Essay on information security

Law, Security

Information security is the protection of information systems and data from access that has not been authorized, from disruption, disclosure, inspection or perusal of the information, destruction or its recording. It is mainly concerned with the maintaining of the integrity of data, its confidentiality and availability of information without regard for form that the data may take; this being electronic data, pint data or any other form of data. Private businesses, financial institutions, health institutions, corporations, militaries, and governments of countries across the world acquire very personal and confident information on people such as employees, certain products, and financial information. If such confidential information from a business that included data on customers, research, products or financial data of the firm fell into the hands of a competitor it would lead to very great losses (Shirtz and Elovici 98). Thus such information has to be protected, this is in recent times becoming an ethical and legal requirement although initially a business requirement.

In the year 2010, there was an increase in insecurity of information and below is a brief record of the threats to information security; malwares were ranked second highest threat to information security for organizations (Shirtz, Sarkani and Mazzuchi 157). They were mainly installed on systems through client-side vulnerabilities of software, it mainly affects browsers. This has greatly helped cyber crime to the extent that it takes more than a billion dollars annually (much more than drug trafficking). In the economic downturn last year many disgruntled employees have tried to exploit the companies they work for, hence malicious insiders has been top of the list of threats to information security. Hacking and data breaches mainly occur

when vulnerabilities in the system are exploited. Thus hackers mainly use third party applications and vulnerabilities of the client's side cloud computing is another source of insecurity of information, although it seemed harmless at first it is a rising threat to information security. Other threats to information security include; carelessness of employees, mobile devices, cyber sponge mostly carried out by governments, social networking, and zero day exploits, and lastly social engineering.

A great information security tool that is commonly used is cryptography. This is a method in which usable information is transformed to a form that makes it impossible to access to anyone else apart from the user that is authorized. Such a process is called encryption. The authorized user of the encrypted information has a cryptographic key which they use to transform the information to be usable again. This is method is mainly used in information security and it helps protect information from disclosure of an accidental nature or without authorization. This is done when the information is in storage or when the data is in transit. Cryptography has been known to have other advantages apart from protecting information; it helps improve the methods used for authentication, better digital signatures, encrypted communication networks and non repudiation. One of the most active users of cryptography is the US justice system. According to the Chief Information Officer at the justice department, Dennis Heretick, the US Justice Department encrypts most of its data even though they use other tools of information security depending on the volume and type of data being handled. The Justice system spends thousands of dollars on training, support and acquiring of product licenses. However when this encryption is handled wrongly and

decryption keys go missing either through loss or theft, the cost is considerably high. When this happened in 2009, 26. 5 million veterans and their spouses had their information exposed (Shirtz, Sarkani and Mazzuchi 163). However the Justice System has been encrypting information for years and will continue to do so. Heretick is very confident with the security of information of the justice system and he says encryption will be around for a long time.

Works Cited

Shirtz, Dov and Yuval Elovici. " Optimizing investment decisions in selecting information

security remedies." Information Management & Computer Security, 19. 2

(2011): 95 - 112

Hall, Jacqueline, Sarkani, Shahram and Thomas Mazzuchi. " Impacts of organizational

capabilities in information security." Information Management & Computer Security,

19. 3 (2011): 155 - 176