SECURITIES AND
FUTURES COMMISSION
證券及期貨事務監察委員會

Report on the 2023/24 thematic cybersecurity review of licensed corporations

February 2025

Contents

A. Executive summary 3

B. Overview of internet broking industry landscape in Hong Kong 5

C. Findings 8

- I. Phishing detection and prevention 8
- II. EOL software management 13
- III. Remote access 16
- IV. Third Party Provider management 19
- V. Cloud security 24
- VI. Compliance with Cybersecurity Requirements 29

Appendix A – Third Party Provider assessment 33

Appendix B – Examples of provisions for contract with Third Party Provider 35

A. Executive summary

1. The Cybersecurity Guidelines[1], which set out 20 baseline requirements, were issued by the Securities and Futures Commission (SFC) in October 2017 and fully implemented in July 2018.

2. The SFC completed a thematic review in 2020 (2019/20 Thematic Review) to examine the systems and related management controls of licensed corporations (LCs) which engage in internet trading business in Hong Kong (referred to as "internet brokers[2]") and assess their compliance with the Cybersecurity Guidelines and the Code of Conduct[3] (collectively referred to as "Cybersecurity Requirements"). Mobile security was also reviewed as an additional cybersecurity focus area.

3. The SFC has recently conducted another thematic review to assess the trend of compliance with the Cybersecurity Requirements. In addition, we also covered emerging cybersecurity risks and threats from phishing attacks, use of end-of-life[4] (EOL) software, remote access, third-party IT service provider (Third Party Provider) and the hosting of trading and back-office systems in the cloud environment.

4. The SFC conducted:

   (i) a survey completed by 50 selected LCs of different sizes and business types, including securities and futures brokers, leveraged foreign exchange trading firms, fund managers which provide online distribution platforms, as well as global financial institutions engaged in carrying out multiple regulated activities (collectively referred to as "respondents");

   (ii) on-site inspections of seven internet brokers to review their systems, procedures and controls; and

   (iii) deep-dive discussions with six LCs, which had global operations, to gain insight of the cybersecurity practices adopted.

5. While we have seen improvement in LCs' compliance with our Cybersecurity Requirements in certain areas, LCs should pay attention to the control deficiencies and non-compliance instances identified in the review, including issues associated with two-factor authentication (2FA) for system login, security control configurations of the system servers and firewall, implementation of security patches and hotfixes released by software providers, encryption of sensitive data and user access to system admin accounts of critical systems and databases.

[1] Guidelines for Reducing and Mitigating Hacking Risks Associated with Internet Trading (Cybersecurity Guidelines).

[2] Internet brokers refer to LCs which are engaged in internet trading and are licensed for (i) Type 1 regulated activity (dealing in securities); (ii) Type 2 regulated activity (dealing in futures contracts); (iii) Type 3 regulated activity (leveraged foreign exchange trading); and/or (iv) Type 9 regulated activity (asset management) to the extent that they distribute funds under their management through their internet-based trading facilities.

[3] These include paragraphs 18.4 to 18.7 of the Code of Conduct for Persons Licensed by or Registered with the Securities and Futures Commission (Code of Conduct) and paragraphs 1.1, 1.2.2 to 1.2.8, 1.3 and 2.1 of Schedule 7 to the Code of Conduct.

[4] EOL software refers to software which has reached the end of its useful life. The software provider has stopped supporting it and no updated security patches and fixes are available.

6. Furthermore, the cybersecurity incidents reported to the SFC by some LCs in recent years and the SFC's inspection findings show a number of security loopholes. The majority of these incidents involved the use of EOL operating systems and unpatched virtual private network (VPN)[5] solutions. Additionally, some of these incidents also involved ransomware attacks, which were potentially instigated by hackers through phishing. LCs should review and enhance (where applicable) their cybersecurity measures to reasonably protect their operations and clients from any losses and disruptions arising from cyber incidents.

7. With increasing digitalisation and automation, it is common for LCs to engage Third-Party Providers to provide IT services and to host their trading and back-office systems in the cloud environment. While leveraging the technology and services provided by these providers may be beneficial, potential cybersecurity breaches by the providers could lead to a range of issues, including system disruption, data leakage and non-compliance with applicable regulatory requirements by the LCs. Hence, we provide general guidance on Third Party Provider management and cloud security in this report to facilitate LCs in assessing and managing the associated risks.

8. We have also included examples of the measures implemented by reviewed LCs to comply with the Cybersecurity Requirements and address emerging cybersecurity risks and threats. LCs may wish to make reference to these examples when designing their own systems and controls. These examples are by no means exhaustive and LCs should review their own circumstances and put in place appropriate and effective measures.

9. The existing Cybersecurity Requirements primarily focus on internet brokers, which have always been targeted by cyber attackers. Notwithstanding, with all LCs' increasing dependence on technology to perform their critical operations, those engaging in non-internet trading business are equally susceptible to cyber-attacks. In this connection, in 2025, we plan to comprehensively review the existing Cybersecurity Requirements and expected standards, and develop an industry-wide cybersecurity framework to provide guidance to all LCs in better managing cybersecurity risks.

[5] VPN creates an encrypted tunnel between user devices and the corporate network. Users can seamlessly connect to corporate applications through VPN.

B. Overview of internet broking industry landscape in Hong Kong

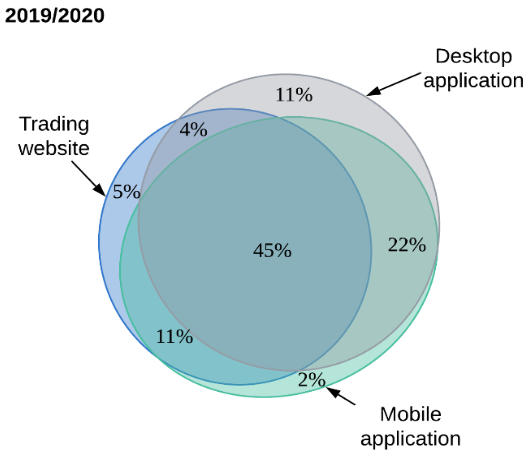
10. Nowadays, it is common for investors to place orders through internet trading channels to buy or sell investment products, including securities, futures and leveraged foreign exchange products, in Hong Kong. This has been evidenced by the returns submitted by firms licensed for Type 1, 2 or 3 regulated activities in the past few years. In 2021, over 90% of active clients[6] traded through internet brokers and this proportion continued to rise to 96.9% in 2023.

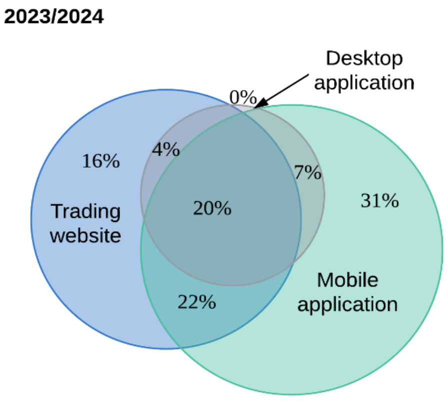
11. The SFC's Business & Risk Management Questionnaire (BRMQ) submitted by internet brokers for 2023 indicates that 92% of the internet brokers have implemented the internet trading systems provided and supported by Third Party Providers[7]. Furthermore, 70% of these internet brokers use the internet trading systems provided by five vendors, and the largest vendor has around 30% market share.

Internet trading channels

12. In general, internet trading channels provided by internet brokers to clients include desktop applications installed on clients' computers, trading websites and mobile applications. Internet brokers may provide one or multiple channels to clients. In the survey conducted for our 2019/20 Thematic Review, desktop application was the most common internet trading channel offered by internet brokers. Our 2023/24 survey shows that mobile application has become the most common internet trading channel offered.

Internet trading channel offered	Percentage of internet brokers in 2019/20 Thematic Review	Percentage of internet brokers in 2023/24 Thematic Review
Desktop application	82%	31%
Mobile application	80%	80%
Trading website	65%	62%





[6] Active clients refer to clients who have completed at least one transaction during the year.
[7] Third-Party Providers include external vendors and affiliates within the same group.

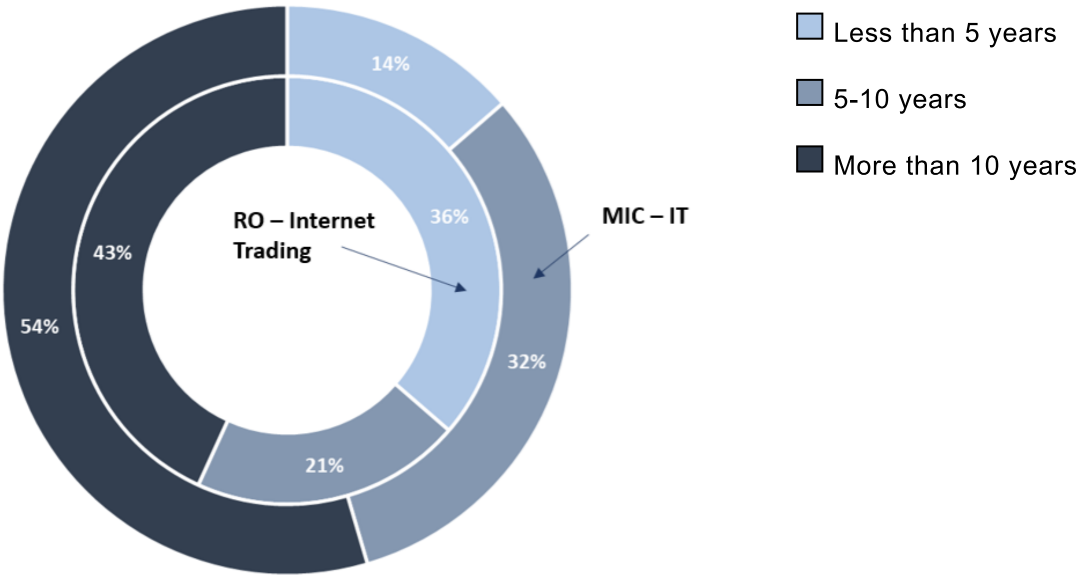
Experience of senior management responsible for the supervision of internet trading systems

13. Of the 50 respondents:

- seven respondents’ responsible officers (RO) for the overall management and supervision of internet trading systems (RO-Internet trading) had IT-related qualifications while 28 respondents’ RO-Internet trading had more than five years of IT management experience in the securities or futures industry; and

- the Manager-In-Charge of IT (MIC-IT) of 25 respondents had IT-related qualifications, while the MIC-IT of 44 respondents had more than five years of IT management experience in the securities or futures industry.

