Name: CK Date: 10/05/16

Research question:

"Cloud computing has the potential to provide many advantages to organizations. However, security risks involved cannot be ignored". Based on evidence from your research, to what extent can these security threats be prevented or minimized?

Companies planning to adopt cloud computing are facing several security threats. Some of them are newly emerging because of the characteristics of cloud computing and some of them belong to the traditional IT threat magnified by cloud computing. These threats impact businesses in a different way and to a different extent, so different solution is needed and the cost and effect vary.

Over the last ten years, cloud computing has developed from a laboratory concept to a widely used technology. Thanks to its flexibility and cost-efficiency characteristic, individuals are able to enjoy many types of useful free online personal storage, such as Dropbox, iCloud from Apple, Google Drive, and Microsoft OneDrive. One significant trend is that after taking photos with a smartphone, these image files are automatically uploaded to the cloud. So when individuals lose their cell phones or delete some images by accident, they can retrieve them from the Internet. Enterprises now can outsource from their whole online businesses to cloud providers, including software, infrastructure, operating system, hardware and IT management. By letting the cloud provider to take care of all the technical issue, the organization can save a lot of time and money. For example, there may be not necessary to hire IT relevant employees. This gives them more opportunity to focus on their core competency. However, there is considerable debate about whether or not the security threats within the cloud computing can be ignored. As there is evidence that many countermeasures are proved to be effective; however, contradictory evidence regarding the fact that cloud computing provider may have access to customers' data, and they are more likely to be the big target of hackers, suggests its threats should not be ignored. Although a better plan and a daily risk management can decrease these risks a little bit.

A definition of cloud computing from the US National Institute of Standards and Technology (NIST) is "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released " (Mell & Grance, 2011, as cited in Brender, Markov, 2013, P. 727). Although it has so many advantages for Ryan (2013) classifies the main concerns of cloud computing security threats as following:

There may be many users sharing the same cloud, any of them could be attacked, thus, the other users (also named tenants) may be affected;

The data in the cloud is designed to be accessed by their user from all over the world through various of APIs and protocols, which could be very unsafe;

Human mistake done by the cloud provider is another factor that can bring risks to data owners;

The cloud provider usually has its contractors or sub-contractors. In some situation, the staff of these companies or organizations have the access to the client's data (P. 2263).

One argument against security threats is that cloud computing technology does not bring more new security threats than other technologies. People who use the computer and the Internet have gotten along with virus or attacks for decades. Countermeasures to these issues are being made faster than ever before. In addition, the cloud computing has entered the enterprises market from the laboratory for many years. According to Ryan (2013, p. 2263), most of its risk management tools, data protect measures are quite advanced. For example, he points out that the security threat as a consequence of multi-tenancy can be controlled by a well separated virtual machine managers and operating systems. For data access issue, he also points out that authorization protocols and frameworks or encryption have been used for a long time to provide data protection. Let alone data loss, it is a common sense that almost every IT system should deploy backup or remote mirror plans for being able to recover from unexpected disaster. In these situations, from the technical point of view, one can adopt various of security modules to build up a safe cloud, thus its threats could be ignored.

Nevertheless, approaches of this kind carry with them various limitations. For many of these solutions inheriting from mainframe or Internet security technologies need to be adjusted to adapt the new cloud computing circumstance; however, some of them do not work very well. For example, according to Ryan (2013, pp. 2263-2264), in most cases, the enterprise or organization do not only store their data in the cloud but also require the cloud provider to extra services such as data mining, statistic analysis, information filtering and access control. This means that the cloud provider must have the access to the customer's data. In this circumstance, the normal encrypting measure would not work. Many IT scientists and companies are working in these areas. Wei et al. (2014, pp. 371-386) research on how to build up a secure cloud taking secure computation into account. They propose a protocol (called SecCloud) to prevent cheating and set up a test environment (called SecHDFS) which prove that it does do some help in an efficient way. However, this solution like the others is still in the laboratory. Since the value of data is becoming a significant competency, the demands of data mining and analyzing play an important role in the whole business process. While except resting the hope on that cloud provider will abide the confidentiality agreement, there is no such a way to guarantee that this intellectual would not be stolen or modify. Furthermore, since the data reside outside of the control of their owner, it is very hard to verify whether or not the cloud provider have a violation. Altogether, the data owners should make it clear that where their data are stored and who helping them to handle their processes (Rong, Nguyen & Jaatun, 2013, p. 49), rather than ignore these risks.

