Group Assignment-

Visahl Samson DAVID SELVAM

HTET OO WAI YAN(ECU-10502149)

PHONE TOE KYAW (ECU-10502161)

Lecturer- Gaven Henry

Implementation PLan

CSG3309.2020.TR1.ALL IT Security Management

Contents

[Executive summary 3](#_Toc34589648)

[SCOPE 3](#_Toc34589649)

[Goal 3](#_Toc34589650)

[Vision 3](#_Toc34589651)

[Timeline 4](#_Toc34589652)

[Costs 4](#_Toc34589653)

[SETA program 4](#_Toc34589654)

[Security Education 5](#_Toc34589655)

[Training 5](#_Toc34589656)

[Awareness 5](#_Toc34589657)

[Incident Response Plan 5](#_Toc34589658)

[Data breach 6](#_Toc34589659)

[Preparation 6](#_Toc34589660)

[Identifying and Scoping 6](#_Toc34589661)

[Data Access Security 6](#_Toc34589662)

[Intelligence gathering 6](#_Toc34589663)

[Eradication 6](#_Toc34589664)

[Recovery & review 6](#_Toc34589665)

[Continuity plan 7](#_Toc34589666)

[Business Continuity Plan 7](#_Toc34589667)

[Disaster Recovery Plan 8](#_Toc34589668)

[Organizational Structure 9](#_Toc34589669)

[Implementation for major Tasks in JOHN DOUGH Pizza 10](#_Toc34589670)

[Database 10](#_Toc34589671)

[Physical Security 11](#_Toc34589672)

[Video Recording & Alert System 11](#_Toc34589673)

[Maintain exterior 11](#_Toc34589674)

[Keep valuable safe 11](#_Toc34589675)

[Implementing Security Policies 11](#_Toc34589676)

[Access control policy 11](#_Toc34589677)

[Two-factor authentication policy 12](#_Toc34589678)

[Backup Policy 12](#_Toc34589679)

[Security audit policy 12](#_Toc34589680)

[Incident reports policy 12](#_Toc34589681)

[Conclusion 12](#_Toc34589682)

[References 13](#_Toc34589683)

[**References** 13](#_Toc34589684)

# Executive summary

The report is to plan the implementation addressing to improve the Information Security & Management issues of JOHN DOUGH pizza which is advised to CTO. Starting from the scope and including goals of the report, timeline for implementation, costs, SETA program, implementation for major tasks (implement security policy, etc.), incident response plan, business continuity, disaster recovery plan and organizational structure.

# SCOPE

The scope is to implement the plans with goal, time and cost. These plans contain:

**-Implementation for major task in JOHN DOUGH**

**-Incident response plan**

**-Business Continuity Plan**

**-Disaster Recovery Plan**

**-Revised Organizational Structure**

Implementation for major task will preventing the JOHN DOUGH from happening same fault.

# Goal

JOHN DOUGH pizza planned to achieve this goal within 5 years:

* Maintain the standards chain of pizza
* To grow their business into remote geographic environment
* To apply latest technology system for the efficient pizza ordering and management system with franchisees
* Use the social media to engage the customers interest in pizza ordering
* Boost the level of IT security for the organization and customer with IT security team and R&D team
* Disseminate the pizza ordering service to different regions

The goal of the JOHN DOUGH pizza will be easily to implement with the well-structured organizational structure.

## Vision

* Can give number1 experience in pizza ordering online
* Become #1 name in pizza ordering

# Timeline

Timeline for implementing the secure the IT system will take over 3 months. Starting from March 10th,2020 to June 30th,2020. For the training the employees’ phase, it’s from start to end of the implementation.

|  |  |  |
| --- | --- | --- |
| Implementations | Start Date (DD/MM/YY) | End Date (DD/MM/YY) |
| Web Security gateways and web application firewall | 10/3/2020 | 15/3/2020 |
| Centralize all business operations | 16/3/2020 | 31/3/2020 |
| New Network segmentations | 1/4/2020 | 3/4/2020 |
| Software | 4/4/2020 | 15/5/2020 |
| Secure Database and others server | 16/5/2020 | 7/6/2020 |
| Backup Systems | 7/6/2020 | 14/6/2020 |
| New Security Policies | 15/6/2020 | 21/6/2020 |
| Employees monitoring system & insider threat detection | 22/6/2020 | 30/6/2020 |
| Training employees | 10/3/2020 | 30/6/2020 |

# Costs

The estimate costs for the implementing the secure system is around $187000 US dollar.