Years of IT management experience in securities or futures industry (RO-Internet trading and MIC-IT)



Cybersecurity incidents

14. LCs reported eight material cybersecurity incidents between 2021 and 2024. Some of these had caused significant business disruptions or hacking of client accounts. Specifically, it was noted that:

- in two cases, the LCs violated most of the baseline requirements and expected standards set out in our Cybersecurity Guidelines and the Circular of “Review of internet trading cybersecurity” issued in September 2020. These vulnerabilities exposed these LCs to significant cybersecurity risks, which eventually led to ransomware attack (potentially instigated by hackers through phishing) that impacted all the IT systems, including internet trading systems, settlement and back-office systems, causing severe disruption to business operations;

- in another case, one LC reported an incident where its back-office services were disrupted when its vendor’s network was compromised and it did not have adequate contingency plan in place; and

- some of these incidents involved security loopholes in the LC’s network, through which fraudsters gained access to the LC’s trading systems and made unauthorised changes to client data. The fraudsters then gained control of the victim clients’ account and conducted unauthorised transactions.

In addition, in some cases, the LCs concerned used EOL software in their systems and servers, which may have contributed to these cyber-attacks.

C. Findings

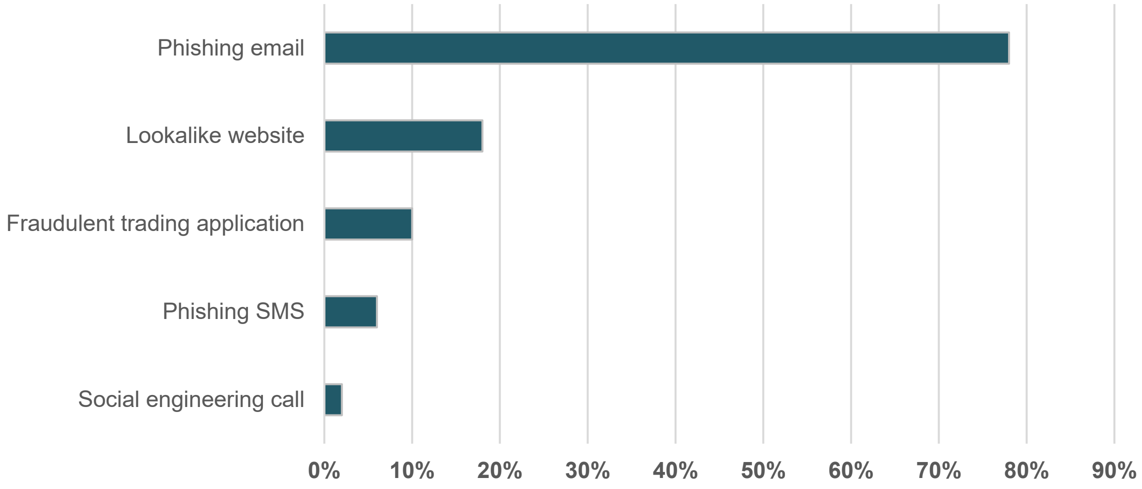
I. Phishing detection and prevention

15. Phishing attack is a form of social engineering attack where phishers pose as trustworthy organisations (eg, financial institutions and government authorities) and individuals (eg, senior executives of the company and acquaintances) to entice victims to provide personal and sensitive information or infect a user's computer or mobile device with malware.

16. Typical attack attempts include phishing emails, phishing SMS, fake internet trading websites and fraudulent mobile trading applications. Phishers may lure users to click the malicious hyperlinks embedded in emails or SMS to direct them to undertake transactions, provide personal and sensitive information, or open infected attachments. These acts may (i) compromise system privileged accounts and (ii) lock the users' devices and the firm's systems by ransomware, thus leading to severe system disruption, data loss and leakage.

17. According to InfoSec[8], phishing attack remains the most common form of cyber-attacks in recent years. Our survey also indicated that most survey respondents experienced different kinds of phishing attack attempts, although these attack attempts were ultimately filtered out or blocked with no actual impact to the respondents' systems and data.

Types of phishing attacks identified by respondents



18. In one of the cybersecurity incidents reported, it appears that the ransomware attack suffered by the victim LC originated from a phishing email. As a result of the attack, the systems and data of the victim LC were encrypted by ransomware and could not be accessed. The victim LC was unable to restore the systems and data, necessitating the rebuilding of the entire system to resume its internet trading business.

[8] https://www.infosec.gov.hk/en/knowledge-centre/phishing

19. The clients of the LCs may also be targeted by phishing attacks, resulting in leakage of their personal and sensitive data.

Key observations

20. Some respondents failed to install anti-malware solution on their trading systems to protect against phishing attacks. Separately, the post-mortem review of one reported cybersecurity incident indicated that the LC failed to update the signature file of the anti-malware software in a timely manner, and the file had been outdated for one year, which may have contributed to the incident. When the signature file is not updated, the anti-malware software cannot detect and block new malwares released by cyber attackers.

21. Some respondents covered phishing related contents in their cybersecurity awareness training, including common types of phishing, potential impacts, and practices to protect against phishing. Without relevant training, staff may fail to identify common signs of phishing, such as grammatical and spelling errors in messages, suspicious links, attachments and domain names. As a result, they may unintentionally click on suspicious links, download suspicious attachments or disclose sensitive information.

22. It is also important for clients to stay alert of phishing emails or SMS. In this connection, some respondents provided anti-phishing tips and reminders to clients. For example, cybersecurity reminders are prompted upon clients' login to the trading application systems or mobile applications, or alerts are posted on the LCs' website. These would remind clients to be vigilant when opening messages or browsing websites purported to be from these LCs.

Expected standards

LCs should:

(a) deploy anti-malware solutions to all servers and workstations, irrespective of the operating systems used, and update the malware signature files of these anti-malware solutions on a timely basis;

(b) not send electronic messages (such as emails or SMS) with embedded hyperlinks that direct clients to their websites or mobile applications to undertake transactions, and not ask clients to provide via hyperlinks sensitive personal information, including login credentials and one-time passwords (OTPs);

(c) keep abreast of latest cybersecurity attacks, refer to the relevant materials published by international standard setters such as National Institute of Standards and Technology[9] (NIST) and utilise local resources, including CyberDefender[10] and InfoSec[11];

(d) provide regular cybersecurity awareness training to all staff, where phishing should

[9] Anti-phishing guidance from NIST: https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/phishing

[10] Guidance notes from Cyberdefender: https://cyberdefender.hk/en-us/phishing_attack/

[11] Knowledge centre on phishing attacks from InfoSec: https://www.infosec.gov.hk/en/knowledge-centre/phishing

be included as one of the training topics;

(e) send clients regular cybersecurity alerts and reminders, including security reminders against phishing attacks; and

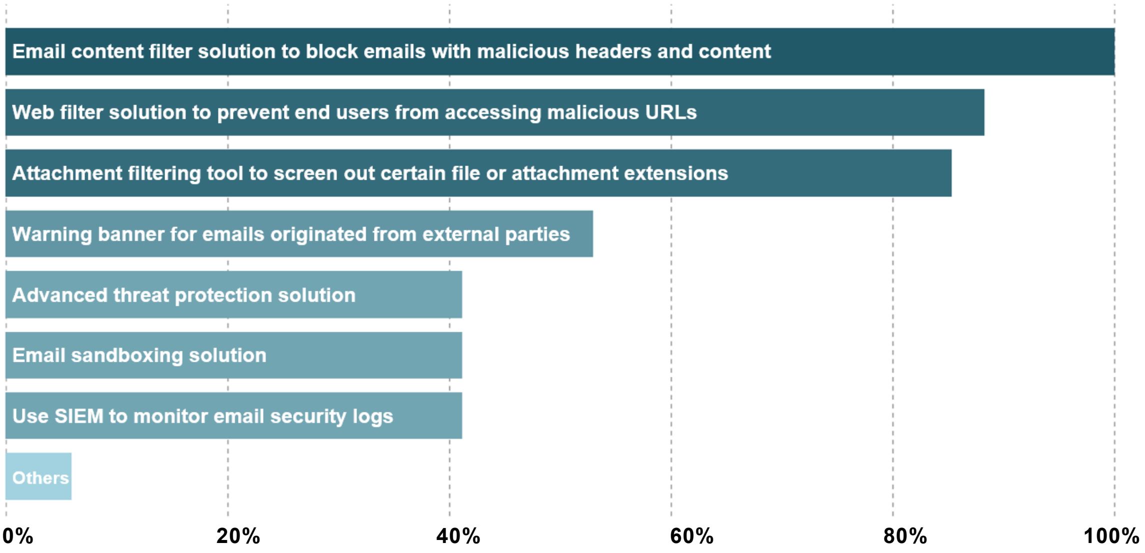
(f) ensure their cybersecurity incident handling and reporting policies and procedures cover phishing attack scenarios that could lead to complete system shutdowns or data leakage, and specify the internal escalation and external reporting procedures.

Examples of measures implemented by LCs

Anti-phishing measures

23. Most respondents implemented anti-phishing solutions such as email filtering and web filtering solutions. For example, a small number of respondents would block access to uncategorised websites by the web filtering tool as newly set-up phishing websites would normally be uncategorised. In addition, some respondents enabled a warning message displayed in emails from senders outside the company. These solutions help to mitigate the risk of phishing attacks, which primarily originated from emails with malicious hyperlinks.

Email security controls for prevention and detection implemented by respondents



24. An inspected LC implemented an email sandboxing solution to analyse emails for any malicious content. Once a suspicious email was identified, an alert would be triggered for security operations centre (SOC) to follow up with respective email recipients. This allowed the LC to identify potential phishing attempts in a timely manner and mitigate any potential consequences.

25. A respondent partnered with a telecommunication company to identify phishing messages sent to staff through SMS, which prevented staff from receiving fraudulent messages and protected their mobile devices.

