Security plan

Business

The presence of a guard at the entrance of a building, magnetic access cards and identity badges provides an illusion that their information assets are physically secure. (The SANS Institute. 007) A report from Justin Kallhoff explains that the highest priority of physical security is human safety and in the event of an incident, the priority should be to ensure all human beings are safe prior to initiating other incident responses.

(Justin Kallhoff. 2007) The below tabular representation briefly describes some of the threats to an organisations information asset. Security ThreatSecurity Threat Description Humans BehaviourIf someone accidentally unplugs or turns off the wrong device, a hacker/cracker executes an exploit and unexpectedly crashes a server, an employee steals a device.

The most common threat is users in an organisation especially contractors including cleaning staff. Obvious ThreatsFires, floods, and natural disasters are obvious threats to physical security; however, every company is vulnerable to these kinds threats Magnetic Access CardsMost building access cards are controlled by the building administration department which might not be linked to the business in any way.

Regardless of the fact we need to ensure our server rooms are full equipped with alarm systems and a separate access systems which is preconfigured and managed by internal IT support.

This will reduce the risk of un-authorised personal accessing server the physical Identification BadgesIdentification badges can provide assurance and restrict social engineering however, we need to secure the source where the ID badges are created and ensure there are effective controls and

authorisations put in place. PasswordsUn-authorised access is normally encountered when employees share passwords or negligently leave them easily exposed. Password policies will be implemented to ensure user is aware of corporate expectations with reference to passwords.

Laptop Computers, Mobile Phones & PDA’sLaptops and smart phones that have sensitive data; for example, corporate e-mail should be pre-configured with encryption and strong authentication mechanisms to prevent data from being exploited to unauthorised users.

USB Mass Storage DrivesUSB devices that hold gigabytes of data in a form factor equivalent to the size of single human finger are widely available and distributed this causes a threat to organisations as data can be stolen or malicious code uploaded to the private network simply because by using the USB most of the logical controls like firewalls have been bypassed.

Access PermissionsThe need to ensure that access privileges of current employees are administered in accordance with the requirements of their positions. It is a great threat to an organisation if the incorrect access is assigned especially with reference to sensitive information such as payroll and human resource data. User Account TerminationsUser Access Accounts need to be terminated when a person leaves. The company is at a higher threat if ex-employee still has access to a company’s information asset.

Generic User Access AccountsDepartments that use generic user accounts with transacting or maintaining information can be very difficult to audit and hence create a threat to the integrity of the actual data.

Effective Cooling / Notification systemsThe server rooms should also be adequately equipped with air-conditioning as well as sensors and monitoring systems to detect any failures. A server overheating can cause a fire and this could lead to various other threats to an organisations information assets.

BackupsA company must ensure that their data is backed up and also need to verify that the backed up data can be restored and stored in a save location. Incident Response ManagementA computer incident security response team (CISRT) together with incident response management will ensure a company can recover from a incident and continue normal services. Malicious Code, including viruses, worms and TrojansDigital attacks , mainly in the form of DOS denial of service through the use of malicious code, viruses, worms, Trojans and many more are a threat to an organisations information portal.

Outsourcing Development and SupportTo remain competitive, the organisation should mitigate security threats when acquiring, outsourced development and support staff including implementation of host software applications. Software Development Methodologies Software development needs to be analysed and examined internally, and also to prevent any threats to our information the business should ensure the software is from an accredited, trustworthy vendor or business partner. There should be no ambiguity. EmailElectronic mail is a great way to communicate both internally and with competitors which is feasible and productive.

However sometimes, email privileges may be abused and can be detrimental to the image of the business. Security policies will be put in place to restrict

large group emails to the entire business and also educate staff and the company email policy.

File Management SystemFiles on File Print servers need to be managed and secured from unauthorised access. Confidential information stored on a shared drive might be at risk if left unsecured. Social EngineeringThe threat where an individual users fake identification and manipulative tactics to obtain information or physical access to hardware within the organisation.

Security Policy Guidelines (All Staff Excluding Information Technology Department) The following security policy guideline has been drafted out by the IT security team. Our goal is to educate and promote security awareness within the organisation.

