IT Security Management CSG3309

Assignment 1 Case Study: John Dough Pizza

Glen TEAKLE

10532981

Due Date: 01/04/22

**Introduction**

John Dough Pizza is a local pizza company operating in Perth. The owner and current CEO is John Smith. The company is a hybrid store model; some stores owned by the company itself, others by separate entities. There currently exists 8 stores in the Perth CBD and surrounding suburbs, with a primary strategy to expand the business and reach more of their market in the Eastern States over the next 5 years.

Numerous security concerns have hindered John Dough’s growth over the last few years however, and the aim of this report is to highlight those areas of concern, discuss previous security breaches and then offer solutions and recommendations.

**Background**

Over the last few years, John Dough has been subject to numerous security breaches, concerns and intrusions. These have involved:

* The John Dough online ordering system.
* Automated stock management system.
* Staff Information access levels.
* System backups.
* Lack of a contingency plan/disaster recovery plan.
* Lack of security policies.
* General low employee morale.

The major cause of security incidents at John Dough appears to be contributed to John’s “Do now, iron out the details later” approach. This has resulted in a backlog of security issues that have gone overlooked, along with an undercurrent of low employee morale, in part due to their lack of involvement in decision making. John has a bold vision for the future of his company, but major InfoSec issues need to be addressed before he can move forward as he has anticipated.

**Project Objective**

The purpose of this proposal is to address numerous security concerns and issues based on past incidents, including which aspect of the CIA triad was breached and what could have occurred in a similar situation. Improvements, solutions and recommendations will be offered and include both short-term (introduced over the coming months) and long-term (to be implemented over the next few years as the business becomes capable) timeframes and are noted as such. These improvements will help improve information security at John Dough, with the goal of ensuring long-term financial gain, business growth and overall greater security posture.

**Project Scope**

This report is to include all communities of interest at John Dough.

Those in the IT field supporting business objectives by supplying and supporting IT. Currently there is a Delphi programmer, a database administrator and a research and development team headed up by Mary (John’s business partner).

Those in the InfoSec fieldprotecting the organisation’s information assets from threats. There does not seem to be specific people currently in this role. The technical support staff are mostly on the road visiting the various franchises, installing and maintaining the IT systems for John Dough.

Those from the rest of the organisation which includesJohn, Mary, remaining staff and any stakeholders with the business.

All communities of interest would ideally share John’s publicly stated 5-year goals which are:

• Grow the business into remote geographic environments.

• Deliver franchisees with the innovative pizza ordering and management systems

• Become the #1 name in online pizza ordering through social media engagement and activities.

To improve security, staff morale, growth of company.

Constraints for this project mostly involve the budget of John Dough, as it is a small business. To fully upgrade the security infrastructure would likely go beyond the affordable boundaries. This has been considered in the evaluation of John Dough.