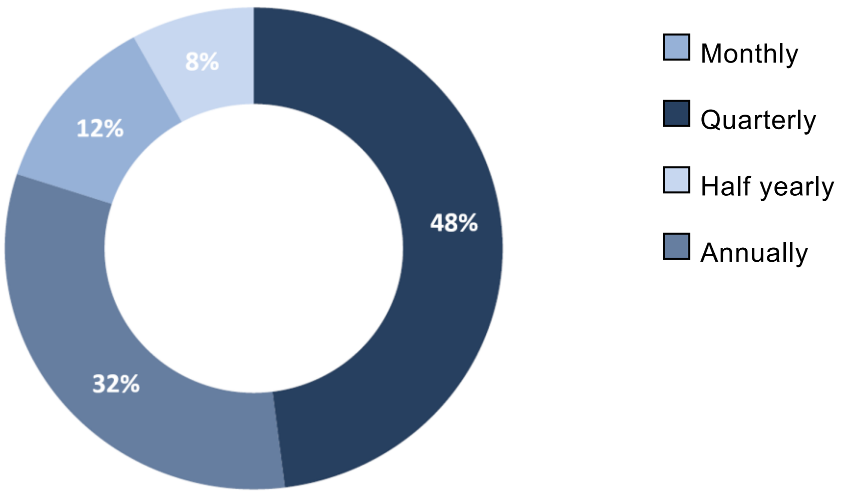
Phishing simulation exercise

26. Conducting phishing simulation regularly is an effective way to test staff awareness and responses to phishing attacks. This also allows the firms to evaluate the overall vigilance level of their staff and assess if additional training is required.

27. Many respondents conducted regular phishing simulation exercises to enhance their staff awareness. Amongst these respondents, around half of them arranged phishing simulation exercises quarterly, and around one-third of them arranged phishing simulation exercises annually.

28. To improve the effectiveness of phishing simulation exercise, most respondents arranged follow-up training to staff who failed the phishing simulation. For staff who repeatedly failed the phishing simulation, a small number of respondents would take disciplinary actions against staff, including salary review or even termination in extreme cases. On the other hand, a small number of respondents would reward staff who performed well in the phishing simulation exercise and reported phishing. Such "carrot and stick" mechanism could enhance effectiveness of phishing simulation exercise.

Frequency of phishing simulation exercise

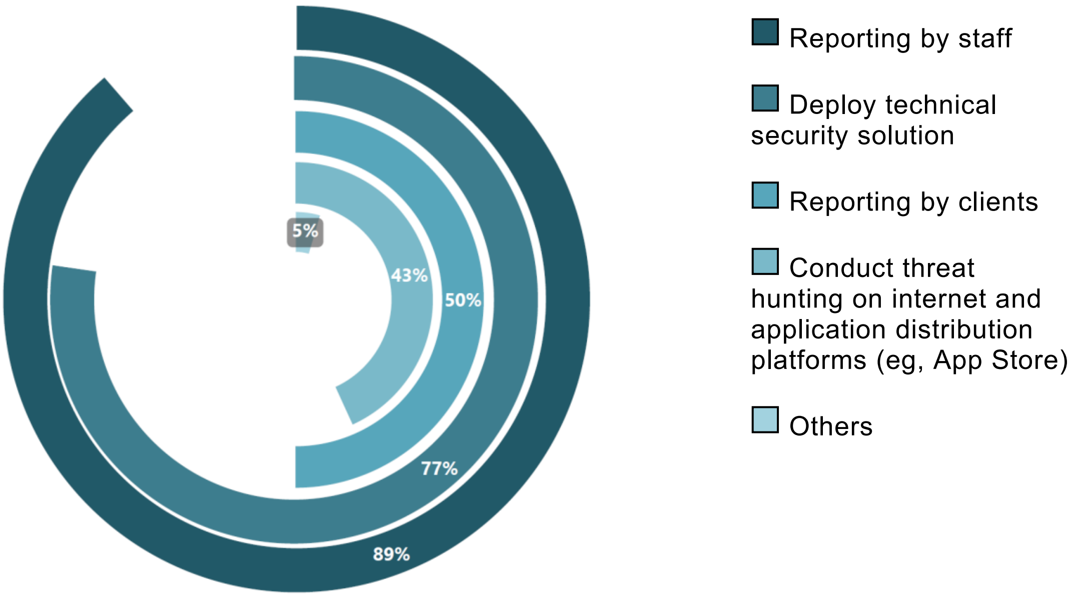


29. An inspected LC would send the phishing simulation result to all staff. The result showed how many staff clicked the phishing hyperlinks and how many staff entered login information on the phishing website. Tips were also sent together with the phishing simulation result to remind staff how to identify phishing emails and stay alert. This helps to foster staff's vigilance against phishing attacks, and strengthen the security culture of the organisation.

Identification and reporting of potential phishing attacks

30. Most respondents identified and detected phishing attacks through reporting by staff or clients, and utilisation of technical security solutions, such as email content and web filtering solutions. This indicates the importance of enhancing staff and clients' awareness as well as implementing appropriate technical safeguards.

Phishing attack identification and detection methods by respondents



31. An inspected LC encouraged staff to report phishing, and offered specific reporting channels, such as a dedicated phone number and an email for reporting phishing. Clear reporting channels allow effective handling of phishing attacks by directing the incidents to responsible teams for investigation and further actions in a timely manner to reduce adverse impacts.

32. In order to protect clients, most respondents conducted regular searches to identify fake or suspicious websites or mobile applications of their firms. One of them deployed an automated solution to proactively monitor and identify phishing websites mimicking its firm's login page, while some respondents adopted vendor services to monitor fraudulent websites of their firms. Upon the identification of a fraudulent website, these firms (i) would request the domain service provider to take down the website and (ii) post alert message on their social media in a timely manner to remind clients to stay alert of the phishing website and scams. In addition to protecting clients, these measures could also help protect the firm's brand and reputation.

33. Some LCs participated in the SMS Sender Registration Scheme, where SMS messages originated from the LCs can be differentiated by Registered SMS Sender IDs prefixed with "#". This helps clients to verify the identities of the SMS senders, thereby preventing fraudsters from masquerading as legitimate entities.

II. EOL software management

34. IT asset lifecycle management refers to end-to-end tracking and management of IT assets to ensure that every IT asset used by the firm is properly identified, maintained, upgraded and disposed of at the end of its lifecycle. EOL is a phase in the software lifecycle where software providers no longer provide a particular version of the software with technical support and maintenance, including updating security patches or hotfixes, features enhancement and bug fixes.

35. EOL software is prone to significant cybersecurity risk. This risk is heightened when vulnerabilities exist in the unpatched software and become targets for exploitation by attackers. The attackers may utilise them as an entry point to penetrate the victims' IT environment, and gain privileged access to critical systems and data. This may lead to data breach and system disruption. Hence, it is crucial for LCs to implement robust EOL software management to ensure software in use are up-to-date and secure.

Key observations

36. While most of the respondents have developed policies and procedures on IT asset management, some of them did not specifically cover EOL software management. Furthermore, it is concerning that some large LCs did not have any IT asset management policies in place. This calls into question whether they could properly manage EOL software.

37. Furthermore, half of the respondents were using EOL operating systems[12] in their IT environment. In an extreme case, a respondent reported to be using six EOL software. It is also highly concerning that most of these operating systems have far exceeded their EOL date. These arrangements significantly heightened the LCs' exposure to hacking attacks.

38. In fact, based on the post-mortem report of cybersecurity incidents provided by several LCs, they all used EOL operating systems on their servers and workstations, eg, Microsoft Windows Server 2008 and Windows 7, which were vulnerable and easily exploited by hackers.

Expected standards

LCs should:

(a) develop policies and procedures on IT asset management which cover, amongst other things, the identification and monitoring of the EOL or close to EOL status of the software in use, software upgrade or migration strategy and the corresponding remedial plans in managing obsolete software, where appropriate;

(b) maintain a complete IT asset inventory list and review this list at least annually to

[12] For example, Windows Server 2008 or prior versions, Windows 7 or prior versions, CentOS 8, CentOS 6 or prior version, Ubuntu 21.10/21.04/20.10/19.10/19.04/18.10, Ubuntu 18.04 LTS, Ubuntu 17.10 or prior version, RHEL 6 or prior version.

ensure its completeness;

(c) monitor the validity of existing software on an ongoing basis, eg, by gathering EOL relevant information from official sources of software providers[13] in a timely manner;

(d) maintain a complete and up-to-date EOL list for all relevant IT assets and proactively plan for replacing or upgrading software that is EOL or close to EOL, where appropriate; if LCs require additional time to address technical compatibility issues or business operational concerns, and thus could not update or replace the software before it becomes EOL, the LCs should adopt the tactical measure to subscribe for extended support from software providers to ensure the availability of security patches or hotfixes; and

(e) cease the use of EOL software on all critical system servers and databases, including internet-facing servers (eg, web servers) and trading related servers and databases. LCs should also upgrade or replace other EOL software in a timely manner (ie, those not on critical system servers and databases), unless they could properly mitigate the corresponding cybersecurity risk.

Examples of measures implemented by LCs

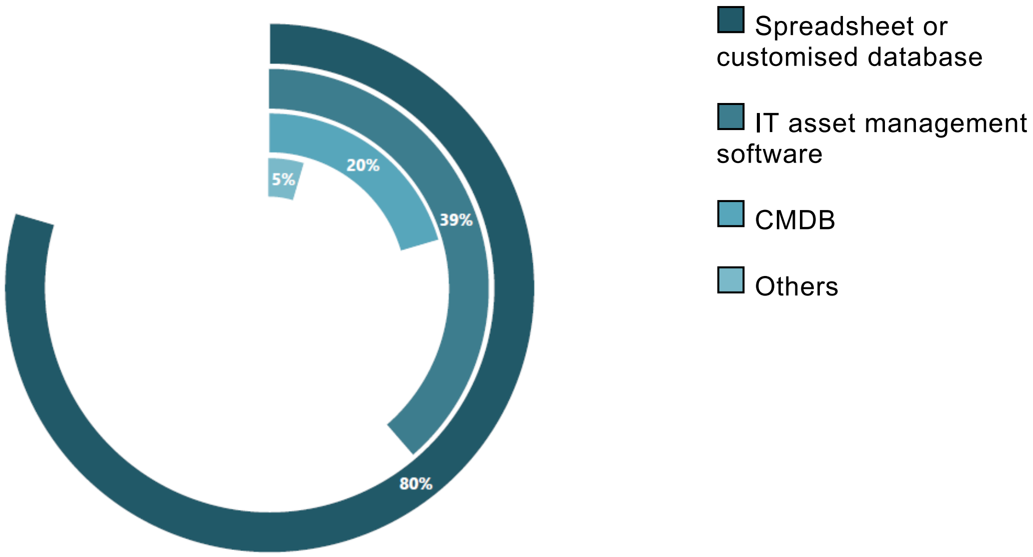
Identification of software inventory

39. To facilitate the IT asset management, our survey results revealed that all respondents used at least one software or tool for IT asset management. Amongst them, spreadsheet or customised database was the most common tool used, followed by IT asset management software and configuration management database (CMDB)[14].

