Study on Privileged Access Governance in Hong Kong Enterprises

Independently conducted by Hong Kong Productivity Council

Commissioned by SSH Communications Security

Publication Date: March 2017

HKPC Study Report

Study on Privileged Access Governance in Hong Kong Enterprises
HKPC, March 2017

Content

Study on Privileged Access Governance in Hong Kong Enterprises
HKPC, March 2017

About HKPC

The Hong Kong Productivity Council (HKPC) is a multi-disciplinary organization established by statute in 1967. HKPC's mission is to promote productivity excellence through the provision of integrated support across the value chain of Hong Kong firms, to achieve a more effective utilization of resources, to enhance the value-added content of products and services, and to increase international competitiveness. HKPC conducts independent Study on cyber security and privacy to enable public and private organizations to have a better understanding on the trends in cyber threats and best practices to enhance their reputation and competitiveness in the global market.
For more information, please visit http://www.hkpc.org.

About SSH

SSH Communications Security (SSH) is the leading provider of identity access management solutions for the governance of the most critical access to on premise and cloud environments. The company's long track record of innovation includes Secure Shell - one of the world's most widely used network security protocols. The expertise of SSH is in key management, enterprise access management, monitoring encrypted privileged access, while help reducing costs and compliance risks. The Company has offices in North America, Europe and Asia and connects to a global network of certified partners. The company's shares (SSH1V) are quoted on the NASDAQ OMX Helsinki. For more information, please visit http://www.ssh.com.

License

Disclaimer

1. Introduction

1.1 Background

This study is commissioned by SSH Communications Security and is independently conducted by the Hong Kong Productivity Council (HKPC). The methodology of this study, the design of questionnaire and the execution of the interview were decided and conducted by HKPC independently.
The study tried to fill in the gap of lack of documentary and statistics on the status of Privileged Access Governance in Hong Kong, to help raising the awareness and preparedness of the enterprises for defending against insider threats and cyber attacks targeting privileged access.

1.2 Objective

The objectives of this study are:

1. Understand the landscape of Privileged Access Governance adoption in Hong Kong leading industries
2. Understand the views of senior management towards Privileged Access Governance among Hong Kong leading industries
3. Provide recommendations on the management and protection of privileged access

1.3 Definition of Privileged Access

Privileged access refers to the “super” capability of a user in a system such as servers, networks or cloud services. The Privileged Access capability of a user of a system is equivalent to that of the administrator (or super-user or root) role of a system that allows such user to freely navigate within the system and perform any critical tasks such as creating or removing a user account, or to create, edit or destroy data or shut down the system.

1.4 Need for Privileged Access Governance

Many enterprises have invested heavily on information security infrastructure to protect information assets. Privileged accesses are often provided to internal staff or external partners to manage critical information assets remotely. Given the access granted, privileged access is potentially an attack vector targeted by sophisticated attackers and as a result, control and management of privileged access is always at the top of the auditor's findings list. Many compliance requirements such as that of the Hong Kong Monetary Authority[1] and Payment Card Industry Data Security Standards[2] have explicitly mentioned the need for privileged access management controls.

Attackers seem to have better awareness of the weakness of privileged access and how to exploit the access provided. In June 2016, HKCERT reported hacked remote access servers from 173 economies, including Hong Kong, were traded in the xDedic underground marketplace.[3] Some ransomware utilized bruteforce attacks on remote access software like Microsoft RDP (Crysis, Sep 2016)[4] and TeamViewer (Surprise, Mar 2016)[5]. Furthermore, with the growing adoption of IT outsourcing and the use of cloud services, exposure of privileged access to the Internet continues to grow. In January 2017, ransomware started to infiltrate default privileged accounts of NOSQL databases such as MongoDB, Redis, ElasticSearch to demand ransom in Bitcoins.[6]

Sophisticated Advanced Persistent Threat (APT) attacks often use privileged access credentials to infiltrate into enterprises and are not discovered because of the stealth use and the brief periods of time used during an attack. The attackers move laterally and attempt to escalate the privileges found. Besides, today most traffic is encrypted, enterprises do not have visibility into encrypted communications so attackers can easily utilize the gapping hole and pose advanced threats. Compromise of privileged accounts is a crucial success factor of sophisticated APT attacks like Red

[1] "Cyber Security Risk Management", 2015, by Hong Kong Monetary Authority
http://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2015/20150915e1.pdf

[2] PCI DSS Reference
https://www.pcisecuritystandards.org/documents/PCI%20SSC%20Quick%20Reference%20Guide.pdf

[3] HKCERT Calls for Tighter Security for Remote Access Servers
https://www.hkcert.org/my_url/en/articles/16062101

[4] Hackers Using RDP Attacks to Install CRYSIS Ransomware
http://www.securityweek.com/hackers-using-rdp-attacks-install-crysis-ransomware

[5] Surprise Ransomware Installed via TeamViewer and Executes from Memory
https://www.bleepingcomputer.com/news/security/surprise-ransomware-installed-via-teamviewer-and-executes-from-memory

[6] Beware of ransomware targeting NoSQL Database
https://www.hkcert.org/my_url/en/blog/17012002

October, Saudi Armaco and Global Payments. Use of privileged access was much harder to detect.

Besides external attacks, insider misuse or attacks cannot be downplayed. Ponemon's study, "Intelligence Driven Cyber Defense" (2015)[7] indicates that the greatest cyber threat was not from the outside. Instead 36% of attacks were tied to negligent insiders and 25% were related to malicious insiders. A recent report "Understanding Insider Threats" by Gartner[8] found that 62% of insider attackers were financially motivated. Usually, this was from the access and misuse of sensitive data, including leaking data to suppliers to undermine the negotiating powers of the company.

