**Access control:**

The Internet industry has advanced dramatically and brought a large number of benefits for people over the past 20 years’ development. On the other hand, this situation may result in some harmful network threats. For instance, phishing, man-in-the-middle, man-in-the-browser and insider fraud. (Commonwealth Bank, 2016) In this case, almost each bank reinforces its access control system and firewall system in order to avoid the loss of property of accounts and companies at utmost.

**Commonwealth Bank:**

Commonwealth Bank is the most representational bank to illustrate the access system in the Australia. It is well known that a standard protect system at least includes these 6 features: comprehensive, flexible, agile, universal, portable and reliable. (Commonwealth Bank, 2016) The CommBiz and the Netlock, created by Commonwealth Bank security department, satisfy all 6 requirements above.

* CommBiz

CommBiz system provide each account with a unique user name and a unique token (unique PIN or password). When an account is logged in the inactive or a new region, it need 2 steps checking. That is, not only the password to log in the account, but also the four or six digits PIN from SMS. In addition, the CommBiz system offer the user permissions service. Users can set up the access hours which means this account cannot deal with any transactions out of the hours defined by the user. Moreover, users can use account permissions and account authority service to authorize some users can view and transact the account, the quality relies on the size of the transaction. Lastly, there are some other services are not for users but belonging to transaction access control, such as Payment restrictions which is used to guarantee users can only transfer money to the existing account.

* Netlock

Netlock is an innovative device like an USB which uses public key infrastructure and digital certificates to ensure the security of transaction. The netlock has a lot of plugins for different Internet browser. However, due to the difference of computer systems, the Netlock is available in the Windows system for people to use. In the future, when the Netlock become popular, it will no doubt increase the safety factor for accounts.

Overall, these 2 methods actualized by the Commonwealth Bank diminish the security risk of the account to a certain extent. Nonetheless, when someone steals the phone which is installed Commonwealth Bank APP and receives SMS from it. He can transfer money to his own account arbitrarily by overleaping the access control because the phone and the bank account only identify whether the password and PIN is correct or not. This is the weakness of the access control system of the Commonwealth Bank.

**The Bank of China:**

As well as the Australian Bank, the Bank of China also designed a security system to response to the Internet attack.

In order to increase the security, the Bank of China designed a deployment plan of the access stratum 802.1x, coordinating with some exchange machines. In addition, the network department of the Bank of China deployed a network management platform which is used to monitor the network devices and illegal attacks by referring the flow data provided by exchange machines.

Certainly, these designs and services benefits users ultimately. The exchange machines which are mentioned above, constitute a protect system called EAD. When users try to log in the Bank of China online, the EAD system will trigger the McAfee antivirus software and WSUS patch management system and monitor the illegal attack behavior and Trojan virus together to ensure the user is in the safe environment. (Bank of China Australia,2016)

The entire enormous system considers many computer vulnerabilities and plays a significant role in protecting users’ accounts indeed. However, the cost of the preinvestment and the maintenance are not a small number.

Not only many banks design protect systems to increase the security of the accounts, but also other famous companies.

**The Apple Inc.**

The Apple Inc. provides the well-known 2 steps verification services (apple ID and touch ID) to apple users, whichever device you use, from iPhone 5S to MacBook. (Apple, 2016)

Especially for iPhone users, it offers a lock screen function which people must type the correct passcode to use the phone, otherwise the phone will keep locking until the right passcode. For iPhone 5s and newer devices, the Apple Inc. has added a fingerprint unlock function called the touch ID instead of the traditional password lock which is more convenient for using. Meanwhile, when the phone is stolen or lost, people who stole the iPhone or pick up it will not activate functions of it. Cooperating with the Find My iPhone functions, the careless owner might find what the last location of the phone is before it powers off. The cooperation of these two services rise the possibilities of getting back the lost phone. (Apple, 2016)

Interestingly, the Apple Inc. particularly create the Swift Program Language to reinforce the security of APPs in OS and iOS System.(Developer.apple.com.,2016) APPs used the Swift Language will be simplified and with less computing vulnerability.

Overall, depend on the rigorous OS and iOS system, the Apple Inc. always plays a leading role in information security. However, when an iPhone is stolen, the thief can destroy the data in it by restoring factory setting. Although bank accounts or other important user names and passwords are invisible for the thief which avoid terrible result, the phone cannot be got back due to the destroy of the location information.

**The Google cloud platform.**

The Google Inc. developed the cloud storage technology in the early days. Hence, in the access control aspect, it takes a leading position in the world. Meanwhile, the method Google used is adopted widely by the leading software companies in the world. In the Google cloud, the access control is demonstrated in two patterns. (white list & limited files) (Google Cloud Platform., 2016) First, users set the white list to decide who or which range of users enable to visit, modify, download and delete the files in your Google cloud. The other one is sharing the time-limited files which means a user cannot visit or do other operations after the setting time.

Although Google consider the access control comprehensively, users in the white list may download the files, modify them and upload to their own Google cloud. Then they forget to set the limit or open limits of authority deliberately. This situation will lead to the failure of the pattern 1 and pattern 2. Therefore, the Google cloud access control depend on the trust between the user and users in the white list.

**References:**

1.Apple. (2016). *Privacy - Manage Your Privacy - Apple (AU)*. [online] Available at: http://www.apple.com/au/privacy/manage-your-privacy/ [Accessed 16 May 2016].

2. Bank of China Australia. (2016). *Privacy Policy Statement*. [online] Available at: http://www.bankofchina.com/au/forms/Privacy%20Policy%20Statement.pdf [Accessed 16 May 2016].

3. Commonwealth Bank. (2016). *CommBiz User Guide Keeping your business secure*. [online] Available at: https://www.commbank.com.au/content/dam/commbank/business/pds/security-whitepaper.pdf [Accessed 16 May 2016].

4.Developer.apple.com. (2016). *The Swift Programming Language (Swift 2.2): Access Control*. [online] Available at: https://developer.apple.com/library/ios/documentation/Swift/Conceptual/Swift\_Programming\_Language/AccessControl.html [Accessed 16 May 2016].

5. Google Cloud Platform. (2016). *Access Control Options*. [online] Available at: https://cloud.google.com/storage/docs/access-control/ [Accessed 16 May 2016].

6. Google Cloud Platform. (2016). *Creating and Managing Access Control Lists (ACLs)*. [online] Available at: https://cloud.google.com/storage/docs/access-control/create-manage-lists [Accessed 16 May 2016].