SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY

Enterprise Standards and Best Practices for IT Infrastructure

4th Year 2nd Semester 2016

Business case for Dell Company

Name : Perera K. A. U

SLIIT ID : IT13019600

Practical Session : WD (Friday 3.30 p.m. - 5.30 p.m.)

Practical Number : Lab 05

INTRODUCTION

Dell is an American privately owned multinational computer technological company, based in Round Rock, Texas, United States. Dell is one of the leading and largest technological companies in the world that develops, sells, repairs and supports computer related products and services. The company was founded in 1st of February, 1984 by Michael Dell.

Dell sells PCs (Personal computers), servers, network switches, data storage devices, software computer peripherals, HDTVs (High definition televisions), cameras, printers, MP3 players, smartphones as well as electronics built by other manufactures.

Dell is a well-known company for its innovations in supply chain management and E-Commerce, mainly its direct-sales model and its "build-to-order" or "configure-to-order" method to manufacturing and delivering individual PCs configured to customer specifications. The company was a pure hardware vendor for much of its survival, but with the gaining in 2009 Perot Systems, Dell entered the market for IT services. It has since made additional achievements in storage and networking systems, with the purpose of expanding their range from offering computers only to delivering complete solutions for enterprise customers.

Why Dell need an Information Security Management System (ISMS)?

ISMS is a framework of policies and procedures that includes legal, physical and technical controls that involved in process of information risk management in an organization.

Organizations have security breaches and therefore larger organizations have to have an appropriate way to secure their information. Since Dell is a leading technological company in the world, the company need to have a proper plan to ensure the security of their information assets. There are three main security pillars. They are, Confidentiality (C), Integrity (I) and Availability (A). Once someone achieves these 3, it is possible to say the system is safe.

Data and information in an organization is the most powerful fact in their business. Dell also has its data which can be considered as a key asset. Some valuable data and information of the company are as follows.

- Product information including product designs, plans, sketches, patents, source codes.
- Process information including new method, plans, techniques.
- A large number of employee details or the records, since more than 103,300 people are employing worldwide.
- Financial information including market assessments and Dell's financial records like income and revenue details, account records.
- Customer information, including confidential information such as credit card numbers, since there are thousands of Dell customers who are in worldwide.
- Since Dell provides IT services, there can be a set of servers and their details.

And also,

- If the intruders get to know passwords of servers and access them it allows them to pass the company secrets to competitors or the outsides. It will be a major risk. It is result of data integrity failure.
- Stolen customer information such as credit card numbers can harm their customers and they can lose the goodwill of the customers. It is a result of confidentiality failure.

To protect above mentioned details Dell need an Information Security Management System (ISMS). It'll ensure the Confidentiality (unauthorized people can't view their details), Integrity (getting to know unauthorized people have modified the information) and Availability (when an authorized person need the service he/ she will be able to get service) and reduce the risk of losing data.

Benefits of implementing an Information Security Management System based on ISO/IEC 27000 series standards (ISO27k) at Dell

ISMS benefits

Following are the ways that ISO27k ISMS will benefits the organization.

- Securing Confidentiality, Integrity and Availability.
- Improve information security awareness.
- Protects the company's reputation.
- Improve credibility, trust and confidence of company customers / Ensure clients that their information is secure.
- Cost saving by reducing incidents.
- Improve the company's ability to recover its operations and continue the business as usual.
- Have a competitive advantage.
- Prompt detection of data leakage and fast reaction.
- Prevent unauthorized alteration of critical information.
- Reduce staff-related security breaches.
- Meet customer requirements.
- Meet international benchmarks of security.

Benefits of standardizations

- Provides a security baseline- cost saving
- An embodiment of good practices, avoids 're-inventing the wheel'- cost saving
- Avoids having to specify the same basic controls repeatedly in every situation- cost saving
- Allows the organization to concentrate effort and resources on specific additional security requirements necessary to protect particular information assets- cost saving
- Based on globally recognized and well respected security standards- brand value

- ISO27k standards suite is being actively developed and maintained by the standards bodies, reflecting new security challenges- brand value

ISMS costs

ISMS implementation project management costs

- Finding a suitable project manager.
- Prepare an overall information security management strategy, aligned with the company and other business strategies, objectives as well ascISO27k.
- Plan the implementation project.
- Getting the management approval to allocate resources necessary to establish the project team.
- Employ/assign, manage direct, consultant costs and track various project resources.
- Hold regular project management meetings with key stakeholders.
- Track actual progress against the plans regular progress updates.
- Identify project risks in advance.

Other implementation costs

- Maintain an inventory of information assets.
- Evaluate security risks to information assets and prioritize them.
- Choose the suitable way to treat information risks (Either mitigate or avoid or transfer or accept them)
- (Re-) design the security architecture and security baseline.
- Review/ update/ re-issue existing information policies, standards, procedures, guidelines etc… or prepare and issue them new.
- Rationalize, implement additional, upgrade, enhance or retire existing security controls and other risk treatments appropriately.
- Conduct awareness/ training programs regarding ISMS.
- May need to ‘let people go’ or apply other sanctions for non-compliances.

Certification costs

- Evaluate and choose a suitable certification body.
- Pre – certification visits and certification audit/ inspection by an accredited ISO/IEC 27001 certification body.
- Risk of failing to achieve certification at first application.
- Staff/ management time expended during annual surveillance visits.