Hong Kong Institute
of CPAs

Securing a Cyber Future: Current Landscape of IT & Cybersecurity Governance in Hong Kong

November 2024

Hong Kong Institute of
Certified Public Accountants
香港會計師公會

The Hong Kong Institute of Certified Public Accountants is the only statutory body responsible for the registrations of accountancy professionals in Hong Kong. The Institute has more than 48,000 members and more than 12,700 students. Members of the Institute are entitled to the description "certified public accountant" and to the designation CPA.

Contents | Page

Message from the Institute President and Chair of the 2024 Best Corporate Governance and ESG Awards Judging Panel

Information technology (IT) and cybersecurity are vitally important topics for companies both locally and globally. New technologies, including Artificial Intelligence (AI), are poised to reshape how many companies do business, whilst cyber criminals are deploying increasingly advanced techniques to breach company defences and gain access to sensitive data.

The impact of a cybersecurity breach can be catastrophic, ranging from lost intellectual property (IP) which could severely impact a company’s ability to achieve their business objectives, to the loss of highly sensitive customer information such as financial or medical records.

Globally there have been many recent instances of high-profile IT and cybersecurity failures leading to significant business and personal disruption. In Hong Kong, concerns regarding cybersecurity have reached such a level that the Government proposed in June 2024 a new piece of cybersecurity legislation. Tentatively titled the Protection of Critical Infrastructure (Computer System) Bill, it is designed to enhance the security of systems relating to critical infrastructure such as energy, banking and financial services and healthcare services. The Government is consulting the relevant sectors with plans to introduce the proposed bill in the near future.

Currently there are no specific requirements in Hong Kong for companies to implement cybersecurity systems, or to disclose in their annual or environmental, social and governance/sustainability (ESG) reports how their governance frameworks apply to IT and cybersecurity. Despite this, many companies do provide detailed disclosure in relation to cybersecurity because of how significant the risk is to their operations, due to a desire to explain in their ESG reports how they are protecting their customers privacy or because they are subject to privacy legislation in other jurisdictions such as the General Data Protection Regulation (GDPR) in the European Union (EU). This is encouraging and indicates how seriously many companies in Hong Kong are taking cybersecurity.

The objective of this report is to provide insight into how companies are governing their IT and cybersecurity systems to help ensure they are effective at identifying and responding to threats and protecting their own, and their customers’ data. As the importance of IT and cybersecurity governance continues to grow, we expect to see companies developing their governance systems and providing focused disclosures for users of their reports, and we have provided key findings and recommendations to facilitate this. We hope that this will be a small step towards a brighter and more secure cyber future.

Roy Leung FCPA (practising)
Institute President
Chair of the 2024 Best Corporate Governance and ESG Awards Judging Panel

Background and definitions

Key definitions

The following key definitions are important for understanding this report:

Information Technology (IT): IT is broadly defined as the use of computers and other electronic equipment to store, process and send information. In the following report we use IT broadly to describe a company's software and hardware systems, encompassing use throughout the company's business and reporting cycles.

Cybersecurity: Cybersecurity is the protection of information, systems and networks from external attacks or data leaks. Related concepts such as information security, data security and privacy protection are used interchangeably by many companies in their disclosures; but for consistency we have used cybersecurity as the key overarching term.

Artificial Intelligence (AI): There is no single definition of AI, though most definitions discuss AI as a technology which, in its broadest sense, replicates some element of human intelligence. This includes learning, comprehension, problem solving and decision making. Machine Learning (ML), a subset of AI, is currently the most commonly deployed form of AI and focuses primarily on analysing and detecting patterns within large data sets.

Implementing robust cybersecurity measures is more vital now than it has ever been. Loss of customer data or a company's IP as a result of cybercrime can have a substantial detrimental impact on a business's financial position and reputation.

Cybersecurity risks are increasing, driven by global business connectivity and a growing dependence on cloud services. Legacy IT systems are likely to become even more vulnerable as time goes on, with the emergence of more advanced cyber-attack tools.

Establishing an effective IT governance strategy, with sufficient dedicated resources for cybersecurity, should be an important focus area for companies, particularly those handling large volumes of sensitive private information. AI will again drive change here, with companies looking to deploy tools in their business processes needing to ensure that their IT governance strategies and systems are well developed to address the unique challenges of AI both as a risk and opportunity for the business.

Background and definitions (cont'd)

In light of the above, we have considered the following key questions in developing this research report:

1. Do companies include disclosure relating to the governance of their overall IT strategy and framework in their annual or ESG reports?

2. Is there a board member with specific IT and/or cybersecurity experience relevant to the company's operations? If "yes", is that member an executive director or an (independent) non-executive director?

3. Do companies include cybersecurity-focused disclosures in their annual or ESG reports?

4. Is cybersecurity identified as a significant risk area for business operations and/or a risk to achieving the companies ESG objectives? If "yes", are mitigation methods also discussed?

5. Do companies disclosed that they have undertaken a review or testing of their cybersecurity systems? If "yes", was the review performed by an internal or external party?