**Past Security Breaches**

* **Security Breach 1. –** A disgruntled employee deleted all past orders from the central database, which resulted in all sales history being erased.
* **Possible Outcomes –** The employee could have taken a copy of the information before erasing it. If login details were not changed after the breach, the employee could repeat their actions. The business’ sensitive information could have been leaked to third parties (including earnings). Deletion of customer sales records could have affected the future growth of John Dough, with no proof of sales, profit etc.
* **CIA Triad Breach –** Confidentiality, integrity and availability.
* **Security Breach 2. –** A management PC containing sensitive information, including passwords and VPN details, was stolen. No security breach related to this theft has been reported as of current standings however.
* **Possible Outcomes –** This could have easily led to complete unavailability of information if the thief was able to access the information contained on the PC. May have been a disgruntled ex-employee. Also could have led to a confidentiality breach; sharing of sensitive information with third-parties.
* **CIA Triad Breach –** Availability.
* **Security Breach 3. –** A staff member used an automated email script, sending an email meant for presumably one person, but instead accidentally sent it to the entire customer base of John Dough. The contents of the email may have been confidential.
* **Possible Outcomes –** Sensitive and/or private information could have been sent to many customers, including profit information, recipe ideas, information involving the John Dough ordering system etc. Any of the email recipients could have sent the information to a third party, possibly for profit. Extortion/blackmail could have occurred if one of the customers had an unpleasant experience with John Dough and was seeking revenge. Customer could also have been a previous (disgruntled) employee.
* **CIA Triad Breach –** Confidentiality.
* **Security Breach 4. – T**he entire John Dough database was accessed by a partner company working on marketing. There is belief that a copy of the database was taken by a separate employee.
* **Possible Outcomes –** The employee could have taken a copy for their own gain, or to pass on to a third party. The information could have been altered and then copied back into the original database, presumably if the marketing employee still had access.
* **CIA Triad –** Confidentiality.
* **Security Breach 5. –** A power outage caused the shutdown of all operations in all stores for 6 hours. No backup power was installed at the time.
* **Possible Outcomes –** Data stored on PC’s, devices etc. could have been corrupted or erased. There is currently no reliable or consistent backup system at John Dough.
* **CIA Triad –** Availability.
* **Security Breach 6. –** A malware infection was discovered in the system. Keylogging and a remote access tool were installed, and it remains unclear what information was gathered, or how long the malware was running before its removal.
* **Possible Outcomes –** A key logger could have stolen login/password information (see “Other Security Concerns” below regarding employees using same login details). Sensitive information could have been stolen and shared. After the breach, system logins/passwords were likely not changed so remote access is still a possibility. Logins/passwords could have been changed by the individual who installed the key logger, locking out all employees.
* **CIA Triad –**Confidentiality.

**Other Security Concerns**

* Use of legacy application and code which contains compatibility issues. Staff report that this is becoming harder and harder to maintain. Several staff have also attempted to rewrite the ‘back end’ with likely no record of what they have changed.
* The John Dough ordering app has not been updated in many years.
* The entire John Dough database is accessible by all employees with little to no security except antivirus software. Customer credit card details are stored on the database with no encryption method.
* There is currently no contingency plan for future security breaches.
* There is no reliable backup system in place. Backups are currently handled by one person, as required. This does not appear to be consistent.
* Centralisation of all business operations. Issues with this include employees not having a ‘voice’, absence of employee loyalty due to not feeling involved in the decision process. This contributes to the low employee morale at John Dough.
* No backup or security policies in place.
* Poor authentication practices in place when connecting to the VPN; all staff share the same username/password for all related sites.
* There is likely varying thoughts from staff regarding what constitutes ethical computer use, due to different cultures forming their own opinions in this area.

Further to all the above concerns, there seems to be an underlying issue of staff morale at John Dough. Reasons for this include:

* Staff feel that there is too much focus on “what is coming next”, rather than maintaining the reliability and security of existing systems.
* Lack of communication between management and the various areas within the company:

*Corporate Staff –* feel they are uninformed when new processes/technologies are implemented.

*Accounting Staff –* say that the rules for how the franchises are run are forever changing.

*Research and Development –* feel they are given too much work to do based on staff levels.

*Development Team –* areworking with legacy code and ordering systems. They feel the system is becoming harder and harder to maintain. Additionally, loyalties are divided between John and Mary.

**Solution Requirements and Strategy**

The major goal is to improve Information Security at John Dough and educate and train all employees in proper practices to ensure that the CIA triad remains intact. The security requirements to implement this strategy are listed as follows in order of importance.

1. **The introduction of store policies.**

* Staff termination policy – This would deactivate staff logins to allow no further access to John Dough systems. Their login details disabled immediately upon termination, possibly erased from the system entirely.
* Password policy that includes usernames that clearly identify the employee (eg J SMITH) and passwords that must be changed every 90 days.
* Database use policy
* Email policy
* Wireless communication policy (for Bring Your Own Device).

Using the System Development Life Cycle (SDLC) approach will ensure adequate introduction and application of policies, making use of the structure of SDLC: Analysis, Logical Design, Physical Design, Implementation, Maintenance and Change.

