HONG KONG MONETARY AUTHORITY

Research Memorandum 12/2025

29 September 2025

ASSESSING CYBER RISKS FOR FINANCIAL STABILITY: EVIDENCE FROM INVESTMENT FUNDS

Key points:

- *As the global financial system becomes increasingly digitalised and interconnected, the frequency and severity of cyber incidents affecting financial institutions have risen sharply. These incidents result in financial losses, data breaches and operational disruptions and raise financial stability concerns. A key concern is that cyber incidents can erode clients' confidence and trigger sudden withdrawals of funding (known as "cyber runs"), increasing liquidity risks for financial institutions affected by these incidents.*

- *Open-ended investment funds are particularly vulnerable to "cyber runs", as investors can quickly redeem investments if they lose faith in fund managers' ability to manage cyber risks. However, the extent to which investment funds are subject to fund outflows has not been studied empirically, possibly due to the lack of comprehensive data on cyber incidents. In this context, this study aims to empirically examine the impacts of cyber incidents on investment fund outflows, and to determine whether better cybersecurity preparedness could mitigate the associated liquidity risk.*

- *Using a novel dataset of global cyber incidents compiled from various sources, our analysis revealed that these incidents could trigger "cyber runs" on investment funds. The severity of these runs decreased with the level of fund managers' cybersecurity preparedness. Less-prepared fund managers (with a cyber-security score in the 10th percentile of the sample) were estimated to experience a weekly fund outflow of 2.9% of their net assets following a cyber incident, far exceeding the average weekly fund inflow of 0.2% over the past decade. In contrast, better-prepared fund managers (with a median cybersecurity score) were estimated to face a much smaller outflow of 1.2%. Furthermore, we found that better cybersecurity preparedness could reduce the risk of cyber incidents occurring.*

- *These findings have three important policy implications for financial stability:*

  - ➢ *First, it is crucial to encourage financial institutions to strengthen their cybersecurity to increase their resilience to cyber risks and the potential consequences.*

  - ➢ *Second, close monitoring of cybersecurity-related liquidity risk is warranted, for example by conducting liquidity tests under cybersecurity-related stress scenarios.*

  - ➢ *Finally, the fragmentation of cyber incident reporting across different data sources may pose challenges for assessing the impacts of cyber risks on financial stability, suggesting the need for international action to strengthen and harmonise cyber incident reporting.*

Prepared by: Victor Leung, Thera Lu and Joe Wong

Market Research Division, Research Department

Hong Kong Monetary Authority

The views and analysis expressed in this paper are those of the authors, and do not necessarily represent the views of the Hong Kong Monetary Authority.

* The authors would like to thank Eric Wong for his helpful comments and suggestions.

1. INTRODUCTION

As the global financial system becomes increasingly digitalised and interconnected, the frequency and severity of cyber incidents[1] have risen sharply, with more than 20,000 cyber incidents affecting financial institutions over the past two decades (International Monetary Fund (IMF), 2024). These incidents result in financial losses, data breaches and operational disruptions, and raise financial stability concerns. A key concern is that such incidents can erode clients' confidence and trigger sudden withdrawals of funds (known as "cyber runs"), increasing liquidity risks for affected financial institutions. "Cyber runs" in banks have received regulatory focus,[2,3] as they are most often affected by cyber incidents in the financial sector, with potentially severe impacts.[4] However, some non-bank financial institutions (NBFIs) that are also vulnerable to bank-like runs, such as asset managers, have been affected by cyber incidents (IMF, 2024).[5] Assessing the impacts of "cyber runs" on NBFIs is therefore important.

Open-ended investment funds are particularly vulnerable to "cyber runs", as investors can quickly redeem their investments if they lose faith in the fund manager's ability to manage cyber risks. However, the extent to which investment funds are subject to fund outflows has not been studied empirically, possibly due to the lack of comprehensive data on cyber incidents. To examine this issue, we constructed a novel dataset by manually integrating a decade of fragmented incident data from various publicly available databases, news articles and regulatory filings. After combining these data sources, we obtained a sample of 72 cyber incidents that occurred at the fund manager level between 2013 and 2024. Our sample included 36 major fund managers, who collectively managed approximately 50% of all open-ended equity funds globally in 2024.

Based on this dataset, our analysis revealed that these incidents could trigger "cyber runs" on investment funds, with the severity of these "cyber runs"

[1] This study follows the International Monetary Fund's (IMF) (2024) definition of "cyber incident": an event that adversely affects the cybersecurity of an information system or the information that the system processes, stores, or transmits.

[2] Duffie and Younger (2019) of the National Bureau of Economic Research and J.P. Morgan conducted a stress test to estimate the liquidity risks of 12 major US banks under three hypothetical "cyber runs" scenarios. Goh et al. (2020) of the IMF also conducted a stress test for 18 Singaporean banks.

[3] In response to escalating cyber threats, the Hong Kong Monetary Authority (HKMA) has stepped up efforts to strengthen the cyber resilience of the domestic banking sector. Please refer to the HKMA's Annual Report 2024 for further information.