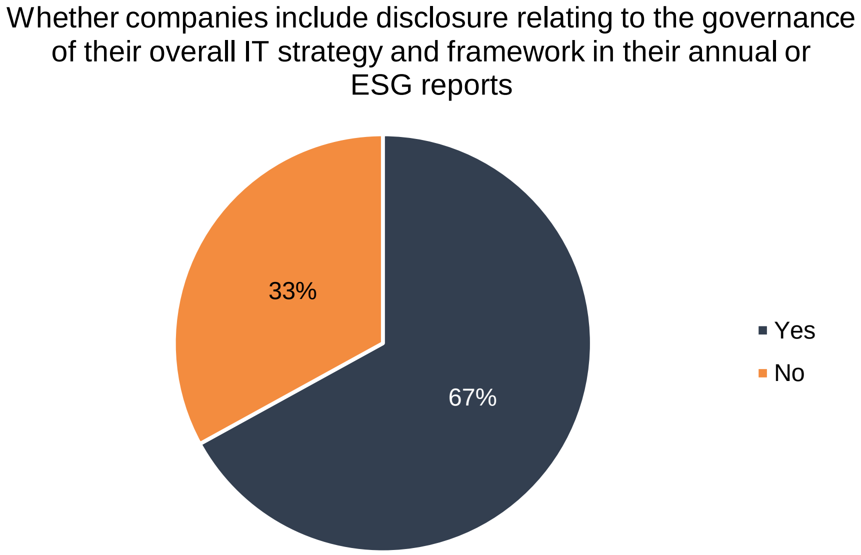
6. Do companies disclose that they have experienced a cybersecurity incident or have identified weakness in their cybersecurity systems? If "yes", do they explain how this was addressed and the remedial actions taken.

7. Do companies disclose whether they have provided cybersecurity training to their staff and directors? If "yes", do they give further details of that training?

8. Do companies include the emergence of AI as a significant risk factor for cybersecurity? Do companies disclose any plans to use AI in their business processes?

This report focuses on the 82 Hang Seng Index (HSI) companies as at 30 April 2024. The companies' annual and ESG reports were reviewed in order to understand how IT and cybersecurity risk are addressed and to understand the extent and quality of disclosure.

Q1. Do companies include disclosure relating to the governance of their overall IT strategy and framework in their annual or ESG reports?



- **67%** of HSI companies make some form of disclosure in relation to the governance of their overall IT strategy and/or framework. These disclosures range from passing references to IT through to detailed discussion of the nature of the company's IT systems and controls and relevance to the business approach and strategy.

- The location of these disclosures within the annual or ESG report varies, with the following locations being most common:

  i. Key disclosure on the company's approach to the governance of their IT systems and the potential risks associated with IT failure included in the **Corporate Governance (CG) Report**, within the annual report. When making IT-related disclosure here, most companies included their disclosures in a **Risk Management and Internal Control** section of the CG Report. This is likely driven by the Listing Rules, Appendix C1, Part 2, D.2.1 – D.2.9. These provisions focus on the board's responsibility for evaluating risk and ensuring that the issuer establishes and maintains appropriate risk management systems, and for overseeing a review of the effectiveness of the systems at least annually. This should include risks relating to cybersecurity where material to the company.

  ii. Discussion on the significance of IT systems to the company's ability to achieve its business objectives included in the **Strategic Report** or other strategy-focused disclosures within the annual report.

  iii. Disclosure of the potential impact of data security leaks on customers within the "Social" or "Governance" section of the company's **ESG Report**.

Q1. Do companies include disclosure relating to the governance of their overall IT strategy and framework in their annual or ESG reports? (cont'd)

Prevalence of generic or "Boilerplate" disclosure

Regardless of the location, many company's disclosures are high-level and do not do enough to link to the company's specific circumstances. The use of generic phrases which affirm commitment to developing robust IT systems, but do not include any real indication of the company's current or planned activities, are not sufficient to allow users of that information to understand how IT governance is addressed within the company. Companies that are adopting best practice link their IT disclosures explicitly to the company's specific risks, including actions taken, metrics for comparison and clear, unambiguous statements on their planned future IT governance activities. We discuss the need for clear, focused disclosures further in the Key findings and recommendations section of this report.

.

- Companies operating in some industries make better, more focused disclosures than others. All seven banks within the HSI for example include reasonably detailed discussion on their IT strategies and frameworks. This is to be expected given the large volumes of very sensitive data held by banks and other financial service providers. Critical failures of IT systems, or cybersecurity incidents, could have a significant impact on their business functions and lead to substantial losses for customers.

- Companies in other industries, for example in more industrial sectors that are less customer focused, often make less extensive disclosure in relation to their IT strategies and frameworks. Whilst this is understandable, given the reduced risk of significant customer data loss, it is important to understand that loss of customer data is not the only potential risk associated with IT and cybersecurity systems. For example, ransomware attacks are becoming more common and sophisticated where criminals may take control of an organizations computer systems or data and release it only when a ransom is paid.

Q1. Do companies include disclosure relating to the governance of their overall IT strategy and framework in their annual or ESG reports? (cont'd)

- Failures in IT and cybersecurity systems can impact companies in many ways outside of losing customers' private information, including:

    i. **Failure of critical systems**. For those companies that rely on automated production lines for example, IT systems are crucial to their function. Failure of IT systems can lead to companies being temporarily unable to produce goods or provide services resulting in lost revenues and, potentially, reputational damage.