|  |  |
| --- | --- |
| Implementations | Costs (Estimated) |
| Web Security gateways (McAfee) and web application firewall (Fortinet) | $22000 |
| Software development | $20000 |
| Secure Database and others server (file server, mail server) | $50000 |
| Backup Systems (Amazon cloud service) | $1000/year |
| Employees monitoring system & insider threat detection (Veriato) | $6000/year |
| Power backup plan – generator (GENERAC) | $5000 |
| CCTV cameras | $3000 |
| Training Employees | $2000 |

# SETA program

SETA program normally employed inside the organization to address and implement information security techniques and training. Inside the JOHN DOUGH’s pizza, this program will be carried out by Chief Information Security Officer (CISO). SETA program is an acronym, briefing the basic security education, training and awareness. It targets the all employees in the organization with the specific program for different jobs and level of technical knowledge.

Purpose of the SETA program is to enhance the level of the security by educating the employee with detailed knowledge. The SETA program will be boosted to implementing the goal the and security needs.

CISO will be responsible for this program and can be done by doing three steps:

1. Security Education
2. Training
3. Awareness

## Security Education

The basic requirement for the technology used organization is Security Education. All the employees and employers need to understand clearly about the basic security measure. This branch of the SETA program is designed to educate members of the organization about why the organization is preparing in the way it has and why the organization responding in the way it does. Members of the organization can gain sight on how the process develops and achieve continuous improvement.

## Training

The training aims to train the member of the organization on how to react and respond to threats in specific situations. All the employees and employees including manager should be trained well because one of the managers in JOHN DOUGH pizza sent an email to entire customers address book without using BCC. Should train them well about cyber security awareness priority, password security training & best practices and train them to recognize phishing and awareness of social engineering and so on.

## Awareness

This section aims to teach the member of organization what is security and what employees should be aware of certain situations. This section offers information about threats and responses.

# Incident Response Plan

Incident response (IR) is the systematic approach to prepare for, detection of incident, incident occurrence, and recovery from a suspected and experienced cybersecurity breach. Incident response plan helps to ensure the effective countermeasure to incidents which can help to protect JOHN DOUGH’s data and reputation. The plan will be estimating the worst from occurring and if happened it will be helping to reduce the damage of incident. The effective incident response plan must be placed to prevent and respond to incident.

To act quickly and professionally while incident is unfolding. We need to implement the response plan with the IR team. IR team must be cross sectionally connected with business and technical experts to be informational and take action on the possible incidents.

## Data breach

### Preparation

This phase needs to ensure the employees to be well-trained and the important (necessary) technology need to be implemented. Data Backup plans must be taken, and the data breaches also must be conducted and evaluate the effectiveness of plan and Computer Incident Response Team (CIRT).

### Identifying and Scoping

The company need to be detecting the security incidents that require the CIRT as soon as possible during the incident by implementing and using the right technologies and tools (e.g. should use Network Traffic Analysis and Endpoint detection of response to detect the suspicious behaviors.)

## Data Access Security

The company also need to find and identify the person who has accessed the sensitive data or critical data and assets, need to know where those data are located and when the data and assets are being accessed. For example, LepideAuditor suite in file server provides the real time information of who has accessed to which data, and what time and changes.

## Intelligence gathering

Intelligence gathering contains threats to prevent the damage and gather the information about the incidents as much as possible. As mentioned above about the LepideAuditor suite, it shows the history of events which took place before incidents and generates several reports and that can use for the legal satisfy compliance requirements and potential legal proceedings.

## Eradication

After the threats to the system has been identified, contained, analyzed and broke down, need to remove the actual threat/s from the network system and reestablish the system framework to a functional. All compromised credentials must be investigated, reviewed and reset.

## Recovery & review

In this phase, all the frameworks and systems are reestablished in the production and need to monitor which they are working functional and showing no signs about the system compromises. Computer Incident Response Team (CIRT) must review overall and documents all the issues during the incidents also include the suggestions for the incident and how to resolve the future incidents.

# Continuity plan

Continuity plan will be conjunction the disaster recovery plan and business continuity plan. A business continuity plan is a strategy developed by the company to continue operations with minimal disruption in the event of a disaster. Disaster recovery plans are more detailed. The plan is recovery plan to restore the lost data that run the business and retrieve plan of failed infrastructure. Disaster recovery plan is like back up plan for the business continuity plan.

The objective of the continuity planning is not to lose the capability of the process, retrieve and protect the information maintained in the case of interruption or disaster resulting in temporary or permanent data loss.