[13] For example, https://access.redhat.com/support/policy/updates/errata for Linux-related resources and https://learn.microsoft.com/en-us/lifecycle/overview/product-end-of-support-overview for Microsoft Windows related resources as reference.

[14] CMDB is a centralised repository that stores and manages information about the inventory of all hardware, software, network components, and other assets in an organisation's IT infrastructure.

IT asset management software and tools adopted by respondents



40. To ensure that the software inventory is complete and up-to-date and could be properly managed:

    - some respondents implemented an automated software identification tool to regularly scan the network infrastructure and identify the software in use but not yet registered or updated in the inventory; and

    - one respondent performed quarterly attestation on the software inventory.

Planning and monitoring of EOL software upgrade or replacement

41. A small number of respondents planned for the prioritisation of EOL software replacement or upgrade 24 months prior to the date of EOL. This allowed LCs to allocate sufficient resources for handling these upgrades or replacements.

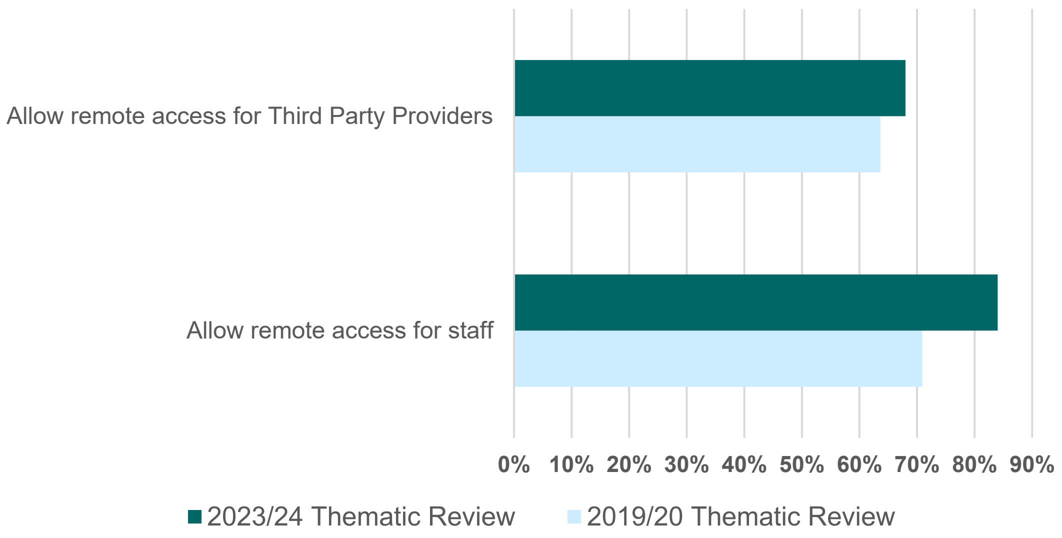
42. A small number of respondents used a centralised system for software inventory management. This system would send automatic email notifications to the corresponding IT owners to remind them to kickstart the EOL planning and formulate the remediation plan prior to the official EOL date.

43. A small number of respondents developed a dashboard or risk matrix to keep track of EOL replacement and upgrade status, and arranged regular meetings for regional Chief Information Officer (CIO) and other IT management to discuss the latest EOL remediation status. These aided the senior management in supervising the LC’s cybersecurity risk management.

III. Remote access

44. Most respondents allowed remote access for staff and Third Party Providers. Upon comparing the statistics of the 2019/20 Thematic Review and this review, we have seen a rising trend in remote access adoption.

Remote access adoption



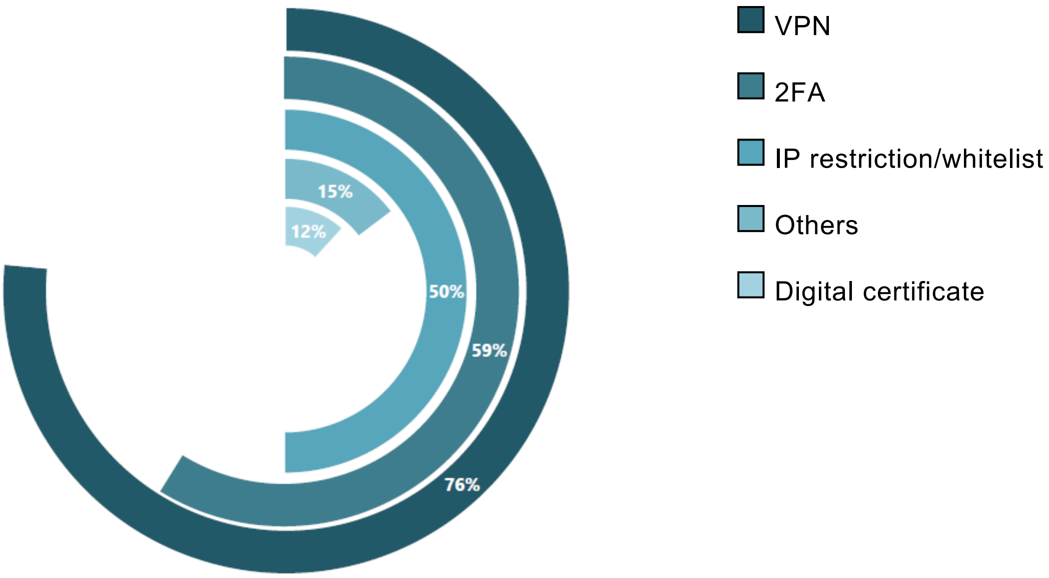
45. The increased use of remote access solutions has given rise to new threats and vulnerabilities to LCs. Cybercriminals such as ransomware groups[15] are targeting vulnerable remote access solutions as an entry point to infiltrate internal networks and access systems and sensitive data. The recent cybersecurity incidents highlight how cyber-attackers can exploit vulnerabilities in unpatched VPN solutions and insecure network management ports, such as remote desktop protocol (RDP) or secure shell (SSH) protocol.

<u>Key observations</u>

46. Many respondents utilise RDP or SSH services to remotely access internal networks for investigation and remediation of technical issues, amongst other things. However, some respondents did not implement 2FA or VPN (or other technical solutions that provide the same security protection) to secure the remote access on RDP and SSH connection, which exposed the internal network to security threats.

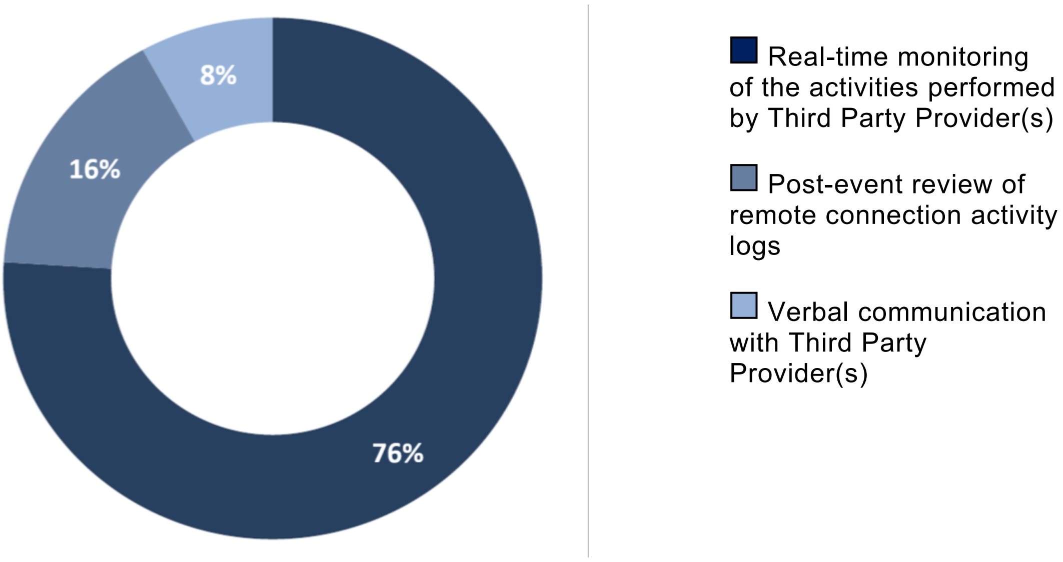
[15] Such as Lockbit ransomware group, exploited a vulnerability in a remote access solution to gain unauthorised access to systems of large organisations around the world in November 2023.

Security controls for RDP and SSH connection



47. To mitigate the risks associated with remote access by Third Party Providers, most respondents performed real-time monitoring[16] of the Third Party Providers' technical support activities through remote connection to quickly detect any suspicious behaviour. Some respondents performed post-event review of the remote connection activity logs to identify irregularities.

Security controls on remote access provided to Third Party Providers



[16] IT staff would monitor vendor's activities through screen sharing to ensure that no unauthorised activities are undertaken. They would also receive system alerts if abnormities were detected.

48. Some respondents did not have controls (eg, temporary access suspension) in place when multiple invalid login attempts were detected. This increased the vulnerability to unauthorised access to the LC's internal systems and potential data leakage.

49. Some respondents did not cover remote access in their security patch management procedure. A small number did not apply updated security patches to VPN software for over one year.

50. Some respondents allowed Third Party Providers to access their internal networks remotely. However, a number of them:

- did not have policies and procedures in place to manage such remote access;
- did not require senior management's (MIC-IT or RO) written approval when granting remote access to Third Party Providers; and
- granted permanent remote access to Third Party Providers.

The lack of proper procedures and controls allows Third Party Providers to have excessive access (or even unauthorised access) to the LC's internal networks. This poses significant cybersecurity risks to the LC and may cause disruptions to its systems and operations.

Expected standards

LCs should:

(a) develop policies and procedures on remote access management to cover, amongst other things, the requirements of remote access assignment, approval, and monitoring;

(b) grant remote access rights on a "least privileged" and "need-to-have" basis;

(c) remove unnecessary remote access rights in a timely manner, and ensure that LCs' senior management, including MIC-IT, or their delegates review the list of users granted remote access, including external parties (ie, business partners and Third Party Providers) and contract staff, on a regular basis (at least annually);

(d) implement adequate security controls over remote access to its internal network, and in particular:

- only allow remote access via VPN or other technical solutions that provide the same security protection, such as Virtual Desktop Infrastructure;
- implement multi-factor authentication (with at least two factors) to ensure that only authorised users can access the network or sensitive data repositories; ensure that passwords, if used as one of the authentication factors, are subject to the same password policies as stipulated in the Cybersecurity Guidelines; and
- implement session timeout control requirements.

