Lecturer- Gaven Henry

Accompanying report

CSG3309.2020.TR1.ALL IT Security Management

Group Assignment

Visahl Samson DAVID SELVAM(10498743)

HTET OO WAI YAN(10502149)

PHONE TOE KYAW (10502161)

Table of Contents

[Executive Summary 1](#_Toc34601505)

[Introduction 1](#_Toc34601506)

[Assumptions 1](#_Toc34601507)

[SCOPE 2](#_Toc34601508)

[In-scope 2](#_Toc34601509)

[Out of Scope 3](#_Toc34601510)

[Asset assessment 4](#_Toc34601511)

[Asset identification 4](#_Toc34601512)

[Asset Evaluation 5](#_Toc34601513)

[Threat assessment 7](#_Toc34601514)

[Vulnerability identification 7](#_Toc34601515)

[Threat identification 7](#_Toc34601516)

[Compromise to intellectual property 7](#_Toc34601517)

[Deviation in quality of service 7](#_Toc34601518)

[Espionage 8](#_Toc34601519)

[Human error 8](#_Toc34601520)

[Information extortion 9](#_Toc34601521)

[Software attack 9](#_Toc34601522)

[Hardware attacks 9](#_Toc34601523)

[Tech obsolescence (outdated technologies) 10](#_Toc34601524)

[Theft 10](#_Toc34601525)

[Threat Evaluation 10](#_Toc34601526)

[Risk Matrix 10](#_Toc34601527)

[Risk control strategies 12](#_Toc34601528)

[Future Research Topics 15](#_Toc34601529)

[Assumption 15](#_Toc34601530)

[Conclusion 15](#_Toc34601531)

[References 16](#_Toc34601532)

# Executive Summary

John Dough Pizza company has several security incidents that have already occurred. The analysis report includes the scope statement, asset assessments, threat assessment including vulnerabilities, threats to a system and evaluation, current IT security issues, concerns for further research, recommendations of IT security programs should be undertaken, including draft of business contingency plans which means incident response plans for security incidents that most likely occurred and disaster recovery plans, budget draft plan (hardware costs, staffing, and training costs, IT technology costs, insurances, and additional research), risk control strategies and residual risks regarding to improve the IT security of John Dough pizza.

# Introduction

This report would provide the analysis of Information Security Management issues of JOHN DOUGH pizza, planning and supporting for it. The implementation plan will help the JOHN DOUGH pizza to achieve spread their business from Perth to the different regions under the franchisee way. JOHN DOUGH pizza aims to control its pizza quality and willing to reform innovative secure online ordering. And linking all the stores in a different region with B2B and B2C web application suite. They want to tighten the security of the web application and prevent the security problems, incidents and breaches from happening again.

# Assumptions

* It is assumed that prices for hardware and software will remain the same throughout the project.
* For weighted factor analysis, in general, it will be calculated for the overall impact since here we need to consider the business perspective the impact is made for 3 objectives.
* It is assumed that Microsoft has been used to host a website and receives 10 GB of new information each day.
* It is assumed that we have access to confidential information of John dough pizza that is required to complete this project.

# SCOPE

## In-scope

The scope of the project is to identify and provide a solution for IT security issues of JOHN DOUGH pizza which is delaying their business goals to achieve. The solution for the IT security issues will be containing addressing the issues, further research and changing the current working IT system for a better situation. The scope of this plan is to create a secure environment for the JOHN DOUGH’s network and system from unauthorized access. Implementing security processes will be carried out by a structured security team which is under CISO (Chief Information Security Officer). Our team will also be structuring the security team for efficient management. IT security risk assessment, the recommendation of IT security programs and contingency plan will be prepared for the security team to be carried out. These actives will be specified in WBS creation to complete the project.

**WBS creation**

**Implementation phase**

1. **Incident Response Plan**
2. **Business Continuity Plan**
3. **Disaster Recovery Plan**
4. **Revised Organizational Structure**

The implementation phase can be divided into four categories according to their approach to the progress of the security of the JOHN DOUGH pizza. For the first phase, we need to prepare a response plan which contains instructions to help IT staff and recover the system from an incident such as cybercrime, data loss and service outages that threaten the services. For the second phase and third phase, we will be developing conjunction with disaster recovery plan business continuity plan. The strategies should be developed to ensure that the JOHN DOUGH can still accomplish its mission and it would not lose the capability to process, recover and protect the information maintained in the event of a disaster that leading to temporary or permeant loss of services. For the final phase, organizational structure will help to clarify how an organization operates and assist an organization from achieving its goals. The organizational structure of JOHN DOUGH will be revised using the organizational chart.

