Information security continuous monitoring challenges and solutions case study ex...

Business, Management

Continuous monitoring

Continuous monitoring of information systems is a move towards ensuring security of the system. It’s a strategy laid down to track down and prevent possible threats to the system before the risk gets out of hand. It seeks to create awareness of how secure the system is by comparing the efficiency of the system to the expected level. Data on performance is collected and analyzed to make this possible (Vacca, 2009).

Continuous monitoring is an important strategy when viewed from different perspectives. Its main importance comes in that it plays a major role in ensuring proper security controls are adopted and implemented in the system. This is the very first move towards system efficiency, since efficiency and effectiveness entirely depends on how competent and relevant the controls adopted are.

Monitoring systems are also major to decision making processes by the top management of an organization. The data collected and recommendations given after analysis has been done are used to determine what is to be done. These decisions directly affect the well-being of the organization as a whole, preventing many risks that may require so much financial inputs. It from this connection to the financial welfare that makes monitoring a great strategy behind achieving cost effectiveness in organizational running (Vacca, 2009).

The real-time nature of continuous monitoring also lays a major role in achieving cost effectiveness. This is true because it replaces the need for persistent auditing which is costly. It also saves on time, allowing for instant decisions and actions, hence, solving system problems at an initial stage which is easier and cheap to handle.

However, there are numerous technical and managerial challenges facing continuous monitoring. A major challenge is the politics of different frameworks to the concept of continuous monitoring. It so happens that the many information security frameworks have diverse views and guidelines to continuous monitoring. There has, therefore, not been a universally acceptable set of guidelines to achieving this, with each framework seeming right to the people implementing it (Kim & Solomon, 20112012).

Incorporation of the various organizational systems towards achieving a common goal has also been a major challenge to monitoring. These results both from the complexity of the technologies adopted, and lack of competent staff to manipulate them and the diversity of these systems hence difficulty in merging them. Managers and the technicians, therefore, resort into independent use of the systems, making monitoring almost impossible (Whitman & Mattord, 2008).

Related to the above challenge, data and security mechanisms complexity has also been challenging and a barrier towards effective management. Managers fail to understand why monitoring is important, what is to be monitored and when monitoring should be carried out. This therefore makes continuous monitoring seem less important and is constantly ignored. The complex nature of the technologies also makes it difficult, more so because they keep changing (Laudon & Laudon, 2002).

A major solution to the challenges mangers face in monitoring is the need to adopt universally acceptable frameworks. Some frameworks, for instance NIST can only be applicable to federal states, and mostly to organizations based in the U. S. adoption of such a framework, therefore, by a company

based outside the United States my cause much complexity in applying the guidelines and in core-working with other organizations, probably using different frameworks.

Another solution is the need to create organizational awareness on the need to carry out continuous monitoring. Once all people understand this, it will be easier to implement the strategy and to curb possible risks before they impact negatively. This, therefore, will mean hiring competent and IT literate staff, which can manipulate the systems and leverage them to work as one (Whitman & Mattord, 2008).

Risk management faces numerous challenges. Some of which seem simple, but it’s interesting how interestingly complex they can be, when it comes to handling them. One such a challenge is the move towards automation. Complexities that come with automation seem to be defeating the move itself, these include computer illiterate staff that cannot use the systems, how rapidly technology changes and the recently acquired technology is rendered obsolete just before it is fully utilized and the maintenance costs incurred in keeping the systems in place (Miller, 2009).

Solutions to such challenges have been suggested, some of which are equally interesting as the challenges themselves. A recommendation to employ people that are computer literate sounds good, but the time they will take to be trained on use of the systems seems equally equal to that which could be used to train the illiterate staff. Then there is the adoption of new technology that seems to be recurring, each time new technology is adopted, another emerges and is too adopted making this solution a viscous cycle that seems not to end (Miller, 2009).

References

Kim, D., & Solomon, M. (20112012). Fundamentals of information systems security. Sudbury, MA: Jones & Bartlett Learning.

Laudon, K. C., & Laudon, J. P. (2002). Management information systems: managing the digital firm (7th Ed.). Upper Saddle River, N. J.: Prentice Hall.

Miller, J. B. (2009). Internet technologies and information services. Westport, Conn.: Libraries Unlimited.

Vacca, J. R. (2009). Computer and information security handbook. Amsterdam: Elsevier;

Whitman, M. E., & Mattord, H. J. (2008). Management of information security (2nd Ed.). Boston, Mass.: Thomson Course Technology.