[4] For instance, First Investment Bank experienced deposit outflows equivalent to 10% of its total deposits following a phishing attack in 2014, prompting it to request liquidity assistance from authorities (Bouveret, 2018; Uddin et al., 2020).

[5] According to the IMF (2024), approximately 10% of all cyber incidents targeted asset managers between 2004 and 2023, resulting in total financial losses of approximately US$2 billion.

decreasing with the level of fund managers' cybersecurity preparedness. Furthermore, our analysis indicated that enhancing cybersecurity preparedness could reduce the likelihood of cyber incidents. Building on these findings, our study highlights the importance of (1) strengthening the cybersecurity of financial institutions, (2) close monitoring of cybersecurity-related liquidity risks and (3) undertaking further international efforts to strengthen and harmonise cyber incident reporting for a more comprehensive assessment of cyber risks.

The remainder of this study is organised as follows. Section 2 describes our novel dataset. Section 3 presents our methodology and empirical results. Section 4 concludes the study and discusses its policy implications.

2. DATA

Our dataset included three components: (1) historical records of cyber incidents affecting major fund managers, (2) the balance sheets and cybersecurity ratings of these managers and (3) detailed data on their investment funds. Each of these components is described in the following sub-sections.

2.1 Cyber incidents

To assess the impact of cyber incidents on fund outflows, we compiled a historical record of incidents in two steps. First, we aggregated cyber incidents from four databases commonly used in academic studies[6]: (1) the Center for International & Security Studies at Maryland (CISM), (2) the European Repository of Cyber Incidents (EuRepoC), (3) the Board Cybersecurity (BC), and (4) the Center for Strategic and International Studies (CSIS).[7] Reporting across these databases was highly fragmented, with over 90% of all incidents recorded in a single source. We meticulously removed duplicates to ensure the integrity of our analysis.

Our review of these databases revealed three notable issues. First, some records lack essential information, such as the precise timing, duration, or consequences of incidents, hindering us from including them in our analysis. Second, these databases predominantly document malicious cyberattacks carried out by external parties and rarely captured incidents arising from internal factors, such as network congestion, software failures, or operational errors by fund managers. However, such internal disruptions could undermine client confidence

[6] For instance, Harry and Gallagher (2018), Choi et al. (2022), Pseftelis and Chondrokoukis (2025).

[7] Please refer to Annex A for detailed information on each database.

and trigger “cyber runs”. Omitting these incidents risks underestimating the full scope of “cyber runs”. Third, these databases appear to underrepresent the total number of cyber incidents in the financial sector. Collectively, they listed only 1,281 incidents, with only 51 incidents directly affecting investment fund managers.

To mitigate potential data gaps, we conducted a comprehensive manual search of cyber incidents in news articles[8] and regulatory filings.[9] This search enhanced our sample in two main ways. First, it allowed us to recover missing information for some database records. Second, it identified 21 additional cyber incidents, including those caused not only by malicious cyberattacks but also by internal factors.

After combining all data sources, we obtained a sample of 72 cyber incidents that occurred at the fund manager level between 2013 and 2024. Nevertheless, readers should be aware that this sample may not fully capture all cyber incidents in the investment fund sector, despite our use of multiple databases and additional manual search. This potential under-coverage calls for cautious interpretation of the results presented in Section 3.

2.2 Fund managers

Our sample included 36 major fund managers, who collectively managed a large number of open-end equity funds with total net assets of US$17.7 trillion, representing approximately 50% of the entire market aggregate in 2024.[10] We retrieved their balance sheets from S&P Capital IQ from 2016 to 2024, which contained fund manager characteristics identified as key factors influencing the likelihood of cyber incidents in prior empirical research, such as total assets, return on assets, Tobin’s Q, leverage ratio, and age (Kamiya et al., 2021).

Beyond these financial and structural factors, cybersecurity preparedness may play a critical role in mitigating the cyber risks faced by fund managers. Well-prepared fund managers may be less likely to experience cyber incidents than less-prepared fund managers. Even if a cyber incident occurs, their

[8] These news articles came from Bloomberg, Financial Times, Reuters, The Wall Street Journal, CNBC, and Yahoo Finance.

[9] These regulatory filings included Form 8-K of the US Securities and Exchange Commission and notices to local US authorities regarding cyber incidents.

[10] According to the Investment Company Institute (2025), the total net assets of global open-end equity funds reached US$35.7 trillion at the end of 2024.

operating procedures and infrastructure are likely to be more resilient to cyber threats, which can mitigate fund outflows.

