Security plan – knowledge and information security

Contents

Executive SummaryGiven the extent of, and the nature of the organisation, the effective operation of the information technology systems is vital to the continuation of business. However, a corporation of 600 staff poses unique security challenges, many of which are satisfied with the implementation of an operational training program completed by all staff.

This plan was developed, in part, to address issues identified in the security audit of 2007. Some of the issues raised have been addressed through the implementation of the Technical Systems and Information Technology Security Policy presented independently of this plan. Other issues of concern include incident response, disaster recovery, and business continuity. General lack of staff awareness of security issues is also a concern. This plan was formulated to be an integral part of the organisation's security policy; it identifies potential threats to physical and electronic information security, designs guidelines in all areas of the organisational operations to minimise risk, and suggests an appropriate training scheme to be completed by both current and future employees at all levels.

Responsible PersonnelChief Security Officer ? Paul Maluga Extension: 8080 The Chief Security Officer (CSO) is responsible for the oversight of the security system and coordinating security activities. The CSO is also responsible for staff security activities including security screening and security awareness training. Electronic Security Manager ? James Brown Extension: 8020 The Electronic Security Manager (ESM) oversees the electronic protection of the network and the administration of the database. Physical Security Manager ? Andrew Ryan Extension: 8035The Physical Security Manager (PSM) is responsible for maintaining physical integrity of the organisation, its employees, and equipment.

Risk Management Officer ? Veronica Kales Extension: 8050 The Risk Management Officer (RMO) is responsible for oversight of the disaster recovery centre as well as investigating alleged security breaches. Assessment of Risk Any organisation may become a target of persons wanting to acquire that information for personal, financial, or competitive advantage. The threats to an organisation’s information security may be both physical and electronic. Physical (Hagen, Rong & Sivertsen, 2008) Building security is meant to safeguard personnel, property, and equipment. Properly instituted, it prevents illegal access to organisational assets.

Threats to the physical security include: 1)Covert security breaches aimed at gaining access to information repositories a)Unauthorised physical access to premises to gain information. During covert entry, data and information may be stolen and/or software installed on computers to facilitate future electronic attacks, electronic surveillance equipment may also be placed in sensitive areas.)Electronic surveillance of premises by third party to gain confidential information, may include: a)Wiretaps on telephones of key personnel b)Electronic audio-recording equipment in key locations such as in boardrooms, or management offices 3)Access agents employed by outside entities to gain access to organisation and information repositories a)Persons in the employ of an outside entity to infiltrate the organisation and gain access to confidential information.)Outside entity may recruit or subvert staff to gain information a)Pressuring or enticing employees to provide information, or to facilitate electronic or physical access to that information for the benefit of the outside entity. 5)Material damage to physical documents and equipment resulting from fire or other unforseen occurrences e. g.

earthquakes and other natural disasters. 6)Portable devices that are used by staff for convenience may be lost or stolen a)Lax password security means that should these portable devices be lost or stolen the information stored on them is available to anyone who cares to view it. Electronic (Volonino & Robinson, 2005) Electronic security is meant to guard databases and networks from unauthorised access and malicious or accidental damage. An instituted electronic security system prevents damage to information by intangible means such viruses, bugs, malware, and other cyber threats. These may include: 1)Viruses are the number one threat to computer systems, the consequences of infection can be disastrous a)The costs the spread of a serious viral infection can be upwards of one billion dollars for a single national economy. A viral infection within a computer network can lead to corruption or complete loss of information.

2)The security audit of 2007 has identified social engineering to be a major risk to the organisation a)Social engineering refers to the process of manipulating people into performing actions or divulging confidential information. This is done either by appeals to people’s emotions or by establishing trust. 3)Key loggers, Trojan horses and other malware programs are used to gather information about computer users, which can be used for a more sophisticated direct attack at a later stage.)Hacking into the organisation’s computer network remains a risk due to lax information technology security. a)Hacking involves finding vulnerability in the security of a computer network and exploiting it to gain access. Poor password and anti-intrusion software security contribute to the risk.

