Sri Lanka Institute of Information Technology

ESBPII

Business case

IT13018474

Hettiarachchi H.A.K.S

Weekday batch

INTRODUCTION

Dell is an American privately owned multinational computer technology company based inRound 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, servers, data storage devices, network switches, software, computer peripherals, HDTVs, cameras, printers, MP3 players, and electronics built by other manufacturers. The company is well known for its innovations in supply 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 need an Information Security Management System?

In a connected world main approaches to security have fallen short. No matter how large or small your company is, you need to have a plan to ensure the security of your information assets. Such a plan is called a security program by information security professionals. The process of creating a security program will make you think holistically about your organization’s security. A security program provides the framework for keeping Dell at a desired security level by assessing the risks you face, deciding how you will mitigate them, and planning for how you keep the program and their practices up to date.

The key asset that a security program helps to protect is your data and the value of Dell’s is in its data. You already know Dell is one of many whose data management is dictated by governmental and other regulations, for example, how you manage customer credit card data. If your data management practices are not already covered by regulations, consider the value of the following:

- Product information, including designs, plans, patent applications, source code, and drawings.
- Financial information, including market assessments and Dell's own financial records
- Customer information, including confidential information you hold on behalf of customers or clients

Protecting your data means protecting its confidentiality, integrity, and availability as illustrated by the C-I-A triangle. The consequences of a failure to protect all three of these aspects include business losses, legal liability, and loss of company

- Failure to protect data's confidentiality might result in customer credit card numbers being stolen, with legal consequences and a loss of goodwill. Lose your clients' confidential information and you may have fewer of them in the future.
- A data integrity failure might result in a Trojan horse being planted in your software, 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 true financial status.

ISMS benefits

ISMS is a system that helps to prevent and counteract interruptions to business activities. It protects critical business processes from the effects of information security incidents, disasters and major failures of information systems and ensures the timely resumption of normal operations.

It is relevant to all organizations, regardless of whether they use stand-alone computers or complex heterogenic network systems. It is applicable to all sectors of industry and business, and not limited to information that is handled by electronic media. It is relevant to any type of information protection, whether in printed format or written on paper, stored electronically, transmitted by post or e-mail, or spoken in conversation.

- Credibility, trust and confidence of your customer
- Greater awareness of security
- Compliance with legislation
- Securing confidentiality, integrity and availability
- Prevention of confidentiality breaches
- Prevention of unauthorized alteration of critical information
- Prompt detection of data leakage and fast reaction
- Competitive advantage - deciding differentiator in contract negotiations
- Meeting international benchmarks of security

Benefits of standardizations

Dell knows security should be managed differently. Their Security software solutions give you the power to protect the organization from endpoint to datacenter to cloud, achieve your most stringent compliance requirements, and transform security to a function of enablement through rapid adoption of new technologies such as cloud, BYOD and etc.

ISMS Cost

These are the main costs associated with the management system elements

- Find a suitable project manager (usually but not necessarily the person who will ultimately become the CISO or Information Security Manager)
- Prepare an overall information security management strategy, aligned with other business strategies, objectives and imperatives as well as ISO27k
- Plan the implementation project
- Obtain management approval to allocate the resources necessary to establish the implementation project team
- Employ/assign, manage, direct and track various project resources
- Hold regular project management meetings involving key stakeholders
- Track actual progress against the plans and circulate regular status reports/progress updates
- Identify and deal with project risks, preferably in advance

- Liaise as necessary with various other interested parties, parallel projects, managers, business partners *etc*.

Other ISMS implementation costs

- Compile an inventory of information assets
- Assess security risks to information assets, and prioritize them
- Determine how to treat information (Re-)design the security architecture and security baseline
- Review/update/re-issue existing and prepare/issue new information security policies, standards, procedures, guidelines, contractual terms .
- Rationalize, implement additional, upgrade, supplement or retire existing security controls and other risk treatments as appropriate
- Conduct awareness/training regarding the ISMS, such as introducing new security policies and procedures[1]
- May need to 'let people go' or apply other sanctions for non-compliance.