The IT security department acknowledges that their function is to act as a liaison between those who own the data and those whom implement the controls. We are happy to further refine this policy guideline as long as sufficient justification in favor of both parties is accompanied with the request. Data Access Security & Application Security

The security team will also be adding tighter controls on data access including application security control. All access requirements will go through an outlook electronic approval form system. This will assist IT with satisfying auditing and compliance requirements. Regardless of the fact that IT has their own policy guideline we feel it is a shared responsibility of both management and IT of the control of access to the company’s information holdings.

Below is a briefing on the new proposed process for setting up and terminating user accounts from the company’s information domain.

Access Account Creation Before setting up a new user account, there is a process that the security team as now put in place which is fully compliant with the Sarbanes Oxley. Below is brief outline of the process requirements for a new access account. Management to log a helpdesk requesting a new user account and include as much detail as possible. There are various ways this can be done- Through the intranet, calling the onsite IT dept or emailing the support department. Once a call has been logged, the service request is normally assigned to a systems administrator at our head office in Perth City.

The Administrator will then send out an Electronic User Access form that needs to be completed and authorised by the manager. The manager will then electronically forward the form back to the administrator once they have authorised the access and completed the user credentials. The administrator will then forward the authorised user access form to the systems accounting manager for approval depending if access to accounting applications has been requested. The IT manager will need to sign off on any IT equipment being requested including mobile phones, blackberries and laptop computers.

The systems accounting manager will verify the access being requested and sign off the form with a digital signature. The administrator will create the user account and password on the server.

The administrator will assign the appropriate security access modules and functions to the new user account. Normally the manager can specify

another user that the access can be modeled off. Once the account has been created the administrator will forward a confirmation email with the login credentials via email to the new user.

The confirmation email will also entail the corporate IT services usage policy. Access Account Terminations For SOX compliance and security requirements, a process for user account terminations has been put in place. The first step is for human resources to log a helpdesk call notifying the IT department of the user account termination.

The helpdesk call will then be cloned and assigned to applications and network teams. The administrators will then remove the profiles and notify the managers via email. The helpdesk request will be updated with resolution comments and closed.

Password Security In order to increase network security and comply with regulatory Sarbanes Oxley audit requirements, the Operating system password policy will be well defined. Our aim is to prevent some of the common and easily guessed passwords from being used by unauthorised users. Passwords must not be written down and left in a place where unauthorized persons might discover them.

Regardless of the circumstances, authorized users must not reveal their passwords to third parties. All passwords will now need to be changed every 90 days by the user.

There are certain requirements when selecting a new password. Guidelines for Password Administration Password must not contain the user ID, first

name, surname, title or email address. Password must contain at least three (3) different characters. Password must contain six (6) or more characters and be different than the past three passwords.

Passwords must not contain the words “ passwords”, “ company name”, “ abx”, or variations of those words that replace letters with numbers. Passwords are case sensitive. Violation of Password Policy

If a password is entered that violates the password policy, the user will be prompted with a standard Windows error message and could possibly have their profile locked. The system will lock the user out on the third incorrect attempt. The user will then need to log a service request on the company helpdesk system portal so that an IT administrator can release the lock from the profile. Network Monitoring It is prohibited to copy or install unregistered software on any company information asset.

The IT security team has recently invested in Network Management software which will monitor all networked computers on the company domain.

Internet Usage The very same Network Management software will also monitor and analyse internet usage including frequent visits to social websites such as my-space and face book. Access to some websites maybe blocked if they are deemed to be inappropriate. All internet usage requests should be logged and authorised by the clients’ manager. Guidelines for Internet Usage When using internet based applications, look for “ Secure Servers” that provide a two-way data encryption. Most large scale vendors provide this service If provided the option, elect to not have your personal information sold to other companies.

Avoid disclosing your co-corporate e-mail address. Do not sign up on non-business related mailing lists. Electronic Mail (E-Mail) To ensure that electronic mail services are used in accordance with this Policy, the security team has been granted the authority to monitor, inspect, and disclose information of any breaches to the policy. The security team does respect your privacy and will seek formal authorization from executive management prior to accessing a users' email and audit logs on both the client workstation as well as the servers for legitimate purposes such as investigation of complaints of misuse.