## Business Continuity Plan

Verifying that the business continuity and disaster recovery plans are compelling to guarantee that data handling abilities can be continued normally after an unexpected interference by inspecting the outcomes from past tests performed.

The BC plan will be running with broad plan to keep a business up and controlling in the event of a disaster. It focuses on the business as a whole but drills down to detailed specific situations that create risks for operations.

|  |  |  |  |
| --- | --- | --- | --- |
| Function | Impact if unavailable | Action | Procedures &  Responsibilities |
| Methodologies and client output | Disturb the ability to persuade the clients of capability | Store in the single database and do backup process properly | JOHN DOUGH SYSTEM team |
| Access to email | Cannot communicate with the client  Unable to provide service, | Incorporate to the exchange server with email to reduce the point of failure | Q message team |
| Access to database | Client unable to identify the service and discover the business | Make sure to provide down time warning message | Developer team |
| Access to server | Client unable to identify the service and discover the business | Make sure to provide down time warning message prepare the backup server for the downtime | Developer team |
| JOHN DOUGH’s web portal | Client unable to identify the service and discover the business | Host on the reliable service provider | Developer team |
| 24 hours Network Security | Can happen data breach  Can lead to massive disaster | Search for the unnormal traffic through the network | Security CISO team |
| Physical security | Employees feel unsafe,  Hardware missing | Hire professional security team | Physical security team |

## Disaster Recovery Plan

Disaster recovery focus on the important business process with active counter. Disaster recovery plan can be considered more focused on the specific part of the business continuity plan. This plan is narrowly focused on each data that is core to the organization. This process could involve everything from recovering small data set to the loss of entire data center.  
  
The DR plan will be running outside the network of JOHN DOUGH with the different type of data. Every important data will be collected and backed up with fully mirrored recovery site.

|  |  |
| --- | --- |
| Core process | Backup Strategy |
| IT operation | Cloud Based Backup |
| Customer data | Cloud Based Backup |
| Software data | Cloud Based Backup |
| Logging data | Cloud Based Backup |
| Finance | Cloud Based Backup |
| Website data | Mirrored recovery site |
| Human Resource | Off-site data storage |
| Contacts admin | Digital backup |
| Business Continuity plan | Cloud Based Backup |
| Implementation plan | Cloud Based Backup |
| Maintenance data | Cloud Based Backup |
| Business E-mail | Cloud Based Backup |
| Warehouse data | Cloud Based Backup |
| Tech support (hardware/software) | Cloud Based Backup |
| Contracts | Digital backup |

# Organizational Structure

To achieve the goal of the JOHN DOUGH’s pizza, we need strong organizational structure with new security team which will be working under the CISO.

Share data

# Implementation for major Tasks in JOHN DOUGH Pizza

## Database

Database protection & security plays as an important role in a company. Since Database was breached at John Dough Pizza company in 2012 and all the customers’ orders and sale histories, this make the company more challenge regarding to increase the security of database. Implementation steps for MSSQL database are as follow.

* Put the server in restricted network segment (using VLAN) so that only authorized network traffic can pass to the database server.
* Correct DB installation: MSSQL offers a lot of additional features. By removing the features that don’t need for current system, can reduce the possibility of exploitations.
* Keep updated: MSSQL regularly patch the vulnerabilities and the administrator must always keep updated. This way can prevent most vulnerabilities to attack.
* Restrict DB processes and traffic: MSSQL is sometimes run as an administrator account or local system that allows the database processes which includes full access and command shell interfaces (e.g. xp\_cmdshell). It should be run with non-administrator account with only few privileges. Allow only the SQL traffic to and from designated IPs so that malicious users cannot harm the server and they will need to connect directly to the server from the secure client front end web application.
* Set strong(unpredictable) admin password, monitor the login logging audits, secure the backup data,

## Physical Security

A burglary case was happened, and PC of franchise was stolen in 2012 at JOHN DOUGH Pizza. This phase is also quite important and big challenge to the company. Here are some ways to preventing burglaries.

### Video Recording & Alert System

This is the best way to protect the company property against burglary. Alarm & CCTV camera systems involve the protection of perimeter and area of important objects. Perimeter covers the outside the surface of the building and area protection covers the entire objects inside the building. CCTV technologies are keep improving and can help to record the videos digitally to hard drive and it helps to catch the thief of burglary and may retrieve the properties.

### Maintain exterior

Thieves and burglaries like to work under the darkness, one of the most effective way to deterrence against crime. Trash dumpsters, vehicles and overgrown grass or shrubbery near the building may provide good cover for them. Keeping the tress away from the doors and windows can minimize the hiding places around the buildings.