When granting remote access to Third Party Providers, LCs should:

(a) not grant them permanent access rights; and

(b) log and monitor Third Party Providers' remote connection to LCs' internal networks and the activities undertaken.

LCs should comply with the expected standards on remote access set out in the "Report on Operational Resilience and Remote Working Arrangements"[17].

Examples of measures implemented by LCs

51. Most respondents allowed users to remotely access their internal networks using personally-owned devices. In order to:

(i) better protect the internal system and data:

- a small number of respondents disallowed copy and paste and drive mapping features in the virtual desktop environment to prevent data leakage;
- a respondent would be able to remotely wipe enterprise applications and data to prevent data leakage once the mobile device is lost or compromised or after the employee has resigned. In addition, it can block mobile devices operating on outdated operating software from remotely accessing its internal system and data; and
- a respondent placed remote access and wireless systems or resources, such as the VPN servers, the wireless controllers and the authentication servers, in a demilitarised zone (DMZ) instead of internal network segments which host sensitive business and client data.

(ii) prevent and identify unauthorised remote access to its internal network:

- a respondent implemented controls to block remote access from certain IP addresses, such as private VPN, sanction countries, blacklisted IP addresses, and when the geolocation of the user's login IP address changes from one country to another country within a short period of time; and
- a respondent implemented IP whitelisting for remote connection by the Third Party Provider so that it would receive email notifications upon the Third Party Provider's remote login which allowed immediate investigation of any irregularities.

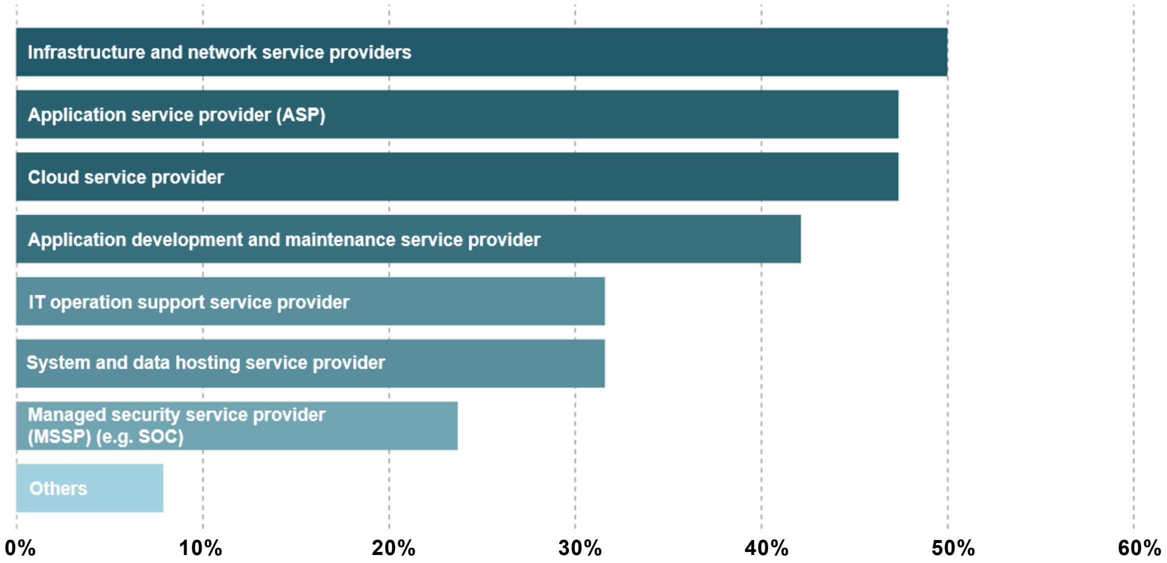
IV. Third Party Provider management

52. With the trend of increasing digitalisation and automation in the financial sector, it is common for LCs to engage Third Party Providers to provide IT related services. Our survey indicates that, to support their business, most respondents engaged with various

[17] https://www.sfc.hk/-/media/EN/files/COM/Reports-and-surveys/Report_Operational-resilience-and-remote-working-arrangements_Oct-2021_EN.pdf

types of Third Party Providers. Their services include application development and maintenance service, IT operation support service, cloud service, infrastructure and network service, system and data hosting service and managed security service (eg, SOC).

Types of Third Party Providers used by respondents



53. While leveraging the technology and services provided by Third Party Providers may benefit LCs by reducing cost, enhancing operational efficiency, etc, LCs must understand the associated cyber risks. Potential cybersecurity breaches by the service providers could lead to system disruption, data leakage, non-compliance with applicable regulatory requirements and other issues. In one of the cybersecurity incidents reported by an LC, its clearing services were disrupted due to a cyber-attack on its service provider.

54. It is also important to note that while LCs can outsource the implementation of the cybersecurity controls to Third Party Providers, their senior management (ie, their ROs and MIC-IT) should be responsible for the overall management and supervision of the internet trading systems, for defining the cybersecurity risk management framework and ensuring compliance with, amongst other things, the Cybersecurity Requirements.

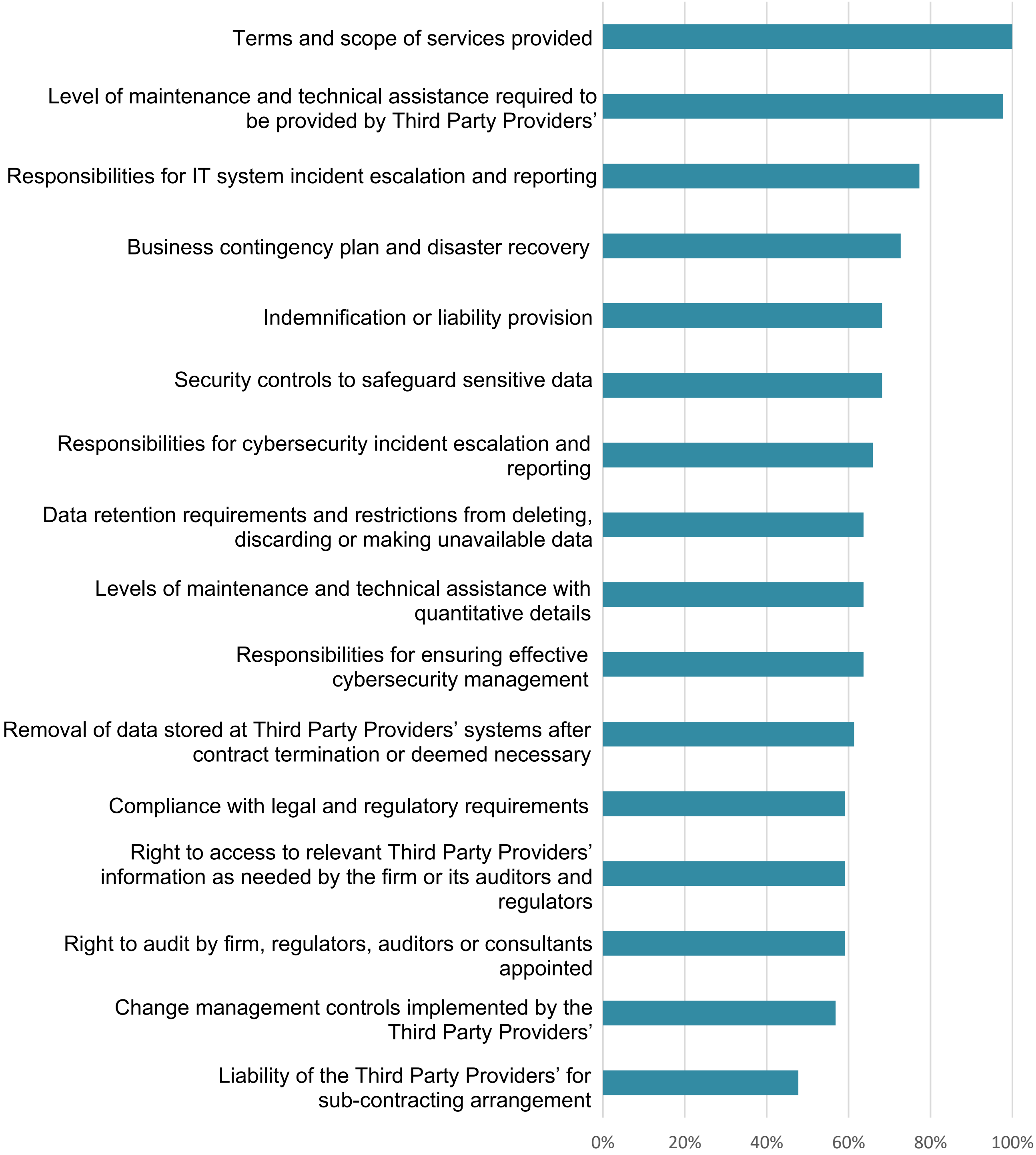
Key observations

55. Some respondents did not have policies and procedures in place on Third Party Provider management to holistically identify, assess, monitor and mitigate the cybersecurity risks associated with using such providers.

56. A small number of respondents did not conduct due diligence prior to the appointment of the Third Party Providers. Without proper due diligence, these LCs may not be able to select the most suitable service providers with the right ability and resources and assess the cybersecurity risk implications associated with the appointment of the service providers.

57. All respondents have entered into a formal contract or service-level agreement (SLA) with Third Party Providers. However, the coverage of these agreements varied. In particular, some did not specify cybersecurity-related requirements and service providers' responsibilities, such as those for cybersecurity incident escalation and reporting to LCs. The lack of clear terms also made it difficult for LCs to properly monitor the performance of these service providers.

Terms stipulated in the SLA



58. Some respondents did not perform regular assessment on the security controls of their Third Party Providers. In some other cases, the scope of regular assessments was not sufficient. For example, some respondents did not assess the Third Party Providers' compliance with respondents' pre-defined cybersecurity-related requirements.

59. Some respondents did not incorporate Third Party Providers-related cybersecurity scenarios and necessary contingency measures into their business contingency plans. This hinders the LCs from effectively responding to IT incidents related to service providers, such as system disruption and data leakage.

60. LCs are required to provide instructions to the service providers on the security control configurations and parameters to be implemented in the internet trading system supplied by Third Party Providers. However, some LCs have failed to properly do so. For example, an inspected LC failed to ensure that the setting in the internet trading system complied with the Cybersecurity Requirements in a number of key areas, such as allowing email OTP as a 2FA means and setting prolonged session timeout.