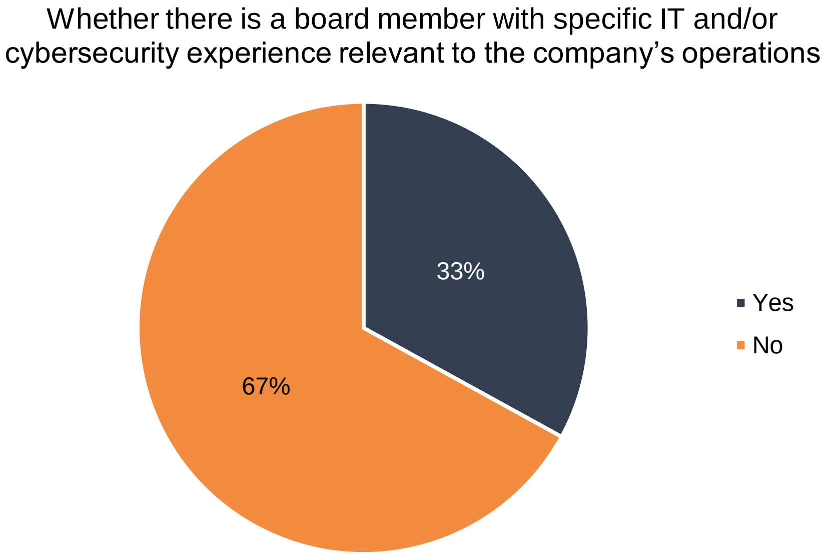
    ii. **Loss of IP**. Breaches of cybersecurity systems can lead to the loss of companies' valuable IP or theft of commercial secrets, impacting on the delivery of products and services, potentially, damaging companies' brand and reputation.

    iii. **Theft of company assets.** Employees falling victim to scams or other cyberattacks can lead to the direct loss of company assets, for example if payments are made to fake suppliers.

    iv. **Ransomware attacks.** Ransomware attacks can lead to companies being unable to access their data, and financial loss if they are forced to pay the ransom for the return of their data.

- Given the above, ensuring good governance of IT strategies and frameworks is vital for all companies, regardless of the products or services that they deliver or the extent to which they hold sensitive information on individual customers.

Q2. Is there a board member with specific IT and/or cybersecurity experience relevant to the company's operations? If "yes", is that member an executive director or an (independent) non-executive director?



- There is no specific requirement in Hong Kong for a company to appoint a board member with specific IT and/or cybersecurity knowledge or experience. Other jurisdictions, such as the United States, have considered introducing a requirement, with the Securities and Exchange Commission (SEC) considering such a rule in their December 2023 update to the SEC cybersecurity disclosure rules.

- The SEC ultimately decided against requiring that a board member with such experience be appointed, on the basis that it may inadvertently pressurize companies into retaining experts at the expense of appointing board members with more relevant experience for the company. The final rules focused on high-level disclosure regarding the board's oversight of cybersecurity threats.

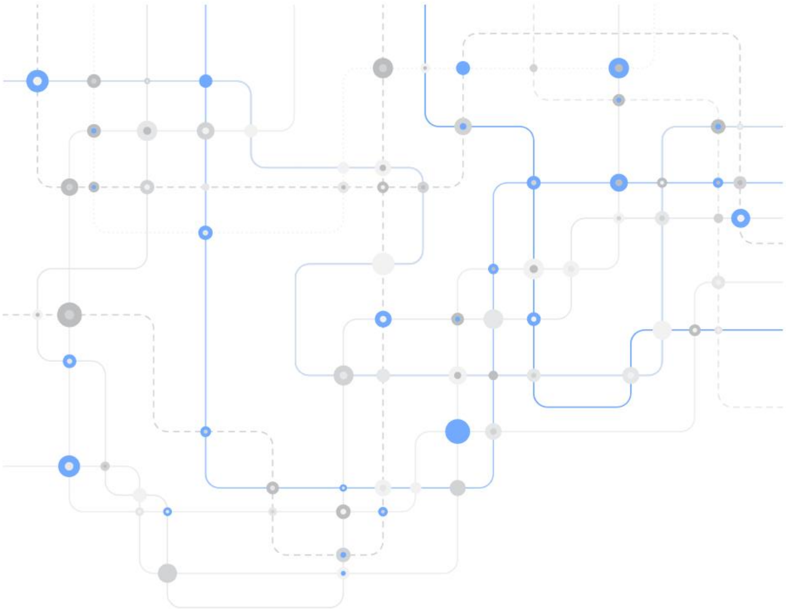
- Despite the lack of any explicit requirement, 33% of HSI companies disclose that they have a board member with IT and/or cybersecurity experience relevant to the company's operations. The experience of these board members ranged from previous experience within other IT-focused companies and organizations, including IT regulatory organizations, to academic experience in relevant topics, such as information security.

- The fact that a reasonable number of companies choose to appoint board members with relevant IT and/or cybersecurity experience illustrates the increasing importance of these topics to companies and that they recognize the need to ensure that they are well equipped to respond to cybersecurity threats and also to take advantage of emerging technology-driven opportunities.