### Keep valuable safe

Put the large amount of money in bank as soon as possible or in safe deposit box. High value or important merchandise should not be left in the unsecure place during the non-business hour.

## Implementing Security Policies

### Access control policy

Access control policy is one of the most significant policy for every business. To know who access should has to what comes under this strategy or policy. This turns out to be considerably increasingly significant because of the human element who often make intentional or unintentional to occur data breaches. Social Engineering is the biggest threat that organization face today. Role based access control is regularly employed and utilized in enterprises where many roles are only required to have access to functionality which is related to their works or jobs.

### Two-factor authentication policy

By using two-factor authentication in IT system, it can mitigate the security risks of data breach because it denies all the illegal account access. Nowadays, SMS two-factor authentication is not that much secure in many cases. Using TOPT (Time-based One Time Password) & HOPT (HMAC-Based One Time Password) are better options for OPT based two-factor authentication.

### Backup Policy

Periodic Backup whether using Cloud service or External HDDs is very important. Ransomware like Wannacry can encrypt entire data on the infected machines. Most of the people who didn’t do backup would lose all the data and effect the negative impacts for them.

### Security audit policy

Security Events such as account logon, directory service access, account management, policy change, privilege use, process tracking, etc. can be audited. If there is no auditors in JOHN DOUGH pizza company, there are some experts auditors available for hire.

### Incident reports policy

Incident report is used to rescue in the disaster management. JOHN DOUGH pizza company should make the detailed policies about the incident reports and the employees also know how to prevent and handle the threats and situation if happens again.

# Conclusion

Implementing the security problem in JOHN DOUGH is a big challenge, need to spend lots of money. However, this is the best to make return in investment implementation. The implementation is done with the lack of backup systems, buggy and legacy software, no security policies, store customers’ data insecurely and problems with web applications After following the implementation instructions, this would have the best experiencing order pizza and become #1 pizza company.

# References

## **References**

11 Steps to Secure SQL. (2020). Retrieved 8 March 2020, from https://www.upguard.com/blog/11-steps-to-secure-sql

Low, C. (2020). Information security policies every business must implement. Retrieved 8 March 2020, from https://www.cio.com/article/3216127/information-security-policies-every-business-must-implement.html

Murphy, D. (2020). Best Practices for Your Data Breach Incident Response Plan. Retrieved 8 March 2020, from <https://www.lepide.com/blog/best-practices-for->your-data-breach-incident-response-plan/

Web Application Firewall - FortiWeb. (2020). Retrieved 8 March 2020, from https://www.fortinet.com/products/web-application-firewall/fortiweb.html?tab=models-specs#models-specs

Retrieved 8 March 2020, from https://arxiv.org/ftp/arxiv/papers/1606/1606.03528.pdf

McAfee Web Gateway | WebSecurityWorks.com. (2020). Retrieved 8 March 2020, from https://www.websecurityworks.com/Web-Gateway.asp

Tips for Preventing Burglary at Your Business. (2020). Retrieved 8 March 2020, from https://www.amfam.com/resources/articles/loss-control-resources/burglary-prevention-tips-for-your-business

Retrieved 8 March 2020, from https://invenioit.com/continuity/difference-between-disaster-recovery-plan-and-business-continuity-plan/

Retrieved 8 March 2020, from https://www.microfocus.com/media/unspecified/disaster\_recovery\_planning\_template\_revised.pdf

Retrieved 8 March 2020, from https://www.undp.org/content/dam/albania/docs/STAR/Disaster%20Recovery%20and%20Bussines%20Continuity%20Plan.pdf

Fruhlinger, J. (2020). What is a CISO? Responsibilities and requirements for this vital role. Retrieved 8 March 2020, from https://www.csoonline.com/article/3332026/what-is-a-ciso-responsibilities-and-requirements-for-this-vital-leadership-role.html

Incident Response | What is an Incident Response Plan?. (2020). Retrieved 8 March 2020, from https://www.crowdstrike.com/epp-101/incident-response-ir-plan/

Team, I. (2020). A Guide to Creating an Incident Response Plan. Retrieved 8 March 2020, from https://www.incidentresponse.com/a-guide-to-creating-an-incident-response-plan/

User, S. (2020). Business Continuity Planning - Information By Design. Retrieved 8 March 2020, from http://www.ibd-us.com/index.php/services/it-security/ibd-business-continuity-planning

Whitman, M., & Mattford, H. *Management of information security*.