## Out of Scope

**Employees turn over plans**

Employees in IT departments play an important role in the business. Once an employee turns over, it is quite difficult to find a new employee which is suitable for the current work of flows. Strategies for employee retention:

* Hiring Process: Personality is very important. The company must do a to-do list for IT tasks when first interviewing for a new employee and explain the culture of the company. If the interviewee is not fit with one of them that’s mean it’s a red flag for the company. The interviewee also needs to get along with existing employees as well.
* Benefits Package: Should schedule the employees to benefit twice a year or every end of the year, which means give them the incentive to work very hard. Also, build loyalty for the company and good for preventing employees to turn over.
* Acknowledge good work: Recognizing good works need small investments, the company should take the team and make a small party after achieving the goals or milestones and retains the employee turnover.
* Provide Career Path: For the ambitious employees who are looking for a better situation, the company should review the achievements of their work and promote them.

**Power Outage Plan**

There are three stages for power outage plan,

* Before power outage: Firstly, have a plan during a power outage. Check the employees whether safe or not, have emergency kits (first aids, flashlights, ropes, and other basic items), check the backup system and train employees on how to use the generators safely.
* During a power outage: Use Mi-Fi devices to complete the critical tasks for the business. Turn off or disconnect unnecessary
* After power outage: Check the hardware and equipment for damage, turn off the generator in the right and safe way.

# Asset assessment

Asset assessment is a primary and foremost part of the security strategic plan in any organization. It covers a wide area includes business processes, people, and physical infrastructure. The phases included in asset assessment are asset identification, valuation, and categorization.

## Asset identification

The asset identification process involves the process of identifying the assets and classifying them in categories such as people, procedures, Data, Software, and hardware (System devices, and networking components).

For JOHN DOUGH the asset identification as follows,

|  |  |
| --- | --- |
| **Asset Identification** | |
| **People** | * CEO (John Smith) * Mary (R&D Division) * R&D Team 5 people * Dev Team * Support Team 2 people (Delphi programmer, and database admin) * Franchise * Head office staff, * “B2B Technical Support” team |
| **Procedures** | * All the data centrally controlled at head office |
| **Data** | * Sales, accounts, customer databases, |
| **Software** | * Stocker 2000 * B2C and B2B web application suite * Web-based API * Xero Accounting software * Cloud-hosted web site * Node.js, * MSSQL * Pascal and Delphi * VPN links |
| **Hardware** | **Networking –**   * Staff laptops * Development team laptops and servers * Internal ordering server * Main branch computers * POS terminal * Managers’ PC * JOHN DOUGH™ store computer, |

## Asset Evaluation

Asset evaluation helps to identify how much security is required for each of the information assets in an organization. Here in John Dough pizza, each category has been evaluated using 3 criteria they are, impact to profit, impact to brand image, and impact on business continuation.

The score has been given based on how severe the damage would be if the specified information asset has been compromised/exploited. The impact on profit is valued by 40%, the impact on brand image is valued by 40%, and the impact on business continuation is 20%.

In John Dough pizza the people category is highly rated asset. The reasons are, at the end of the day all the systems, and network is handled by them. Also, the secret survey results show that people/employees are not so delighted with the organization and its decisions. Furthermore, according to Verizon’s 2019 Annual threat report (Verizon, 2019), 34% of all the security breaches occurred in 2018 are due to insider threats and the percentage is 6% higher than 2017 and 9% higher than 2016.

The second high rated category is hardware (networking) because the entire John Dough pizza is depending upon the network. It includes business and sales activities. Compromising the network leads to a possible security breach and spoil its recognition. There are several incidents in the past where the entire breaches occurred by compromising the company’s network. A famous breach happened of this type is the data breach of PlayStation in the year of 2011 where the hackers compromised the network and stole the information of almost 77 million users (Thomas, 2011). And here in John dough entire operations depend on their network.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Information asset** | **Impact to brand image (in %)** | **Impact to**  **Profit (in %)** | **Impact to business continuation (in %)** | **Total (in %)** |
| **Criteria (in %)** | 40 % | 40 % | 20 % | 100 % |
| **People (Employees)** | 95% | 95% | 95% | 95% |
| **Hardware (Network)** | 90% | 90% | 90% | 90% |
| **Ordering systems** | 85% | 95% | 80% | 86% |
| **R&D resources** | 65% | 70% | 75% | 70% |
| **Financial data** | 60% | 60% | 60% | 60% |
| **Customer data** | 80% | 80% | 80% | 80% |
| **POS terminals** | 50% | 70% | 50% | 56% |
| **Xero accounting** | 5% | 20% | 10% | 11% |

# Threat assessment

## Vulnerability identification

Vulnerability identification is used to find out the vulnerabilities that can cause an impact on an organization.