To assess each fund manager's level of cybersecurity preparedness, we constructed a composite cybersecurity score, defined as the weighted average of two components derived from S&P's Global Corporate Sustainability Assessment[11]: (1) the cybersecurity measures score and (2) the IT infrastructure score.[12] The cybersecurity measures score reflects the adequacy of a company's policies and procedures aimed at enhancing employee awareness of cyber risks and the importance of strengthening cybersecurity, such as training programmes, protocols for reporting suspicious activities and cybersecurity-focused evaluations of employee performance. Meanwhile, the IT infrastructure score assesses a company's readiness to respond to system disruptions and cyberattacks, considering factors such as regular testing and certifications of IT systems, as well as third-party vulnerability analyses. A higher composite cybersecurity score indicates better preparedness in terms of cybersecurity measures and/or IT infrastructure, and vice versa.

The trend (Chart 1) and distribution (Chart 2) of the composite cybersecurity scores are visualised below and provide two insights. In terms of trends, it is encouraging to note a significant improvement in fund managers' cybersecurity preparedness in recent years, with the average score rising from 50 in 2016 to 69 in 2024. This reflects a general improvement in these managers' cybersecurity preparedness in the face of escalating cyber threats. In terms of distribution, we observe considerable variation in the level of cybersecurity preparedness among fund managers, with scores ranging from 7 to 100. This wide range indicates different levels of resilience among managers to cyber threats, which is explored in more detail in Section 3.

[11] The S&P's assessment is an annual evaluation of companies' sustainability performance, conducted through a detailed questionnaire survey that includes a section dedicated to information security, cybersecurity and system availability issues. The two scores from this assessment are originally called "IT security/cybersecurity measures" and "IT security/cybersecurity process and infrastructure".

[12] The S&P's assessment assigned weightings to the cybersecurity score and the IT infrastructure score based on expert judgment. We adopted these weightings to calculate the composite cybersecurity score for each fund manager in our baseline analysis. To test the robustness of our results across differing weighting methods, we also calculated the composite cybersecurity scores by extracting the first principal component of both cybersecurity measures and IT infrastructure scores through principal component analysis. Our findings remained robust to this alternative approach.

Chart 1: Trend of composite cybersecurity scores

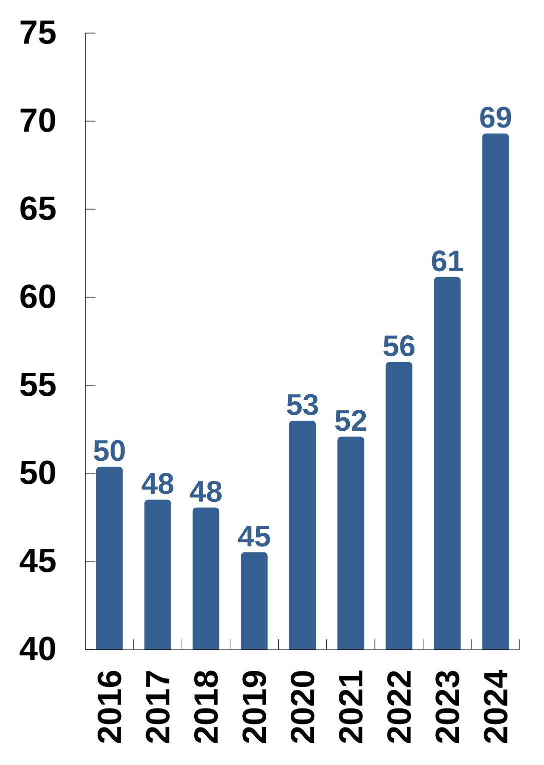
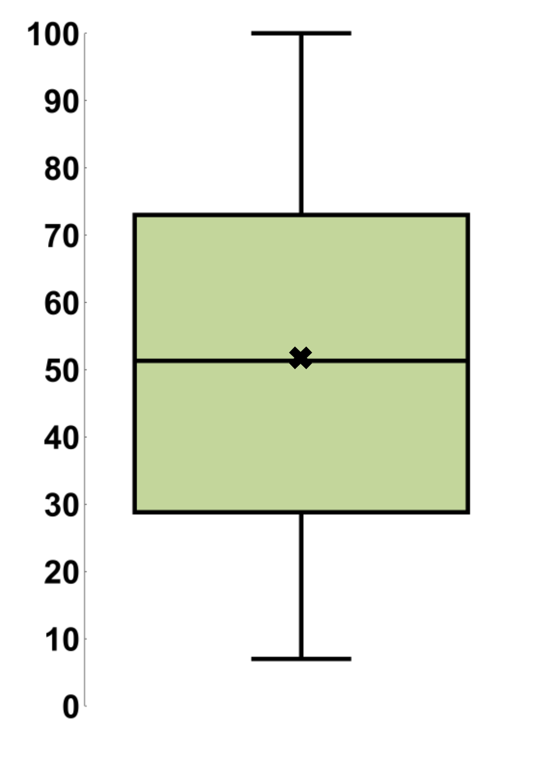


Chart 2: Distribution of composite cybersecurity scores



Notes:

a) The LHS chart illustrates the trend of year-end mean composite cybersecurity scores of sampled funds, defined by the weighted average value of the cybersecurity measures score and the IT infrastructure score.

b) The RHS chart is a boxplot representing the distribution of composite cybersecurity scores of sampled funds. The mean value is denoted by the cross inside the box. The median value is represented by a horizontal line within the box, with 50% of the values falling within the 25th and 75th percentile range shown by the box. The upper and lower end points of the thin vertical lines indicate the maximum and minimum values, respectively.

