Information Security Planning Project

Binod Lamsal

CYB-605-Z6 Principles in Cybersecurity

Utica College

Abstract

Information Security Plans are to be developed and documented for IT applications, as per the Company’s Information Security Policies. This is the paper where I had decided, planned and developed the informations security policies for my organization Holy Cross Hospital.

It’s containing the descriptions of the various security processes for the system, procedural and technical requirements and organizational structure to support the security processes. This plan is also including security requirements and processes for the ‘Life Cycle Support’ of the system.

Before starting any kinds of social security plans the first step starts with the assessment of the risk and it’s performed first.Identifying risks provides guidance on where to focus the security requirements. Security requirements and controls should reflect the business value of the information assets involved and the consequence from failure of security. Security mechanisms should be ‘cost beneficial’, i.e., not exceed the costs of risk. On the same way I had planned and written some Information Security systems in this paper as being the part of my my organization(Holy Cross Hospital).

Information Security Planning Project

**A high-level Security Awareness Campaign To Assist Users In Recognizing And Identifying Social Engineering Attacks**

**Decision Making**

Being the lead for information security management for the part of organization holy-cross hospital the first step in the information security management from my end will be the Decision making. Decision making is one of the vital aspect of the security planning and most of the people easily ignore this step. This is the first step and I am going to quickly decide how the holy cross hospital resources are going to address the information security challenges. Let’s say the company security team is an workshop.In this phase the following things will be done:

1. The information security goals and objectives for the cooperate will be discussed.
2. We will be identified all the attendees of the the workshop and it should includes all information security constituents -- executive management, finance, IT & personal should be considered for the workshop.
3. The agendas will be created how we will be governing the security policies starting from their website, CRM application , email and other security critical informations systems.
4. We will be discussing who will do what action so all our decisions will be totally oriented to the actions before we start doing any planning will be really helpful for executing the things later.
5. We will generate the discussion points, well documented decisions and will be given it to the everyone so most of our team member will have knowledge that’s the department will be doing.
6. The strong agreement should be made with the decided thing at this phase so everyone working with the same phase or different phase will have idea of the things going on.

**A high-Level Plan To Protect Network Resources And Assets**

It contains two phases plannings and implementation and both section were researched and those are as follows:

**Planning**

Once the Decision phase is completed, project planning can begin. In the best of worlds, planning can be done on the back of an envelope, with little risk to either the organization’s security or its business. In other more complex cases, detailed plans will have to be developed to manage project risk. For my organization, there are the several sectors where plans should be done and at first, we need find out what IT services the company is using and here are the different aspects of it.

* Website Files and codes
* Website Database
* CRM application
* Hospital management software
* Email management
* Employee Information system
* DevOps

The next step in the planning include establishing the management committee for the plans of the information security projects, creating the oversight committee, Accessing the important business section of the organization, planning on the budget for the information security, carrying out the risk assessment, Developing the security architectures from the network and IT component level, Evaluating the solutions of the information security from the latest technologies through each and every component of the organization. And in the holy cross hospital what had found out after doing the brief research on the company budget and the management committee ideas here are the list of plans presented:

* Securing the main website of the hospital from the development level includes the code checking, secure software development tools, secure coding practices such as input validation, separation of concerns, and single access point input validation etc. This starts with the DevOps for different arrange of developing, staging and testing and production servers.
* Database security checking, analysing the DB schema and the administration frame it's using like MongoDB with plain text is very less secure and includes lots of security loopholes.
* Cross-checking the website administrator password strength and forcing all employees, patients, doctors etc using the website and applications to change their password in each month.
* Password storage awareness for different roles of organization
* Payment and purchase history information security and penetration testing on the website
* Strong firewall setup with the server and cross-checking what is going out from which port.
* Strong SSL certificates for TLS encryption
* Antivirus solutions for the hospital computers and computer operators.
* Update the operating system and applications program at each level of the organization
* Create a program to force change password for each application and the websites we are using.
* Securing the mobile devices of the employees
* Strong backup plans
* Regular supervision and penetration testing
* Access logs and bot deletion to the sites and applications.
* Creating the strong alert system like network & website monitoring tools
* Better email management
* Educate the employee about the information security
* Plan for the attacks and incidents report system.

**Implementation**

This is another phase of the high-level plans were are going to implement the plans those were discussed above most of the important aspects of the plans have clear options for the implementation so I am going to discuss on some of those which generally need more detail explanations.

**Password Management**: This is one of the vital aspects of information security as these days lots of data breaches were happening because of information being stored in the plain text. Attackers can use malware or ransomware to target those plain text password through the email of the organization that's why better password management come to the important aspect of the organization, we need to use the updated tools that are available in the latest tech.

**Email Management:** Another important aspect is Email management and I already mentioned lot's of attackers are using emails as the option of the target so I am going to talk about how we can secure email management within the organization and especially with the holy-cross hospital.

* Getting better cloud anti-spam software like Everycloud, Proofpoint etc.
* Add encryption and archiving, continuity in the email management technologies.
* Setup an email monitoring tool like mail flow monitoring so your organization will get an immediate alert if any attacker down the email software within the organization.
* Add Advanced threat protection and web filter as the email security components which will save from the CEO frauds etc.