## Threat identification

Threat identification helps the organizations to find out the threats that bring risks to them. Information security threats can be covered in 12 categories (Whitman & Mattord, 2018). Threat identification for John Dough pizza is followed,

### Compromise to intellectual property

**Insider threat**

According to the secure survey results, it is clear that the employees are not happy with the management. So, it quite possible that the employee may release the source code, database information, or any other sensitive information that can cause a severe impact on their business.

**Third-party contractors**

Also, considering the previous security incidents it’s clear that there is a possibility for the compromise to intellectual property that might from the third party contractors who are handling specific operations of John Dough Pizza.

### Deviation in quality of service

**Webhosting/ordering system**

Webhosting/ordering system disruption can cause a severe impact on the organizations' review since it’s the method widely used by customers to order from John dough.

**Electricity**

It’s already stated in the case study that the electricity supply got stopped and the UPS was handled only for 30 minutes. Deviation in electricity/power supply causes an impact in John dough business continuation.

**ISP**

ISP deviation would cause server impact on John Dough’s entire system. Because all the John Dough’s work totally depends upon the internet. So, ISP deviation in John dough’s internal network will affect the ordering system and cause an impact in profit, brand image, and business continuation as well.

### Espionage

**VPN**

Since it’s stated in the case study that one of the store’s computers got stolen and it contains the VPN access related things a technical guy can take advantage of it. So, using the VPN access the intruder can gain access to John dough’s network and can cause severe damage to the organization.

**Corporate Espionage**

This situation can happen if John dough’s competitors performed espionage on John Dough’s organization to gain financial, political, or business advantages. If this occurs and the competitors succeed the espionage then they can access sensitive information such as customer database, sales details which results in an impact on business continuation for John Dough’s pizza.

### Human error

Human error is one of the major reasons behind a data breach. According to reports (Hill, 2020) in the UK, 90% of the data breaches are caused by human error.

In John dough, human errors can come from if the employee is unaware about organization security policies, not having enough security awareness where they become a victim of Phishing or any other form of cyber-attacks, error while using any of the John Dough business applications such as Stocker2000, Xero accounting software, or any other software components.

**Employee targeted attacks**

Presently when we look at most of the cybercrimes, they are not targeting an organization’s executive/board members rather they’re targeting low-level employees. Recently in the USA (Lindsey, 2020), it has been found that hackers are targeting the potential employees to spread malware on the organization’s system.

These targeted attacks include Phishing, sophisticated email attacks.

### Information extortion

Information extortion can be happening in several ways. The primary loophole would be through the employee. The possible incidents are the misuse of privileges by the employee, selling/leaking critical organization data such as R&D information to the competitor/public. These acts will cause an impact on business continuity.

### Software attack

In John dough, the software attacks can cause an impact on its revenue. Because all the processes are partially depending upon the website and other software suits. The possible software attacks are as follows,

**Website takedown**

According to statics (Lyne, 2013), everyday 30000 websites are getting hacked. And Most of the websites belong to small size businesses. Took down website is used to host malicious code which will put the organization in the danger of losing their brand image.

**SQL injection**

The SQL injection is one of the famous ways to take down web applications with the help of automated tools like SQL map, etc... This attack lets the intruder extract the databases contain sensitive information that can cause a severe impact to the organisation’s business continuation and profit.

### Hardware attacks

**MSSQL server**

Since it stated in the case study that MSSQL is being used there are several possibilities that the server can be compromised. Several vulnerabilities have been updated with patches (CVE Details, 2019). And new exploits are developed frequently.

**Network**

While seeing John Dough Pizza’s network topology map a possible security vulnerability has been identified. The vulnerability is customer free wifi zone also connected with the franchise network directly which will allow the intruder to exploit the franchise network. Also, franchise BYOD possibly allow threats to take advantage.

### Tech obsolescence (outdated technologies)

**Legacy PHP**

Since John Dough using legacy PHP for their site it increases the security risk. Because it has been reported that (Elena, 2018) running legacy PHP versions makes the site vulnerable. So, this issue causes an impact on John dough’s business continuation.

### Theft

In John dough pizza, theft is another factor that needs to be considered. Because it previously stated in the case study that one of the branch's computers has been stolen and no information about the device has been known.

