Free term paper on principles of information security

Countries, England

A brief analysis of CIA Triangle, threat and vulnerabilities, risk mitigation and legislations

Information security and data integrity is one of the major difficulties facing organizations of any scale. One of the frameworks used in analyzing security related problems and solutions are the CIA Triangle. However the constantly evolving threat environment has necessitated a more robust and intellectual method, that can address short comings effectively. Security threats and vulnerabilities are a challenge for organizations, both going hand in hand, with each threat corresponding to a particular vulnerability. Cyber crime legislations provide legal support for organizations in their endeavor for their information security. Cyber crime legislation is however a relatively new and developing field, and countries have their own legislations. These may differ from country to country, in what they perceive as an offense. Risk mitigation and management is an ongoing activity involving risk mitigation strategies and action plans for organizations.

The CIA Triangle

The CIA Triangle is an established model used in identifying problems and necessary solutions in the implementation of security policies. CIA is the acronym for ‘ Confidentiality, Integrity and Availability’ of information, which serve as benchmarks on which the security scenario of an information system is evaluated (Perrin, 2008). Conformity with the CIA criteria is undertaken every time a software application or a computer server is setup, or when access to information or data is provided.

Since the development of mainframe, the CIA triangle had been reflective of the industrial standard with regard to computer security. However the model is no longer able to sufficiently address the requirements of the computer industry, given its constantly changing environment. The three described factors are under constant, new and evolving threats arising from a plethora of causes. These include unauthorized modifications, theft, destruction, intentional or accidental damage etc (Northeastern State University, 2010). These constantly evolving threats and the resulting environment have necessitated a more robust, intellectual method that is capable of addressing these complexities. Another important drawback of the CIA Triangle is the inability to manage information security from a socio-organizational perspective (Kolkowska, Hedstrom and Karlsson). The objectives of the CIA triangle may be relevant for a specific type of organization, but however organizations vary widely in their goals, strategies and culture, which again render the model ineffective.

Threat and vulnerabilities

The security of their data had been an issue of major concern for all organizations (Rosenthall, 2003). Security threats and vulnerabilities are a challenge for organizations with vulnerability being the weaknesses or the absence of security procedures and technical controls. An organization’s information assets are threatened by a hacker, when there are vulnerabilities in the media and systems associated with it. While the threats and vulnerabilities go together hand-in-hand, each threat corresponds to a

particular vulnerability (The Open University, 2012). Some of the common threats and their associated vulnerabilities are:

Careless employees: Untrained employees, malicious employees and those who are careless could be a serious threat to organizations. Employees that could be duped or made to fall prey to engineered attacks are also a threat. Network protection and data protection requires different approach in each case (Help net Security, 2012). Policies and procedures, training and technologies can make a difference to the threat exposure of an organization.

Social networking: Social networking through social media websites has changed the way how people communicate with each other. However these are a serious threat to organizations. Trust is an integral aspect of these websites like Facebook, Myspace, Twitter etc; which however render them vulnerable to identity thieves. These social networking sites are ideal for launching several attacks including spam and scareware. Also the third party applications on these social networks could be prone to attacks, when these are unmonitored. Such applications that have gained the trust of the users, could trick them in many ways.

Mobile malware: Malware is among the highest ranked organizational threat. Malware can be installed on a system by several methods. Although mobile malware is considered a little more than a nuisance, it sometimes grabs headlines. Attackers are focused on attacking the windows systems, mainly through the operating system and third party plug-ins. For instance the

Android smart phone hacking has driven manufacturers to create locked-down Android smart phones.

Code review: The vulnerabilities in applications are reflected by the associated bugs. As attackers often exploit this, developers need to code cautiously to eradicate all security flaws, before the code is integrated into production. Developers however require support to all levels to ensure code quality. Scanning of codes to pinpoint and fix flaws can be achieved by on-demand code review services.

Cyber espionage: Cyber espionage has been a threat for quite a long time. Government organizations and their agencies have been most affected by these incidents. Cyber espionage has considerable implications for the government, and needs to be closely monitored; for instance, the recent cyber espionage involving Iran and other Middle East countries. The Israeli company Seculert has recently revealed that it has identified about 150 new victims of the virus Mahdi Trojan. These viruses are capable of changing their codes to evade detection by anti-virus program (Finkle, 2012).

Cyber crime legislation

Cyber crime legislation is relatively a new and developing field. Nations have their own legislations to interpret cyber crimes and the punishments they carry. Therefore we observe that the legislations relevant to cyber crime differ from country to country. In the US, the legislations relevant to unauthorized records access are covered under Title 18, Part 1 of the US Code. Falling under Chapter 121, Sections 2701 to 2112 are related to stored

wire and electronic communications and transactional records access (Global Cyber Law Database, 2012). These sections and their amendments are very exhaustive and cover all major areas of access including unlawful access to stored communications, voluntary disclosure of records, required disclosure of records, backup, delayed notice, civil action and cost reimbursement.

In the UK, the legislations corresponding to computer misuse and records access are covered under the Computer Misuse Act 1990, together with its sections. While unauthorized access and modification of information is covered by Sections 1. 1 to 1. 3, its jurisdiction is covered under Sections 2. 1 to 2. 6. There are several differences between the US and the UK legislations with regard to cyber legislations. Some among these include:

Defining unauthorized access:

The US legislations under Section 2701a (1) views any intentional access to an electronic communication facility without authorization as an offence. In case an authorization is provided, it could still be an offense if the authorization is exceeded. The offense is punishable when the unlawful access results in obtaining, altering or preventing an authorized access to electronic communications. However in the UK legislations, under Sections 1. 1a to 1. 1c, a person is guilty of unauthorized access to electronic material if he uses a computer with an intention to gain access to data held. The individual is guilty of an offense if the access he strives to secure is unauthorized and he knows it. Thus while the US legislations rules physical entry into the electronic communications facility as an offense, the UK legislations does not incorporate physical access into the facility in its

clauses. In the UK, unauthorized access happens only when a computer is used, therefore physical access into the facility is not covered by UK cyber crime clauses (Global Cyber Law Database, 2012).