Contents and audit logs for both sent and received emails can be inspected (including personal email) at any time without notice.

We have also implemented a solution called surf-control which automatically scans all emails for viruses and " spam" content. If viruses or spam content are detected, these messages are blocked and will be quarantined. Guidelines for Email Users Be polite as messages sent via email can often seem abrupt, even when this is not the intention. Use professional courtesy and discretion.

Messages should be clearly addressed to those from whom an action or response is expected; " cc" or " bcc" should be used for other recipients of the message. Respect privacy and consider this aspect before forwarding messages.

Delete unwanted or unnecessary email. It is the user's responsibility to manage their email folders. Avoid subscribing to unnecessary mailing lists. Unsubscribe from mailing lists when they are no longer required. Email

transmissions and postings to electronic notice-boards should normally be restricted to matters of Company business.

Use of system mass email distribution groups, e. . , +China – All Employees, should be strictly for business-related. Using distribution groups to transmit non-business items such as jokes and pictures rapidly consumes available systems resources and such use may result in restrictions on an individual’s access to system address books and distribution groups. Risk Management Information security risk management is regarded as crucial for the organisation especially since it being a well established and reputable financial institution.

The business as whole is expected to maintain the highest standard of trust and security.

Risk is to be managed effectively with the ultimate aim of protecting the institution from both internal and external security sources. In addition to our corporate goals, we will be implementing a systematic approach to managing risk which will have an ongoing investment in information security and the right controls in place. The IT security implementation team will be implementing a risk management project which will aid to assess the probability of both internal and external deliberate and accidental threats to the companies physical and electronic information holdings.

We will be involving the business system owners and executive management to assist us with identifying the organisations critical business assets in categories of level of risk.

Disaster Recovery The business is dependant on a stable IT infrastructure to support core business processes and increase competitive advantage. Unfortunately business processes can be halted in the event of a disaster which will have an impact on the business process which could influence our position in the market. (Trade Federal Commission. 2007) A simple definition of a disaster is a scenario that results in failure to access the IT infrastructure. Hewlett-Packard Development Company, L. P.

2006) Types of disasters may include fires, gas leaks, accidents causing serious injuries, storms or damages to adjacent properties and much more. Employees are advised not to panic in the event of a disaster and follow the disaster recovery plan which will be administered by the department warden. We will also be running simulated disaster recovery operations to improve our existing solution and also to prepare staff for an actual occurrence. It will now be a company obligation for all staff to adhere to simulated scenarios driven by the disaster recovery team.

Personal Security The highest priority objective on our disaster recovery plan will be to ensure the safety of all staff. A compliance hotline (133 200) will be implemented during phase two of our information security project.

Staff will be able to report any suspicious activity without disclosing their identity. The purpose of this hotline is to ensure personal security by tackling corporate espionage, bribery and intimidation. All members of the organisation are encouraged to make use of this facility provided. Security Breach Notifications

Employees are also encouraged to use the compliance hotline to notify IT of any security breach incidents. We will have a fully trained CISRT (computer information security response team) that can be assigned to each incident. Security Education Program It has been acknowledged that security training and awareness and governance for security have become a critical initiative for organisations.

The main reason for implementing an education and awareness programs is because security breaches continue to occur regardless of the technology and policies in place.

Human error is recognized as the main culprit to the cause of these breaches, the second being regulatory bodies such as Sarbanes Oxley. The security team does recognise, implementation of an efficient security program can be complex and expensive and hence have set key performance indicators (KPI’s) reports to measure the effectiveness of a security program as well as justify costs. The KPI’s have clearly defined the expected outcomes, performance targets, efficiency measures and other reporting requirements. We believe this will justify to management on the need for such awareness programs.

The following will elicit some steps considered necessary to enhance information security by means of a security and awareness education program which will tie into governance for security. All new staff will be expected to undergo an online training program that will provide a solid foundation of the importance of information security and their contribution towards info-security as an employee. Compulsory refresher courses will be

run annually for all staff to ensure employees are updated on the latest security threats. Certifications will be provided to staff to acknowledge their commitment to the security and awareness training program.

