CHAPTER 5

DISCUSSION

5.1 Factors Affecting the Threats

There are many factors that might be the trigger for threats to attack a system. Specifically for the insider threats, one of the factors is economic pressure. This economic pressure drives people's motivation to abuse the privileges they have and sell the confidential data to outsiders. Furthermore, the data is sold at a very high price. And as an insider, gaining confidential data is less difficult than the outsiders. They do not have to go through the complicated firewall or IDPS, easily get pass the guards and access the restricted areas.

The second most dangerous threat, which is the data loss or leakage, will not happen without a reason. Since data is the essence of the system, the providers should implement a layered defense, to protect the data. One example of the layered defense is the layered encryption. But the insider threat is considered as the threat that can trigger this data loss or leakage. All of these explain that the defense for the internal threats should be as strong as, or even stronger than the defense for the external threats.

The competition among providers also becomes even tougher. Damaging the company reputation is the easiest way to eliminate a competitor. Using the malicious insiders to compromise the data is the common practices in the

5.2 Risk Analysis

From the risk determination, there are two threats that posses the highest likelihood and impact. They are the malicious insiders and the data loss or leakage. The malicious insiders are dangerous because the source of this threat is within the organization. According to the CIA (Confidentiality, Availability and Integrity) aspect, this threat attacks the confidentiality of the data and the availability of the system at first. They can bypass all the security system and go straight to the data. They can also disrupt the processes carried by the system. That means, this threat is linked to the second most dangerous threat, the data loss or leakage. It is not easy to compromise such security system without the help of the insiders. The insiders will show the way to the data, either by giving the passwords or disable the security, and the attackers or the hackers will do the action. When this happens, then the integrity of the data is threatened.

New or existing cloud providers always consider this combination of threats as the most dangerous threat. It can damage almost everything from the company, including the system, the data, the people and the business process. If one of those aspects is damaged at the early stage of cloud computing development, the impact will be hazardous to the company. But the problems that threaten those aspects are always there. It is up to the providers to handle it.

5.3 Control Analysis

Before the controls were implemented, the probability of the insider risk is very high. They know every details of the infrastructure and can easily ruin the security system. With the proposed controls placed, the risk can be reduced. Previously without the

layered encryption, the malicious insiders only need to find the encrypted message and the keys to open the real message. Now with the layered encryption, they must find all the multiple keys to open the real message. This will protect the confidentiality and integrity of the data. Even though it does not completely protect the data, but they have to face more complicated processes. Besides slowing down their movement, the complexity will reduce their malicious intention little by little.

The IIRP plays an important part in reducing the risk. Without such planning, it will take some time providers to take actions when an incident happened. Furthermore, it can also disrupt the services, which can also impact the customers as well. With this plan in mind, the providers can identify the source of incidents and react faster. It will definitely reduce the impact of the incident. And if they learned some lessons from the incidents, they can improve the IIRP and further minimize the incidents in the future.

Specifying the job distribution is also important. Without the specific job distribution is implemented, all the people behind the cloud can access cloud completely. Now with the divided privileges, some people will be responsible for some areas only. The interactions between employees can be limited as well. It protects the confidentiality of an information by reducing the probability of social engineering between the employees as well as limited moving space for the employees.

Traffic monitoring also plays an important role to reduce the risk. Before the traffic monitoring is implemented, the providers do not know the transmission coming in and out of their system. They also will not realize if there are malicious activities or unusual

activities in the network. But with this control implemented, they can maintain a better security in the network. Pre – emptive actions will help maintaining the availability of the system. In addition, they can also log all the activities to the restricted areas in the network. In case of incidents, they know the cause and able to react faster to the incidents. This log files can be used as evidence to support the computer forensics.

Maintaining a good environment also plays an important role. Without this approach, the employees live and work in a competitive environment. They want to be ahead of each other and sometimes they want to achieve it with the improper methods. Furthermore, with the economic pressure and other pressures that might affect their performance, they might do dangerous actions and turn them into malicious insiders. Better environment can provide better atmosphere for the employees. They will find that their place is right in the company. So they will do their best to stay focus on their job and maintain the harmony in the company, because they feel comfortable working in the environment.

5.4 Residual Risk

Although the controls are implemented, it does not mean that the system is safe from the risk, whether it is from the inside or outside the system. According to Whitman [6], there are risks that still remain in an asset even after the controls are implemented. Moreover, risk that is related to human is unpredictable. Human have can think or learn something from the company. They also have emotions that can change their behaviors. This is what makes human the weakest link in the system.

The layered encryption sounds like a sophisticated security mechanism. In fact, there are some risks associated with this controls. There is a possibility that the malicious insiders can get the data before it gets encrypted or after it gets decrypted. Social engineering and laptop theft enable the data to be stolen before encrypted.

The IIRP is also associated with residual risks. If the team members are absent when an incident occurs, other employees without the knowledge will be in panic. Or there is a possibility that one of the IIRP team members is the malicious insider itself. People with the knowledge of the system are the most probable people to compromise the system since they know everything. This also applies the same for the other controls related to human.

Log monitoring also does not guarantee that the insider's incident or data loss will not happen. This control is limited only to monitor the activities. Moreover, malicious insiders' activities cannot be easily distinguished from the normal activities. The log might trick the security team. And when they realized it, it was already too late.

Although these controls have limitations and the residual risks, it is not a reason to give up. The residual risks can be minimized by keeping up to date with the latest threats. Minimizing risk is not a one-time process. It is rather a continuous process to keep developing the controls by staying ahead of the threats. Below is the table that summarizes the proposed controls and the residual risk.

Proposed Controls	Residual Risk
Layered Encryption	The key is stolen or lost by laptop theft Social engineering
IIRP	Malicious team member Absence of team
Job Specification	Unmonitored activities of employees
Traffic Monitoring	Power outage, carelessness of employees
Manage a Comfortable Environment	Strong malicious insiders not affected

Table 12. Residual Risk Table

Then this table below will summarize all the threats, vulnerabilities, controls, proposed controls and the residual risk. It will show the relation of each attributes.

Threats	Cloud Specific Vulnerabilities	Current Controls	Proposed Controls	Residual Risk	Risk Rating
Internal threats	Insecure cryptography	Physical security Cryptography Background check Security policy	Layered encryption Insider incident response plan Job specification Traffic monitoring Maintain a comfortable environment	The key of encryption is stolen Intelligent people have a probability to become a malicious insider Difficult to detect malicious insiders	High
External threats	Insufficient network based controls in virtualized networks	Cryptography Firewall Antivirus IDPS Background check	Layered encryption	The external controls are disabled by the malicious insiders	Medium

Table 13. Summary of threats

From the table, the threats are classified into two types, the internal threats and the external threats. In this case, the internal threats are malicious insiders and the data loss or leakage. For the external threat is the abuse and nefarious use of cloud computing. The table also shows that even with the current controls and proposed controls, the danger of the internal threats are still high. As for the external threat, the numbers of controls are sufficient to protect the system from the external attack. This makes the risk rating is only medium.

5.5 Study Limitations

This research is limited due to the fact that cloud computing is relatively new in this country. There are only few companies who have started their business as the cloud computing providers. This makes the research process a bit difficult, to find the resource for this study. Furthermore with the limited time available, there are some important processes that cannot be done. They are the vulnerability scanning and the testing of controls. The vulnerability scanning and the testing of proposed controls will be added as the recommendation for future research.