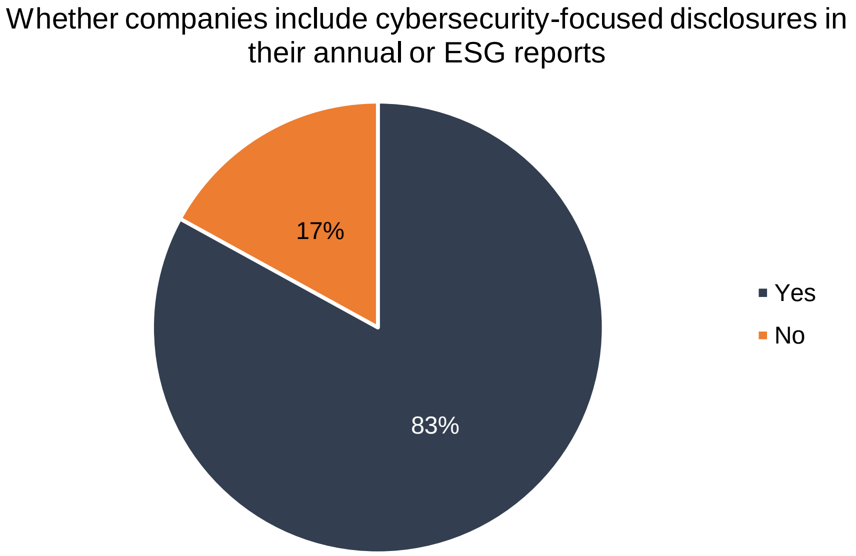
Q2. Is there a board member with specific IT and/or cybersecurity experience relevant to the company's operations? If "yes", is that member an executive director or an (independent) non-executive director? (cont'd)

Board members position

Of those companies that have appointed a board member with relevant experience, 44% are non-executive directors (NEDs)/independent NEDs. The rest are split covering a number of positions such as chief information officer and chief digital officer and other executive members.



Q3. Do companies include cybersecurity-focused disclosures in their annual or ESG reports?



- **83%** of HSI companies make some form of disclosure specifically relating to cybersecurity, or similar concepts, such as information security and data privacy protection, in their annual or ESG report.

- This is a greater percentage of companies than those making the more general IT disclosures discussed in Q1.

- This is likely driven by a number of interrelated factors, including:

  i. Greater public interest in cybersecurity-specific incidents compared with broader IT policies.

  ii. The potentially more detrimental impact of cyber-attacks on companies' operations and reputation relative to broader IT issues.

  iii. SEC Form 20-F requires, for periods ending on or after 15 December 2023, specific cybersecurity disclosures. For some companies with United States reporting obligations, this requirement appears to have driven them to include a greater level of cybersecurity disclosure in their Hong Kong filings.

  iv. The importance of cybersecurity to the "Social" aspect of ESG disclosures. Some companies framed their discussion on cybersecurity in the context of the United Nations Sustainable Development Goals (SDGs), which have a more explicit link to cybersecurity through SDG-9 "Build resilient infrastructure, promote inclusive and sustainable industrialization and foster innovation".

Q3. Do companies include cybersecurity-focused disclosures in their annual or ESG reports? (cont'd)

- Most companies include disclosure on the main elements of a cybersecurity system, namely:

    i. **Threat detection** – Disclosure here focuses on the systems of control that companies have implemented in order to detect any threats to their data, network and systems. Many companies state compliance with International Organization for Standardization (ISO) 270012 Information Security Management. ISO 27001 is a widely-recognized standard which sets out a framework for companies to establish, review and maintain an Information Security Management System. Such certification is a good indicator of a company's commitment to cybersecurity and provides users of the reports with some comfort that data is being properly protected. Some companies disclose compliance with other equivalent certifications, which may be more relevant in the jurisdictions where they operate or have other listing/reporting requirements to fulfil.

    ii. **Threat prevention** – In this area, disclosure includes actions that the company has taken in order to prevent threats from becoming incidents. This includes automated monitoring systems, preparatory drills, the establishment of new controls and governance processes and implementing training programmes.

    iii. **Threat response** – Disclosure here focuses on how companies respond to any incidents, including their incident response plans and details on how damage to the company would be mitigated in the event of an incident.

- Companies with a significant EU customer base include disclosures regarding their need to comply with the GDPR and the potential onerous impact that failure to comply may have for the company. This could come in the form of significant fines or reduced capacity to provide goods and services within the EU.

Q3. Do companies include cybersecurity-focused disclosures in their annual or ESG reports? (cont'd)

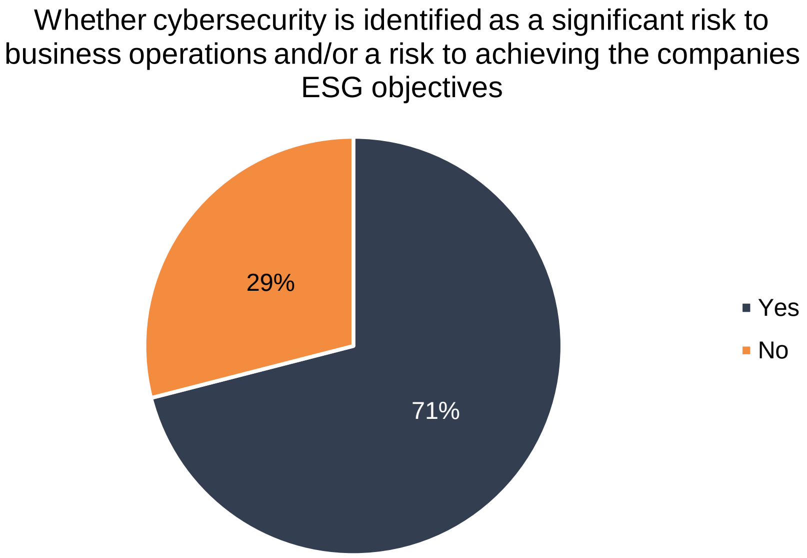
Disclosure quality in the Annual Report vs the ESG Report

Although some companies include detailed cybersecurity disclosures in their annual report, it is much more common for companies to make brief, or even no, mention of cybersecurity in their annual report and to include the more substantial disclosures in their separate ESG report. This approach generally has a positive impact on the overall quality of disclosure, with those companies focusing on the ESG report as their primary channel of disclosing cybersecurity governance often producing more detailed disclosure. Cybersecurity is most often included under the "Social" or "Governance" elements of ESG, depending on the particular focus, with the focus of disclosures under "Social" on the potential harm to society of privacy breaches.