Policies will also clear up any varying opinions on ethical computer usage, as they will plainly detail what is allowed and by who. **Short-term solution.**

1. **The introduction of a dedicated Information Security team and IT manager** who would govern all things related to Information Security at John Dough. Recommend this to not be John or Mary, however they must still be involved once all changes are in place, to still have an awareness of their current infrastructure and oversee all changes, policies etc. The current IT staff would be deemed suitable with the correct training on new policies and security measures/contingency planning. As the budget for John Dough to introduce a large IT department is low, this would be the best solution for now. The first concern would be to implement a strategic plan to help achieve a more secure infrastructure. **Short-term solution.**

This will include:

* Acknowledging John Dough’s 5-year plan/business objectives.
* Working through SWOT, (strengths, weaknesses, opportunities, threats).
* Acknowledging John Dough’s overall long- term direction.

1. **Daily backups by IT department of all stores (onsite). Short-term solution.**
2. **Regular backups offsite by IT.** Offsite data storage would allow for recovery after natural disaster occurrences, (fire, flood, storm damage, power outages), theft from break-ins, damage from viruses and would give peace of mind to all employees. **Long-term solution.**
3. **Physical security onsite.** The office containing the management PC must be locked when not in use. Only John, Mary and IT staff to have access. They must have their own keys or swipe cards for the office. They must have their own individual login details that are not shared with others, and these must be logged by the system when accessed each time. The office must be clearly posted as “restricted access” to prevent other staff accessing the database. This is also covered under the use of SETA (see below). **Short-term solution.**
4. **All staff/employees require ongoing training regarding use of technologies.** This includes regular updating of apps and software, regular changing of passwords, correct email safety and etiquette (CC, clicking malicious links, scanning files attached to emails). **Long-term solution.**
5. **An incident response plan m**ust be created, explained to staff, adhered to, and clearly marked and distributed within all branches of John Dough. Also regular ‘refresher’ meetings every 3 months. **Short-term solution.**
6. **A disaster recovery plan** must be created and implemented. **Short-term solution.**
7. **To help improve staff morale** and possible disgruntled employees causing security breaches, it is suggested that employees be allowed to put forward their own ideas for the running of John Dough (ie menu ideas, customer rewards/loyalties, staff incentives, monthly bonuses, social media activities/customer engagement etc). Also, their own suggestions for improving security if any. **Long-term solution.**
8. **Regular software updates and security checks.** Daily malware scans of the John Dough ordering application and entire database. **Short-term solution.**
9. **Update of programs/code being used to maintain the ordering system.** This would include training for the IT department with current tech. **Long-term solution.**
10. **Security Cameras installed in main office/store (CCTV).** Deterrence is the best method for preventing unethical or questionable behaviours. Security cameras are an effective way to enforce this. **Long-term solution.**

**Security Education, Training, and Awareness Program – SETA**

The SETA program is a control measure designed to minimize accidental employee security breaches. SETA programs enhance the general education and training of staff in the field of InfoSec by building on their general knowledge that helps them do their jobs in the most secure manner possible. This will be aided by the introduction of policies.

A picture containing text, indoor, light

Description automatically generated

Chart

Description automatically generated

The **CIA** triad refers to the 3 main aims of Information Security: Maintaining Confidentiality, Integrity and Availability of information to ensure a secure infrastructure.

These are maintained through various means including; physical security (door locks, security guards), communications security (cryptography), operations security (policies) and network security (antivirus). Essentially, any security breach in InfoSec can be narrowed down to a breach in one or more of these key areas.

The previous security breaches at John Dough have involved all 3 of these.

For example, the employee who erased the orders on the database in 2014 shouldn’t have been allowed access in the first place; this was an availability breach.

A breach within one aspect of the triad can easily lead to another, for example:

A stolen login/password (confidentiality) could result in the details being changed (integrity) to prevent the user logging into the system (availability).

Using the threats concerned with John Dough as examples:

The malware that was discovered could have led to an availability breach if the hacker changed login details. This could have led to an integrity breach if website/app/payroll details or any number of sensitive details were changed. Confidentiality would also have been breached.

Graphical user interface, text, application

Description automatically generated

**The 12 Threat Categories to Information Security**

These are the 12 major threats in InfoSec that a business needs to be protected against. The threats coloured red in the above diagram are those that have already occurred, to some extent, within John Dough. Details below.