1.5 Structure of Report

This report sets out our approach and methodology in conducting the study, whereby we provide the survey findings and then presents the results of data analysis.

Following this introductory chapter, the rest of this document is structured as follows:

- Chapter 2 describes in detail the methodology adopted to carry out the study;
- Chapter 3 presents the survey results, data analysis and major findings;
- Chapter 4 sets out our conclusions and recommendations.

[7] "Intelligence Driven Cyber Defense", 2015, by Ponemon Institute LLC
http://www.lockheedmartin.co.uk/content/dam/lockheed/data/isgs/documents/isgs-cybersecurity%20-report-2252015.pdf

[8] "Understanding Insider Threats", 2016, by Gartner
http://blogs.gartner.com/anton-chuvakin/2016/05/09/our-understanding-insider-threats-paper-publishes/

2. Methodology

To gain a robust understanding of the views of senior management within enterprises of the Hong Kong leading industries towards Privileged Access Governance, telephone interviews were applied to provide for quantitative analysis.

2.1 Scope of Study

The information to be collected is illustrated as follows:

- Company Profile
- Security Issues Encountered
- Compliance, Audit and Management
- IT Outsourcing
- Shared Account with Privileged Access
- Investment in IT Security in the coming 12 Months

2.2 Sample Size

In this study, 51 responses were successfully collected in December 2016, which targeted enterprises who had a significant size or were listed in Hong Kong Stock Exchange in the following leading industries in Hong Kong, namely:

- Finance and Insurance
- Logistics and Transport
- Government and Public Organizations
- Wholesale, Retail and Import/Export
- Other business sectors

2.3 Questionnaire Design

To facilitate the interview process and enhance record management, a designated questionnaire was developed with reference to similar study in other countries. Please refer to Appendix I for the questionnaire.

3. Survey Statistics

This chapter presents the survey findings and data analysis for the study and is divided into six sub-sections. The topics covered are as follows:

1. Company Profile
2. Security Issues Encountered
3. Compliance and Audit
4. IT Outsourcing
5. Shared Account with Privileged Access
6. Investment in IT Security in the Next 12 Months

51 respondents were successfully interviewed in this study.

3.1 Profile of Respondents

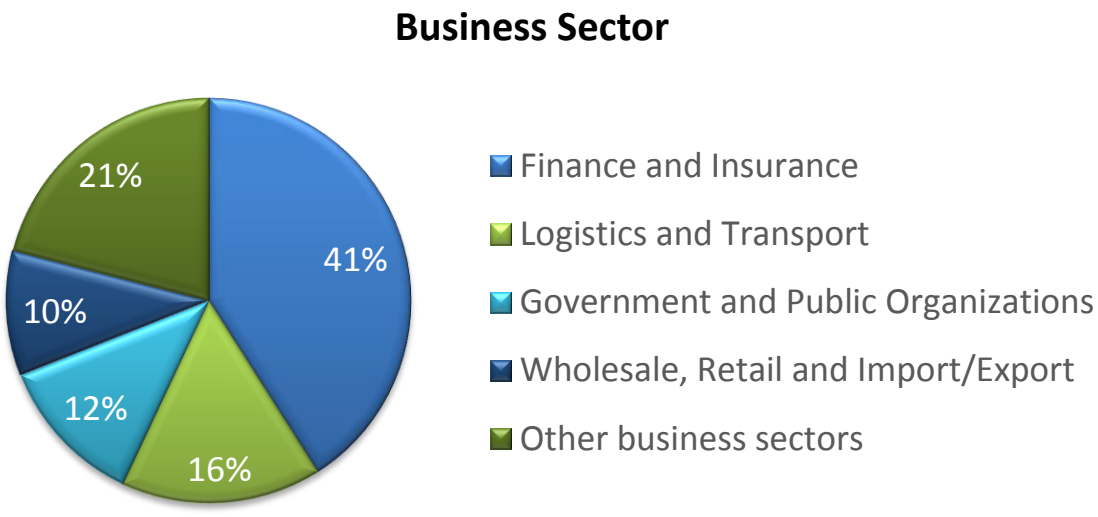
This sub-section discusses the profiles of the 51 surveyed companies, including

- Business Sector
- Size of Company
- Listing Status in Hong Kong Stock Exchange
- Importance of IT System & Data

3.1.1 Business Sector

The business sector of the respondents covers the critical industries of Hong Kong Economics contributors:

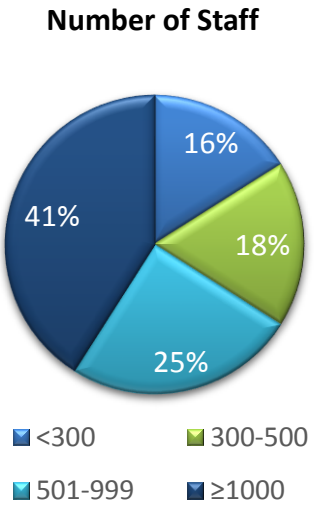
Business Sector	Number of Respondent	%
Finance and Insurance	21	41%
Logistics and Transport	8	16%
Government and Public Organizations	6	12%
Wholesale, Retail, Import and Export	5	10%
Other business sectors, including • Food and Accommodation • Real Estate • Information Technology and Communication • Manufacturing • Education	11	21%
All Companies	**51**	**100%**



3.1.2 Size of Company

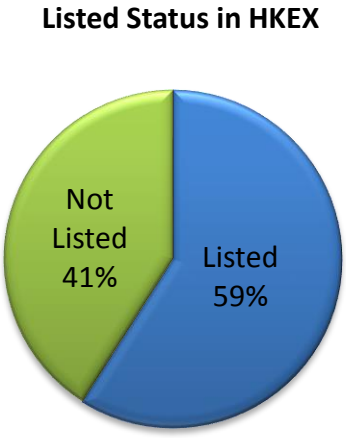
Size of Company is one of the criteria to capture valuable results for this survey as it is believed that the usage of Privileged Access is more common in a sizable company. In this survey, most of the respondents (84%) of this survey are in significant size that had ≥300 staff.

