Types of security risks to an organization information technology essay

Technology, Information Technology

IT security is important to implement because it can prevent complications such as threats, vulnerabilities and risks that could affect the valuable information in most organizations. In order to improve GANT’s IT security, we must assess the threats, vulnerabilities and risks. Threats are something that can potentially cause damage to an organization, IT systems and network. Threats can be classified into two main categories such as accidental and deliberate threats. Accidental threats can be referred to as hazards such as human error, systems malfunctions and natural disasters. Meanwhile, deliberate threats are such as hacking, cyber terrorism and hi-tech crime. Threats in GANT’s include valuable information about the members, group’s activities, their meeting places, website and other aspects of their work that might be easily accessed by unauthorized people. Hackers can obtain unauthorized access without the organization being aware. The second threat is that the information about the habitats of the Natterjack toad and the organizations’ motives might be used by those who are not inclined to support its on-going existence. The third risk is the website might be compromised and unofficial messages might be added into it. Next, we evaluate on the possible vulnerabilities. Vulnerabilities are weaknesses in the organization that can be exposed by threats. Sometimes a person’s carelessness such as writing down the password on a piece of paper and placing it on a work table where it is not hidden could amount to as vulnerability as hackers could easily access the person’s information. The first possible vulnerability is the records of the members are maintained in a variety of ways including paper and unreliable computer systems. Inconsistent forms of securing and maintaining records of the members can

make it highly vulnerable. The second vulnerability is the information about the toads' habitats is maintained on an old internet-based server with very limited assurance in place. Without updating to a new server, the work will be done inefficiently and it will be cost and time consuming if the server crashes. The third vulnerability is that there is no firewall between the website server and the internet. Without firewall to prevent unauthorized access, it will make your computers vulnerable to attacks. The results of having vulnerability and it being exploited by a threat can result in a risk. Risks are threat potentials that exploit vulnerability in an asset that can cause damage or losses to the assets. There is a risk that corrupt property developers might gain access to the personal details of members of GANT and take severe action against them or their property. This could lead to a serious security breaches when an unauthorized person gained access to the members' files as well as the others usernames and passwords. The second risk is that the habitat of the Natterjack toad might be destroyed by someone who is not interested in the toads' existence. Lastly, the third risk is a risk that someone (unauthorized person) might gain access to the code of the GANT website and change the message to offensive information to those who are interested in conserving their existence and nature.

Task 2 – Discuss risk assessment procedures (2. 1)

Likelihood or probability:

There are few certainties in this world, and risk management is no exception. The greater the vulnerability, the greater chance there will be a threat carried out. Quantitatively and Qualitatively are the two basic ways in which

likelihood can be carried out. Quantitatively may be gained from previously recorded information such as statistical data. Meanwhile qualitative assessment is where the work is more subjective and depends on opinions rather than facts. For example, companies who produce anti-virus software can point to the large number of viruses which their products can scan for and remove, from which one can conclude that without anti-virus software, the risk of infection is high. On the other hand, one does not need to know the exact number of incidents to be aware that the likelihood of a breach of confidentiality or integrity is high without proper password protection. Both methods of assessment have their place. The important thing is that likelihood assessments are carried out according to agreed criteria. Meanwhile, the impact of the risk actually happening is perhaps the most important concept that needs to be considered. It is this potential impact which has to be managed properly. If the impacts are small and irrelevant then there is no need to take further action but instead just monitor it every so often. For example, when an ATM cash dispenser broke down, the impact would usually be low especially if it’s only one machine in the bank’s network that fails. On the other hand, if the potential impact could be the loss of vital company information, then more appropriate countermeasures need to be considered. As far as businesses are concerned, the impact on the organization and its daily activities are usually the crucial consideration and will often warrant further measures being taken. (Falla, 2013)The business impacts of realized threats include the loss of confidentiality, integrity and availability, and frequently lead to financial loss, inability to trade, brand damage, loss of customer confidence, etc. (Falla, 2013)

RISK MATRIX

GANT’s has a high risk of providing no backup of the information and no proper documentation to create their records. As a result, GANT’s information is highly vulnerable. The likelihood is possible hackers might gain access to GANT’s records. In order to assess the consequences of the loss or failure of the computer, it is recommended for the organization to carry out the qualitative approach. Qualitative approach is one of the methods to carry out risk assessments. It can evaluate hard facts relating to impacts and frequency of events that are difficult to come by. Having identified the impacts for each threat, we have to assess the likelihood or probability of each occurring. ImpactsHIGHHigh riskMEDIUMMedium riskLow riskLOWLOW MEDIUM HIGHLikelihoodFig. 1 3x3 risk matrixThe diagram above is the 3 x 3 matrix which is the simplest form of risk matrix. It has High, Medium and Low ratings for both impacts and likelihood shown above. For instance, the highest combination of impact and likelihood give the highest level of risks. These risks are crucial and needs to be treated and fixed as soon as possible. The lower down of the matrix are less urgent. These low risks have low impact and likelihood therefore it is not urgently needed to be treated as fast as the high risks.