# Threat Evaluation

## Risk Matrix

The risk assessment has been conducted for John Dough pizza and given below. This assessment based on the likelihood of occurring the vulnerabilities listed in the identification part along with the impact if that occurs and ends with a risk rating. The most important threat category in John dough pizza is compromise to intellectual property where it causes severe impact in all the 3 categories. The second most important threat category is deviation is QOS. Because the John Dough pizza id knowns for its online ordering system so deviation is QOS also cause a severe impact in all the 3 categories.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Impact | | | Colour coding | | | Rating /Score |
| Threat category | Likelihood | Brand image | Profit | Business continuation | Brand image | Profit | Business continuation | (Likelihood x impact) |
| Compromise to intellectual property | Severe | Severe | Severe | Severe |  |  |  | 100 |
| Deviation in QOS (Webhosting, ordering system) | Severe | Severe | Severe | Severe |  |  |  | 100 |
| Human error  (Employee targeted attacks i.e. Phishing, Email based attacks) | Severe | Severe | Severe | Severe |  |  |  | 100 |
| Software attacks | Medium | Medium | Medium | Medium |  |  |  | 25 |
| Website takedown |
| Sql injection | Medium | Medium | Medium | Medium |  |  |  | 25 |
| Tech obsolescence | High | High | Medium | Medium |  |  |  | 50 |
| Theft | Medium | Low | Medium | Low |  |  |  | 15 |
| Hardware attacks | Severe | Severe | Severe | Severe |  |  |  | 100 |
| Espionage | Low | Low | Medium | Low |  |  |  | 10 |

The risk score is the result of risk matrix this score is calculated using the formula Consequences X Likelihood

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Consequences | | | Low Impact | Medium Impact | High Impact |
| Likelihood | High | 1.0 | 10 | 50 | 100 |
| Medium | 0.5 | 5 | 25 | 50 |
| Low | 0.1 | 1 | 5 | 10 |

Low Impact Medium Impact High Impact

# Risk control strategies

The last process in risk assessment is applying relevant risk control strategies. According to NIST SP 800-30, Rev. 1, ISACA and ISO/IEC 27001 (Whitman & Mattord, 2018) the five risk control strategies are,

* **Defend –** Applying controls in place to prevent the vulnerability from being exploited
* **Transfer –** Attempt to shift the risk to other assets, or other organizations
* **Mitigate –** Attempts to reduce the impact by applying effective contingency planning
* **Accept –** Taking no action and accepting the outcome
* **Terminate –** Eliminating all the risks associated with an information assent by removing it

Risk control strategies for the identified threat are given in the following table.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Threat** | **Strategy type** | **Strategy** | **Residual risk (Overall)** | | | | |
| **Liklihood** | **Impact** | | **Sevearity** | |
| Compromise to intellectual property | Defend | * Legal contracts that will allow JDP to take legal actions. * Applying access controls * Using encryption while data at rest | Severe | Low | | Low | |
| Insider threat | Defend | * Usage of employee monitoring software | Severe | Medium | | Medium | |
| Website/ordering system | Defend | * Installing a web security gateway, and Web application firewall | Severe | Low | | Low | |
| Mitigate | * Effective backup policy. If any incidents occur backup can be used for business continuation. | Severe | Medium | | Medium | |
| Electricity deviation | Defend | * Installing UPS/generator power backup to all the systems | Severe | Low | | Low | |
| ISP Deviation | Defend | * Increase the bandwidth service | Medium | Low | | Low | |
| Theft | Defend | * Encrypting the devices would be helpful. So even if it’s stolen none of the information can be taken | Severe | Low | | Low | |
| Human error  (Human targeted attacks i.e. Phishing, Email-based attacks) | Defend | * According to ISO 27001/2 clause 7.2.2 (Pollard, 2019) sending employees to security awareness programs will help them to increase the security awareness that should be followed in the company. | Severe | Medium | | Low | |
| Mitigate | * A good build incident respond plan. Because if one employee makes a mistake then it will affect the entire organization. | Severe | Low | | | Low |
| Human error (unaware of organization policy) | Defend | * Creation of workplace internet usage/access policy (Sans, 2013) and making employees aware of them is recommended. | Severe | Medium | | | Low |
| Information Extortion  (Dealing with databases) | Defend | * Placing web application and database firewalls. * Encrypt the data inside the database (Paul, 2016) * Providing the required privileges only to authenticated employees. (Paul, 2016) | Medium | Low | | | Low |
| Transfer | * Effective logging (Jim, 2012) for databases would be a good choice. Because if something goes wrong the logging will help the incident response plan to trace out the beginning point. | Medium | Low | | | Low |
| Mitigate | * Setting up an effective backup plan (Jim, 2012) would be a choice to mitigate this threat. So, if something goes wrong the backup can be used to ensure the business continuity. | Medium | Low | | Low | |
| Software attacks  (SQL injection) | Defend | * Performing a secure code review (Paul, 2019). It will not only stop SQL injection but also stops multiple web application security issues. | Medium | Low | | Low | |
| Tech obsolescence | Terminate | * The only risk control strategy (Whitman & Mattord, 2010) that can be applied here is replacing all the outdated technologies with latest/updated technology whether it’s a database or firmware. | High | Low | | Low | |
| Theft | Defend | * Implementing surveillance in head office and as well in the franchise stores. Placing CCTV cameras and actively monitoring. * Enabling physical locks on the devices | Medium | Low | | Low | |
|  | Mitigate | * Resetting the credentials or suspending the affected employee’s account would be an effective mitigation strategy. | Medium | Low | Low | | |
| Network | Defend | * Segregation of franchise LAN with the help of VLANS. | High | Low | Low | | |
| Espionage |  | * Placing strict policies against information disclosure. * Training employee about the information that can be shared | Low | Low | Low | | |

