COMP7330 Assignment 1

Student Number: 15451682 Student Name: CHEUNG Saiho Program: MSc AIS

Question 1

Google e-mail cloud system, provide e-mail service for many business companies, academic institutes and personal. It is a software as a service (SaaS) of cloud system model which is provided the wide range of application services for all users, instead of e-mail service only. E.g. calendars, file storage, office productive software and collaboration service, it has synchronized the directory service [LDAP, Active Directory] of user accounts Gmail service, implementation of single sign on mechanism.

Risks concerning: virus and malware infections, sensitive data leakage, network attack such as DDoS and man-in-middle, natural disasters which is interrupted e-mail service, prevent receiving of inappropriate e-mail which is contained the spam and bad content.

Countermeasures:

- virus and malware infections → install anti-virus software and update virus definitions files frequently for scanning files when users have uploaded their attachments in e-mail.
- sensitive data leakage → implementation of data encryption techniques, e.g. password field using MD5 encryption in database
- network attack → implementation of intrusion detection system and secure service layer tunnel, encrypt data transaction, hackers cannot break the system easily.
- natural disasters → e.g. earthquake, typhoon, water flooding. Need to facilitate the backup site in difference locations and places, implementation of failover service to distribute network request to difference group of servers
- prevent receiving of inappropriate e-mail → implementation of content filtering system and blacklist some known spam e-mail servers, if the cloud system has triggered some bad content in e-mail, such as gambling, pornographic and terrorism, the system should be removed them automatically.

Question 2

according to this case, it is mainly focused on the operating security control strategy which is involved to purchase IT assets for the whole corporation, including hardware and software. as the chief internal auditor has investigated that all purchases have not approved by top management and no department has managed IT system design and allocated the computer resources for each subsidiary in centralization. it has used over one million dollar for purchasing, but most of purchases has involved small expenditures and occurred for the last three years by individual. there is a big problem for financial auditing and lost of control in expenditures.

operating security control:

- operational procedures and responsibilities, need to establish information system department which is separated responsibilities for each roles, what kinds of related to IT system design and purchases has managed in this department. for example, segregation of duties that employ the system project manager and quality assurance manager, monitor project development process and IT activities for the corporation. actually all subsidiary purchases and system development request must be approved from IS department.

advantage: good financial planning and budget control during checking period

disadvantage: high operation cost when establish new department.

- third party service delivery management, the controller has concerned which user developed systems are potential impact on operation, there may need third party service to outsource and evaluate the manufacture work flow when the service company can provide some professional IT system solution and design.

advantage: release human resources for internal and exploit latest IT technology which is provided by service company.
disadvantage: risk of leakage manufacture critical information to other companies.

- system planning and acceptance, according to IT assets purchases, need to consider the requirement of project future capacity and demand.

advantage: appropriate IT assets planning for implementation of project capacity and decrease to purchase redundant the hardware and software.
disadvantage: need to spend time and extra human resources doing proposals, investigate project capacity requirement for all subsidiary, complex process and training for system acceptance.

physical control:

- physical lock and badge system, need to protect exist IT assets, total over one million dollar. restrict authorizing staff for accessing only

advantage: easy to monitor usage record for these IT assets, prevent loss and damage case for unauthorized person.
disadvantage: increasing operation cost regularly, such as change key lock and update badge system when the staff has left out.

Question 3

1. GitLab database erased accidently, prevention smart phone cold call apps with leakage personal phone book information to 3rd party public database, fake Google e-mail portal for collecting login information illegally
2. Pleased find my e-mail and attachments to Dr Fion Lee on 1 March

Case [1] http://technews.tw/2017/02/03/gitlab-com-database-incident/
Case [2] http://hk.apple.nextmedia.com/realtime/news/20161121/55944339
Case [3]
https://hk.news.yahoo.com/%E9%BB%91%E5%AE%A2%E5%81%87%E5%86%92%E7%86%9F%E4%BA%BA%E7%99%BC%E6%94%BE%E4%BB%BF%E9%9B%BB%E5%AD%90%E9%83%B5%E4%BB%B6-%E5%B0%88%E5%91%83gmail%E7%94%A8%E6%88%B6-145900507.html
3.
Case 1, weakness: segregation of duties that single system administrator has the top of superuser access control right, cannot avoid to execute the erasing command and recovery deleted data in filesystem for wrong decision making, solution: need to facilitate two system administrators, if executed the critical command, need to double confirm from other system administrator, e.g. rm -rf.
Case 2, weakness: leakage over 3 billion personal mobile phone number on public database without authorization when users have installed the prevention of cold call apps, solution: the apps program design should be encrypted phone number to store in database and does not synchronized this record in public database.
Case 3, weakness: hackers have stolen a large set of user´s Gmail login information very easily, retrieve many private data via these accounts illegally, such as e-banking financial report, home address etc. solution: Google has

notified the e-mail user and require to change login password immediately when the e-mail account is detected abnormal activity via sms, such as login different country, input wrong password many times frequently

4. in these three cases have mainly involved the logical control, including system access right, security mechanism and program logic design. nowadays, most of mobile apps, network service data have stored in database for cloud system. It is very high risk without good logical control, the storing data would be leakage or loss, so the strongly encryption algorithm, system security policy are extremely important for the web-based computer systems, or even the public cloud system. Users have responsibility to consider which kind of information and apps could be used and sent on public cloud system.