Belief and culture

Business

The framework suggested by Scheiner on matters of security is that security decisions over and over again are much less coherent than one would make preference. Scheiner purports that security managers should be informed about themselves, their mangers in business as well as their corporate user faction in that they can come up with major security decisions founded on just acknowledged irrational response and fear impressions instead of studying facts cautiously.

According to Schneier (2007), security is indeed a tradeoff focusing on what an individual gets from what he or she gets. Regardless of the consciousness therein, there must be a trade off. Looking at the argument asserted by Scheiner, the risk involved determines what people would use as a security measure. I strongly agree with what Schneier postulates. Scheiner's framework is well connected with the framework suggested in module one as all attempts are made to safeguard losses through risks in a similar manner. Tradeoffs are the main subject in each perception.

Psychology plays a significant role in the process of making decisions concerning acquiring defenses of security. Scheiner bases his argument in human psychology, university research on the manner in which people make choices and on behavioral science. There is a feeling against a certain reality in that an individual could feel secure while in actual sense, there is no security. It is also true that a person may feel insecure whereas in the real sense, there is security (Hoepman & Jacobs, 2007). A primitive brain portion known as amygdala according to Scheiner (2007) feels fear and provokes flight-or-fight reaction.

Despite being faster than consciousness, other brain parts can override it. Neocortex linked to consciousness in the brain of any mammal is however slower although it is flexible and adaptive. Neocortex is designed to function in a way to confront fear as well as making decisions of promoting security. Moreover, the fight in the brain for logical response often functions in ways individuals “ amplify risks that are rarely talked aout, spectacular, immediate, man-made or even morally offensive.” These are just but a few that Scheiner mentions in his description. Risks that are downplayed are those that are common, under human control, rarely discussed, long-term, slowly evolving or affecting others.

Schneier also makes reference to presents people having optimism bias. People tend to have a conviction that they will be luckier than any other person. Research based on psychology shows that the vividly recalled things usually indicate the “ the most horrible memory is most present”. On tendencies of human psychology like anchoring, a mental focus on proposed options that function to manipulate bias in most cases trigger entirely responses which are not rational in the making of decisions (Hoepman & Jacobs, 2007). The framework of psychology presented by Schneier dictates that security managers must realize that the response to risk of security by users and management in stead of them could be extremely irrational.

Bad security tradeoffs are usually made when our reality and feeling are out of strike (Schneier, 2007). Politicians and vendors have been found to manipulate such biases. The advantage security managers who comprehend such human inclinations towards reality and feeling is the fact that they can apply some of well-placed fear of security that will assist in deployments of

security or even make individuals feel better. Reflection on Mark Seiden Basically, security by obscurity is a security engineering principle which tries to provide security through secrecy. Seiden calls for an understanding of individual’s firm assets and plausible threats therein (Mercuri & Neumann, 2003). The risks belong to the owner of the business and regardless of whatever action it is the owner’s reputation on the spot even if the formal liability moved to some other place.

Creating controls of compensation is normally cheaper than preventing them initially. In such instances, the issue of obscurity is thought to be most efficacious. A healthy degree off suspicion could be advantageous. However, this is not enough. Building trust would require verification in order to effectively carry out the process. Independent validation would be very useful rather than relying on self-certification alone.

Open source in my opinion can be a great way of offering security, although there has been criticism in that open source renders the source code to inspection by all people. Both the defenders and attackers, and rational people differ about the critical impact of this condition. The nature of open source like Linux offers an excellent vehicle to spot and at the same time fix vulnerabilities of security. This model compels individuals to write more comprehensible code, and to stick to standards. There is still more that open source can offer in matters of security.

Managers in an organization can build their security awareness and proper perceptions by establishing some policy and succinct process and make verification of the dynamics, cultural appropriateness and the logic in the

policies as well. It is very important as described by Seiden to keep one person who actually comprehends such policies and assist in keeping things clean. Auditing and testing of manual processes and procedures beefs up the efforts. Hiring a consultant is a very crucial step in ensuring high standards of security. The consultant will be there to act like a bad person and offer probable deniability (Mercuri & Neumann, 2003). Security through obscurity could play a very significant role in preventing automatic threats from hard-coded scripts meant to attack particular ports of HTTP and worms.

Managers can also protect their web applications and relevant databases by using various machines for running individual web servers, database server and applications. In conclusion, the operating systems in the individual machines would require testing for vulnerabilities of security and hardened founded on the best countermeasures and practices. Moreover, built-in web-server features of security can be used to handle access controls together with process isolation.