Some skeptics argue that cloud computing does not make one's data more dangerous, contrarily, it innate characteristics the end-users' information system safer. A study by Bendandi (2009) found there is five important security benefits embed in cloud computing. First, while customers share the cloud resource, they share the cost of security solutions. The customer thus able to affords the better and higher lever protect. Second, in order to win customer and market share, cloud computing providers usually willing to invest money on expensive security products and services. Third, other security solution company can provide their service to cloud computing user via standardized opened interface. In addition, the ability of real-time dynamic resource allocation can help a customer to resist sudden attack such as distributed denial-of-service (DDoS) attack. Last, a copy of the image of the virtual machine can be used as evidence in the court, rather than shutting down the whole server physically (p. 40, cited in Bisong & Rahman, p. 7). These advantages are essential because of the fact that not every company or organization have the IT expertise and be able to afford this investment. So cloud computing seems a good choice and it risks can be ignored.

However, while this may be true, over-dependent upon cloud computing still very dangerous. First, the interruption of cloud computing may affect hundreds of to thousands of customers. Hoover (2008) points out that Google's Gmail, Citrix's GoToMeeting and GoToWebinar and Amazon.com's Simple Storage Service experienced hours of interruption (as cited in Bisong & Rahman, 2011, p. 36). Unlike the traditional private server who have more opportunity to take precaution, the cloud computing customer may have to wait for the cloud service recovery rather than to maintain their virtual machine. This downtime brings direct or indirect inestimable loss to enterprise organizations.

Meanwhile, "[a] result of the survey confirms that Cloud service outages would be unavoidable no matter how smart or successful the provider is." (Li, Liang, O'Brien and Zhang, 2013, p. 329). These outages come from a various of reason, such as power loss, human mistake, hardware mistake, network error, software bug, virus, and hacker attack. Furthermore, A big cloud company is more vulnerable to hackers in comparison to a traditional server, because many top hackers devote to study their technical defects and develop the latest viruses to attacks the cloud. Some of them would not have opportunities to recover after this disaster.

By acknowledging the security threats should not be ignored, it is possible to try to avoid some risk, thus, give confidence to the organizations to use the cloud. One important approach is to choose the right business and data to migrate to the cloud. Thus, the organization would be able to not only take the advantage of cloud computing but also control the loss to an acceptable extent. In order to analyze the risk level, Kalyvas, Overly & Karlyn (2013, pp. 10-11) introduce two important dimensions. One is the criticality of customer's workflow that running on the cloud, another one is how sensitive about the customer's data that being stored in the cloud. They point that from workflow criticality perspective, putting high criticality workflow to the cloud leads to higher risk. Meanwhile, storing high sensitive data to cloud leads to higher risk. So deploying that uncritical business together with less sensitive data leads to the cloud could be a compromise to the security threats; however, they still should not be ignored.

Since the security threats of cloud computing are unneglectable, it is necessary for the cloud customers themselves to build up a risk mitigation strategy. This view is supported by the US chief information officer Kundra (2011, pp. 26-27), he introduces a risk management framework which consists of six different steps. These steps build up a procedure to guide every activity to ensure a security life cycle. He also points out that this would help the US government to reduce the security threats of cloud computing. Some control points are also mentioned as important approaches to minimize the cloud computing risks, such as data security, administration and control, logical access, network security, physical security, compliance and virtualization (Carroll, Van Der Merwe & Kotze, 2011, p. 8). This framework or control points form the strategy for protecting the organization's data and service. By following this strategy in daily IT management, instead of ignored those embed risks, one organization can really benefit from the cloud computing.

As this essay has shown, the security threats of cloud computing cannot be ignored. While it is generally true that the cloud computing has been commercially used for years, and many security threats of it have been addressed. However, as the fact that more and more new computation tasks have been outsourced to the cloud provider and its sub-contractor, there is no specific technical measure to prevent customer data from being the intentional or unintentional stolen. In addition, the cloud computing system and the network are usually the big targets of hackers and other viruses. Ignoring its threats could lead to an unacceptable loss. In this situation, choose the proper process and data to migrate to the cloud and follow a risk management framework are vital to controlling risks. Clearly, cloud computing represents the future of the computing, but saying it is 100% safe is too early. The IT managers of company or organization still have the responsibility to follow and update their risk management framework. And keep up-to-date with the latest IT and security technologies, so as to really benefit from cloud computing.