**Compromises to Intellectual Property** – Refers to the malware that was found, the marketing employee that copied the database and the stolen PC.

**Espionage or Trespass** – Only those persons authorised to access sensitive information should have access. These people should be known by all employees; they should have their own access (user/login) and any outside person who attempts to gain access/copy files etc should be locked out and the attempt logged in the system to be investigated.

**Forces of Nature** – Data needs to be protected in 3 key areas: in storage, in transmission and in use. Backups should be completed daily onsite, and at an offsite location. Having backups in 2 areas will give you peace of mind and allow for quicker recovery after an incident.

**Human Error or Failure** – Ongoing staff training is required for use of technologies, email and password policies, multi factor authentication, accidental erasure of files/emails, reading of confidential emails.

**Software Attacks** – Malware is extremely dangerous when left un-noticed. Behind the scenes damage can be ongoing. A key logger can steal all your passwords and they can be used to access your system remotely. Daily virus scans and system/software updates will help in preventing this from occurring again.

**Theft** – In case of theft, data needs to be protected to make it harder for the thief to access. This includes encryption, regular changing of logins/passwords. Any room/office that houses PC’s/devices must be locked and only authorised employees are to have access via keys.

The remaining threats that could occur without proper security measures being implemented are the remaining threats in black in the above diagram.

A picture containing text

Description automatically generated

**Policies**

The introduction of policies will help to protect the business against employees doing the wrong thing (deliberately or accidentally) and ensures Management can enforce rules regarding behaviour and procedures.

Different cultures have varying opinions about what constitutes ethical behaviour regarding private information (ie password sharing). The introduction of an ethics policy for example will help ensure all employees are on the same page regarding the ethical nature of John Dough.

The introduction of several other policies will help define:

* What employees can/cannot do
* How they should conduct business
* Standards, expectations and consequences

These must be made readily available to all employees: physical, digital, posted on walls etc. Employees must read, sign and adhere to them.

Information Security is the responsibility of everyone, and people are the most critical link in InfoSec.

**A person with the hand on the face looking at a computer

Description automatically generated with medium confidence**

Currently at John Dough, employees are confused and divided in their loyalties. This confusion can lead to anger, and disgruntled employees can take advantage of the business, (as already happened in 2014 when the database of orders was erased).

Rushing of technology, ideas (proof of concept) can lead to unfinished tech with bugs, resulting in unhappy customers/staff who must deal with them.

A picture containing food, indoor, dish, pizza

Description automatically generated

Analysis has been completed on John Dough’s security infrastructure. What follows is a list of key areas that need to be overhauled and/or implemented. These improvements offer both short-term and long-term solutions. The low-end budget has been considered.

Store Policies

Dedicated IT Security team/manager

Backup plans

Contingency plans

Incident response plan

Disaster recovery plan

Onsite security (including CCTV)

Staff training

Technology updates and regular security checks

**Conclusion**

The overall security posture of John Dough will be greatly enhanced following these recommendations. Staff will have a clearer indication of how to deal with incidents and work more securely. They will feel more assured, and thus employee morale will improve. Customer records and business records will be secure and safe. Policies and plans will further help contribute to maintaining Information Security at John Dough.

**References**

Inc., C. E. (2015). Centralization. [https://corporatefinanceinstitute.com/resources/knowledge/strategy/centralization](https://corporatefinanceinstitute.com/resources/knowledge/strategy/centralization/)

Shanley, L. (n.d), CSG3309 Introduction to Information Security Fundamentals: Module 1 [Lecture notes]. Canvas. https://courses.ecu.edu.au/

Shanley, L. (n.d), CSG3309 The Need for Security Threats to Information: Module 2 [Lecture notes]. Canvas. https://courses.ecu.edu.au/

Shanley, L. (n.d), CSG3309 Legal, Ethical and Professional Issues: Module 3 [Lecture notes]. Canvas. https://courses.ecu.edu.au/

Shanley, L. (n.d), CSG3309 Governance, Strategy, Policy and Planning: Module 4 [Lecture notes]. Canvas. https://courses.ecu.edu.au/