CompliancePlus Consulting

Compliance Consulting • Funds Consulting
Regulatory Consulting • Compliance Training

The article is for general information only and is not intended to constitute legal or other professional advice.

Cybersecurity- How to Step into the Cloud and Avoid the Thunderstorms

A discussion on the "Circular to All Licensed Corporations – Alert for Cybersecurity Threats" dated 26 January 2017 issued by the Securities and Futures Commission of Hong Kong ("SFC")

Is it the cloud up on the sky?

There is a growing demand of cloud computing, such as Google Platform and Amazon Web Services, among different enterprises in recent years due to its various advantages, such as high flexibility and low cost. It is predicted that the usage of cloud computing will continue to expand in the next few years with improved cloud solutions. On the flip side of the same coin, cloud computing has imposed risks, such as possible data leakage, which has attracted the attention of the regulators.

Cloud computing services has gained popularity among the businesses as it generally improves efficiency. It brings higher flexibility as there is no need for office relocation due to expansion or scaling down of business. It is highly cost-efficient as it reduces the cost of renting or purchasing a space for storage of data and cuts the cost of hardware. The data from the cloud is also easily accessible from everywhere with only internet connection and removes the restriction of location limitation.

The word "cloud" is a metaphor for "the Internet". Cloud computing is a type of Internet-based computing that allows the users to share the computer processing data and resources to their electronic devices according to their demand. Through electronic devices such as personal computer and smart phones, users may upload the relevant files into the system. There are three types of service models for cloud computing, namely Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). Users may choose their cloud computing service model, provider and platform according to their preference.

Although the cloud computing system has its benefits, one should be aware of the cybersecurity issue. According to the Hong Kong Police Force, there is an 52% increase in the financial losses due to computer crime cases in Hong Kong from 2014 to 2015 and over 6862 technology crime cases reported in 2015 (http://www.infosec.gov.hk/english/crime/statistics.html). Particularly, attacks on cloud-based infrastructures is one of the major malicious attacks.

Regulators' responses

Following the circulars issued by the SFC in 2016 on cybersecurity, clearly cybersecurity is continue of the spotlight in 2016 among different businesses especially the asset managers. On 26 January 2017, the Securities and Futures Commission issued the Circular to alert the Licensed Corporations on the increasing Cybersecurity threats that they may face (http://www.sfc.hk/edistributionWeb/gateway/EN/circular/doc?refNo=17EC8).

This circular addressed the recent distributed denial of service ("**DDoS**") attacks on several securities brokers, causing disruption and inconvenience to their services, and reminded licensed corporations to implement cybersecurity controls.

Besides DDoS, the SFC also focuses on cybersecurity threats prevention on cloud systems and provides a few control defence mechanisms for the licensed corporations. As stated in the circular by SFC dated 23 March 2016 "Circular to all Licensed Corporations on Cybersecurity" (http://www.sfc.hk/edistributionWeb/gateway/EN/circular/openFile?refNo=16EC17), it identified five major areas of concern:

1. Inadequate coverage of cybersecurity risk assessment exercise
2. Inadequate cybersecurity risk assessment of service providers
3. Insufficient cybersecurity awareness training
4. Inadequate cybersecurity incident management arrangements
5. Inadequate data protection programs

The SFC recommended that the following measures should be adopted:

- Establish a strong governance framework to supervise cybersecurity management;
- Implement a formalized cybersecurity management process for service providers;
- Enhance security architecture to guard against advanced cyber-attacks;
- Formulate information protection programs to ensure sensitive information flow is protected;
- Strengthen threat, intelligence and vulnerability management to pro-actively identify and remediate cybersecurity vulnerabilities;
- Enhance incident and crisis management procedures with more details of latest cyber-attack scenarios;
- Establish adequate backup arrangements and a written contingency plan with the incorporation of the latest cybersecurity landscape; and
- Reinforce user access controls to ensure access to information is only granted to users on a need-to-know basis.

.