5)Denial of Service attacks are a major threat to an organisation heavily reliant on information technology a)Denial of Service is an attack whereby the user is denied the use of his Internet access. In cases of wireless networks, it can also affect the Local Area Network.)The extent to which wireless networks have been utilised remains a threat as physical networks can be accessed through a wireless network a)Wireless systems face a problem with both data security and Denial of Service attacks. Theft of Internet bandwidth is also a tangible risk associated with wireless networks. 7)Excessive file sharing has been also identified as a major security risk. a)With any networked computer systems, users of such systems tend to share files unrelated to work.

As such, this allows infections isolated to particular computer units to spread throughout the network.)Loss and/or corruption of data through malicious or accidental means, which leads to inaccessibility of information a)This may occur because of an organised malicious attack, or something as simple as a power failure. 9)Accidental unauthorised disclosure of private or confidential information Data Access Security General Security Every computer on the organisation’s network is to be operated in a manner that can be reasonably expected to prevent unauthorised access to the network (Hagen et al. , 2008) User Authorisation 1. 1.

Every member of staff is to be issued with a security clearance based on their level within the organisation and their work requirements. 1. 2. Security clearances must be issued subject to the need-to-know principle. User Authentication 1. 3.

All users are required to authenticate to obtain network access. 1. 4. Each staff member must be issued with a unique username and password. 1. 4.

1. The password must be regarded as strong and is not to be stored where unauthorised persons may have access to that password. 1. 4. 2.

The password must be changed on a weekly basis. 1. 5. User authentication must be logged, and the logs maintained for a period of three years in a form that can identify which user account was using a particular Internet Protocol (IP) address.

1. 6. Peripheral devices (e. g. printers) must be tracked so that the networked computer unit using that device can be readily identified. 1.

7. Time stamps in user authentication logs must be synchronised to a reliable time reference and must be accurate to the nearest second. Secure Database 1. 8. The electronic database containing private, secure, and confidential information must be kept in access-controlled areas with added security.

. 9. The database must be maintained as a stand-alone network with no outside access. Computer units connected to the secure servers must be located in separate access-controlled areas and must have no outside access.

1. 10. Computer units connected to the database must not be connected to pooled resources but to peripheral units located in the immediate vicinity of the computer unit. 1. 11.

There must system administrator-imposed limits on the access to confidential information contained within the database based on the security clearance of the user. Physical Files 1. 12. Physical documents must be security and access classified in the same manner as the electronic database. 1.

13. Each copy and each page of the document must be sequentially numbered. 1. 14.

A distribution list of every copy is maintained. 1. 15. A Classified Documents Register is maintained and all documents released require identifiable information registered, along with a signature.

An authorisation signature is necessary for certain documents. Electronic Intruder Deterrence – Viruses and Malware McHugh & Deek, 2005) 1. 16. Every computer unit within the organisational network must be installed with complete protection systems against viruses, malware, and other computer threats. 1.

17. Every security software system installed computer units within the organisational network must be kept up-to-date with every update possible. 1. 18.

For the purposes of identifying computer units within the organisational network – private computer units shall be so designated as long as they are connected to the organisational network. 1. 19. For the purposes of identifying possible security breaches on the organisation's computer network, it is necessary to establish an automated Intrusion Detection System. Social Engineering (Workman, 2007) 1. 20.

Social Engineering has been identified as a major risk to the organisation. In order to avoid disclosure of confidential information to unauthorised persons all staff will undergo extensive security awareness training. 1. 21. When dealing with customers, proof of identity is always required to the point where the operator is positive as to the identity of the person in question.

File Sharing . 22. The organisational network for work purposed exclusively. File sharing within the organisation must be limited to such purposes as private files may contain pathogens. 1.

23. The organisation retains the right to screen outgoing staff emails and other possible communication to ensure that confidential information is not being transmitted. Wireless Networks (Woodward, 2005) 1. 24. The use of wireless networks within the organisation must be kept within a secure environment at all times; all efforts must be made to ensure that unauthorised access to the wireless network is prohibited.

. 25. Whenever possible, users are encouraged to encrypt their wireless transmissions to ensure privacy and confidentiality of the network is protected. Staff Vetting and Separation Procedures General Statement Security checking on potential staff is essential in an organisation that deals heavily with private, secure, and confidential information. Termination procedures are also necessary to ensure that past employees have not used their position to their advantage (Solms, 1999). Staff Screening 2.