# Future Research Topics

**Replacement of current applications/services to new technology/devices**

Before implementing this a detailed research needs to be done regarding the cost and suitability.

**Information classification**

Information classification is a process of assigning adequate security measures based on the value of an information asset. Depending on the organization the classification would either have 3 or 4 types. The most common classification levels are internal, restricted, public, and confidential.

In John Dough Pizza information classification had not been conducted since it requires details research in information assets.

**Physical security**

No research/assessment has been conducted on how the franchise maintains the physical security.

# Conclusion

All the information security management issues have been analyzed and effective risk assessment demonstrated all the issues in JOHN DOUGH pizza company such as insider threats, weak website application system, human errors, information extortion (database), network segmentation and also including risk controls to mitigate those risks and weigh factor analysis. There is also future research for JOHN DOUGH pizza company.

# References

CVE Details. (2019). Microsoft Sql Server: List of security vulnerabilities. Retrieved from <https://www.cvedetails.com/vulnerability-list/vendor_id-26/product_id-251/Microsoft-Sql-Server.html>

ECU. (2018). Retrieved from <https://datagovernance.ecu.edu/wp-content/pv-uploads/sites/2038/2019/01/ECU-Data-Classification-DSC-Approved-20181113.pdf>

Elena. (2018). Legacy PHP Versions Make Your Site Vulnerable - Reasons | FastComet. Retrieved from <https://www.fastcomet.com/blog/legacy-php-versions-makes-your-website-vulnerable>

Hill, M. (2020). 90% of UK Data Breaches Due to Human Error in 2019. Retrieved from <https://www.infosecurity-magazine.com/news/90-data-breaches-human-error/>

Jim, H. (2012). *Setting Up a Database Security Logging and Monitoring Program*. SANS Institute Information Security Reading Room. Retrieved from <https://www.sans.org/reading-room/whitepapers/application/setting-database-security-logging-monitoring-program-34222>

Lindsey, O. (2020). Iranian Hackers Target U.S. Gov. Vendor With Malware. Retrieved from <https://threatpost.com/iran-hackers-us-gov-malware/152452/>

Lyne, J. (2013). 30,000 Web Sites Hacked A Day. How Do You Host Yours?. Retrieved from <https://www.forbes.com/sites/jameslyne/2013/09/06/30000-web-sites-hacked-a-day-how-do-you-host-yours/#53d218d51738>

Paul, I. (2019). Security Code Review 101, How to ensure secure coding practices when doing code review [Blog]. Retrieved from <https://medium.com/@paul_io/security-code-review-101-a3c593dc6854>

Paul, R. (2016). 7 Database Security Best Practices. Retrieved from <https://www.esecurityplanet.com/network-security/6-database-security-best-practices.html>

Pollard, B. (2019). The Guide to ISO 27001 Security Awareness Training. Retrieved from <https://blog.getusecure.com/post/iso-27001-security-awareness-training>

Sans. (2013). Retrieved from <https://www.sans.org/security-resources/policies/retired/pdf/internet-usage-policy>

Thomas, K. (2011). PlayStation Network users reporting credit card fraud. Retrieved from <https://www.csoonline.com/article/2128427/playstation-network-users-reporting-credit-card-fraud.html>

Verizon. (2019). Verizon: 2019 Data Breach Investigations Report. *Computer Fraud & Security*, *2019*(6). doi: 10.1016/s1361-3723(19)30060-0

Whitman, M., & Mattord, H. (2010). *Management of information security* (3rd ed.). Australia: Course Technology Cengage Learning.

Whitman, M., & Mattord, H. (2018). *Principles of Information Security, Sixth Edition* (6th ed.). Boston, USA: Cengage Learning.