Expected standards

LCs should:

(a) develop policies and procedures on Third Party Provider management, including Third Party Provider due diligence, selection and approval, contract management, performance monitoring, risk management (including cybersecurity risk management), compliance with regulatory requirements, dispute resolution, termination and exit strategy, and record keeping;

(b) maintain a complete list of Third Party Providers, including the name, contact details and description of services provided, to facilitate ongoing Third Party Provider management and monitoring;

(c) conduct proper due diligence on Third Party Providers prior to appointment, and in particular, assess the adequacy of the cybersecurity measures implemented by the Third Party Providers;

(d) enter into a formal SLA with Third Party Providers which specifies the terms of service and the responsibilities of the providers, particularly:

- the cybersecurity measures to be implemented by the providers; and
- the reporting procedures for cybersecurity incidents;

(e) regularly review and where appropriate revise the SLA to reflect any changes to the outsourcing arrangements or regulatory developments;

(f) monitor the performance of the Third Party Providers on a regular basis to identify any non-compliance with the SLA or unsatisfactory performance in a timely manner;

(g) set the security control configurations and parameters utilised in the systems supplied by Third Party Providers in compliance with relevant requirements, including the Cybersecurity Requirements; and

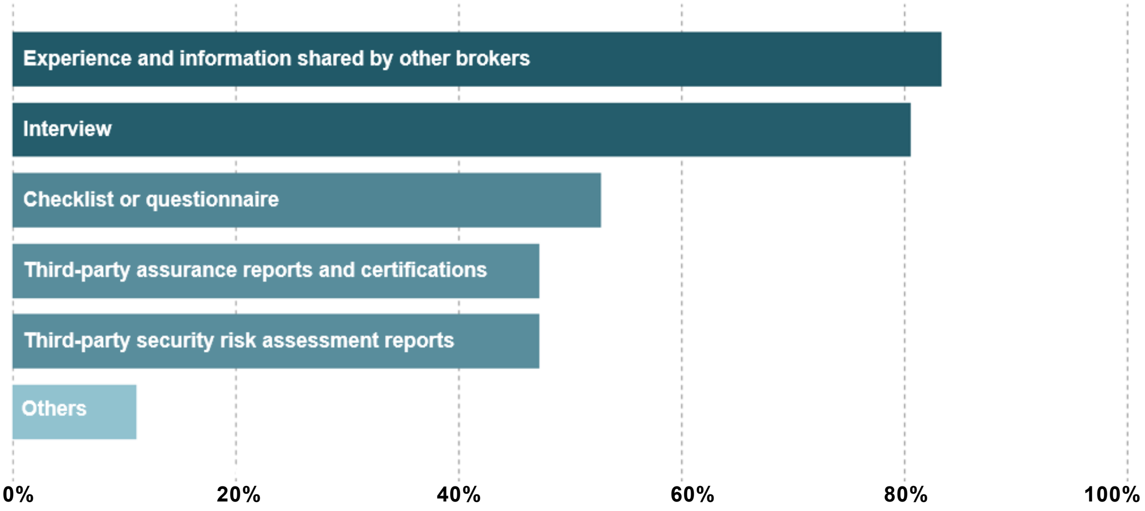
(h) incorporate into their business contingency plans the unavailability of services provided by the Third Party Providers and related cybersecurity scenarios and corresponding contingency strategies. Where possible, they should conduct regular drills and recovery tests together with these providers.

Examples of measures implemented by LCs

Third Party Provider selection

61. When conducting due diligence and selection on Third Party Providers, the respondents exchanged information with other brokers which also outsourced these systems, conducted interviews with the Third Party Providers, requested the Third Party Providers to complete a checklist or questionnaire, and reviewed third-party security risk assessment reports such as penetration testing and vulnerability scans, as well as third-party assurance reports and certifications such as System and Organization Controls 2 (SOC2) and ISO/IEC 27001.

Third Party Provider due diligence approaches by respondents



62. Specifically,

- a respondent developed a comprehensive questionnaire to assess the control environment of the Third Party Providers, including a technical assessment report such as a penetration testing report, third-party assurance reports and certifications such as SOC2 and ISO/IEC 27001, patch management, encryption, identity and access management, backup, etc; and

- another respondent evaluated and risk-ranked Third Party Providers, and performed on-site testing and validation on high-risk Third Party Providers, such as the business critical system providers, to ensure their security controls were aligned with its corporate standards and in compliance with applicable regulatory requirements.

- some respondents obtained explanatory documents from their Third Party Providers to assist them in assessing how the features in the internet trading system supplied by Third Party Providers could enable the LCs' compliance with the requirements stipulated in the Cybersecurity Guidelines.

Some sample Third Party Provider assessment areas are included in Appendix A for reference.

Third Party Provider contract management

63. Some respondents developed standard contract templates that outline cybersecurity measures expected of the Third Party Providers. This benefits both parties in understanding their rights and obligations to reduce the risk of non-compliance and potential disputes. Examples of cybersecurity-related provisions for contracts with Third Party Providers are listed in Appendix B for reference.

Third Party Provider risk management

64. Most respondents established procedures to bring the services in-house in the event of service disruption, unexpected termination of contract and liquidation of the Third Party Providers.

65. Most respondents had alternative service providers to resort to in the event of service disruption, unexpected termination of contract and liquidation of their primary Third Party Providers. These measures enhance the LCs' readiness in maintaining business operations in the event of disruption triggered by Third Party Providers.

66. Many respondents coordinated with the Third Party Providers to perform drill tests. Specifically, one inspected LC annually performed collaborative business resumption planning and recovery exercises (at least a desk-top exercise) with the critical Third Party Providers. Gaps identified and lessons learnt via the drill tests were used to enhance the incident response procedures.

Contingency planning

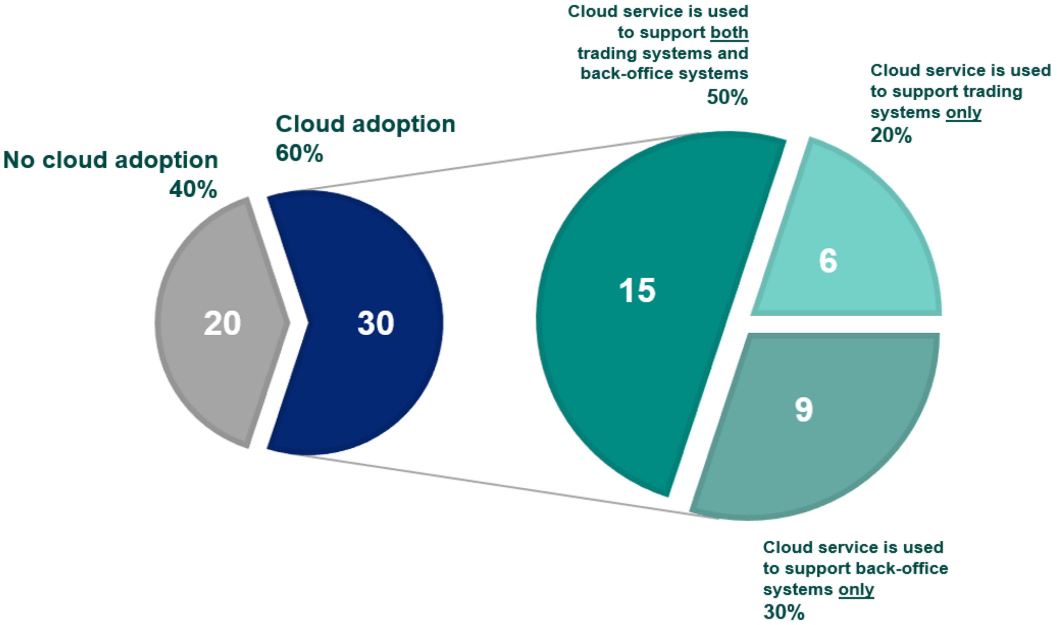
67. One respondent performed post-incident analysis following any major internal or external cybersecurity events to assess the potential impacts, including the impact on the IT services provided by Third Party Providers, and identify key lessons learnt. Where appropriate, the analysis results would be used for reviewing and updating the scenario analysis in the contingency plan.

68. The Third Party Provider lists maintained by some respondents outlined the interdependencies amongst the providers. This helps identify and evaluate the potential impact of affected services holistically and enables the effective implementation of the contingency measures to tackle cybersecurity incidents.

V. Cloud security

69. In recent years, the use of cloud computing services is increasingly prevalent in the financial service industry. Many LCs are hosting their business application and back-office systems in the cloud environment to enhance operational efficiency and save costs.

70. 60% of the respondents have adopted cloud computing services, and half of them adopted cloud service for hosting both their trading systems and back-office systems.



There are three common cloud deployment models[18], including Infrastructure as a Service[19] (IaaS), Platform as a Service[20] (PaaS), and Software as a Service[21] (SaaS). Each model offers varying levels of control, flexibility and management on cloud-hosted systems and data. In short:

- under the IaaS model, LCs are responsible for the network implementation, application system implementation and operations for cloud-hosted systems and data;

- under the PaaS model, LCs are responsible for the application system implementation and operations whereas third-party cloud service providers provide and maintain the underlying infrastructure; and

- under the SaaS model, LCs use the application systems and the third-party cloud service providers provide and maintain the underlying infrastructure.

These three models are all used by the respondents as follows:

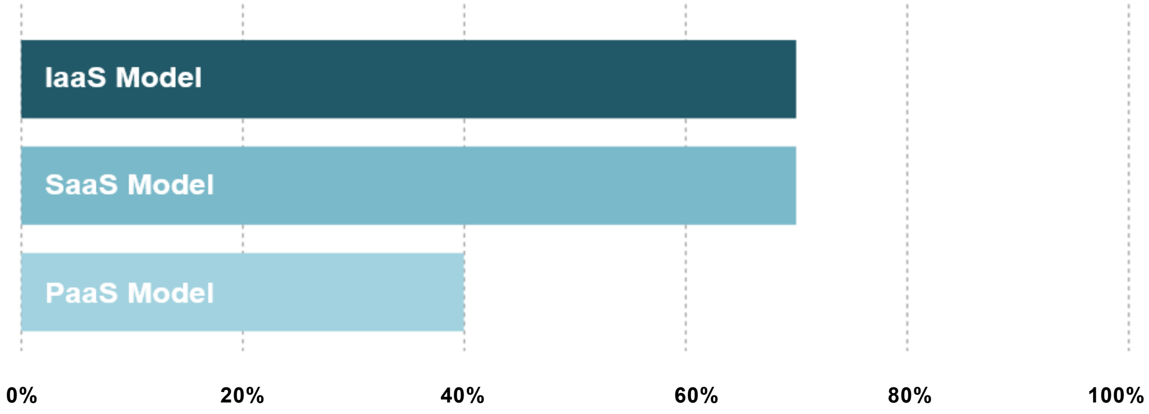
[18] The NIST Cloud Computing Definition provides three cloud service models. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-322.pdf

[19] The NIST defines "Infrastructure as a Service" as "the capability provided to the cloud service customer (CSC) to provision processing, storage, networks, and other fundamental computing resources where the CSC can deploy and run arbitrary software, which can include operating systems and applications".