Task 3 – Data Protection (2. 2)

GANT has an increasing number of members over the years and because of that it is an appropriate time to take a step on registering with the information commissioner which means complying with the requirements of the Data Protections Act 1998. Data Protection Act 1998 provides proper

protection and process personal data. The Data Protection Act 1998 came into force in March 2001, replacing the Data Protection Act 1984. (Information Commissioner's Office, 1998)The EU Data Protection Directive (also known as Directive 95/46/EC) is a directive adopted by the European Union designed to protect the privacy and protection of all personal data collected for or about citizens of the EU, especially as it relates to processing, using, or exchanging such data. (Rouse, 2008)

AIMS

The Data Protections Act’s aims are providing individuals with important rights, including the right to find out what personal information is held about them. It is also to make new provision for the regulation of the processing of information relating to individuals, including the obtaining, use or disclosure of such information. The other aim is to protect the rights and privacy of the individuals and to ensure the data about them are processed with their consent wherever possible. Anyone who processes personal information must accomplish the 8 data protection principles. These are the 8 data protection principles:

1. The information must be fairly and lawfully processed.

It means that we should be informed about which data is being collected and the reason as to why the data is collected. We have to make sure we do not do anything unlawful with the information and ensure that people will not misinterpret about the use of the information.

2. Processed for specific purposes

Personal data shall be obtained only for one or more specified and lawful purposes. It has to state why they want to collect and store information when they apply for permission to be able to do so. If they use the data they have collected for other purposes, they are breaking the law.

3. Adequate, relevant and not excessive

Personal data must only collect the information that is necessary to properly execute its purpose and it should not be kept longer than necessary. Irrelevant data should be properly disposed.

4. Accurate and up-to date

Companies should make an effort to ensure that they do not record the wrong facts about a data subject. It is best to update the data and information regularly and consistently.

5. Not kept for longer than necessary

Organizations should only keep personal data for a reasonable length of time. When the data is no longer needed for its purposes, it must be disposed of securely. To comply with the fifth principle, data controllers should adopt a systematic review policy for personal data and delete information if it is no longer required. You should therefore set up data retention policies and review schedules for different categories of personal data to help you comply with this principle. (McDonald, 2002)

6. Processed in line with individual rights

Data Controller, a person who decides how personal data is processed, deserves the right to inspect the information held on them. If the data being held on them is false or incorrect, they have the right to change the particular information.

7. Secure

Appropriate measures should be taken seriously to keep the information secure so that they can prevent unlawful and unauthorized processing. Adequate steps are needed to ensure that the data is protected against accidental loss and destruction or damage.

8. Not transferred outline the European Economic Area without adequate protection.

This means that if a company wishes to share data with an organization in a different country, that country must have similar laws to our Data Protection Act in place.

Task 4 & Merit 3 – Security Policies (3. 1)

In order to ensure the safety of the organization’s information, security policy and procedures must be implemented to provide effective security. Designing and implementing security policy for user passwords (new and existing users) is one of the first policies that we will evaluate. The purpose of this policy is to protect confidential information and documents and as well as to ensure a consistent steps of security for organizations. The implementation of this security policy can protect confidential information of all associated organizations and individuals. When imposing requirements for

a password policy, there are several issues that are worth taking precautions. It is recommended for a password policy to include policies such as to always use passwords that can be easily remembered. However, it is not best to use the " Remember Password" feature of application programs. Another password policy that needs to be acknowledged is to always use a strong password with at least 8 characters with combination of alphabets, numbers, special characters and upper and lower case letters. This helps decrease the chances of people trying to guess their password. It is not wise to use passwords which reveal the user's personal information and passwords should not be written down and shared over the phone or emails. SETUPThe next policy that we are going to evaluate is the System back up policy. System back up means copying computer data so that it can be used to restore the original data after a data loss. PURPOSEIt is crucial to back up any important information and know what to do to recover data from a system failure. Security policies for system backup are such as to ensure files are not currently in use during a backup process. If the system is in use, the files can change and the backup copy will not be accurate. The other policy is the frequency of back-ups shall be more often based on the mission criticality of the system as threat levels are increasing. SET UPLastly, we are going to evaluate and implement the security policy for removable media. Removable media is a common source of malware virus and has resulted in the loss of sensitive information in many organizations. The purpose of this policy is to minimize and reduce the risk of those sensitive information being exposed and malware infections. The security policy for removable media is that removable media may not be connected to or used in computers that

are not owned by the company without explicit permission. All media introduced to Department of Defense systems shall be virus scanned prior to executing application/ file. SETUP