Sources: S&P Capital IQ and HKMA staff estimates.

2.3 Investment funds

For the 36 major fund managers in our study, we collected detailed data on their investment funds from Morningstar Direct[13], which provides each fund's net asset values, weekly returns, fund flows, benchmark index, fund manager, domicile and inception date.

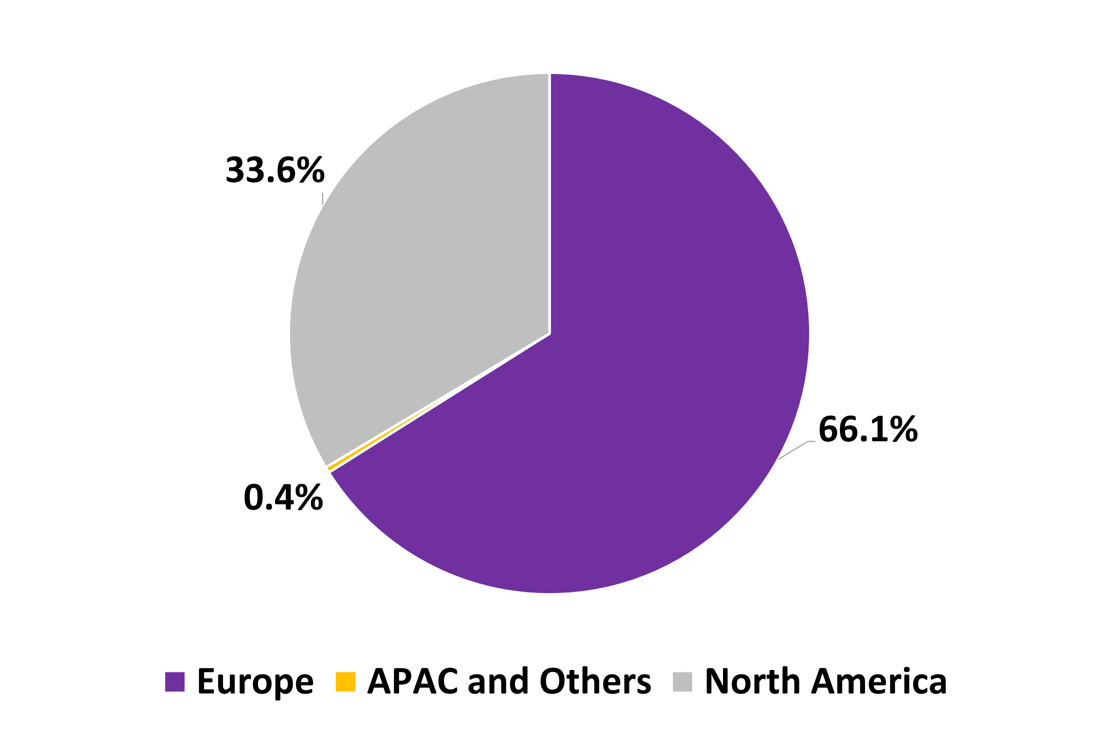
To accurately estimate the impact of cyber incidents on fund outflows, we constructed a fund sample where fund flows were minimally influenced by factors other than the occurrence of cyber incidents. To this end, we limited our

[13] Morningstar Direct's data providers do not guarantee the accuracy, completeness or timeliness of the information they provided and assume no liability for their use.

sample to index-tracking open-ended equity funds rather than their actively managed counterparts. This sampling strategy is intuitive: investment funds vary widely in their characteristics, particularly in the portfolio decisions of their fund managers. Even within the same investment segment, managers of actively managed funds can adjust their portfolios at their discretion, thus influencing their relative performance and in turn fund flows. In contrast, managers of index-tracking funds simply replicate the composition of a specific benchmark and have no discretion to deviate from it, allowing us to better isolate the effect of cyber incidents on fund flows and minimise the impact of omitted variables.

Applying this sampling strategy, our final sample consisted of 3,910 open-end funds tracking 740 stock indices, with a cumulative net asset value of US$1.2 trillion. In terms of geographical distribution (Chart 3), the largest group included funds domiciled in Europe, representing 66.1% of the total net asset value of the sample. The second largest group consisted of funds domiciled in North America, accounting for 33.6% of the total net asset value. The remaining funds, which were considerably smaller in asset size, were domiciled in the APAC and other regions.

Chart 3: Domiciles of sampled funds (in terms of net asset values)



Note: This chart represents the domiciles of sampled funds, expressed as the shares of the net asset values of sampled funds.
Sources: Morningstar Direct, S&P Capital IQ, and HKMA staff estimates.

