

Organizers



Sponsor



# Report on Hong Kong SME Cloud Adoption and Security Readiness Survey

---

Collaborated by Internet Society Hong Kong and Cloud Security Alliance (HK & Macau Chapter)

*Sponsored by Microsoft Hong Kong*

Jointly compiled by

*Chester Soong, Chairman, Internet Society Hong Kong*

*Michael Yung, Chairman, Cloud Security Alliance Hong Kong and Macau Chapter*

**2 April 2014**

*Copyright of this report is held jointly by Internet Society Hong Kong, Cloud Security Alliance (HK & Macau Chapter) and Microsoft Hong Kong.*



## Table of Contents

|  |    |
|--|----|
| Executive Summary .....                          | 3  |
| Introduction and Background .....                | 5  |
| Survey mechanism and technical information ..... | 5  |
| Findings and recommendations .....               | 6  |
| Policy design .....                              | 6  |
| Findings .....                                   | 6  |
| Recommendations .....                            | 6  |
| Physical security .....                          | 7  |
| Findings: .....                                  | 7  |
| Recommendations: .....                           | 7  |
| Data privacy management .....                    | 7  |
| Findings: .....                                  | 8  |
| Recommendations: .....                           | 8  |
| System management .....                          | 8  |
| Findings: .....                                  | 8  |
| Recommendations: .....                           | 8  |
| Incident management .....                        | 10 |
| Findings: .....                                  | 10 |
| Recommendations: .....                           | 10 |
| Cloud technology adoption and application .....  | 10 |
| Findings: .....                                  | 11 |
| Recommendations: .....                           | 11 |
| Conclusion .....                                 | 12 |
| Appendix I – Survey Questionnaire .....          | 14 |
| Appendix II - Statistics and Charts .....        | 19 |



## Executive Summary

In January 2014, the Internet Society Hong Kong (ISOC HK) and Cloud Security Alliance – Hong Kong and Macau Chapter (CSA HK), with the sponsorship from Microsoft (HK), jointly conducted the first Hong Kong SMEs Cloud Readiness Survey. We have received feedback and interviewed 100 local SMEs coming from various industries including retails, manufacturing, Information and communications, imports/exports, financial services, etc.

The questionnaire was prepared with six major areas of consideration for adopting Cloud computing services from the SMEs' perspectives:

- Policy design
- Physical security
- Data privacy management
- System management
- Incident management
- Cloud technology adoption and application

We are encouraged to know from the survey that over 50% of the responding SMEs have adopted some kinds of Cloud computing services. While there are many factors an SME considers before using Cloud services, security is still among its top consideration. Manufacturing comes out the least mature in terms of security maturity and adoption of Cloud services.

Compared to those who don't, SMEs using cloud services show a remarkably higher level of security readiness in their overall data management and information security systems, as well as in their ability to handle incidents. This shows that data security should not be perceived as a barrier to using cloud services; on the contrary, adopting cloud computing may be one solution to information security issues (Q7-15)

Many SME owners already have some knowledge about cloud security and its execution on a company policy level. However, on a technical level, companies are still limiting proactive security measures to personal computers, such as installing anti-virus software. SMEs in general still lack an understanding about proper software update and protection processes for their important databases and servers – case in point, according to the survey results, only 42% of the surveyed SMEs have installed data recovery applications.

With limited resources in manpower and specialist knowledge, SMEs can consider a phased implementation of cloud technologies. For example, adopting a hybrid solution that combines a public and private cloud lets SMEs manage and store sensitive data separately from other

## Organizers



## Sponsor



information. In addition, with personal and commercial cloud services differing greatly in the level of data protection and security, SMEs should choose reliable cloud services providers and commercial cloud services that offer server software and better protection technology. This will allow SMEs to protect their company data and property more comprehensively and effectively,” he suggested. Selecting a respectable Cloud service provider is obviously important, and they can follow the Security Guidance for Critical Areas of Focus in Cloud Computing and Cloud Controls Matrix (CCM released by CSA and the Practical Guide for Procuring Cloud Services released by Office of the Government Chief Information Officer.



