SLIIT

COMPUTING | BUSINESS | ENGINEERING

Lab Assignment

Business Case for DELL

Gimhana Dewapura

IT13030568

Introduction

Dell Inc. (stylized as **DELL**) is an American privately owned multinational computer technology company based in Round Rock, Texas, United States, that develops, sells, repairs, and supports computers and related products and services. Eponymously named after its founder, Michael Dell, the company is one of the largest technological corporations in the world, employing more than 103,300 people worldwide.

Dell sells personal computers (PCs), servers, data storage devices, network switches, software, computer peripherals, HDTV s, cameras, printers, MP3 players, and electronics built by other manufacturers. The company is well known for its innovations insupply chain management and electronic commerce, particularly its direct-sales model and its "build-to-order" or "configure to order" approach to manufacturing—delivering individual PCs configured to customer specifications. Dell was a pure hardware vendor for much of its existence, but with the acquisition in 2009 of Perot Systems, Dell entered the market for IT services. The company has since made additional acquisitions in storage and networking systems, with the aim of expanding their portfolio from offering computers only to delivering complete solutions for enterprise customers.

Why Dell needs an Information Security Management System?

Dell is a multinational organization with lots of information. Dell also has a centralized server and a huge data farm. So the information has to be protected since the key value of DELL lies within the information. Protecting data means protecting its confidentiality, integrity and availability. Consider the following examples.

Eg : 1. Failure to protect your data’s confidentiality might result in customer credit card numbers being stolen, with legal consequences and a loss of goodwill, customers may leave the company.

2. Data integrity failure might result in Trojan horse being planted in your server, allowing an intruder to pass your corporate secrets on to your competitors. If an integrity failure affects your accounting records, you may no longer really know your company’s true financial status.

As described above having an informtion security management system means that you have taken steps to mitigate the risk of losing data in any one of a variety ways, and have defined a life cycle for managing the security of information and technology within your organization.

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

An ISMS is a systematic approach to managing sensitive company information so that it remains secure. It includes people, processes and IT systems by applying a risk management process.

ISMS benefits

These are the ways in which an ISO27k ISMS will typically benefit the organization.

1. Business managers of the organizations will make informed decisions regarding potential risk and should be able demonstrate compliance with standards and regulations such as SOX, GLBA, HIPAA, DPA to their critical information on regular basis.

2. An ISMS is a defensive mechanism to any APT(advanced persistent threat) to minimize the impact from these external threats of various cybercrime.

3. Informed information security decisions will be made based on risk assessment to implement technical, management, administrative and operational controls, which is the most cost effective way of reducing risk. Highest priority risks are tackled first to attain best ROI in information security.

4. Information security is not an IT responsibility; In general everybody in an organization is responsible for protecting information assets and more specifically business manager. The business manager may delegate their responsibility.

5. Organization will improve credibility and trust among internal stakeholder and external vendors. The credibility and trust are the key factors to win a business.

6. ISMS raises awareness throughout the business for information security risks, involve all employees throughout an organization and therefore lower the overall risk to the organization.

Benefits of standardization

1.Provides a security baseline, almost universally required information security controls on which to implement specific additional controls as appropriate – **cost saving.**

2.An embodiment of good practices, avoids ‘re-inventing the wheel’ – **cost saving.**

3.Is generally applicable and hence re-usable across multiple departments, functions, business units and organizations without significant changes – **cost saving**.

4.Based on globally recognized and well respected security standards – **brand value.**

5.ISO27k standards suite is being actively developed and maintained by standards bodies, reflecting new security challenges (such as BYOD and cloud computing) – **brand value.**

ISMS costs

These are the costs associated with the management system elements of an ISO27k.

ISMS implementation project management costs.

1.A suitable project manager has to be found to implement isms.

2.Overall information security management strategy has to prepared.

3.Project implementation planning.

4.Employ/assign, manage, direct and track various project resources.

5.Identify and deal with project risks, preferably in advance.

Other ISMS implementation costs.

1.Preparing an inventory of information assets.

2.Assessing the security risks of the assets, and prioritize them. (eg:- Protection of the centralized server is more important.)

3.Determine how to treat information risks.

4.Conduct training sessions regarding isms for the employees.

Certification costs.

1.Assess and select a suitable certification body.

2.Pre-cerification visits and certification audit/ inspection by an accredited ISO/IEC 27001 certification body.

3.Cost of keeping the standard of company consistent throughout the company.

4.Staff/management time expended during annual surveillance visits.