One downside of including cybersecurity disclosures within the ESG report is a weaker link between business risks identified in the CG Report in the annual report and the potential impact of cybersecurity on those risks. This weaker link makes it more challenging for users of the information to understand how fundamental a risk cybersecurity issues are to the company. This linkage to business risk is discussed in greater detail in relation to Q4.

.

Q4. Is cybersecurity identified as a significant risk to business operations and/or a risk to achieving the companies ESG objectives? If “yes”, are mitigation methods also discussed?



- **71%** of HSI companies disclose cybersecurity either as a significant risk to business operations or as a risk to achieving their ESG objectives.

- Some companies make general comments about the importance of cybersecurity to the company, but do not explicitly link it to risk, instead including general high-level statements.

- Where companies identified cybersecurity risk as a risk to business operations, most include it as a significant factor contributing to operational risk or compliance risk, rather than treating it as a separate risk in its own right. These disclosures are generally made in either the CG Report or other risk management reporting within the annual report.

- Some companies identified cybersecurity as having such a potentially detrimental impact on the business that a separate risk is included, described as network and cybersecurity risk or similar. Of those companies that disclose separately, only a minority explicitly indicate that they believe risk is increasing as a result of cybersecurity, though other many companies make passing reference to general increases in IT risk, without quantification.

- Where risk disclosure is located, primarily, within the annual report, the focus is generally on the risk that data loss could lead to potential fines, loss of licences or certifications, reputational damage, or other issues that would potentially lead to lost revenues and an inability for the company to meet its business strategy objectives.

- Where companies discussed cybersecurity, primarily, in the ESG report, disclosure is often less explicitly linked to business risk and more general in its connection to the company’s efforts to ensure that society is not impacted adversely by any data leakage, for example by emphasizing the potential impact of data loss on individuals lives.

Q4. Is cybersecurity identified as a significant risk to business operations and/or a risk to achieving the companies ESG objectives? If "yes", are mitigation methods also discussed? (cont'd)

- Ensuring clear links are drawn between the potential impacts of cybersecurity issues and the significant risks facing companies is important for users of the reports. Even when disclosure on cybersecurity risk is included within the ESG report, it should clearly link to the company's CG Report and the significant risks that may impact the company. This helps to improve clarity on the governance measures the company has taken to help manage and mitigate cybersecurity threats.

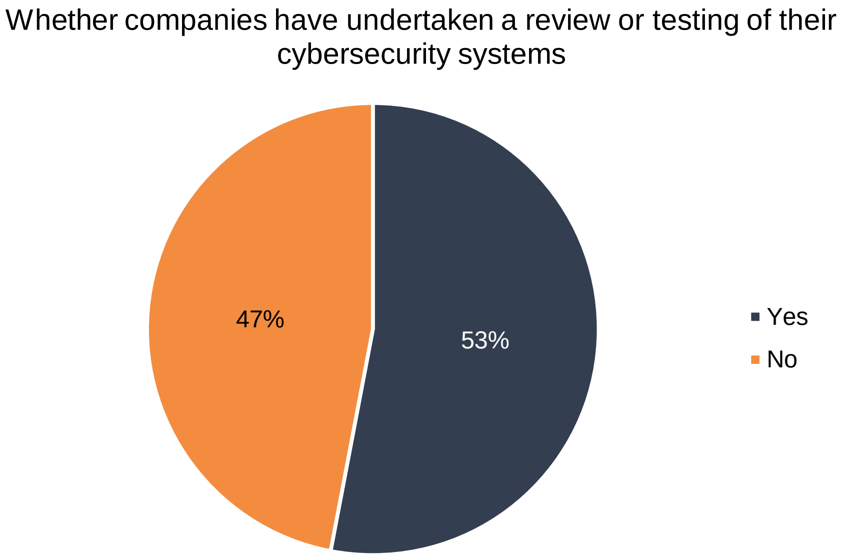
Risk mitigation methods

Those companies that identified cybersecurity as a significant risk to business operations or an ESG risk describe a range of mitigation methods. Disclosure of these methods again varies from general high-level statements to specific mitigation methods described in detail, including:

- Undertaking regular cybersecurity threat assessment exercises or reviews to identify vulnerabilities. We discuss this in more detail in Q5.
- Implementing threat detection and early warning systems.
- Regularly updating security systems and installing patches promptly to ensure that systems are up to date. This includes implementing a robust series of controls to ensure access to critical systems is appropriately restricted. It also includes controls such as only permitting administrators to install software, in order to prevent employees installing malicious software inadvertently.
- Arranging regular training to ensure all staff are aware of the importance of cybersecurity controls and protocols. We discuss this in more detail in Q7.

.

Q5. Do companies disclosed that they have undertaken a review or testing of their cybersecurity systems? If "yes", was the review performed by an internal or external party?