## Introduction and Background

The Hong Kong Small and Medium-sized Enterprises (SME) Cloud Adoption and Security Readiness Survey was conducted by the Internet Society Hong Kong and the Cloud Security Alliance Hong Kong and Macau Chapter, who commissioned the Hong Kong Productivity Council to carry out telephone interviews to Hong Kong SMEs (<100 employees) over the course of three weeks and to review data from the Census and Statistics Bureau. The Council successfully collected 100 responses to the survey. The research covered major industry sectors in Hong Kong. The survey questionnaire was developed based on the Cloud Security Alliance Cloud Control Matrix international standard with questions adapted to local conditions. The survey was sponsored by Microsoft Hong Kong.

## Survey mechanism and technical information

The survey was conducted between January 29, 2014 and February 20, 2014 with Small-Medium Enterprises (SMEs) locally in Hong Kong with less than 100 employees. The participating candidates selected from HKPC's in-house database, industry directories, and Yellow Pages.

Each SME was interviewed by telephone based on a structured Chinese questionnaire with 20 questions. A total of 100 questionnaires were completed at the end of the survey period. The 20 questions try to address the following areas of concerns in terms of Cloud security:

- Policy design
- Physical security
- Data privacy management
- System management
- Incident management
- Cloud technology adoption and application

Except with the first two questions about the background of the interviewees, others are given from a 1 to 5 scale indicating the SME's readiness in using Cloud computing services. Detailed analysis and recommendations are discussed in the following sections by their respective areas of concern.



## Findings and recommendations

### Policy design

From the survey results, we can conclude that:

- 55% of companies surveyed has security policy in place
- 65% of companies' management will review the policy to ensure it can effectively protect the company's information
- 61% of companies put in place access right management to data
- 29% of companies performs security audit and certifications by external parties

### Findings

Most of the companies surveyed have good understanding in security policy setting, review and execution, but most of them have not factored in the need of external auditing and security certification. It indicates slightly over half of the interviewed SMEs have formal or structured security measures implemented within the organization, and that means the rest of them, for whatever reasons to be discussed elsewhere, would rely on the security measures already included in Cloud computing services by the service providers for such protection. This might be the fact that some small companies rather adopt no security measures at all or use only primitive security measures such as the built-in firewall and antivirus solutions from the off-the-shelf software providers due to cost.

### Recommendations

Therefore it is suggested to procure IT solutions from reputable services providers that possess related security certifications and resources. For bigger companies, it is suggested to conduct external security audit regularly, preferably once a year. CSA provides documents regarding Cloud security evaluation such as Security Guidance for Critical Areas of Focus in Cloud Computing and Cloud Controls Matrix (CCM). SMEs can rely on the Cloud service providers on evaluating the security measures from typical PaaS and SaaS.



## Physical security

From the survey results, we can conclude that:

- 62% of the companies manage their IT systems with proper access right and password control, as well as audit trail and exercise.
- 63% of the companies have people or team to in charge of hardware / software maintenance, as well as support.

### Findings:

Most companies manage their passwords, physical access right, and IT asset appropriately. However, inadequate security control can adversely affects their business continuity and effectiveness of what they believe to be cast-iron defense. For example, once the product license has expired, so go the technical and product support as well. Then the product will run on with known vulnerabilities and waiting to be exploited

### Recommendations:

Companies who are considering or implementing cloud computing solutions shall assess the security risks they are possibly facing, and further strengthen the relevant controls. SMEs are not going to use Cloud computing totally and some office automation software will be installed in-house. So a good but simple security management practice should be recommended and all employees shall be educated in forms of circulars and post-ups.

## Data privacy management

From the survey results, we can conclude that:

- 63% of companies understand the needs of data access right protection
- 50% of companies have good understanding or implemented data encryption
- 70% also have implemented data backup strategy and process.
- 40% of companies surveyed have data disposal policy devised.



### Findings:

Most companies seem to understand the needs of data access right and backup, and about half of the companies surveyed have good understanding or implemented data encryption. However, most of them lag behind in data disposal. We should praise this kind of good practice, but also remind them many of whom still forget to back up and test them regularly. Backing up to the cloud storage doesn't mean that this is done automatically on a regular basis.

### Recommendations:

As more and more companies placing their company data to the cloud storage, it is important for those companies to establish clear and concise data protection and disposal policy on the cloud. They have to review the data protection policy and service level of the cloud service providers. Paper review on the backup and restore plan is one example that can be done easily.

## System management

From the survey results, we can conclude that:

- 42% of the companies implemented security patches policy
- 85% of the companies implemented anti-virus solutions and review / apply regularly
- 67% of the companies installed firewall devices to further improve the security

### Findings:

Most companies surveyed are poor in implementing security patches in a timely fashion, even though most companies have implemented anti-virus and firewall protection solutions.