3. Empirical analysis and results

Our empirical analysis was divided into three parts. In Section 3.1, we provide a descriptive overview of the cyber incidents affecting the sampled fund managers over the past decade. In Section 3.2, we examine the magnitude of "cyber runs" on investment funds and assess the effectiveness of cybersecurity preparedness in mitigating their impacts. Finally, in Section 3.3, we investigate whether enhancing cybersecurity preparedness reduces the likelihood of cyber incidents.

3.1 Cyber incidents affecting investment funds

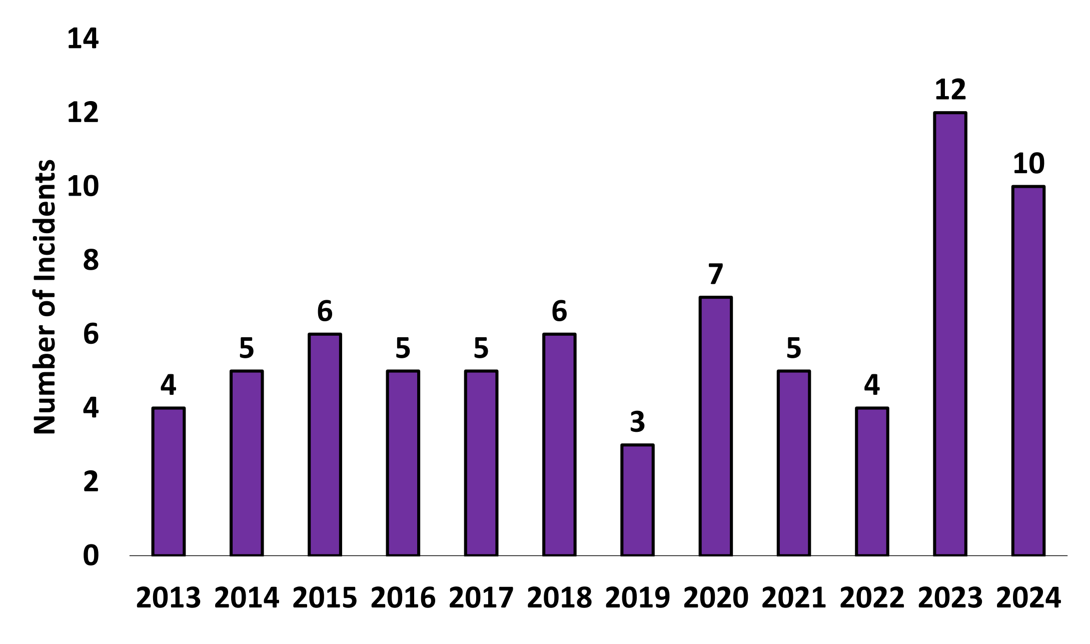
Our novel dataset reveals that cyber incidents became increasingly frequent among major fund managers between 2013 and 2024 (Chart 4). Notably, the annual number of incidents recorded in 2023 and 2024 was approximately double the average observed in the earlier years of the sample. This finding highlights the growing cyber threats in the investment fund sector.

Meanwhile, our analysis showed significant variations in the number of cyber incidents across fund managers. Although many have experienced only one incident in the past decade, some have experienced as many as six incidents. This large disparity probably reflects significant differences in cybersecurity preparedness among fund managers, as discussed in Section 2.2. In Section 3.3, we assess whether better cybersecurity preparedness reduces the probability of such incidents[14].

These cyber incidents can be attributed to three main causes (Chart 5). Specifically, 39% resulted from internal factors, such as network congestion, software failures, and operational errors by fund managers. The remaining incidents stemmed from external factors divided into two categories: 44% were cyberattacks targeting fund managers, while the remaining 17% were disruptions to fund managers' third-party service providers, which subsequently impacted the managers. These incidents had varying consequences for fund managers, including financial losses, data breaches, and operational disruptions, which accounted for 3%, 47%, and 50% of the total, respectively (Chart 6).

[14] During our sample period, the average probability of a fund manager experiencing at least one cyber incident in a year was approximately 14%. This probability was calculated by dividing the number of years in which a fund manager experienced at least one incident by the length of the sample period, which spanned 12 years from 2013 to 2024.

Chart 4: Trend of cyber incidents faced by fund managers



Note:
The chart illustrates the number of cyber incidents affecting the sampled fund managers from 2013 to 2024.
Sources: CISM, EuRepoC, CIT, SCE and HKMA staff estimates.

