upon its operating systems and platforms testified to the popularity of these products.[42]

4.54 For serious vulnerabilities, it is critical that the provider release the patch as soon as possible. Until the patch is available, most of their users will be vulnerable. Lately, software providers like Microsoft Australia have improved response times and have been releasing patches in a timely manner, often before any major attack has occurred.[43]

4.55 The Australian UNIX and Open Systems Users Group (AUUG) acknowledged the improved timeliness of the provision of patches by closed source vendors, but stated that patches had not always been made available in adequate time frames and that this may also be the case in the future.[44]

4.56 In some cases, the patch may have been developed very quickly so that it could be released as soon as possible. Because of this, it may not have undergone proper quality control. Consequently, installing a patch may have unintended consequences, including introducing a new vulnerability or causing the computer system to become unstable. System administrators should therefore be cautious when installing patches. Each one should be carefully tested before being applied to a live system.

4.57 ANAO strongly recommends that agencies test and install security patches in a timely manner.[45]

---

40 Australian Taxation Office, *Submission No. 14*, p. 12.

41 Microsoft Australia, *Submission No. 12*, p. 5.

42 Mr Russell, *Transcript*, 16 June 2003, p. 281.

43 Mr Vohra, *Transcript*, 31 March 2003, p. 49; Mr Paddon, *Transcript*, 2 April 2003, p. 165.

44 Mr Paddon, *Transcript*, 2 April 2003, p. 165.

45 ANAO, *Submission 17*, p. 13; ANAO, *Internet Security within Commonwealth Government Agencies*, Audit Report No. 13 2001-2002, p. 23.

Correcting a Vulnerability

4.58 If the system administrators understand enough about their computer system, then they may try to fix the vulnerability themselves.

4.59 Open source software can be fixed by system administrators because the source code is included in the software release. Fixing the problem may involve changing the source code and recompiling the software. Information on how to do this is often included in the report of the vulnerability released by the software provider.

4.60 Source code is often large and complicated and altering it may have unintended consequences. System administrators should be cautious when altering source code and always test any changes before implementing them on a live system.

4.61 Closed source software cannot be fixed by the system administrators. When a vulnerability is found, the administrators must wait for the provider to release a patch. This may limit agencies' control and create additional risk.

4.62 If a vulnerability is discovered in a hardware component, the system administrators may be able to fix it by replacing the component or altering its configuration. If the problem is in a process, the system administrators must alter the existing process or implement a new process that avoids the problem.

4.63 ANAO recommends that risk assessment techniques be applied at the process-level with the aim of enhancing control structures, detection of control weaknesses and prevention of breakdown; all of these improvements leading to increased operational efficiency.[46]

Working Around a Problem

4.64 The situation may arise where a threat requires immediate action, but the necessary patch is not yet available so that the problem cannot be immediately fixed by the system administrators. Alternatively, there may not be time to properly identify the threat and implement a specific solution.

4.65 In these cases, it may be necessary for the system administrators to institute a 'work-around'. This is a temporary change that will avoid the vulnerability until a better solution can be implemented. Once the problem has been overcome, the administrator may remove the work-around.

46 ANAO, *Capitalisation of Software*, Audit Report No.54 2002-2003, p. 35.

4.66 In extreme cases, a work-around may involve shutting down the computer system or disconnecting it from the internet. Measures like these may be necessary to protect the system from a particularly dangerous virus or a Denial of Service (DoS) attack.

4.67 In less serious cases, a work-around may involve blocking some kinds of internet traffic or disabling some of the system's functionality, to prevent it from being compromised.

Testing

4.68 Testing is the process of verifying that the modifications made in the Implementation stage effectively protect the computer system from the threats identified in the Analysis stage. The process may include a controlled simulation of an attack which targets an identified area of vulnerability.

4.69 The testing process must cover the entire system, to ensure that the solution has not introduced any new vulnerability or other unintended consequences.

Committee Comment

4.70 The Committee noted the concerns expressed by various witnesses, regarding the necessity for continual awareness of changing threats to a computer system. It stressed the necessity for administrators to know their system in detail.

4.71 The Committee noted with concern the comments by DSD about the lack of complete and up-to-date documentation on agencies' IT network architecture. The Committee expects Commonwealth agencies to consult with DSD and to complete the necessary documentation without delay.

4.72 The debate between the security advantages associated with closed and open source systems is on-going. The Committee accepts that each of these systems has advantages and disadvantages and agencies should be aware of the opportunities offered by each type of system.[47]

47 Ms Connick, *Transcript*, 16 June 2003, p. 261.

Recommendation 6

4.73 **The Australian Government Information Management Office (AGIMO) monitor and report on the performance of Commonwealth agencies:**

- **implementation and maintenance of a flexible and responsive security risk management strategy for IT networks including hardware, software and data protection; and**
- **maintain an awareness of current and emerging threats to their computer networks and the recommended countermeasures.**

AGIMO should advise the Committee in an Executive Minute, of the status and completeness of these arrangements.