Number of Staff in the Company	Number of Respondent	%
<300	8	16%
300-500	9	18%
501-999	13	25%
≥1000	21	41%
All Companies	51	100%



3.1.3 Listing Status in Hong Kong Stock Exchange (HKEX)

Besides the size of company, the listing status of companies is important since IT Compliance and Audit is a major element for a company being listed in the Hong Kong Stock Exchange. In this survey, 59% are listed companies while 41% are not. All (100%) of the respondents with fewer than 300 staff were listed companies. In other words, all respondents of the survey were from companies with over 300 staff or otherwise they were listed in the Hong Kong Stock Exchange.



Listing Status of Companies	Number of staff in the Company			
	< 300	**300-500**	**501-999**	**≥1000**
Listed	100%	33%	23%	76%
Not Listed	0%	67%	77%	24%

3.1.4 Importance of IT System & Data

The summarized view of respondents on the importance in business sectors is calculated from the average score obtained (on a 0 – 4 marks scale) based upon their perception of importance, with 0 representing "not that important" and 4 representing "extremely important".

All respondents treated IT system and data as an important matter, with 100% of them rating "Important" or above, with a majority (67%) stating IT system and data as being extremely important.

	Extremely important (4 marks)	Very important (3 marks)	Important (2 marks)	Somewhat important (1 mark)	Not that important (0 mark)	Average score (0 – 4 marks)
All Companies	**67%**	**25%**	**8%**	0%	0%	**3.59**

In the view of business sector, regulated industries (such as "Finance and Insurance") and "Government and Public Organizations" have higher awareness with an average score of 3.67. "Logistics and Transport" is relatively in lower awareness with an average score of 3.13.

Business Sector	Extremely important (4 marks)	Very important (3 marks)	Important (2 marks)	Somewhat important (1 mark)	Not that important (0 mark)	Average score (0 – 4 marks)
Finance and Insurance	71%	24%	5%	0%	0%	**3.67**
Logistics and Transport	38%	38%	25%	0%	0%	**3.13**
Government and Public Organizations	67%	33%	0%	0%	0%	**3.67**
Wholesale, Retail, Import and Export	80%	0%	20%	0%	0%	**3.60**
Other business sectors	73%	27%	0%	0%	0%	**3.73**

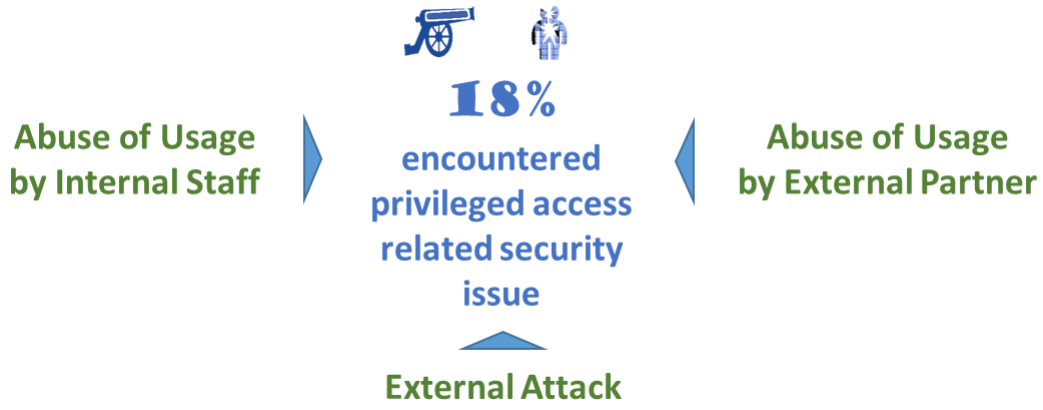
It is also noted that listed companies in general treat IT system and data more important than non-listed companies. For size of company, companies with staff <300 are extremely aware of the importance of IT system and data.

Listing Status	Average score (0 – 4 marks)
Listed Company	3.63
Non-listed Company	3.52

Number of Staff in Company	Average score (0 – 4 marks)
<300	4.00
300-500	3.22
501-999	3.69
≥1000	3.52

3.2 Security Issues Encountered

This sub-section discusses the information of security issues encountered among the respondents.



Around one-fifth of the enterprises (18%) encountered privileged access related security issue in the past while 4% have no idea whether they had encountered or not.

Below are the business sectors that encountered privileged access related issues with the type of incidents.

Business Sector	External Attack - Succeeded	External Attack - Failed	Abuse of Usage by Internal Staff	Abuse of Usage by External Partner
Manufacturing	●			
Finance and Insurance			●	
Real Estate	●	●		
Transportation and Logistics		●		
Government and Public Organizations		●	●	

No respondent reported privileged access related issues related to the abuse of usage by external partners. “Government and Public Organizations” and “Finance and Insurance” sectors did not encounter external attacks that were successful, but they do have abuse of usage by internal staff. Non-regulated business sectors such as manufacturing and real estate had experienced successful a compromise.