Chart 5: Causes of cyber incidents

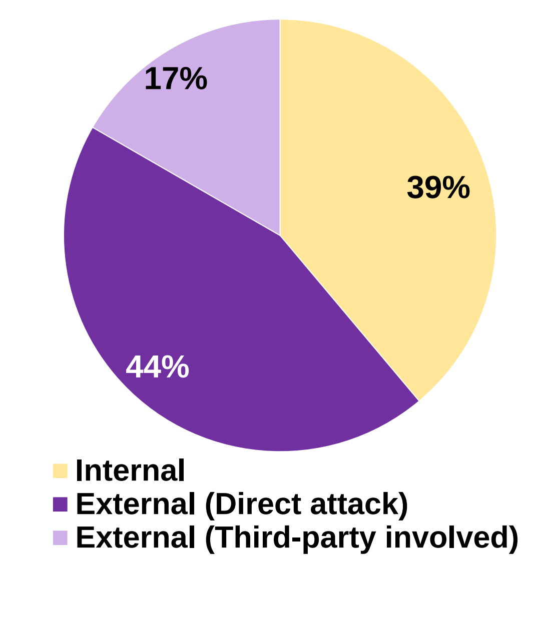
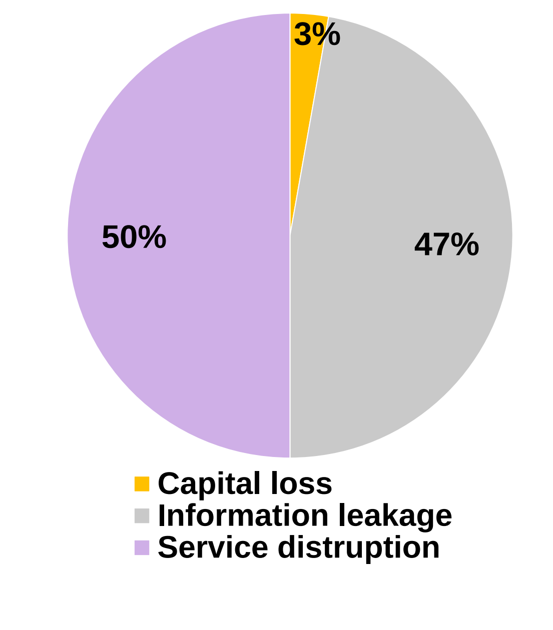


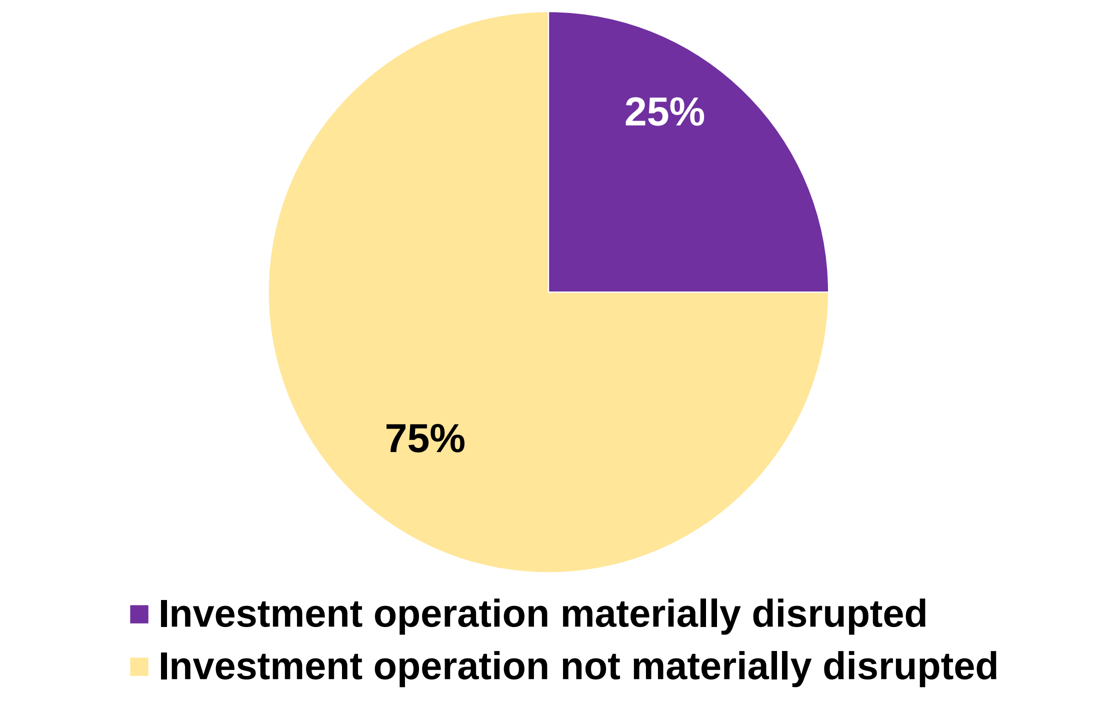
Chart 6: Consequences of cyber incidents



Note: The LHS chart shows the causes of sampled cyber incidents, expressed by the shares of cyber incidents with a particular cause. The RHS chart shows the consequences of sampled cyber incidents, expressed by the shares of cyber incidents with a particular consequence.
Sources: CISM, EuRepoC, CIT, SCE and HKMA staff estimates.