1. Every potential new employee must undergo extensive security checking. 2. 2. The security checking involves: 2. 2.

1. A security questionnaire, 2. 2. 2. An interview with the CSO, 2.

2. 3. Positive security checking including referee and personal integrity checking, and an Australian Federal Police check. Separation Procedures 2.

3. Once a member of staff ceases to be employed by the organisation, the following procedures must be performed as a process of disengagement: 2. 3. 1. Removal of all electronic and physical access rights, 2. 3.

2. Key personnel informed of the departure, 2. 3. 3. An audit undertaken to detect any breaches of security, 2.

3. 4. Confirm that the leaving person has not attacked the database in any way, 2. 3. 5.

An exit interview, 2. 3. 6. Return of all department equipment 2.

3. 7. Removal from contact lists. Personnel Security General Statement It is a common assertion that an organisation's employees are its biggest asset. It is also true that employees can, knowingly or otherwise, cause the greatest disruption to daily business activities and security procedures. Passive Monitoring 3.

1. Supervisors are encouraged to monitor suspicious behaviour of staff and produce reports regarding concerning behaviour. . 2.

Staff are likewise encouraged to report suspicious incidents or events. 3. 3. Whenever an incident is reported, management is required to treat it with the outmost seriousness and notify the RMO. 3. 4.

Confidentiality of the report-maker must be guaranteed. 3. 5. Every report must be handled with delicacy and discretion. Positive Monitoring 3.

6. The organisation retains the right to the monitoring of staff in accordance with publicised policies: 3. 6. 1. Checking staff telephone and email logs 3. 6.

2. Security audits of access to secure information e. . databases 3. 6. 3.

Audits of physical documents 3. 6. 4. Access log and video records of staff movements and access to secure areas are to be kept. 3. 7.

Should a security breach be reported mechanisms must be in place to: 3. 7. 1. Ascertain whether an actual security threat has occurred, 3. 7. 2.

Assess the nature of the threat, 3. 7. 3. Repair or prevent damage caused, 3. 7.

4. Identify the culprits, 3. 7. 5. Interview the suspected persons, 3. 7.

6. Report the incident and recommend improvements. Physical Security General StatementPhysical integrity of the organisation is imperative to the security of private and confidential information that the organisation holds (Irvine & Thompson, 2005). Authority for Access 4. 1.

Access to the building is limited to authorised key cardholders. 4. 2. The key card must be individuated to the particular person to whom it belongs and will allow access to particular secure areas according to security clearance level. 4.

3. Visitors to the building must be announced and must complete the Visitor Register. Access Criteria 4. 4. Organisation personnel – Key card holders are permitted access according to their security clearance. 4.

5. Visitors – Visitors must be announced and receive a clearance from the CSO. All visitors must complete the Visitor Register. 4. 6.

Maintenance personnel – Maintenance personnel must be accompanied by an authorised employee at all times. 4. 7. Contractor personnel – Contractor personnel must be accompanied by an authorised employee at all times. 4.

8. Emergency personnel – Emergency personnel must produce identification and be accompanied by an authorised employee wherever possible. The CSO must be notified as soon as possible. Intrusion Detection Systems 4. 9. Both the main organisational office building and the offsite information backup storage facility must be equipped with intrusion detection systems.

4. 10. These systems will include door alarms, cameras, and motion detectors in all areas. 4. 11.

Sensitive and secure areas will be equipped with greater security measures such as backup intrusion detection systems and greater scope on the placement of such devices. 4. 12. Roof cavities and other vulnerable areas must have adequate protection to ensure against infiltration.

Equipment Security 4. 13. The organisation must insist on a Clear Desk Policy – any sensitive document is to be put away under lock whenever the employee using it is away from his or her desk. 4. 14. The organisation must also insist on a Clear Bin Policy – any document that contains personal or confidential information is not to be put into an open garbage bin but rather into a secured bin for later shredding.

4. 14. 1. Documents that are to be shredded must be destroyed using a crosscut shredder to avoid the risk of future restoration of those documents.

. 15. All equipment is to be security marked and catalogued for future identification. 4. 15. 1.

Asset inventory is to be performed four times annually. 4. 16. Desktop computers and laptops are to be security locked and password protected and any external media are not to be used except with express permission from the system administrator. 4.