Reference Cases Related to Privileged Access Compromises

The consequence of security compromises due to mismanaged privileged access can be disastrous. The following compromises have occurred in both the public and private sectors.

Government and Public Organization

The most well-known case was the leakage of national secrets by former National Security Agency (NSA) employee Edward Snowden in 2013.[9] It was an insider threat caused by privileged user who could access multiple systems, some of which he should not have access to. Snowden collected over a million documents; and he leaked information about NSA by using privileged access in order to uncover programs which were collecting customer phone call records of telephone companies, requesting data of citizens from technology companies, spying on leaders of foreign countries, efforts in breaking encryption and under Internet security.

[9] Edward Snowden: leaks that exposed US spy programme
http://www.bbc.com/news/world-us-canada-23123964
The 10 Biggest Revelations From Edward Snowden's Leaks
http://mashable.com/2014/06/05/edward-snowden-revelations/#L7F2sfM9KPqc

Financial Institutions

Attackers target money in financial sector. Bangladesh's central bank was compromised in 2016.[10] Attacker bypassed the bank's weak network defense and infiltrated into the core network, using privileged access to transfer $80M out of the bank's account nearly undetected. In August 2016, Taiwan's First Commercial Bank got hacked by a sophisticated attack in which attacker first compromised a user via phishing and then traversed laterally, and subsequently gained additional privileges to install a malware on to the bank's ATM. That malware enabled the attacker to dispense $2.6M from the infected ATM.

Retail Sector

Attackers target credential data in retail industry. The US retail chain store Target was attacked in 2013 and attacker was able to exfiltrate 100M customers' payment card information leaked[11]. The attacker entered Target's corporate network by compromising the refrigerator contractor with a phishing email. The attacker then used the contractor's credential to access some of Target's systems and abused a web vulnerability to gain privilege, subsequently reaching a stage when they could infect the point of sales systems to scrape the memory for credentials.

Logistics and Transport Sector

In 2014, attacker infected hand-held scanners installed with embedded WinXP used in the logistics industry with Zombie Zero malware[12]. Once infected the zombie scanner device scanned the network for SMB file share services from inside and infiltrated the companies' ERP system via default privileged account/password to steal financial, logistics and customer information.

Energy and Utility Sector

Attackers target to bring down systems in the utility sector. In 2015, attacker compromised the Ukraine power plant and caused a power grid failure for days.[13] Attacker infiltrated the system via remote access to the control system, then traversed laterally, harvesting credentials and escalating privileged access.

[10] Bangladesh central bank hacked
http://www.bbc.com/news/technology-36110421

[11] Target data breach (Dec 2013): Hackers tapped vendor credentials
http://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/

[12] Zombie Zero Underscores Supply Chain Threat
https://securityledger.com/2014/07/zombie-zero-underscores-supply-chain-threat/

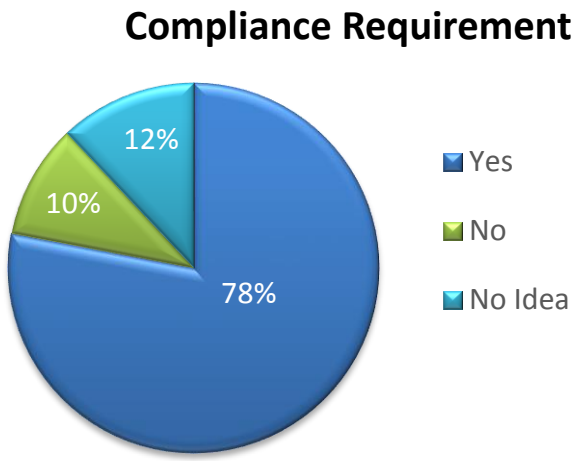
[13] More Signs Point To Cyberattack Behind Ukraine Power Outage
http://www.darkreading.com/threat-intelligence/more-signs-point-to-cyberattack-behind-ukraine-power-outage/d/d-id/1323927

Privileged Access Misuse and Exploitation a Threat for Enterprises

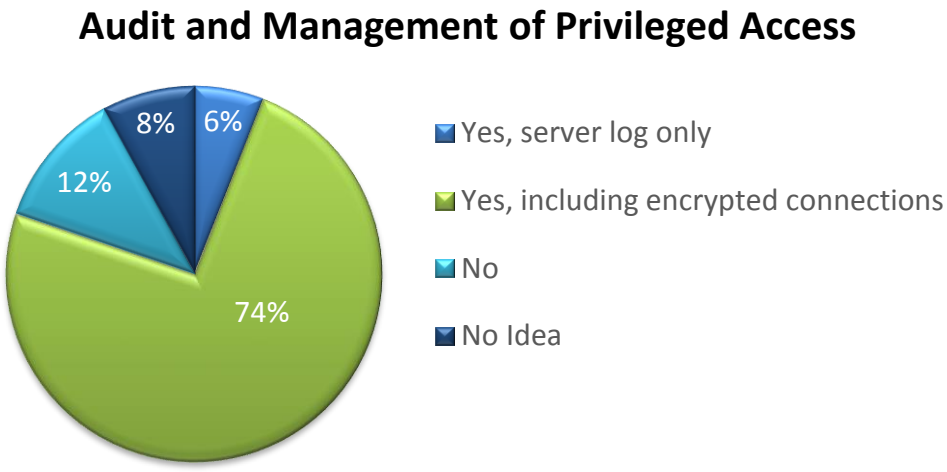
The Verizon Data Breach Investigations Report (DBIR) 2016 report highlighted long-standing vulnerabilities around privileged access misuse and exploitation. Top industries affected include healthcare, finance, and the public sector, three sectors with extremely sensitive and lucrative data. From the DBIR 2016 report, privilege misuse accounted for over 15 percent of all incidents. The report also found that 77 percent of those privilege misuse breaches involved an internal actor. It's important to note that the privilege misuse breaches are not always the result of a malicious former employee or disgruntled worker, but often stem from carelessness and lack of awareness regarding sound IT policies and protocols. Additionally, data in DBIR 2016 showed that insider and privilege misuse has been a consistent problem over the past six years that isn't going away, accounting for close to 15 percent of breaches each year since 2010.