Another way to classify these impacts is by determining whether the cyber incidents lead to material disruptions to fund managers' investment operations, such as the execution of incorrect trading orders or the breakdown of the internal investment system. Theoretically, such disruptions are more likely to undermine clients' confidence and lead to "cyber runs", compared with other impacts such as information leakage or disruptions to non-investment operations. In our sample, a quarter of the cyber incidents caused material disruptions to investment operations (Chart 7). The following sub-section examines whether the magnitude of these "cyber runs" varies depending on the type of disruption of the cyber incidents.

Chart 7: Types of disruptions of cyber incidents



Note: This chart shows the types of sampled cyber incidents, expressed by the shares of cyber incidents that materially disrupted the investment operations of fund managers and those that did not.
Sources: HKMA staff estimates.

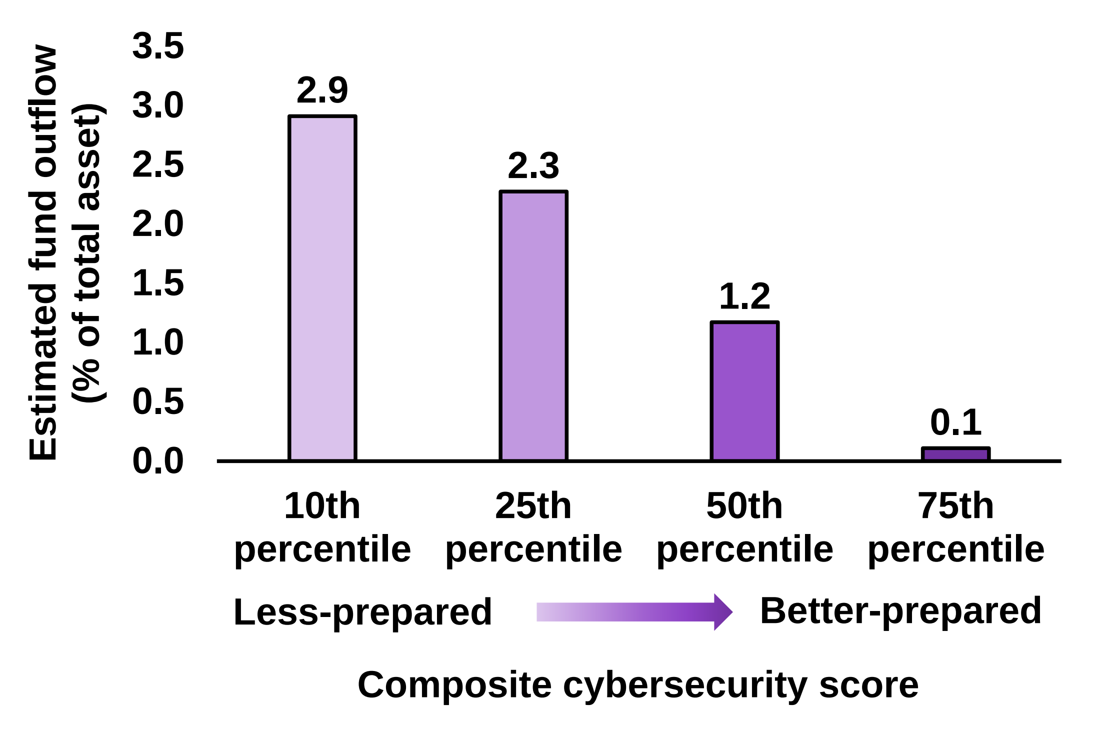
3.2 The magnitude of "cyber runs" and the mitigating impact of cybersecurity preparedness

To estimate the magnitude of "cyber runs" on investment funds and the mitigating impact of cybersecurity preparedness, we conducted a regression analysis using a fixed effects model.[15]

[15] For the specification of the regression model and results, please refer to Annex B.

The results confirmed our conjecture that investment funds suffer from "cyber runs" when a cyber incident materially disrupts fund managers' investment operations. In particular, we found that the severity of "cyber runs" strongly depended on the level of fund managers' cybersecurity preparedness (Chart 8). Specifically, less-prepared fund managers (i.e., those with composite cybersecurity scores in the 10th percentile in our sample) were estimated to witness a weekly fund outflow of 2.9% of their net assets following a cyber incident. This estimated outflow is economically significant, as it far exceeds their average weekly fund inflow of 0.2% over the past decade. In contrast, better-prepared fund managers (i.e., those with composite cybersecurity scores in the 50th percentile) were estimated to face a much smaller outflow of 1.2%. If their composite cybersecurity scores reached the 75th percentile, they were estimated to experience a significantly reduced outflow of 0.1%. These findings suggest that better cybersecurity preparedness can reinforce investor confidence in fund managers. This in turn can reduce outflows and limit liquidity risks for open-ended funds affected by cyber incidents.