Interpretation of authorized access:

The US legislations restricts authorized access, by interpreting an exceedance of the authorization as an offense. However the UK law is silent on exceedance of authorized access. Another important aspect of the US legislation is that it sees unauthorized access to records an offense, irrespective of the fact whether the intruder was aware of it or not, that he was committing an offense. However the UK legislation under Section 1. 1c requires that the intruder must have been aware of the fact that his performance was unauthorized, for it to be an offense.

Punishments:

With regard to punishments for unauthorized access, under Section 2701 b1(A) of the US law, the intruder can be punished by a fine or imprisonment by 5 years or both, in the first instance. For subsequent offenses the punishment is a fine or imprisonment of 10 years, or both. The punishment under UK legislation is varied corresponding to the region of conviction. For England and Wales, it is a prison term of not over 12 months or a fine not exceeding the statutory upper limit. For Scotland, the prison term should not exceed six months or a fine corresponding to the maximum. Thus we also infer that the US views unauthorized access as a much bigger offense compared to the UK.

Risk Mitigation

The main aim of risk identification and analysis is to be prepared for risk mitigation. Mitigation may be defined as a reduction in the possibility of occurrence of a risk event or the reduction of the effect of risk, in case it occurs. Risk management is an ongoing activity involving risk mitigation strategies and action plans. Although some risks can be eliminated or reduced when identified, most risks are difficult to mitigate, particularly the ones having a low probability but high impact (National Academies Press, 2012). A few approaches used in risk mitigation planning are:

Automated defenses to target malware:

For most businesses, the first line of defense is the need to block and eliminate viruses, worms and spyware. These malware including Trojan downloaders require to be blocked at the gateway and endpoint. Anti-malware and filtering software need to be deployed for all e-mail gateways. This can help to prevent spam and malware from reaching PCs of the users. This is facilitated by using a unified threat management appliance (Schwartz, 2007)

The importance of backups:

Data integrity is subject to several threat factors. Human error, both intentional and accidental; and other causes like hurricane, tornadoes, theft etc, can impact data integrity. However the impact of these can be rendered ineffective, if the data has been backed up. By deploying an automated backup software and making sure that the backup data is not located on site, can guard against physical disasters.

Password setup:

Almost all access to systems and devices are based on passwords. Employees need to make sure that they use only effective passwords. Given the fact that many employees use only their names for logins and passwords, it renders it possible for a hacker or online identity thieves to guess it right. Also the possibility of dictionary based automated attacks uses permutations and combinations of thousands of known words, which could possibly guess a password in minutes. Therefore employees have to be taught to form complicated passwords like for instance memorizing a sentence and using the first letter of each word for the password.

References

Finkle J (2012) Cyber spying spreads in Iran after operation blown – researchers. Retrieved from http://in. reuters. com/article/2012/08/29/cybersecurity-middleeast-idINDEE87S07X20120829

Global Cyber Law Database (2012) Computer Misuse Act 1990 Chapter 18. Retrieved from http://cyberlawdb. com/docs/uk/cma. pdf

Global Cyber Law Database (2012) Unlawful access to stored communications. Retrieved from http://cyberlawdb. com/docs/usa/2701. pdf

Help net Security (2012) Top 10 information security threats for 2010. Retrieved from http://www. net-security. org/secworld. php? id= 8709

Kolkowska E, Hedstrom K and Karlsson F. Swedish Business School Information security goals in a Swedish hospital. Retrieved from https://docs. google. com/viewer? a= v&q= cache: RLUp3ONK1nYJ: www. iris31.

se/papers/IRIS31-009. pdf+CIA+triangle+is+outdated&hl= en&gl= inπd= bl&srcid= ADGEESjphWHTswJQVAyhk3sIcM-05TuDNySBDVfFohmoCf_pe5LpgXaaxLvt2SI-QWIEcdR3xHmEn3_TS1Aon4g-9eagsDUkQVQFVPqaDOAVklFBg6igf6s7E3icZdIz5IbNSGTs2Qxa&sig= AHIEtbTQW5YofMO5cyWH-bAlzamzwoBIlA

Northeastern State University (2010). Introduction to information security. Retrieved from http://arapaho. nsuok. edu/~hutchisd/IS_4853/C6572_01. pdf

Perrin C (2008). The CIA Triad. Retrieved from http://www. techrepublic. com/blog/security/the-cia-triad/488

Rosenthall B. E., (2003) How offshore providers ensure data security Retrieved from http://www. outsourcing-offshore. com/opi. html

Schwartz M. J (2007) 10 ways to Mitigate Your Security Risks. Information Week. Retrieved from http://www. informationweek. com/10-ways-to-mitigate-your-security-risks/201806086

The National Academies Press (2012) Risk Mitigation. Retrieved from http://www. nap. edu/openbook. php? record_id= 11183&page= 41

The Open University (2012) Threats and vulnerabilities. Retrieved from http://openlearn. open. ac. uk/mod/oucontent/view. php? id= 397613§ion= 6. 2. 2