### Recommendations:

Careful planning and deployment of applications to the cloud platform can mitigate the risks imposed by outdated security patches. It is suggested to review the vendor solutions and implementation plan cautiously. Companies adopting SaaS mode of cloud services will rely more on Internet browsers and plugins/extensions to access their data. They are more exposed



Organizers



Sponsor



to the Internet than opening files in the local network. They are reminded that they must keep security patch update to mitigate the additional security risks.

Companies can refer to Threat & Vulnerability Management as well as the Infrastructure & Virtualization Security sections of the CSA Cloud Control Matrix V3.0 to adopt the best practices.



## Incident management

From the survey results, we can conclude that:

- 65% of the companies have put in place Incident Response Plan
- 63% of the companies also have Disaster Recovery Plan prepared.

### Findings:

More than half of the companies already have incident response and disaster recovery plan in place. This result is quite different from previous information security survey done historically as SMEs usually have little resources, and therefore priority, in addressing incident response and DR issues. So there may be a gap exist for the SMEs in terms of the real meaning of incident response and DRP. For the companies claimed to have such measures in place, the maturity and effectiveness of their plans are questionable.

### Recommendations:

When companies migrate to cloud, they need to factor in the role of cloud service providers in incident response, to keep the incident response and disaster recovery plans up-to-date and conduct regular drill, to make sure the plans can perform as designed. Again, we can leverage CSA's Security Guidance for Critical Areas of Focus in Cloud Computing and Cloud Controls Matrix (CCM) or Microsoft's Cloud Security Readiness Tool for guidance.

## Cloud technology adoption and application

From the survey results, we can conclude that:

- 55% of companies are using or planned to use Cloud services
- The top two cloud usages are email and storage.
- Top two reasons of using Cloud Services are the flexibility and good vendor services provided.
- For those who have not adopted cloud technology, 23% are concerned about information security.

Organizers



Sponsor



### Findings:

Only half the companies surveyed are using cloud with email and storage as their primary functions. In addition, most companies understand the various benefits of cloud computing, but some think they don't need that yet. For those who have not adopted cloud technology, most (23%) are concerned about information security, and some think cloud services are not reliable. About 13% of the responding companies are not familiar with cloud computing.

### Recommendations:

While security is one important factor that companies consider whether to use cloud services or not, the benefits of using cloud technologies in terms of on-demand provisioning, pay-as-you-go and scaling flexibility, etc. shall be assessed objectively. Cloud services also enable the provision of Security as a Service, which may not be widely known to SMEs at the moment, and more promotion on the advantages of such area is required.



## Conclusion

The adoption of Cloud computing services is getting to the implementing stage. While the multi-national companies and government agencies are implementing their cloud services to take advantage of the cost and technologies of Cloud computing, SMEs and even individuals Internet users are playing an increasing part of the whole landscape.

The results of this Cloud Security Readiness Survey give a positive outlook of such technology. Most of the respondents have indicated they are aware of the security requirements of adopting such technology, and many of such SMEs have already using many of the subsets of the Cloud services. But as we all know in the practical world, things are always on the move and we still have much to improve to make Cloud computing services to be easily and more confidently adopted by SMEs where such part of the commercial sector can be benefited most.

### **About the Cloud Security Alliance Hong Kong and Macau Chapter**

The Cloud Security Alliance (CSA) is a not-for-profit organization with a mission to promote the use of best practices for providing security assurance within Cloud Computing, and to provide education on the uses of Cloud Computing to help secure all other forms of computing. CSA is led by a broad coalition of industry practitioners, corporations, associations and other key stakeholders. The CSA Hong Kong and Macau Chapter is launched in 2012 by a group of local IT professionals, to further expand its presence and focus in Asia-Pacific,

### **About the Internet Society Hong Kong**

Internet Society Hong Kong (ISOC HK) is the local chapter organization of the Internet Society (ISOC), which is an international and not-for-profit membership society. ISOC HK was formed in 2005 by local veteran Internet professionals with the mission to improve the practice of Internet governance and online civil society in Hong Kong. Consistent with the ISOC statement of purpose, ISOC HK believes in “maintaining and extending the development and availability of the Internet and its associated technologies and applications – both as an end in itself, and as a means of enabling organizations, professions, and individuals locally and worldwide to more effectively collaborate, cooperate, and innovate in their respective fields and interests.”