The Hong Kong Monetary Authority ("**HKMA**") also announced a launch of "Cybersecurity Fortification Initiative" ("**CFI**") at the Cyber Security Summit 2016 (the **"Summit")** in 18 May 2016. It aimed to improve the level of cybersecurity in order to be compatible with the advancement of technology and the maintenance of Hong Kong's status as a prestigious international financial centre. The CFI comprised of 3 different components, comprising of

- Cyber Resilience Assessment Framework；
- Professional Development Programme；
- and Cyber Intelligence Sharing Platform.

These three approaches were proposed to strengthen the current cybersecurity system by training more experts in the cybersecurity field and to enhance awareness of cybersecurity.

Industry Responses

Regarding the thrive of cloud computing system, professionals at the APAC Annual Forum 2017 hosted by the Alternative Investment Management Association ("**AIMA**") dated 19 January 2017 shared some tips on cloud migration and reminded licensed corporations on the precaution measures of cyber-attacks.

With the increasing trend of cloud migration, corporations usually rely on outsourced information technology service providers for the management of their cyber systems. The problem of third-party liability is highlighted as some corporations have the misperception that outsourcing means that the responsibilities will be transferred. However, it was reminded that both parties are liable in times of cybersecurity breaches. As cybersecurity is of a major concern now, it is suggested that a corporation should not solely depend on service providers, but rather build its own information technology team to monitor risk and deal with cyber issues in real time. The in-house information technology team should keep record of any cybersecurity breach and should implement contingency plans to deal with these issues.

Regarding this general trend, the speakers highlighted some insights during cloud migration. First of all, corporations should have a clear objective to use the cloud systems, for instance, for dealing with compliance, or for business expansions. Next, they should be familiar with the rules of the regulatory bodies that they must abide by, which would be the SFC if the company is incorporated in Hong Kong. Then the corporations should pick the cloud service providers with careful considerations on areas especially the scope of services to see if it matches the business needs of the company. They should either maintain the same degree of protection or further enhance their level of security after cloud migration by conducting due diligence on the service providers to ensure suitability and safety of the outsourced parties. The speakers also reminded that for the corporations operating or planning to operate in China, they should take one more step to make sure that there are local connections and the system would run well in Chinese regions.

Cybersecurity is inevitable due to the increase in the number of cyber-attacks nowadays. As Ms. Carrie Leung, the Chief Executive Officer of Hong Kong Institute of Bankers, had said in the Summit, cyber threats had become a growing risk to the banking and financial services sectors. To prevent leakage of private information and other breaches that bring harm to society and its clients, it is reminded that the licensed corporations should be alert of their cybersecurity systems and the guidelines from the respective regulatory bodies, and implement adequate risk management solutions and cybersecurity measures. Dealing with cloud migration, it is recommended that the corporations should choose the service providers that best suit their objectives and ensure the security of their computing systems.

Conclusion

Last but not least, it is expected that Licensed Corporations should conduct frequent check and ensure:

1. Comprehensively and effectively review and assess cybersecurity risk;
2. Rectify any identify weaknesses; and
3. Enhance cybersecurity controls with priority.

If you have any further questions regarding this issue of CP insights or have any topic you would like us to cover, please submit your response here https://goo.gl/forms/gDLVThTmxGvMl4r12.

CompliancePlus is an independent consulting firm focused on providing a complete range of proven and reliable compliance solutions to fund management companies and hedge fund managers in Asia. Our dedicated team of compliance officers has years of professional experience equipped with in-depth knowledge of both functional and compliance experience in managing and minimizing regulatory, operational and reputational risks.

We have been providing real time compliance support and proactive recommendations to start-up hedge funds, fund of hedge funds and multi-strategies hedge funds with our solid compliance knowledge.

By partnering with **CompliancePlus**, our clients gain access to compliance solutions that they can trust and the latest knowledge of regulatory policies and procedures. Through building up strong relationships with our clients and by ensuring our availability to them, we are trusted advisors helping clients to navigate a challenging and changing regulatory environment.

Contact:

Josephine Chung is Director of CompliancePlus Consulting Limited specializing in compliance matters for hedge fund managers and mutual fund management companies with over 15 years of industry experience. Before joining CompliancePlus Consulting, she was the Head of Legal and Compliance for a major asset management company in Hong Kong.

Josephine can be contacted at +852-3487 6333 (email: jchung@complianceplus.hk)

END