3.3 Compliance, Audit and Management

Most of the respondents had compliance requirement (78%).



Majority (81%) had applied audit & management for privileged access (6% audit server log data only, and 75% also manage encrypted connection).

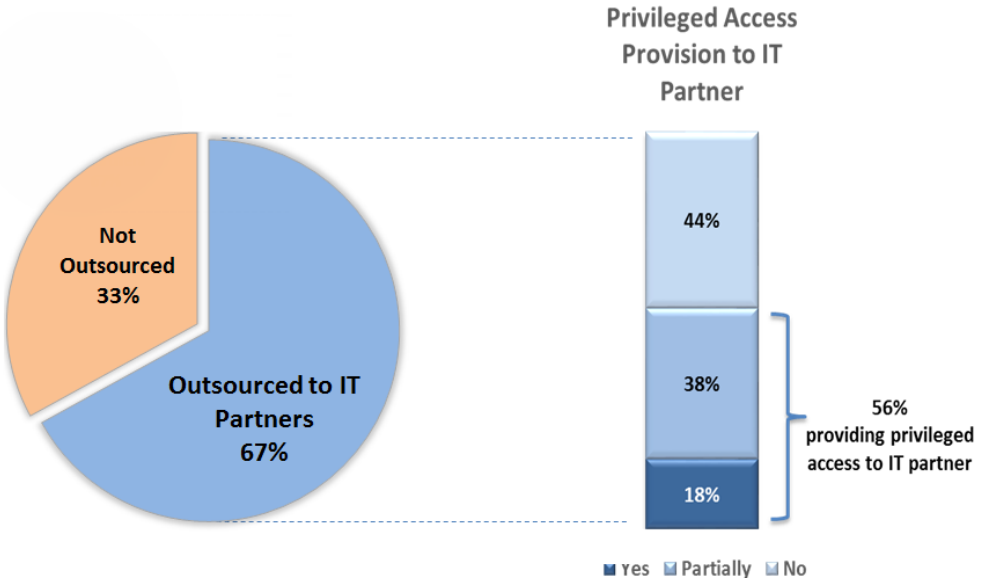


The major reason for audit & management of privileged access was to enhance security protection (78%), followed by compliance requirement (63%). This shows that enterprises are not deploying the security measures only to fulfil the compliance requirement but they do see the importance of enhancing security protection. However, enterprises were not driven much (only 20%) by the need to manage external partner access and cloud based systems to manage privileged access. Only 10% of the enterprises saw the value of Privileged Access Governance in intrusion detection and accountability management. This may be due to immaturity of privileged access market and/or the user awareness in the area was still low.

3.4 IT Outsourcing

Usage of IT outsourcing service is common within enterprises. Cloud adoption also raises the reliance of enterprises on external parties. The CloudView 2016 Research of IDC[14] found that cloud adoption would increase from 22% in 2016 to 32% in 2018, achieving a 46% growth.

In this study, over 67% of respondents did outsource part of their IT job duties to their partners. While enjoying the outsourcing services, it is noticed that providing privileged access to IT partner is unavoidable - over half of them (56%) are providing such access, either fully (18%) or partially (38%).

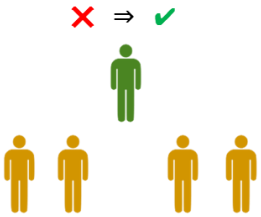


[14] Roundup Of Cloud Computing Forecasts And Market Estimates, 2016
https://www.idc.com/getdoc.jsp?containerId=prUS41039416

Around one-quarter (24%) of the respondents expected that they would provide additional privileged accounts to IT Outsourcing Partners in the next 12 months. For those who were not currently providing privileged access to IT Outsourcing Partners, 20% indicated that they plan to open such access in the next 12 months.

24%

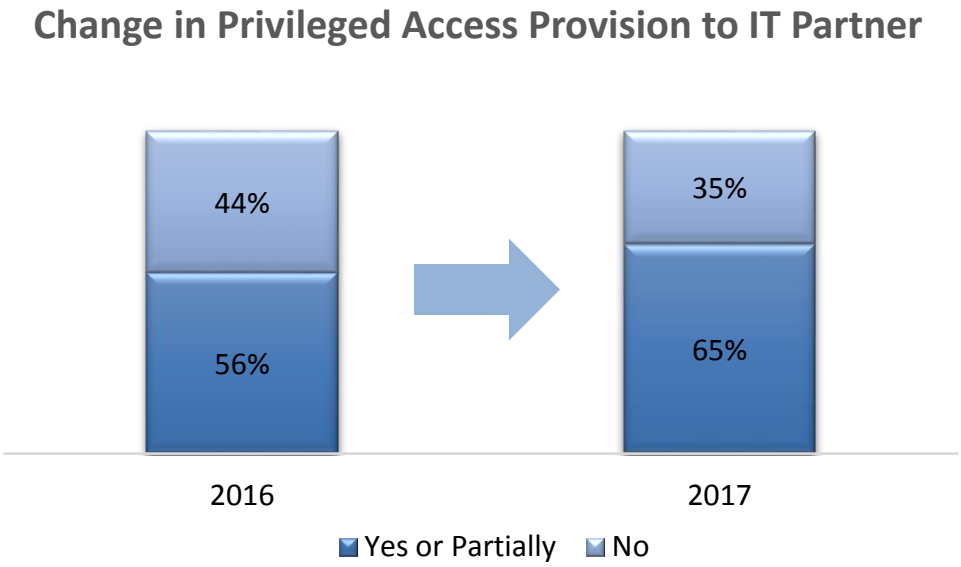
of surveyed enterprises planning to add Privileged Account within 12 Months