Organizers



Sponsor



### **About Microsoft**

Founded in 1975, Microsoft (Nasdaq "MSFT") is the worldwide leader in software, services and solutions that help people and businesses realize their full potential.

The Cloud Security Alliance ("CSA"), Internet Society Hong Kong ("ISOC") and Microsoft Hong Kong have designed and created 2014 Hong Kong SME Cloud Adoption and Security Readiness Survey (the "Work") primarily as an educational resource for SME, cloud computing users, providers and those interested in cloud computing. The CSA, ISOC and Microsoft make no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of any proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, security, governance and assurance professionals should apply their own professional judgment to the specific control circumstances presented by the particular systems or information technology environment



## Appendix I – Survey Questionnaire

### 香港中小企雲端應用及保安就緒程度調查 – 問卷

#### Hong Kong SME Cloud Security Readiness Survey – Questionnaire

#### 調查簡介

您好！香港互聯網協會及香港生產力促進局正進行一項有關雲端應用及保安就緒程度的調查。現誠邀閣下參與。是次調查可於 10 分鐘內完成。

#### A. 公司資料確認

1. 貴公司主要業務為：*(只可單選)* (Q1)

1.  製造

2.  進出口貿易及批發

3.  零售

4.  住宿及膳食服務

5.  資訊及通訊

6.  金融及保險

7.  專業服務(包括法律、會計、顧問服務、廣告、室內設計、速遞服務) 8.  地產(包括地產經紀、裝修)

9.  其 他 ( 請 註 明 ) :

2. 貴公司現時於香港辦公室之總員工人數：                     (Q2)

*(註：中小企業 = 於香港聘用少於 100 名員工；如受訪公司未能符合上述定義，需終止訪問)*

於以下部份，請就有關句子，於 4 個答案選項中，選出最符合貴公司現時情況的一個選項。

#### B. 公司整體資訊保安政策 (Policy Design)

| 句子  | 答案選項 | 完全不符合(1)  | 少部份符合(2) | 大部份符合(3) | 完全符合(4) |
|---|------|-----------|----------|----------|---------|
| 3. 公司具備正式的資訊保安措施，以監察、審核及持續提升全公司的資訊保安水平。Q3                                     |      | (5) = 不確定 |          |          |         |
| 4. 公司管理層會檢視內部的資訊保安措施，以確保有關措施能有效保障公司的資訊保安。Q4                                   |      | (5) = 不確定 |          |          |         |
| 5. 公司的資訊保安措施，每年均會由外間獨立機構 / 人士透過審計 (Auditing) 或再續証 (Certification) 等過程，進行檢視。Q5 |      | (5) = 不確定 |          |          |         |
| 6. 公司具備守則文件，闡述不同崗位員工的資訊存取權限，並指示如何處理離職或內部轉職員工之資訊存取權，包括刪除及更改存取權。Q6              |      | (5) = 不確定 |          |          |         |

### C. 實體保安管理 (Physical Security Management)

| 句子   | 答案選項 | 完全不符合(1)  | 少部份符合(2) | 大部份符合(3) | 完全符合(4) |
|--|------|-----------|----------|----------|---------|
| 7. 公司透過一系列措施，包括為不同崗位員工制定使用權限、採用密碼、保存使用記錄或進行審計等，以便中央管理公司的資訊科技系統 (如伺服器)。Q7 |      | (5) = 不確定 |          |          |         |
| 8. 公司有專責職員管理內部資訊科技資產，包括中央監察相關軟硬件的保養期，及中央統籌相關軟硬件的支援。Q8                    |      | (5) = 不確定 |          |          |         |

### D. 數據保安管理 (Data Privacy Management)

| 句子 | 答案選項 | 完全不符合(1) | 少部份符合(2) | 大部份符合(3) | 完全符合(4) |
|----|------|----------|----------|----------|---------|
|----|------|----------|----------|----------|---------|



|   |           |  |  |  |
|---|-----------|--|--|--|
| 9. 公司透過一系列措施，包括為不同崗位員工制定使用權限、保留並檢視存取記錄等，以確保公司所儲存的客戶數據之安全。Q9 | (5) = 不確定 |  |  |  |
| 10. 公司有採用數據加密技術於資訊系統上，以加強保護內部資料數據，防止外洩，並定期檢視數據保安情況。Q10      | (5) = 不確定 |  |  |  |
| 11. 公司定期將內部數據備份，並就備份過程定期進行檢視和測試。Q11                         | (5) = 不確定 |  |  |  |
| 12. 公司具備守則文件以指示員工銷毀內部數據，並會保留數據銷毀紀錄，以及定期檢討數據銷毀過程。Q12         | (5) = 不確定 |  |  |  |