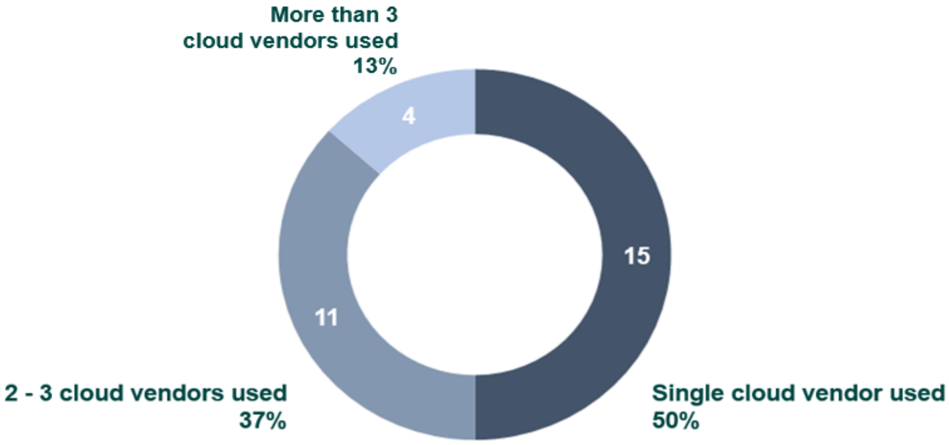
[20] The NIST defines "Platform as a Service" as "the capability provided to the CSC is to deploy onto the cloud infrastructure CSC-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider.

[21] The NIST defines "Software as a Service" as "the capability provided to the CSC is to use the cloud service provider's applications running on a cloud infrastructure".

Cloud service models used by respondents (30 in total)



71. In addition, many respondents adopted multiple clouds.



When a multiple-cloud strategy can help enhance system resilience and minimise the risk of service interruption, additional risks and operational challenges may arise amidst increased complexity and inconsistency in managing different cloud environments. For example, strong encryption is required to protect data-in-transit between cloud environments.

72. Cybersecurity management could differ significantly for cloud-hosted systems and data from those in the traditional on-premises IT environment. Hence, it is important for LCs to understand the cloud service models they adopt and implement the corresponding security measures. Any misunderstanding or gap may result in unaddressed security vulnerabilities in the cloud environment and potential leakage of client information.

Key observations

73. Some respondents failed to set up the DMZ or implement cloud-native segmentation controls in the cloud, which exposed them to higher hacking risk. In one case, the

inspected LC implemented network policies[22] to control access between internet-facing system services and sensitive internal system components, including trading systems, that were hosted in the same network cluster. However, its lax network policies allowed direct network connection from the internet-facing services to the database, thus heightening the risk of data leakage.

74. Some respondents stored client account data, trade data, and system configuration data on cloud. However, they did not implement adequate data backup procedures and thus may not be able to restore the data when needed. For example:

- some respondents did not back up these data to an offline medium on at least a daily basis, nor did they keep a copy of the data in a medium isolated from the cloud environment;

- some respondents did not disconnect the data source upon completion of the backup process. As a result, the backup data may also be deleted or encrypted when the connection between the production environment and the backup environment is compromised by hackers under ransomware attacks; and

- the cloud-based backup solution adopted by some respondents did not have in place immutable data backup control, ie, Write-Once-Read-Many (WORM).

Expected standards

LCs should:

(a) develop policies and procedures on cloud security management which include access credential management, secured cloud infrastructure, data encryption, security logging and monitoring, backup, compliance controls, regular audits and incident response and reporting;

(b) conduct proper due diligence on the third-party cloud service providers, particularly the security controls implemented by these providers;

(c) implement a secure network infrastructure[23] and properly segregate the network segment or security group hosting critical systems and data from other network segments or security groups that are subject to higher hacking risk exposure[24];

[22] Network policies refers to the network connection rules that control the communication between components within a container cluster.

[23] The design and implementation of network infrastructure to host systems and data in the cloud environment would be different from the network infrastructure set up in the "non-cloud" environment, eg, on-premises data centre. Hence, LCs may not necessarily deploy the network segmentation through a typical DMZ with multi-tiered firewalls. They should use cloud-native segmentation controls and adopt micro-segmentation approach to deploy the network segmentation in a granular manner, ie, access restriction between segregated network clusters, security groups and even individual system service and component.

[24] For example, web servers or internet-exposed services.

(d) implement adequate controls to guard against unauthorised access and usage of the root account of the cloud platform[25]; and put in place sufficient controls, such as 2FA and IP whitelisting, to prevent unauthorised access and usage of this account;

(e) properly secure and manage the cloud access credentials, which include application programming interface (API) keys and access tokens, for interacting with internet trading systems and data and grant the access rights assigned to these credentials on a "need-to-have" and "least privilege" basis. LCs should also apply this expected standard to data access and communication between application systems on different clouds (eg, between trading system and settlement system);

(f) change API keys regularly, and avoid using permanent keys;

(g) back up business records, client and transaction databases, servers and supporting documentation in an offline medium on at least a daily basis; also ensure that the backup is "immutable", ie, WORM and "air-gapped", ie, the backup medium should be disconnected from the cloud environment after each backup process; and

(h) collaborate with third-party cloud service providers to formulate the cloud-related cybersecurity and unavailability scenarios in their business contingency plans, and where possible, coordinate with the third-party cloud service providers when performing drills and recovery tests.

Examples of measures implemented by LCs

75. Many respondents implemented advanced cloud-related security tools to safeguard systems and data hosted in the cloud environment. These security solutions include Cloud Access Security Brokers (CASB)[26], Cloud Workload Protection Platforms (CWPP)[27], Cloud Security Posture Management (CSPM)[28] and Cloud-Native Application Protection Platforms (CNAPP)[29]. They may help to address the risks associated with cloud misconfiguration and cloud workload issues, and also enhance vulnerability management and access control.

76. Some respondents performed technical security assessment, including penetration tests and vulnerability scan, on the cloud environment at least annually. They also conducted

[25] Root account of cloud computing platform is the highest privileged account with full access to all system services and resources in the cloud environment.

[26] Cloud Access Security Brokers is a security solution placed between cloud users and vendors to enforce security policies and protect the data communication to and from the cloud environment.

[27] Cloud Workload Protection Platforms is a security solution that provides protection for workloads running in cloud environments, including virtual machines, containers, serverless functions and runtime environment.

[28] Cloud Security Posture Management is a security tool and process to identify and remediate security risks and misconfiguration in cloud environments.

[29] Cloud-Native Application Protection Platforms is a security solution to protect cloud-native applications by integrating security features such as workload protection, vulnerability management and compliance monitoring within the cloud environment.

cloud configuration reviews to evaluate the effectiveness of the security controls in the cloud control plane[30].

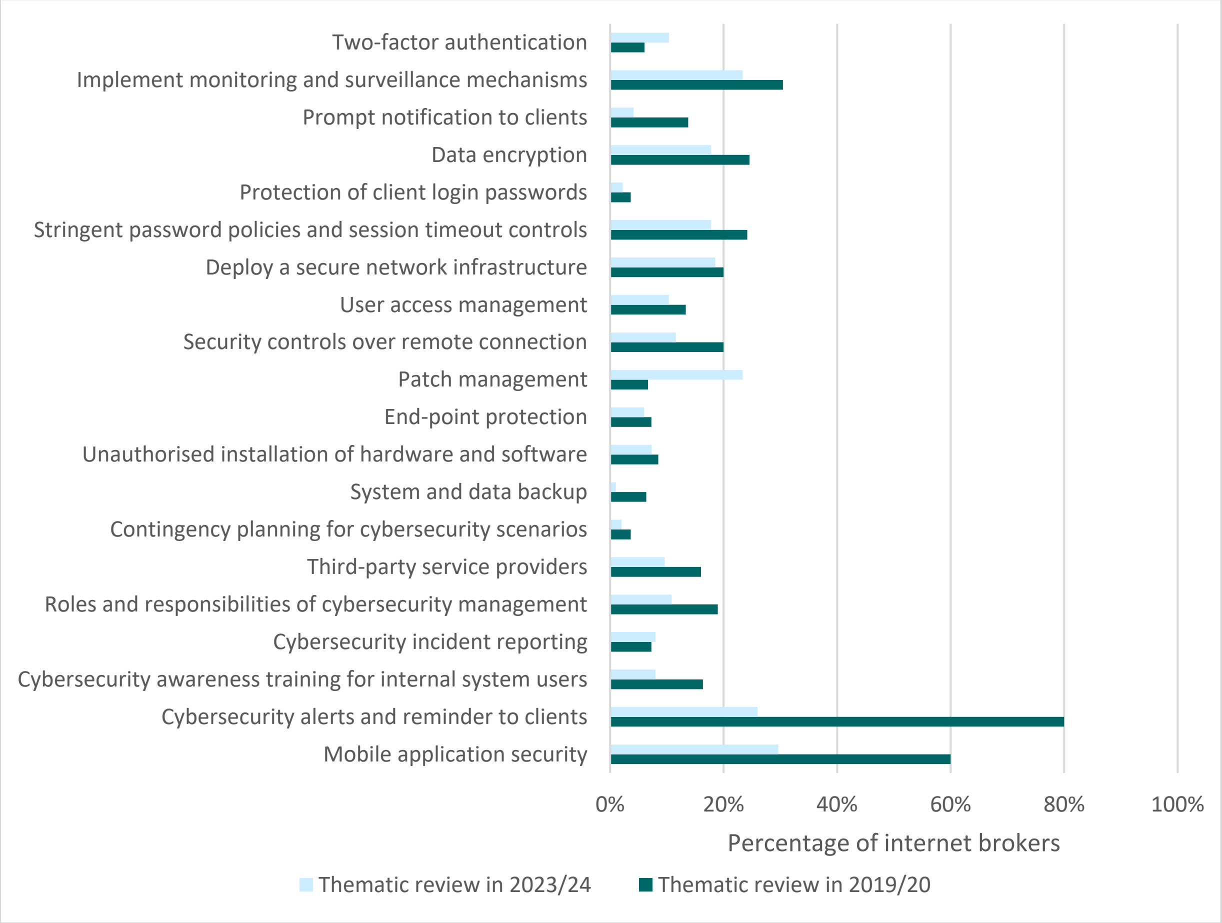
77. To enhance the security of the cloud computing platform, some respondents used zero-trust architecture to enforce strict identity and access management controls in the cloud environment.