- **53%** of HSI companies disclose that they have reviewed or tested their cybersecurity systems during the year, using a variety of approaches.

- Of those companies, **54%** focus on how their internal functions have tested controls in relation to cybersecurity as part of their routine controls work. Other companies describe how internal audit undertook focused reviews of cybersecurity systems, including penetration testing. Another approach taken by companies is to have a specific programme of testing and drills to simulate a cybersecurity breach and to ensure the company's systems are able to respond appropriately.

- **9%** of companies who disclose that they have undertaken a review or testing of their cybersecurity systems indicate that the testing was undertaken by an external party, such as their auditor. Though not a requirement, seeking external assurance on cybersecurity systems illustrates a commitment to safeguarding cybersecurity and provides users with comfort that a third party has assessed the company's systems. On the other hand, those that have undertaken external assurance generally do not provide much detail on the results and recommendations of those reviews.

- Although some companies provide good detail in relation to the review and testing of their cybersecurity systems, many include only general disclosure without any substantial detail. These high-level disclosures referred to "security system reviews" or other general terms, making it challenging to understand what has actually been undertaken and who has conducted the review.

- In these circumstances, although it is helpful to understand that a company has undertaken some review work, not enough information is provided to make the disclosures very useful to end users.

Q6. Do companies disclose that they have experienced a cybersecurity incident or have identified weakness in their cybersecurity systems? If "yes", do they explain how these were addressed and the remedial actions taken.

- No companies disclose that they experienced a cybersecurity incident during the reporting period or that they have identified weaknesses in their cybersecurity systems. Some companies qualify their disclosure by indicating that they had not experienced any "material" or "significant" cybersecurity incidents or events. They do not provide any additional disclosure to indicate if they had any "immaterial" or "minor" cybersecurity incidents.

- Applying the concepts of "materiality" or "significance" to cybersecurity incidents is a reasonable approach to ensuring that disclosure is relevant and focused. Providing key information about significant incidents helps stakeholders to understand the potential impact of an incident on the company and potentially themselves, whilst preventing "over-disclosure" for minor events. The SEC has taken a similar approach to their recent cybersecurity rule changes, with disclosure focused on material incidents.

- The challenge with this approach is defining what is "material" or "significant" and the perspective of those assessments. Even if a cybersecurity incident appears immaterial to the company, it could be material to any individuals it impacts upon. In determining if disclosure of an event should be made, companies should refer to criteria that they have established internally, or reference criteria set by external parties, such as regulators or data privacy authorities, for what constitutes a disclosable event. Including some reference to these criteria in their cybersecurity disclosures would help to improve transparency.

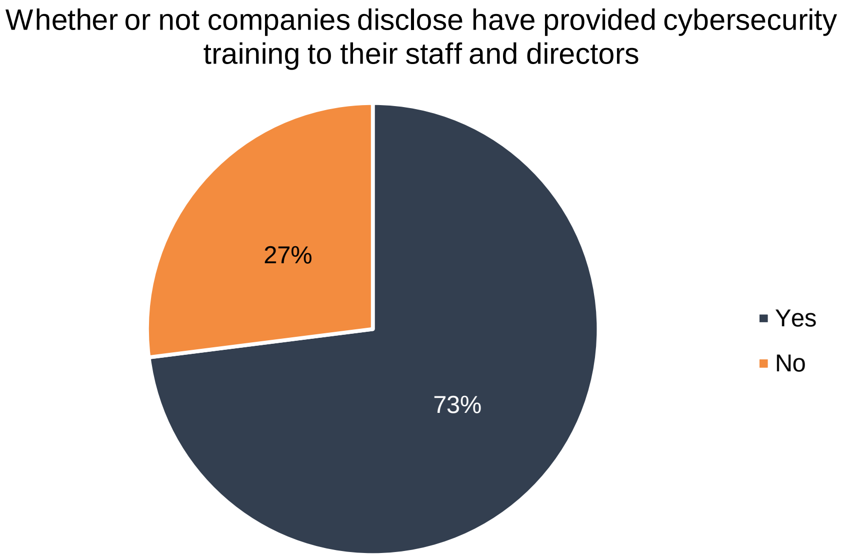
Remedial actions and threat response systems

Although no companies disclose a material cybersecurity incident, 53% of HSI companies disclose details on how they would respond if there were an incident. Information provided includes:

- Disclosing the existence of an incident response plan, with regular review of the plan to ensure it is up to date on the latest cyberattack threats.
- Maintaining an incident-reporting log which ensures incidents are investigated and addressed promptly.
- Explaining that any cybersecurity breach occurring as a result of an employee not following protocol would be treated as a disciplinary event.
- Obtaining cybersecurity incident insurance to protect the company in the event of a cybersecurity breach or incident.

.

Q7. Do companies disclose whether they have provided cybersecurity training to their staff and directors? If "yes", do they give further details of that training?



- **73%** of HSI companies indicate that they provided, or required employees to undertake, cybersecurity-focused training.

- Ensuring that staff and directors are up to date on cybersecurity systems and are able to effectively recognize and respond to threats is a crucial part of any cybersecurity system.

- The level of detail provided in disclosures is highly variable. Some companies with better disclosure describe in detail their training on cybersecurity, including information such as:

  i. Regularity of training for different staff roles.

  ii. If the training is mandatory.

  iii. If staff are able to obtain recognized certifications on completion of more advanced cybersecurity training.

  iv. The number of overall hours of training completed by all staff in relation to IT and cybersecurity issues.

  v. The percentage attendance rate for cybersecurity training across the whole company.

  vi. Any on-going training activities, such as simulated phishing attacks and how compliance with this is monitored.

