# Future trends in data security and information assurance course work

Business, Company

The future of data security and information assurance is aimed at providing quality services to the right people and at the right time. In recent times, data security and information assurance aims to improve its services to the immediate consumer in the world of business which is currently adapting the internet-centric environment. This means that the internal enterprise is operating with the external enterprise in its service provision- management of its operation and application (Whitman & Mattord, 2011, p. 98). This internet centric environment is advantageous in that it is able to cover a larger system rather than monitoring a small field, and also ensuring that quality services are being provided to its consumers hence ensuring that quality and accurate work is provided.

Data management companies are currently working closely with those dealing in information security. This will help to display a positive image of the enterprise which is useful in exploiting the information security company to its advantage. The information assurance will also be able to link one enterprise with another, providing standard services and also help in data sharing with the other enterprises. For it to be successful in the provision of quality and security to its customer, an enterprise must display some integrity, show some responsibility and be transparent with its consumers. For security purposes and to ensure that there are no errors encountered in the enterprise, organizations are now forecasting to factor in the staff in the enterprise, the surrounding, and the condition under which the staff are working in (Schou & Shoemaker, 2009, p. 375). The management should ensure that the workers remain focused on the set goals and objectives, maintain the security, and ensure that they are consumer friendly.

Still on security, data security and information assurance are expected to focus more on controlling data theft which has been a problem since data sharing started. The main focus here will be on how to identify and deal with botnets set on networks to steal data in real time. It is expected that there may be more security protocols made to try and prevent these botnets accessing vital information about individuals or organizations (Whitman & Mattord, 2011, p. 103). Also to reduce this data loss, data security and information assurance companies will insist more on ethical conduct among its employees to minimize unethical behavior that may result in loss of data.

In future, data assurance is aimed at creating an environment that will enhance people in the enterprise to become innovative, to have freedom, and make their own judgment. The senior manager in the organization will also have the duty to supervise the service being provided by the staff using set boundaries. To ensure that there will be no data leakages within the organization, digital democracy is to be adapted hence ensuring that the organization delivers simple and meaningful services. Changes in climate and the change in attitude of the youth must be put under consideration as recent studies show that they are some of the major challenges to corporate (Reynold, 2009, p. 82).

It is also expected that advancement in technology may lead companies to be inquisitive on an employee's personal life. To this the companies are expected to penetrate more into the employee's social network. This is a good move but however there may be rogue companies that may exceed their mandate in looking for the employee's information. It is hence

forecasted that future trends in data security will aim to tackle this problem through creation of a legal framework for such information to be found. This framework will ensure that the company gets the information required about its employee while at the same time limiting just how far the company can go in its digging for information.

The discussion above shows that future trends in data security and information assurance will be mainly focused on ensuring good customer relations, meeting customer expectations, maintaining integrity, and ensuring data security.

## References

Whitman, M. & Mattord, H. (2011). Principles of Information Security.

Manhattan: Course

Technology.

Schou, C. & Shoemaker, D. (2010). Information Assurance for the Enterprise.

New York:

Career Education.

Reynolds, G. (2009). Ethics in Information Technology. Manhattan: Course

Technology.