17. Storage of physical documents must be with regard to security. All filing cabinets and safes are to be lockable, security rated, and able to withstand unforseen circumstances (e. g. fire). Monitoring Services .

18. The organisation has employed State Security Services (SSS) to provide onsite and patrol security at both the main organisational office building as well as the offsite information backup storage facility. 4. 19. State Security Services are to provide after hours security patrols of both facilities.

4. 20. State Security Services is to provide regular physical and electronic examinations of both premises. 4. 21.

The contract for the monitoring security of the organisation (currently with SSS) is to be re-examined every two years. Security Breach Notification Incident Response Any breach of security, or a suspected breach in security, must be investigated fully to ensure that damage suffered from the breach is kept to a minimum, and that perpetrators are identified (Maley, 1996). Change in Culture 5. 1. First and foremost there must be an organisational culture where reporting security-affected incidents is tolerated and are appreciated. Incident Tracking 5.

2. An automated tracking system is to be set up whereby any anomalies within the network are recorded, analysed and logged. 5. 3. Lessons learnt from dealing with incidents must be incorporated into improving overall security. 5.

4. For optimal efficiency, this system must be synchronised with the Intrusion Detection System (see 1. 5. 4.) 5.

5. In order to facilitate the detection and investigation of unauthorised access to the network, the use of file signature recording software (Tripwire or Aide) must be implemented. Incident Response Team 5. 6.

When an incident is reported, a specialised team is to be dispatched to investigate the incident and assess any damage caused. Disaster Recovery General StatementRegardless of how well an organisation may protect itself from security risks, there is always a possibility that vulnerabilities within that security system may be exploited and data is either corrupted or lost. Backup Files 6. 1. Files must be backed up regularly. Backup files must be stored in an off-site location to prevent compromise of the backup data.

6. 2. Local data used for immediate work purposes must be backed up on a regular basis to prevent work being lost. 6.

3. Physical documents should have copies stored at an off-site location to prevent loss of information. . 4. There must be regular testing of backup mechanisms to ensure continual effective storage of vital information. Security Awareness Training General Statement Most problems with security

in an organisation arise from lack of security awareness among the organisation’s personnel.

To enhance security awareness in the workplace all staff must complete security awareness training and refresher courses on a regular basis (Smith, 2006). Initial 7. 1. All staff must undergo general security training that is useful in any regard.

7. . Depending on their position within the organisation, all relevant staff must undergo specific security training relevant to their specialisation. Periodical 7.

3. Each member of staff must undergo security training as part of their three months’ orientation with the organisation. 7. 4. All staff personnel are obliged to review their training and undertake refresher courses in both general and specific areas of security. Content General 7.

5. Each staff member will be required to undertake training in the areas of: 7. 5. 1.

The need to have access control over use of the organisational network, 7. 5. 2. Computer-borne threats such as viruses and malware, and means of securing against those threats; this includes the risks associated with file sharing among employees which is not work-related, 7.

5. 3. The need for physical integrity awareness training, in particular the handling of confidential documents, shredding, etc. 7. 5.

4. Password security and ways of maintaining password security, 7. 5. 5. The threat posed by social engineering and other social type information attacks and ways of minimising the risk, .

5. 6. Identifying possible security breaches and other security-related incidents and measures to be taken. 7. 6. The initial introductory course shall be completed online and will be assessed.

7. 7. Personnel must sign a security declaration form having completed the security training. 7.

8. Follow-up courses will be in a seminar-style setting and attendance will be taken. Specific 7. 9. Each officer of the organisation identified in " Responsible Personnel" will establish specific guidelines to be followed for each particular department.

General Security Awareness Training 8. 1. The need to have access control over use of the organisational network. ? The integrity of the computer network is vital. If it is suspected that security of the network is compromised the RMO must be notified immediately. ? It is imperative that no-one other than the authorised user has access to a particular computer unit.

8. 2. Computer-borne threats such as viruses and malware, and means of securing against those threats; this includes the risks associated with file sharing among employees, which is not work-related. It is crucial that every computer unit on the network be up-to-date with all relevant security updates and patches.

The antivirus installed on organisation’s computer units must be operational at all times. ? As the organisation cannot ascertain the origin of personal file, file sharing among personnel for private use is not permitted as those files may deliver infections into the organisational network. 8. 3.