#### E. 系統管理 (System Management)

| 句子  | 答案選項      | 完全不符合(1) | 少部份符合(2) | 大部份符合(3) | 完全符合(4) |
|---|-----------|----------|----------|----------|---------|
| 13. 內部專責職員通常於修補程式 (Patch) 發佈後的一段固定時間內 (如發佈後一個月內)，測試修補程式。通過測試後，修補程式會被自動安裝於公司所有連接網絡的電腦內。Q13 | (5) = 不確定 |          |          |          |         |
| 14. 公司所有連接網絡的電腦均裝有防毒軟件。該套軟件由公司提供並負責定期更新。公司亦會定期檢視防毒軟件的表現，以確保公司的資訊保安水平。Q14                  | (5) = 不確定 |          |          |          |         |
| 15. 除了使用互聯網服務供應商的防火牆外，公司亦自行裝設額外防火牆 (硬件或軟件) 以加強保護。公司會中央管理該防火牆，並會定期為該防火牆進行審計工作。Q15          | (5) = 不確定 |          |          |          |         |

#### F. 事故處理 (Incident Management)

| 句子 | 答案選項 | 完全不符合(1) | 少部份符合(2) | 大部份符合(3) | 完全符合(4) |
|----|------|----------|----------|----------|---------|
|    |      |          |          |          |         |





|  |           |  |  |  |
|--|-----------|--|--|--|
| 16. 公司具備守則文件以指示員工處理內部資訊保安事故（例如電腦失竊、資料外洩）。公司亦會定期檢視、測試及更新相關守則。Q16                            | (5) = 不確定 |  |  |  |
| 17. 公司備有災難復原計劃（Disaster Recovery Plan）、備用電腦和備份數據庫，以便於資訊保安事故後，盡快恢復公司運作。公司亦定期檢視和測試災難復原計劃。Q17 | (5) = 不確定 |  |  |  |

### G. 雲端資訊科技應用情況（Cloud Technology Application）

18. 貴公司有否使用任何雲端資訊科技應用方案（「雲端資訊科技應用」定義：讓中小企透過互聯網和流動網絡，以相對低廉的起動成本，採用切合其運作規模的資訊科技應用 – 出自立法會）？(1 = Yes, 0 = No)

- 現正使用，請註明（可選多項）：Q18 (0)
- 電郵 (1)
  - 辦公室協作工具 (2)
  - 銷售 (3)
  - 客戶關係管理 (4)
  - 資料存儲 (5)
  - 財務 (6)
  - 企業資源規劃 (7)
  - 人力資源管理 (8)
  - 數據運算 (9)
  - 軟件開發 (10)
  - 軟件測試 (11)
  - 其他（請註明）：\_\_\_\_\_ (12)
- 完成選擇後，往 Q19

- 現在沒有使用，但正考慮 / 研究相關方案 → Q20 (13)
- 現在沒有使用，短期內亦不考慮 → Q20 (14)

19. 請闡述**使用**雲端資訊科技應用方案的原因（可選多項）：Q19 (1 = Yes, 0 = No)

- 起首的投資較少（軟 / 硬件）(1)
- 可倚賴方案供應商的支援 (2)
- 費用投資方面的彈性較大 (3)
- 可享用最新科技 (4)
- 其他（請註明）：\_\_\_\_\_ (5)

20. 請闡述**不使用**雲端資訊科技應用方案的原因（可選多項）：Q20 (1 = Yes, 0 = No)

Organizers



Sponsor



- 對雲端資訊科技不太認識 ) (1)
- 資訊保安的考慮 (2)
- 感覺上，雲端服務不太穩定 (3)
- 害怕雲端服務供應商倒閉，因而損失正使用的雲端方案中的數據 (4)
- 害怕雲端服務供應商倒閉，因而損失所繳費用 (5)
- 其他（請註明）： \_\_\_\_\_ (6)

**問卷完**

Organizers



Sponsor



## Appendix II - Statistics and Charts



SME\_CloudSecurity\_  
APPENDIX\_II\_Charts