Risk Analysis for (4) organizations

* **Common Wealth Bank and Bank of China**

Out of the consideration that these two banks are quite similar except their client source, we simply combine the risk analysis process of these two.

The objective and constraints are looking for a best balance between the security achieved and the corresponding cost.

The relevant stakeholders are actually quite complex, to simplify, we only consider about the bank itself, its clients and the government. Its assets include currency, stokes, insurance, credit and all kinds of financial products, the huge information storage of its clients and even some secret information of the country. The value related with assets not only refers to its all kinds of possessions, but also its power to influence the whole country’s economic and financial market and in some content, the decisions of the government. The harm could be theft towards client information causing the loss of money and also the loyalty of customers, wrong data access leading to the crash of the system, some crucial data exposure doing harm to the reputation and perhaps fines from government, data update delay decreasing the efficiency.

Possible threats include environment accidents and mostly attacks. Vulnerability includes its power supply, networking facility, storage media and automated process, also with involved human work.

Existing safeguards cover wide ranges, from physical to digital. Common ways are maintaining security, net channel encryption, access control, firewall and anti-malware software.

So in general, the risks banks are facing may come from both the real world and the digital world. Those digital ones include malware attacks, database theft, system crash and so on. Risks from humans mainly focus on theft and Malicious Fraud.

Hence, as described above, risks caused by environment accidents and most natural factors are inevitable and out of the control of these two banks’ access control systems. Generally, the bank access control system enables to address the risks of most human attacks such as malware attacks and database theft by some hardware like exchange machine. However, when the system has a new vulnerability which is found and utilized by hackers, the risk is still existing and ineluctable. (Securelist.com.,2016)

* **Apple Inc. and Google Cloud Platform**

Different from banks, Apple and Google are two most influential Internet companies around the world. Though their business could be different, for the convenience of analysis, here we just combine them into one.

The objectives and constraints should still be a balance.

The relevant stakeholders should be the company itself and its clients. Their assets not only cover all their physical possessions, the huge database of their clients, more importantly, but their core technology patents. The related values include their market capitalization, market occupation rate, future outlook which may directly influence the confidence of investments and also the reputation. Some possible harms could be directly data loss, core technology disclosure, wrong client access leading to the mass of the platform and all kinds of server crash.

Their vulnerability mainly relies on the quality of their system design, algorithms and also hardware. Work staff capability and physical environment setting up also count. Most threats may come from digital level, including all kinds of attacks from hackers and the original flaws of their products.

We mainly care about safeguards on the digital level. It could be special algorithm or mechanism for ID verify, patches for system loopholes, channel encryption, digital signature, database management, firewall and so on.

As technology-based companies, they will face risks and challenges from both outside and inside. Outside risks appear like attacks from hackers, theft aiming at their database and even their technology secrets, those trying to gain illegal accessibility and so on. Inside parts cover original design loopholes, algorithm out of date, system crash, file backup loss and so on.

Therefore, different from banks, the Apple Inc. and Google Inc. may reinforce the protection of software aspect. As technology-based companies, they may face more risks by hackers due to more computer vulnerabilities, increasing attention and usage rate by people. However, for users, except the natural and companies’ internal reasons (like the server is attacked), they primarily enable to address generic risk including Trojan virus to steal the account information unless they download files from unknown website or browse the risky website. (Kaspersky Lab United States., 2016) It is well known that Trojan virus is the most significant reason for people to lose account information and money online. (Usa.kaspersky.com., 2016)

References:

1. Kaspersky Lab United States. (2016). *Online Banking Theft | Kaspersky Lab US*. [online] Available at: https://usa.kaspersky.com/internet-security-center/threats/online-banking-theft#.Vz2ydBJ96CQ [Accessed 19 May 2016].
2. Securelist.com. (2016). Software vulnerabilities – Securelist – Information about Viruses, Hackers and Spam. [online] Available at: https://securelist.com/threats/software-vulnerabilities/ [Accessed 19 May 2016].
3. Usa.kaspersky.com. (2016). What is a Trojan Virus | Malware Protection | Kaspersky Lab US. [online] Available at: https://usa.kaspersky.com/internet-security-center/threats/trojans#.Vz2zdRJ96CQ [Accessed 19 May 2016].