- In a similar trend to the other cybersecurity disclosures discussed above, many companies do not include relevant details in relation to training and only make high-level disclosure regarding training in general or comments that they recognized the importance of cybersecurity training.

Q7. Do companies disclose whether they have provided cybersecurity training to their staff and directors? If “yes”, do they give further details of that training? (cont’d)

Board training

Though some companies indicate that additional training is available to senior members of staff, only three companies explicitly state that they arranged cybersecurity training for board members. Though board members responsibilities differ from those of staff, and they are less likely to be involved in day-to-day operations, particularly NEDs/ INEDs, it is important to ensure all individuals with a governance role at the company are up to date on the latest cybersecurity threats.

.

Q8. Do companies include the emergence of AI as a significant risk factor for cybersecurity? Do companies disclose any plans to use AI in their business processes?

- Of the 82 HSI companies, only three make an explicit link between AI and cybersecurity. Of those three companies, only one provides substantial additional detail and explains that AI is being deployed in their threat detection mechanisms to detect unusual patterns of network activity.

- AI is likely to have a significant impact on cybersecurity, both in terms of creating additional risks and presenting opportunities to improve cybersecurity.

- The potential risks to cybersecurity driven by AI include:

  i. AI-powered phishing attacks that are able to target more individuals, with greater accuracy and a higher chance of success.

  ii. Automation of other social-engineering attacks

  iii. Malware with built in AI-driven learning that is able to learn and adapt to a company's cybersecurity systems.

AI in business process

Though most companies do not discuss AI in the context of cybersecurity, almost all HSI companies include some disclosure on how they are considering AI's impact on their business processes. Most disclosure is high-level and quite general, with little detail on any proposed AI governance systems, though some companies include disclosure in relation to:

- Using AI to better target products to customers.
- Deploying AI to help identify where efficiencies can be found in the production process for goods.
- Integrating AI into products in order to improve end-customers user experiences.

Only two companies include sufficiently detailed disclosures on how they are developing an AI governance strategy to ensure that AI is used safely in their business.

.

Q8. Do companies include the emergence of AI as a significant risk factor for cybersecurity? Do companies disclose any plans to use AI in their business processes? (cont'd)

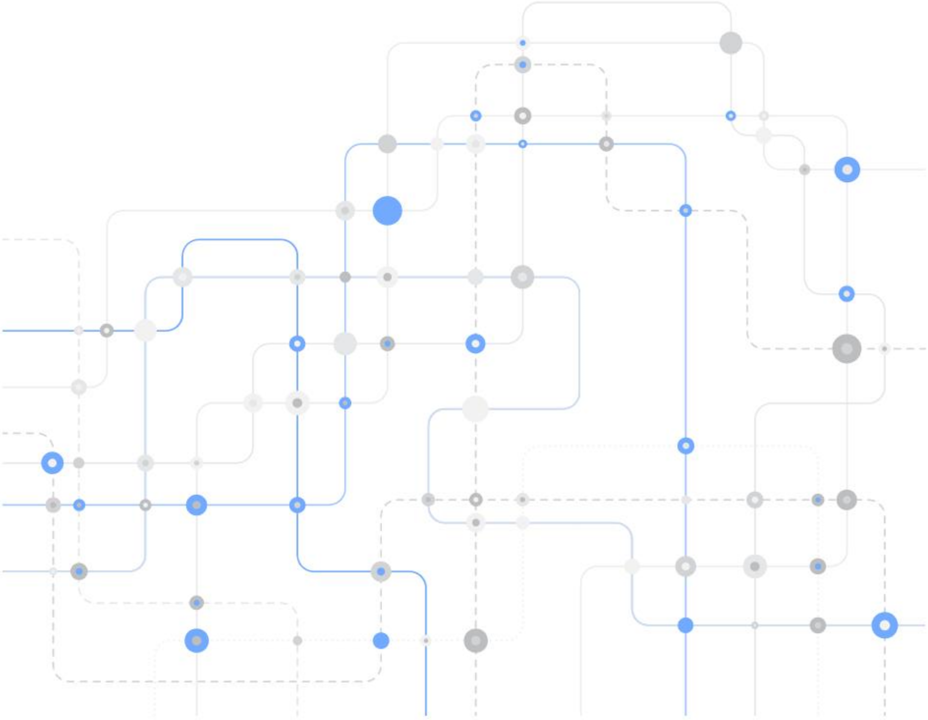
- AI also presents opportunities for companies to improve the effectiveness of this cybersecurity systems, including:

  i. Improved threat detection systems that utilize AI to analyse patterns in network traffic and detect potential vulnerabilities which would be very challenging for traditional techniques to perform.

  ii. Real-time processing of network traffic to allow for automatic triggering of threat response systems.

  iii. Enhanced vulnerability assessments and improved cybersecurity testing approaches.

- Given the potentially significant impact of AI on cybersecurity, we expect to see increasing references to AI in companies' cybersecurity disclosures in the coming years, and it is for companies to consider how they may need to adapt their systems of governance and control in response to this development.



Key findings and recommendations

IT and cybersecurity disclosures can be high-level and lack specific information on the company’s IT and cybersecurity governance strategy.