20%

of those currently without providing privileged access to IT partner plan to add Privileged Account within 12 Months

As a result, 65% of companies with outsourcing partners would provide privileged access to their partners in the next 12 months from the date of the study (i.e. December 2016).



3.5 Shared Account with Privileged Access

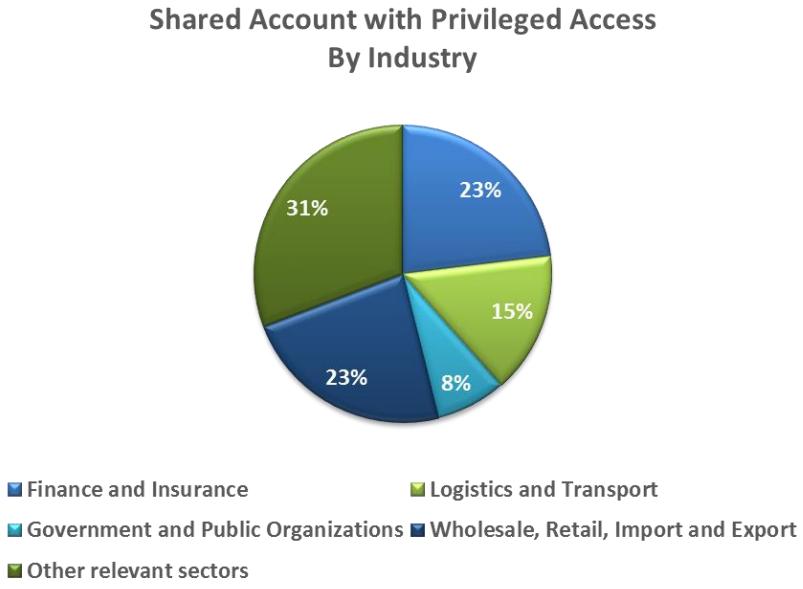
There were 31% of respondents who were at risk in term of abuse of usage by internal staff (25% having shared account and 6% no idea). They included both non-regulated ("Logistics and Transport", "Wholesale, Retail, Import and Export") and regulated sectors ("Finance and Insurance"). These enterprises are at risk of abuse of usage by internal staff.

31%

of surveyed enterprises are at risk in term of abuse of usage by internal staff

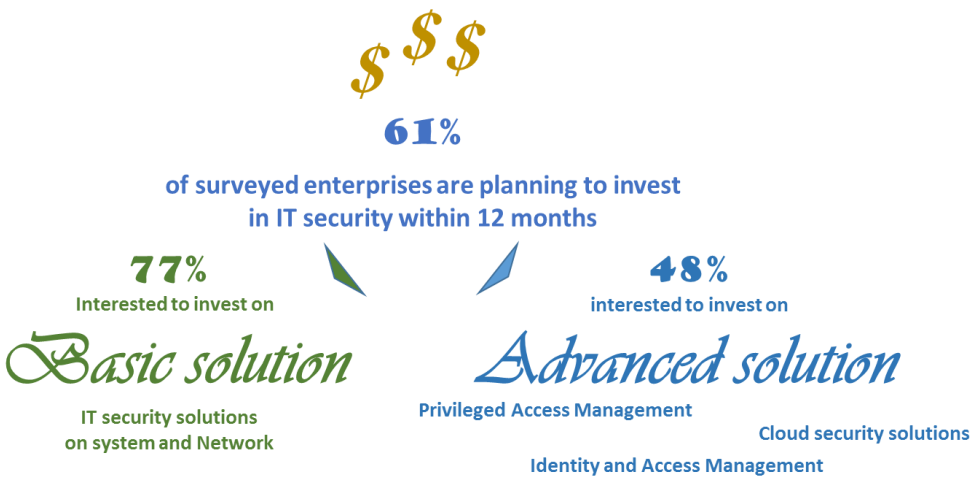
Among them, 25% admitted that they do not impose additional measure to shared accounts, while 19% do not have any idea about their shared account, which implied that the management on the shared account is not sufficient.

