Information security overview for managers and policy makers case study sample

Law, Security

[Tutor Name]

Information is an essential asset in the functioning of any business. The information captured, recorded and shared each day precisely defines the business relationships between vendors and clients, along with the basis for an organization’s internal processes and business operations. Protection of this data is as crucial as protecting your money, and needs as much attention and planning (Herold, 2010). Business personnel need to be made aware of information security since it is about safeguarding the critical data pertaining to the functioning of the organization. Information security also pertains to ensuring the integrity of the data on which decisions and transactions are made, its accessibility to the business processes and its confidentiality for the vendor as well as the customers alike (Garrett, 2004). In a move to ensure that business information remains secure and confidential, Bruce Schneier devised a framework of how awareness and perfect sensing about information security can be created. In his article ‘ The Psychology of Security’, Schneier cites that ‘ Security is a trade-off’ (Schneier, 2008) and absolute security is non-existent. To gain security, trade-off is mandatory and one needs to have an in-depth understanding on how security works psychologically. Security can be traded with money, liberty, capabilities or time. He suggests that people must make the best security trade-off keeping in mind the magnitude, probability, and the level of risk being taken; and how urgently cost and the risks can be equated. Through the framework, Bruce advocated that individuals are mostly concerned about the wrong things since their security perception is different from the security reality. They tend to ignore the magnitude of the risk being

taken and worry about the small risks and ignore the bigger risks. In short, security trade-off is subjective in nature (Schneier, 2008). According to Scheiner’s framework, the trade-offs of security is dependent on agenda and power.

It is greatly connected to module one framework. Firstly, module one framework proposes one of the ways used by the government and legal system to provide better security, thereby considering the government or the law as the sole entity that controls the acts of all people. Scheiner's framework indicates the mind as the main part that controls one’s planning of implementation and improvement of security and in which areas.

Unlike module one framework, Scheiner's framework suggests the use of regulatory approaches to attain a complete security. Module one framework considers the legal system to ensure perfect and the required security. It also advises the development of full regulatory framework, solutions to insecurity, nuclear safety regimes, similar to Scheiner's framework (Schneier, 2008).

Seiden, in his speech, refers to the people one needs to trust with their data. For him no one can be trustworthy particularly in this business world. In internet business, since goods are intangible, fraud rates are commonly higher. Companies change their models without prior notice to the public in a move to maintain security. Even the inanimate entities like networks, software and hardware are not to be trusted; many software lead to abrupt system crashes and hardware malfunctioning.

He concludes by saying that that obscurity security technique helps in hiding the frauds of the system from attackers thereby giving maximum protection

to the system as there is no way the attackers will find out.

I strongly believe that openness of source will enhance security in the long run, since opening the source of systems in use will increase their exposure. This will allow all interested parties to access the system exposure, detect bugs and suggest solutions, and increase the overall security of the system and the stored information (Hoepman & Jacobs, 2007).

I still hold my previous views even by referring to Seiden's speech on security through obscurity. The reason for this is that every system has a flaw or a loop hole and assuring that only those people one can fully trust can access the system's functions, the external attackers attempting to hack the system will never be able to do so; hence the safety of the system is preserved (Mercuri & Neumann, 2003). If I was responsible for helping managers create security awareness and proper perception in their organizations, I would propose policies through which no single business activity can be performed without two persons getting involved and these two persons ought to be from different departments. I would also look to employing professional IT experts to ensure that the security software and systems are regularly updated and upgraded; by this I'd make sure the system in use is latest and ahead of the competitors. Furthermore, I would suggest a single central place of storage of crucial data and sensitive information and every person must first receive the manager's authority before accessing that place.

These two frameworks aim to demonstrate how in today's world of sophisticated attacks, how maintaining privacy of information, building

awareness and perfect perception of the information security is all-important.

References:

Schneier, B. (2008). The Psychology of Security. Scheneier. com. Retrieved from

http://www. schneier. com/essay-155. html

Garrett, C. (2004). Developing a Security-Awareness Culture –Improving Security Decision

Making. SANS Institute. Retrieved from

http://www. sans. org/reading_room/whitepapers/awareness/developing-security-

awareness-culture-improving-security-decision-making_1526

Mercuri, R. T., Neumann, P. G. (2003). Security by Obscurity. Communications of the ACM,

46(11), 160.

Hoepman, J., Jacobs, B. (2007). Increased Security through Open Source. Communications of

the ACM, 50(1), 79-83.

Herold, R. (2010). Why Information Security Training and Awareness Are Important. In,

Managing an Information Security and Privacy Awareness and Training Program.

New York: Auerbach Publications.