Employee’s that are not able to attend training programs will need to go through a company security training handbook and sign off an acceptance form with their respective manager. All employees will need to fill out a training feedback form which will assist improve the quality of the training awareness programs.

All courses will also need to be signed off by the company compliance manager. Info-Security Objectives The information management and security team collectively would like to achieve the following main objectives in the first phase of the information security project.

Regulatory Governance All our strategic objectives will be aimed at compliance with the Sarbanes-Oxley Act of 2002. The act established a number of new standards for corporate accountability including management assertions that focus on internal controls and procedures for financial reporting. (ISACA. 2007) More specifically, Sarbanes-Oxley requires that companies assess and certify with respect to their internal controls over processes supporting financial reporting and the information technology supporting those processes.

(Australian Computer Society. April 2005) Data Management

The company’s data management controls provide reasonable assurance that data recorded, processed and reported remain complete, accurate and

valid throughout the distribution and storage process. The data management policy will also comply with our SOX requirement. The focus on data-management is Data Backup, Data Retention, and Data Restoration. (Rosenoer, J.

Feb 2002) Data Backup The backup process will copy data from the shared file/application management servers onto tape devises to protect against data loss. These tape media’s will be stored off site in a secure location away from the city centre.

Data Retention Data retention deals with the retention period of various types of data stored and back-up by the company. A detailed retention pyramid can be provided by the information security department if necessary. Data Restore Monthly restorations to a test environment will be performed to ensure that our back up services is efficient and also to confirm the integrity of the backup process.

Effective Disaster Recovery We are also aiming to ensure the company has the appropriate disaster recovery plans in place so that normal business processes may continue with minimum interruption after a disaster has occurred.

Our main objectives under this category are Planning, Protection and Recovery in conjunction with constant reviews to ensure plans are efficate. (Pfadenhauer, D. Nov 27, 2006). Planning We are aiming to develop and maintain a recovery plan to identify the key business processes, hourly costs of services not being available, mapping them to applications, then mapping

the applications to the IT infrastructure. The planning process will include the steps that need to be followed in the even of a disaster.

Protection

This will involve the design, implementation and operations of the recovery plans to protect the corporate data centre’s and employees. Recovery The recovery part will focus on business continuity by moving to a fully equipped recovery centre to continue operations to prevent further losses of market share and competitive advantage. Incident Management Systems The information security department would also like to implement an appropriate incident management system which will include a specialized internal CSIRT to assist with incidents. All incidents will be logged on an incident management system.

Web Content Filtering and Monitoring Systems Improve our current web content filtering and monitoring system to a more advanced solution to provide intrusion detection.

Wireless Security Solutions We will also be working with a local vendor on providing secure wireless access to our networks which in the past has often been overlooked. We will be comparing proposals from Telstra and their competitor Orange to compare the most economic, viable and secure solution. VPN Secure Remote Access ; RSA Tokens We are also aiming on securing remote access to our application servers with the use of VPN and RSA technology.

This will also mean centralizing VPN access allocation to our main IT head office. Security Compliance Tools As an effort to promote IT compliance, we have set an aim to have a security compliance tool installed at each centralized data centre. This will be linked to a fraud detection and prevention system in phase 2 of the IT security project.

Security Plan Efficacy The IT department is a pro-active dept and will be testing the efficacy of the proposed security plan in a number of ways. Spot checks will be carried on a sample of users to ensure training and awareness programs are working.

Sample user access listing will be provided to internal auditor to ensure permissions have been assigned adequately. The same test will also test to see if our process for new user accounts and terminations is being used. Random backup restorations will be instructed by CIO including data verification. Simulated disaster scenarios will be set quarterly at random date.

Monthly audits will be run on application administrators to ensure they are not processing or transaction on the system with their high level of access as a SOX requirement.

We will use a reputable security organisation to assist with penetration testing and ethical hacking to find vulnerabilities in our infrastructure and also test fixes and software patches. Conclusion In conclusion the IT security team would like to thank all employees for their cooperation through our security project. We have elicited the importance of protecting our organisations physical and electronic information holding and provided an

outline of our objectives. We anticipate continuous support from executive management and employees during this transition phase.

Regards