Recommendations: In order to ensure that IT and cybersecurity disclosures are specific and provide relevant information to users, companies should:

i. Ensure any disclosure is focused and linked to the company’s operations and risks. This could include articulation of how threats to IT and cybersecurity systems could lead to adverse outcomes for the company and how they have mitigated those risks.

ii. Include relevant metrics and data (as set out in other recommendations) to allow users to understand the extent and effectiveness of the company’s IT and cybersecurity governance strategies.

iii. Focus on material issues, and not include overly high-level statements that do not provide specific relevant information on the company.

To improve the information available to investors, and encourage greater consistency between companies, we would suggest that HKEX consider introducing some comply-or-explain provisions in the CG Code and/or ESG Reporting Guide covering IT and cybersecurity disclosure requirements, such as:

i. Disclosure relating to a company’s IT and cybersecurity governance systems and policies, where these have been established.

ii. A clear indication of responsibilities for IT and cybersecurity governance and systems at the board and management levels.

iii. The company’s policy for reviewing its cybersecurity systems, including frequency and responsibilities.

iv. How the company has complied with any relevant laws and regulatory requirements on personal data protection, cybersecurity, etc., in addition to any disclosures under KPI B6.5 of the Environmental, Social and Governance Reporting Guide (Appendix C2 of the Listing Rules).

v. Confirmation that the board is kept informed of IT governance and cybersecurity risks among others.

.

Key findings and recommendations (cont'd)

IT and cybersecurity disclosures, particularly when included in the ESG report, are often not explicitly linked with risk.

Recommendations: When making disclosure on IT and cybersecurity systems, companies should ensure that they are integrated into the company's broader framework for identifying and mitigating risk. This should include:

i. Ensuring that the risk of IT and cybersecurity failure is linked explicitly to business risks and/or the risk of failing to achieve ESG objectives.

ii. Avoiding general discussion of cybersecurity in the ESG report without explaining how this impacts the company directly.

iii. Ensuring that mitigation methods are embedded into the company's wider risk management framework.

iv. Consideration of the most appropriate location for disclosure. Given the generally higher-quality disclosure observed in ESG reports, focusing disclosure there, with explicit links to risk, may provide the best quality information for users.

Some companies have not established a review process for their cybersecurity systems.

Recommendations: Companies should consider implementation of a formal review policy for their cybersecurity systems in order to ensure they remain sufficient to protect the company. A formal review policy should include information such as:

i. The frequency of review, which should be at least annually.

ii. Criteria for trigger events which dictate that a review may be required outside of the normal cycle.

iii. Who is responsible for the review, including the specific responsibilities of, e.g., the audit committee and internal audit in relation to the review.

iv. If, or when, an external assurance provider should be engaged to conduct the review.

v. Considering whether adoption of a recognized cybersecurity certification would be beneficial to the company.

Key findings and recommendations (cont'd)

Disclosure relating to company's cybersecurity incident response plans is highly variable in detail and quality.

Recommendations: Companies that do not disclose any detail about their cybersecurity incident-response plan governance should consider including relevant disclosure in either their annual report or ESG report.

For those companies that disclose, sufficient information should be included on:

i. How the cybersecurity response plan is governed and designed to address the company's specific risks.

ii. How often the plan is tested and how any issues detected in those tests are addressed.

iii. On-going monitoring activities to ensure that the plan is effective.

.

A majority of companies provide some on-going cybersecurity training to employees, though many companies lack board level IT and cybersecurity experience.

Recommendations: Companies should consider whether the extent of their cybersecurity training is sufficient to mitigate IT and cybersecurity threats to the company. Companies should also review their board training and expertise to determine if appointing a board member with specific IT and/or cybersecurity experience may be beneficial to achieving the company's objectives.

Best practice for disclosure in relation to IT and cybersecurity training should include:

i. An indication of the level of staff the training is provided to i.e. directors only or all staff etc.

ii. The frequency of any training and the number of staff hours/attendance rates.

iii. If the training is mandatory or voluntary and how staff attendance is monitored.

iv. Information on training provided to the board.

.

Further resources

Disclosure resources

SEC Disclosure Guidance for Cybersecurity: Although specific to SEC filings, this guidance includes discussion of important concepts related to risk factors and materiality.

FRC Digital Security Risk Disclosure: Focuses on the quality of cyber-related disclosure within the UK FTSE 350, including discussion of “over-disclosure” and detailed guidance on the key factor’s investors are considering.

SFC Cybersecurity circulars: A series of circulars and FAQs on a number of important cybersecurity related topics.

Digital Policy Office: Although directed at Government departments, these guidelines provide helpful information on topics such as penetration testing and mobile security.

AI resources

Office of the Privacy Commissioner for Personal Data, Hong Kong, AI: Model Personal Data Protection Framework: Provides practical recommendations and best practises to assist organisations in procuring, implement and using AI, in compliance with the Personal Data (Privacy) Ordinance (Cap. 486).

Thomson Reuters Foundation, AI Disclosure Initiative: An initiative to walk companies through a review of how AI might be used in their business, including how they address data privacy and bias concerns.

Hong Kong Institute of Certified Public Accountants
37th Floor, Wu Chung House
213 Queen's Road East, Wanchai, Hong Kong
Tel: (852) 2287 7228
Fax: (852) 2865 6603
Email: hkicpa@hkicpa.org.hk
Website: www.hkicpa.org.hk