VI. Compliance with Cybersecurity Requirements

78. In comparison with the results of the 2019/20 Thematic Review, based on the survey results, LCs have shown improvements in compliance with some Cybersecurity Requirements and expected standards, including monitoring and surveillance mechanism and mobile security.

79. However, non-compliance with the requirements of certain key control areas was noted, eg, unqualified two-factor authentication is used for system login and regular monitoring is lacking for the availability and deployment of updated security patches.

Non-compliance comparison between thematic review in 2019/20 and 2023/24



[30] Cloud control plane provides command and control of all the system services and resources on the cloud platform.

80. Furthermore, during the inspections, it was noted that some deficiencies may expose LCs to significant cybersecurity risks. This included lax security control configurations of the system servers and firewall[31], delay in implementing security patches and hotfixes released by software providers, weak algorithm used for encryption of sensitive data and inadequate encryption for data-in-transit and data-at-rest, and excessive user access to system admin accounts of critical systems and databases.

81. In addition, in some of the cybersecurity incidents reported by LCs, it was noted that there was a lack of audit trail in the key systems and servers. This hindered the LCs' ability to conduct regular monitoring and investigations upon the occurrence of cybersecurity incidents.

82. In this connection, LCs are reminded to be alert for cybersecurity threats and implement adequate cybersecurity controls to protect their systems, client accounts and data and to ensure compliance with the Cybersecurity Requirements.

Examples of measures implemented by LCs

83. This section highlights some measures implemented by the respondents and inspected LCs to comply with the Cybersecurity Requirements. LCs may wish to make reference to these measures when designing their own systems and controls.

Two-factor authentication

84. Currently, SMS OTP is one of the most common authentication factors for system login and device binding. However, there are some security concerns associated with their use, eg, fraudsters can intercept these OTPs through malware installed on the victim's mobile phones. To mitigate such risks, some respondents have adopted more secure authentication methods, such as biometrics (including facial recognition technology) and software token. LCs are reminded to keep abreast with the latest technological developments and review the risks associated with using SMS OTPs. They are also encouraged to stop using SMS OTPs for authentication or implement compensating controls where appropriate.

85. Some respondents used multiple identifiers for device binding. For example, some respondents utilised more than one identifier on the device for device binding. This increases the difficulty for hackers to mimic the device. The identifiers utilised by respondents for each platform are set out in the table below for reference.

Platform type	Identifiers used for device binding
Desktop application	• Globally unique identifier (GUID) • Identifier generated by proprietary algorithm • MAC address

[31] For example, unnecessary service ports of system servers, such as File Transfer Protocol (FTP) and SSH, were opened, and unnecessary access was allowed in the access control list of the firewall.

Platform type	Identifiers used for device binding
Mobile application	• AndroidID • Client device public key and device version • Digital certificate • Identifier for vendors (IDFV) • Identifier for Advertisers (IDFA) • Identifier generated by proprietary algorithm • MAC address • Open Anonymous Device Identifier (OAID) • Universally Unique Identifier (UUID)/unique device identifier (UDID)
Web-based trading platform	• Browser plugin and extension • Browser type and version • Device size • Screen resolution • System language • Time zone • User agent strings

Note: Identifiers used for device binding on web-based trading platforms provide additional information for authentication checking, but they are not strong enough to uniquely identify each device. Respondents adopted device binding for web-based trading platforms also adopted other authentication factors.

86. An inspected LC adopted OTP-free authentication solution for system login to its trading website. During login process, a digital code would be displayed on the trading website and the mobile application bound with the client's device. The client can then authorise the login via the mobile application.

Data encryption

87. An inspected LC can automatically identify weak encryption algorithm used on its web servers via an online scanner.

Patch management

88. A global IT incident arose from the faulty update of a cybersecurity solution in July 2024. The update was rolled out by the software provider and sent to all of its customers for auto-update. Some LCs which disabled the automatic update averted the impact of this incident. These LCs evaluated the implications of the update and/or phased the update of the solution across different groups of systems to manage potential issues with such updates.

89. An inspected LC registered all the software components and libraries used for software development in a centralised system, which allowed it to efficiently monitor the availability of their security patches.

90. An inspected LC kept abreast of the latest cybersecurity risk trends through threat intelligence subscribed from different sources to identify emerging vulnerabilities and

availability of security patches, such as Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT)[32], InfoSec[33] and Cybersec Infohub [34].

Contingency planning for cybersecurity scenarios

91. Many respondents validated the effectiveness of business continuity plans by performing regular drill tests which covered cyber-attack scenarios. They also participated in the industry-wide drill tests involving financial regulators and other industry practitioners.

92. A number of respondents who relied on third-party IT service providers performed the drill tests on the contingency plans in collaboration with their Third Party Providers. This enhanced their preparedness for any potential disruption in Third Party Providers' services.

Mobile application security

93. Many respondents obtained cybersecurity assurance over the mobile trading application by conducting regular penetration tests. They also conducted security source code review regularly over the mobile trading application to address emerging vulnerabilities.

[32] https://www.hkcert.org/
[33] https://www.infosec.gov.hk/en/
[34] https://www.cybersechub.hk/en/home/highlights

Appendix A – Third Party Provider assessment

Area of assessment	Description
Reputation	Review the reputation of the Third Party Provider and compare against its competitors.
Risk management and information security policy	Review whether there are risk management and information security policies and procedures to address the risk from the usage of technology.
Separation of duty	Review whether there is proper separation of duty from its IT staff, eg, developers cannot access the production environment.
Separation of production and development environments	Review whether there is separation between production and development environments.
Network architecture design	Review whether there is architecture design document for proper network segmentation, anti-DDoS and availability.
Identity and access management	Review whether there is proper governance on account creation, modification, deletion and recertification.
Privileged access management	Review whether there is proper governance on the usage of privileged account.
Physical access, network access and remote access control	Review whether there is proper physical access, network access and remote access control.
Software development life cycle	Review whether a proper software development lifecycle is defined and whether cybersecurity risks are addressed during development lifecycle, eg, perform source code review, vulnerability scan and penetration test before the system is launched to production.
IT asset lifecycle management	Review whether a process is in place to avoid using end of life software and hardware.
Change management process	Review whether there is proper governance on change management.
Patch management	Review whether there is proper governance on patch management to apply security patches and bug fixes.
Anti-malware	Review whether an anti-malware solution is deployed.
Email security	Review whether technical controls are deployed to lower the risk for data leakage and phishing attack through email.
System configuration management	Review whether there is a standard for baseline configuration in systems to address cybersecurity risk and whether there are regular reviews to ensure that configuration remains in compliance with the standard.
Encryption	Review whether the encryption algorithms used are up-to-date, subject to regular review, and applied for sensitive data during transmission and stored in databases.
Backup	Review whether there is proper backup arrangement.

Area of assessment	Description
Data loss prevention	Review whether technical controls are in place to avoid leakage of sensitive information.
Business continuity plan	Review whether a business continuity plan is in place to provide service to customers.
Incident management and problem management	Review whether there are proper incident management and problem management processes.
Logging, monitoring and alert handling	Review whether a process is in place for proper logging, monitoring and alert handling.
Threat intelligence management	Review whether a process is in place to regularly collect, analyse and handle threat intelligence from different sources.
Third party management	Review whether there is a third party management policy and procedure to properly manage the risk from the Third Party Provider’s vendors.
Cloud computing	Review whether there are governance and technical standards on the usage of cloud service.
Cybersecurity awareness training	Review whether regular cybersecurity awareness training is arranged for its staff.
Audit and compliance	Review whether there is regular audit exercise to ensure that the Third Party Provider is in compliance with its policies, law and regulatory requirement.
Technical assessment report	Review technical assessment reports, such as SOC 2 reports, penetration test reports and vulnerability assessment reports, to estimate the Third Party Provider’s security posture.
Certification	Review whether the Third Party Provider holds a certificate for cybersecurity, eg, ISO/IEC 27001.

Appendix B – Examples of provisions for contract with Third Party Provider

Items included in the contract	Description
Cybersecurity management practice	State the requirement for cybersecurity management practice, which should be comparable with internationally recognised frameworks, such as ISO/IEC 27002 or NIST SP800-53.
Physical access control	State the requirement for physical access control to avoid unauthorised access to its systems and premises, such as (i) permit only authorised personnel to have access to secure areas; (ii) restrict access using biometric or proximity card access screening; (iii) continually monitor ingress and egress points using security guards and video surveillance.
Logical access control	State the requirement for logical access control to avoid unauthorised access to its systems, such as (i) access controls following the principle of least privilege; (ii) privileged account and elevated and/or system-level access controls; (iii) any system access must be temporary, just-in-time and must enforce segregation of duties for authorisation; (iv) all access and changes must create an audit trail; and (v) post-access reviews must be timely.
Remote access	State the requirement for remote access with multi-factor authentication and encryption, and the security control on the device used for remote access.
Software development lifecycle	State the requirement for design review, threat modelling, code review and security testing during software development life cycle.
Change management	State the requirement for proper change management.
Anti-malware	State the requirement for anti-malware.
Data protection	State the requirement to protect data when it is transferred, processed and stored, eg, encryption, and the requirement to prevent data from corruption, leakage and unauthorised access, including the process for data destruction.
Encryption	State the requirement to encrypt data with up-to-date industrial encryption algorithm.
Data backup	State the requirement for backup frequency and retention period.
Cybersecurity incident monitoring, handling and reporting	State the requirement and timeline for cybersecurity incident monitoring, handling and reporting.
Business continuity	State the requirement to maintain an up-to-date business continuity plan and procedure.
Cybersecurity awareness training	State the requirement for cybersecurity awareness training provided to its staff, including training before onboarding and annual training.
Annual security audit	State the requirement for annual security audit by an independent third party to assess its effectiveness on cybersecurity

Items included in the contract	Description
	management.
Vulnerability scan	State the requirement for regular vulnerability scan and timeline to resolve vulnerability at different risk levels.
Penetration test	State the requirement for regular penetration tests.
Audit rights	State the requirement for audit rights, on-site control assessment and verification performed by the LC or an independent third party.
Legal and regulatory compliance	State the requirement for legal and regulatory compliance.
Liability, penalty and termination rights	State the liability and penalty for security breach, and termination rights for security breach.