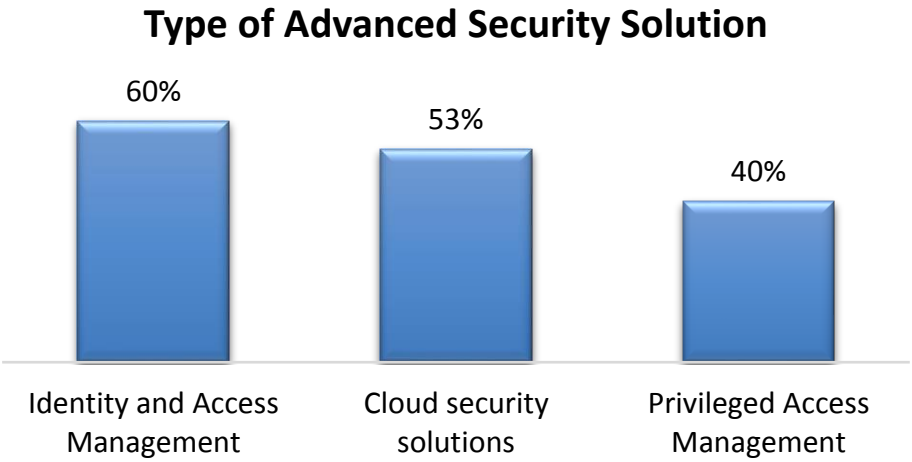
Shared account with privileged access was more common in "Finance and Insurance" (23%) and "Wholesale, Retail, Import and Export" (23%). For the other business sectors, the survey revealed that shared accounts do exist in these sectors - "Real Estate", "Education", and "Accommodation and Catering".



3.6 Investment in IT Security in the next 12 Months

There were 61% of the respondents who were planning to invest in IT security in the next 12 months. Most of them (77%) will invest in basic solutions for systems and their network. Around half of them were interested to invest in advanced solutions, where "Identity and Access Management" was the most popular choice (60%), following by "Cloud security solutions" (53%) and then "Privileged Access Management" (40%).





We further compared the behaviour of enterprises with more security exposure to those with lower exposure; by using two attributes to identify respondents with more security exposure:

(1) "Having shared privileged access accounts" means higher security risk because of the lack of accountability and confidentiality

(2) "Providing privileged access to external partner" means higher security risk because the less control of external party

We compared the interest to invest on IT security between enterprises with higher risk exposure and those with lower. We found that enterprises that had higher risk exposure (bearing both exposures) were more inclined to invest (83%) on IT security. On the other hand, enterprises having none of the exposure had lower interest (56%) to invest.

Investment in IT security in the coming 12 months

Enterprises with more security exposure	Investment in IT security in the coming 12 months
(1) Having shared accounts with privileged access	69%
(2) Provide privileged access to external partner	68%
Higher Security Exposure (Both (1) & (2))	**83%**
Lower Security Exposure (None of (1) & (2))	**56%**

The same group of enterprises that had higher risk exposure (bearing both exposures) were found to have a significant inclination (62%) to invest in advanced security solutions. On the other hand, enterprises having none of the exposure had lower interest (36%) to invest in advanced solutions.

Investment in Advanced Solution

Enterprises with more security exposure	Advanced Solution
(1) Having shared accounts with privileged access	56%
(2) Provide privileged access to external partner	62%
Higher Security Exposure (Both (1) & (2))	**60%**
Lower Security Exposure (None of (1) & (2))	**36%**

Out of the advanced solutions, Identity and Access Management was ranked at the top. Awareness of investment is higher when companies had shared account with privileged access or were providing privileged access to external partners.

Type of Advanced Solution invested

Enterprises with more security exposure	Identity and Access Management	Cloud security solutions	Privileged Access Management
(1) Having shared accounts with privileged access	80%	40%	20%
(2) Provide privileged access to external partner	63%	50%	25%
Higher Security Exposure (Both (1) & (2))	100%	33%	33%
Lower Security Exposure (None of (1) & (2))	60%	60%	80%

4 Conclusion & Recommendations

4.1 Key Findings

(1) Importance of IT system and data was well recognized

All respondents treated IT system and data as important matter, with 100% of them rated "Important" or above, with majority (67%) rated "extremely important".

(2) Government, regulated industry and listed companies had higher security awareness

Government and regulated industry sectors had higher security awareness (score 3.67, higher than the average of 3.59). Other business sectors like "Logistics and Transport, Retail" had relatively lower awareness. Listed companies had higher security awareness than non-listed companies.

(3) Government and regulated industry had fewer successful compromises related to privileged access but insider abuse still existed.

Among enterprises that encountered privileged access related security issues in the past, **government and regulated industry did not encounter successful external attacks but they do have abuse of usage by internal staff**. Manufacturing and Real Estate sectors had successful compromises in privileged access.

(4) Enterprises see the value of Privileged Access Governance

Enhancing security protection (78%) was the main reason for audit and management**,** even more than that for compliance requirement (63%). However, only a few respondents (10%) used Privileged Access Governance for intrusion detection and accountability management. This might imply that there are **rooms for improvement** in the maturity of integration of privileged access management with SIEM and other IT security infrastructure.

(5) IT outsourcing and cloud adoption are major driving force of Privileged Access Governance

Majority of respondents (67%) outsourced IT job duties to partners. Over half of these respondents (56%) had already granted privileged access to the partners and 24% would provide additional privileged accounts to partners in the coming 12 months. It was expected that **65% of enterprise which outsourced IT jobs would provide privileged access to partners in the next 12 months.**

(6) Management of shared account not satisfactory

There were 31% of respondents who were at risk of abuse of usage by internal staff.

Management on the shared account is not sufficient. 25% of these organizations did not impose additional measure to shared accounts.

(7) Enterprises with more security exposure had higher interest in advanced security solutions
Enterprises with more security exposure (having shared privileged access accounts or providing privileged access to external partner) **had higher interest in investing on IT security (up to 83%) than those with less exposure (56%).** These enterprises also **tended to be more willing to invest on advanced solutions (up to 62%) than those with less exposure (36%)**.