**Server Management**: It's just another important aspect of the information security component within the website and with the server, everything comes in like the email solutions, website management, DevOps solutions, any CRM and cloud computing software hosted for the organization and so better server management is one of the important information security component. Here I am discussing how we can secure the server in different ways:

* Better firewall management for the server and checking establishing the better IP whitelisting and blacklisting technologies
* Network monitoring tool like New Relic can give real-time information an alerts what going on inside the server.
* Regularly checking if any brute force attack is going on in the network.
* Strong network passwords and regularly monitoring the sudo, FTP and SFTP users
* Checking access logs in regular interval of time.
* Strong server backup management using disk images and snapshots at regular intervals.

**Website And Code Management:**Common security attacks in the web applications come from the XSS, XSRF, Session Hijacking and Direct object reference etc and many more. And another database attack comes from the SQL injection as well. We need to properly follow the best coding approaches to mitigate these loopholes to secure the web application, Being on the side of the information security we can enforce the developers to follow the best practices to do this kind of practices. Mitigating security risks is a web developer's core job. Learn by example how you can prevent script injection, use secure tokens to mitigate XSRF, manage sessions and cookies, sanitize and validate input, manage credentials safely using hashing and encryption etc.

**Explanation Of The Benefits And Challenges Of Securing Cloud Computing Services**

Cloud computing, one the vital aspect of the information technology these days which address an open problem old built-in tradition data centers. It enables the IT generation and provides the main alternatives to the working platforms and it's surrounding tiers. Nowadays there are thousands of cloud computing services starting from the major corporations like Amazon, Google, Microsoft, Yahoo etc and also there are lot's of cloud computing services provides in their mainly being based from the Sass applications. In this section, we are discussing the benefits and challenges of cloud computing services:

**Benefits**

Discussing about the benefits of the cloud computing services it the way of reduced the total cost of ownership because we will single application used by different users and no need to install in the multiple places. It just improves the scalability and reliability than the traditional system. It just helps to manage the collaborative applications like Microsoft word, project management softwares. Despite the improvements in middleware by vendors it remains unnecessary hardware and software tax that greatly complicates application development and deployment, so it’s basically reduce the middleware tax. It also helps applications development in better and faster pace. Because everything is being available in the cloud the end user will have very ease operating with the cloud tools that generally improves the end users computing.

**Challenges**

With having multiple amounts of the benefits it has fewer challenges as well. We need service level agreements to run the cloud-based applications. With hosting of the cloud-based tools in the international way where high availability of the internet and bandwidth of available the country’s important data will be hosted outside of their control so the governmental agencies basically dislike the approaches. The application security comes as the part of the important challenge being hosted in the cloud it could be easily targeted by the attackers and setal the important information from it so security measures comes in front as well in comparison with the traditional system. With the loosely coupled service design more employee training and education are needed to operate the cloud services. For the most of the recent web and mobile applications were dependent upon the API services it’s basically lacking the Query oriented programming which can slow the application. The data is stored in the different server and application running in different we need to maintain both servers appropriately failures to manage it well just disconnects the applications times to times which is considered as the major drawback of the cloud computing tools.

**Holy Cross Hospital Cloud computing examples**

Being specific with my organization here are few benefits and challenges were discussed for the cloud computing services it is using. Here are the two examples:

1. Website backup in the third party software(Code guard)
2. Using Microsoft exchange as the email solutions and third-party anti-spam software

**Website backup in the third party software(Code guard)**:Code Guard is one of the important and popular modern days cloud computing software which can backups the websites and applications of the small companies to the enterprise companies. Using the backup management tool as codeguard for the holy cross hospital there are more benefits and few challenges of it as compared to the traditional way of creating backups in own servers and local computers which are discussed below:

***Benefits***

1. Being a third party backup provider & its main function is to backup the data a higher reliable system is gained.
2. It has more backup functionality than the traditional system like instant restore
3. Easy setup and can get great supports
4. Our local server cost could be generally high than the cloud computing software like code-guard

***Challenges***

* Being hosted in the third party servers our data can be leaked if they will be breached
* Remote backup system if their system will be down we can no longer access our own data backups
* Need to agree in certain level of license and agreement with them

**Using Microsoft exchange as the email solutions and third-party anti-spam software**

Microsoft exchange is one most important and popular email management software provided by the microsoft. And lot’s of small and enterprise level of business were using it. And most of organization are using the anti-spam softwares as well like holy-cross is using Everycloud anti-spam software. Here I am talking about the advantages and disadvantages of using these as cloud computing softwares:

***Benefits***

* It provides better way email management then the way of traditional system
* It has calendar, docs sharing, events etc kinds of features
* We can easily create accounts for our users and it’s out of the best and robust email client.
* Having a good anti-spam software helps to grow business with removing viruses and malware from the emails

***Challenges***

* Having reliable on different service providers for emails our data will be always passing from their networks
* We need to change our MX records of the servers to their Mail exchange servers.
* Causing down of any intermediate system will have company losing their emails.

**References**

Information security planning inside the organization

https://citadel-information.com/wp-content/uploads/2010/12/success-strategy-for-infosec-planning-and-implementation-0801.pdf

Important aspects of information security implementation

<http://searchsecurity.techtarget.com/tip/Steps-in-the-information-security-program-life-cycle>

Modern days techniques for information security checks

<http://www.businessinsider.com/10-essential-data-security-measures-every-business-should-take-2010-6#monitor-diligently-8>

Information security project management

<https://www.projecttimes.com/articles/information-security-project-management.html>

Benefits and challenges of cloud computing

<http://www.jot.fm/issues/issue_2009_05/column4/>