The need for physical integrity awareness training, in particular the handling of confidential documents, shredding, etc. ? This organisation deals heavily with confidential documents. It is imperative that these documents are kept secure and do not pass to unauthorised persons. For that reason, whenever the user of a document is required to leave his or her workspace unattended confidential documents are to be put away to secure against unauthorised access to information contained therein.

? Private or confidential documents that are no longer needed must be shredded and must be stored appropriately to avoid unauthorised access to those documents before they are destroyed. 8. 4. Password security and ways of maintaining password security (PACE University). The need to maintain password security is to avoid unauthorised access to confidential information contained on the organisational computer network.

? The password issued to the user is not to be written or stored on any device where unauthorised persons may gain access to that information. ? The password is to be changed on a weekly basis so that if a password becomes compromised there is little time for damage to be done. ? A strong password must always be used. A strong password is one that is a combination of letters and numbers, cannot be found in a dictionary, and is at least eight characters long. Conclusion and Recommendations Considering the recent security audit that was performed, several key areas of security are in need of an upgrade. The upgrades proposed are designed to considerably enhance the overall security of the organisation, personnel, and equipment.

The following additions to the security package are recommended for careful consideration: 1. Guardhouse at the entrance to the employee car park. 2. Two additional CCTV cameras at the organisation's car park. 3.

Glass break detectors throughout the office building and the offsite information backup storage facility. . Additional motion detectors located on the roof of both buildings. 5.

Biometric identification linked to personnel key cards for added security. It is hoped that this document has assisted the reader in understanding the step that are required to ensure that the organisation's electronic and physical information, personnel, and equipment is secure against unauthorised contact. It is the belief of the security team that by implementation of this security plan and associated security awareness-training program, the organisation will be as secure as possible. Bibliography Eguren, L.

E. , " Beyond Security Planning: Towards a Model of Security Management", Journal of Humanitarian Assistance, July 2000, www. jha. ac/articles/a060.

pdf, accessed: 15 Aug. 08. Hagen, J. , Rong, C.

, and Sivertsen, T. , " Protection against Unauthorised Access and Computer Crime in Norwegian Enterprises", Journal of Computer Security, vol. 16: 3, 2008, pp. 341-366. Irvine, C.

and Thompson, M. , Expressing an Information Security Policy within a Security Simulation Game, (U. S. Naval Postgraduate School: 2005).

Maley, G. “ Enterprise Security Infrastructure”, IEEE Proceedings of WET ICE, 1080-1383, 1996. McHugh, J. and Deek, F.

, “ An Incentive System for Reducing Malware Attacks”, Communications of the ACM, June 2005, pp. 94-99. Mazzariello, C. , Multiple Classifier Systems for Network Security: From Data Collection to Attack Detection, Ph. D.

Thesis – Supervisor: Prof. Cordella, L. Nov. 2007. PACE University, Your Guide to Password Security, PACE University, Division of Information Technology, http://www.

pace. edu/emplibrary/PasswordFlyer101707. pdf, accessed: 15 Aug. 08. Smith, M. “ The Importance of Employee Awareness to Information Security”, The Institution of Engineering and Technology Conference on Crime and Security, 13-14 June 2006.

Solms, R. , “ Information Security Management: Guidelines to Management of Information Technology Security”, Information Management and Computer Security, vol. 6: 5, 1998, pp. 221-223.

Solms, R. , “ Information Security Management: Why standards are Important”, Information Management and Computer Security, vol. 7: 1, 1999, pp. 50-57.

Volonino, L. and Robinson, S. , Principles of Information Security: Protecting Computers from Hackers and Lawyers, (Readcon, New Jersey: 2005). Wagner, A.

and Brooke, C. , “ Wasting Time: The Mission Impossible with Respect to Technology-Oriented Security Approaches”, The Electronic Journal of Business Research Methods, vol. 5: 2, 2007, pp. 117-124. Woodward, A. , Recommendations for Wireless Network Security Policy: An Analysis of Current and Emerging Threats and Solutions for Different Organisations, (Edith Cowan University: 2005). Workman, M. , “ Gaining Access with Social Engineering”, Information Security Journal: A Global Perspective, vol. 16: 6, 2007, pp. 315-331.