4.2 Advices to Secure Management of Privileged Access

(1) HKPC advised enterprises to **pay more attention to Privileged Access Governance**. **Considerations should be made to the growing reliance on external parties**, including IT outsourcing and cloud adoption, **and provision of shared accounts**.

(2) **Privileged Access Governance should be included as part of the enterprise information security strategy. Critical privileged services like remote access, VPN and cloud administrative accesses are key areas to protect**. Security controls applied should be proportional to the risk levels derived from a risk assessment.

(3) For effective management, **enterprises can consolidate and centrally manage user identities and authentication**. Role-based access control with least privileged access model should be applied with granular control down to individual commands.

(4) To provide **traceability and accountability**, privileged access activities should be logged, monitored and audited. To enhance accountability, more advanced features of privileged access management like session recording and forensics, implement reporting services (on 'who' has access to 'what', and 'when' an access occur) could be useful. **The issue of individual accountability of shared account must be addressed**, either by converting to non-shared accounts or by applying complementary measures.

(5) **Privileged Access Governance can help with the detection of APT and stealthy attacks**. Integration of privileged access management with IT security infrastructure such as IDS/IPS, IAM, SIEM or DLP can provide analytics that can help identify suspicious behaviour in privileged activities much earlier if and when an attack might occur.

- End of Report -

Appendix I: Questionnaire of Telephone Interviews

特權存取(Privileged Access)管理調查

公司名稱： _____
被訪者姓名 ： _____ 職稱： _____
聯絡電話：_____ 電郵：_____ 日期 ：_____

此部份由調查員填寫 To be Completed by Interviewer		
問卷編號：	調查員：	__日期：

公司類別 Type of Company

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.☐ 會計 8.☐ 法律 9. ☐ 顧問服務

10.☐ 專業服務(包括廣告、室內設計、速遞服務) 11.☐ 地產(包括地產經紀、物業管理)

12.☐ 建築 13.☐ 其他(請註明)：_____

如受訪者問甚麼是特權存取：

企業在不同的系統，例如企業內部的伺服器 (server)、網路或外判服務如雲端、數據中心等，給予使用者在該系統上擁有權限進出及操作，或給予使用者特權帳號 (Privileged Account) 等，權限相等於管理員 (administrator，superuser 或 root)，可以在系統內來去自如，進行任何任務。不過，如果特權存取落入不法份子手上，卻可以對系統及數據造成極大的損害。

A. 公司資料 Company Profile

1. 請問 貴公司主要從事甚麼業務？

2. 請問 貴公司有多少員工？

1. ☐1-300 2. ☐301-500 3. ☐>500

3. 請問 貴公司是否上市公司？

1. ☐是 2. ☐否

(註：如受訪公司員工人數 **少於 300 人及非上市公司** ，終止訪問。)

4. 請問 你認為 IT 系統及數據對貴公司業務的重要性

1. ☐ 極度重要 2. ☐ 非常重要 3. ☐ 重要 4. ☐ 有點重要 5. ☐ 不太重要

5. (a) 您是否遇到過與特權存取相關的安全事件 (無論是否被入侵/濫用)

1. □有　　2. □ 沒有 (跳至 #6)
3. □不知道 *[不讀出]* (跳至 #6)

(b) 安全事件的性質是 (可選多項)

1. □ 外間攻擊者成功入侵，並獲得特權存取　2. □ 外間攻擊者嘗試取得特權存取，但失敗
3. □ 內部人員濫用特權存取　　4. □ 合作伙伴濫用特權存取

6. 貴公司有否合規（Compliance）監管要求

1. □有，並已實施　　2. □有，正計劃實施　3. □暫時沒有，預期有
4. □沒有　　5. □不知道*[不讀出]*

7. 貴公司有否對特權存取的操作進行審核 (Audit) 及管理

1. □有，對所有有關的操作 (包括加密連接)　2. □有，但只包括非加密連接的操作
3. □有，只包括伺服器日誌 (log) 的數據　　4. □沒有 (跳至 #8)
5. □不知道*[不讀出]* (跳至 #8)

(b) 審核／管理特權存取的主要目的（最多二項）

1. □合規要求（如監管或審計要求）　　2. □改進涉及外部夥伴和雲端系統的安全管理
3. □增強安全保護　　4. □檢測入侵的行徑，並找出負責者
5. □其他（請說明：_____）

8. (a) 貴公司有否使用 IT 外判服務？

1. □有　　2. □ 沒有 (跳至 #8C)
3. □不知道*[不讀出]* (跳至 #8C)

(b) IT 外判服務帳號有沒有特權存取

1. □全部都有　　2. □根據需要，部分有
3. □全部沒有

(c) 貴公司未來 12 個月有否計劃增加特權帳戶的使用？（若公司會增加使用 IT 外判服務或增聘人手，就很大可能增加特權帳戶）

1. □有　　2. □ 沒有
3. □不知道*[不讀出]*

9. 貴公司有否共享帳戶(Shared Account)，是有特權存取的?

1. □有，但保留使用記錄　　2. □有，但需要額外的安全措施（例如雙重驗證）
3. □有，基於信任用戶，不設額外安全措施　　4. □沒有
5. □不知道*[不讀出]*

10. (a) 貴公司未來 12 個月有否計劃 投資在 IT 保安上?

1. ☐有
2. ☐沒有 (跳至問卷完結)
3. ☐不知道*[不讀出]*

(b) 計劃投資的領域

1. ☐特權訪問管理
2. ☐帳戶身份和存取管理
3. ☐雲端保安解決方案
4. ☐系統或網絡的保安解決方案
5. ☐其他（請說明：

_____）

問卷完結，多謝合作！