Chart 8: Estimated impacts of a cyber incident on fund outflows by cybersecurity preparedness



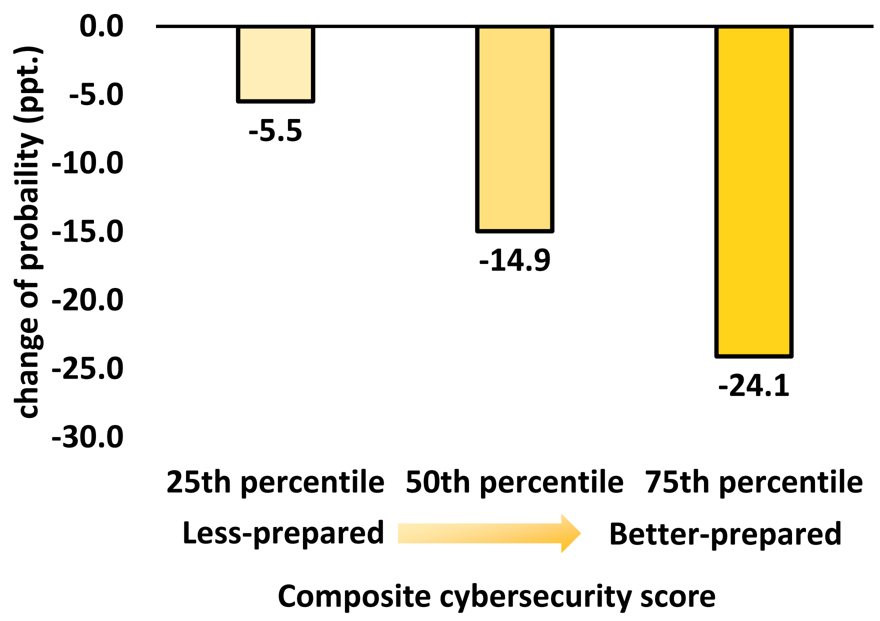
Note: Each bar represents the estimated fund outflow of investment funds, whose composite cybersecurity scores rank at the specified percentile across funds in our sample. A higher score indicates better cybersecurity preparedness, and vice versa.
Sources: HKMA staff estimates.

3.3 The effect of cybersecurity preparedness on the risk of a cyber incident

To further examine whether better cybersecurity preparedness could reduce the risk of fund managers experiencing a cyber incident in the coming year, we conducted a regression analysis using a fixed effects probit model.[16]

Using less-prepared fund managers (i.e., those with composite cybersecurity scores in the 10th percentile) as the baseline, our findings indicated that as their composite cybersecurity scores increased, the probability of a cyber incident occurring in the subsequent year decreased substantially (Chart 9). Specifically, for better-prepared fund managers with a composite cybersecurity score in the 50th percentile, this probability was estimated to decrease by 14.9 percentage points (ppts) from the baseline. If their composite cybersecurity scores reached the 75th percentile, the probability was estimated to decrease even further by 24.1 ppts. These findings show that better cybersecurity preparedness can significantly reduce the probability of a cyber incident, and thus enhance the liquidity resilience of investment funds.

Chart 9: Estimated reduction in the probability of a cyber incident occurring compared to that of less-prepared fund managers



Note: Each bar represents the estimated decrease in the probability of a cyber incident occurring to fund managers, whose composite cybersecurity scores rank at the specified percentile across fund managers in our sample, compared to the less-prepared fund managers with scores in the 10th percentile. A higher score indicates better cybersecurity preparedness, and vice versa.
Sources: HKMA staff estimates.

[16] For the specification of the regression model and results, please refer to Annex C.

4. CONCLUSIONS

In conclusion, our empirical analysis sheds light on the magnitude of “cyber runs” on investment funds. The results underscore the importance of cybersecurity preparedness to mitigate fund outflows and reducing the risk of cyber incidents.

These findings have three important policy implications for financial stability. First, it is crucial to encourage financial institutions to strengthen their cybersecurity to increase their resilience to cyber risks and their potential consequences. Second, closer monitoring of cybersecurity-related liquidity risk is warranted, for example by conducting liquidity tests under cybersecurity-related stress scenarios. Finally, the fragmentation of cyber incident reporting across different data sources may pose challenges in assessing the impacts of cyber incidents on financial stability, highlighting the need for further international action to strengthen and harmonise cyber incident reporting.

Meanwhile, it is important to recognise the limitations of this study. Despite our efforts to address data gaps, our analysis may not have captured all cyber incidents that affected the investment funds in the sample. Additionally, the lack of detailed information on some incidents may have led to the misclassification of incident types. Furthermore, the cybersecurity preparedness assessment was based solely on the annual questionnaire survey conducted by S&P as part of its Global Corporate Sustainability Assessment. This approach may be vulnerable to self-reporting issues and may not accurately reflect actual practices in place. As such, the findings of this study should be interpreted with caution, as the potential data gaps and measurement limitations may affect the accuracy of our results.

REFERENCES

1. Bouveret, A. (2018). Cyber risk for the financial sector: A framework for quantitative assessment. IMF Working Paper No. WP/18/143. International Monetary Fund.

2. Choi, J. S., Gallagher, N., & Harry, C. (2022). Effect-centric approach to assessing the risks of cyber attacks against the digital instrumentation and control systems at nuclear power plants. Center for International & Security Studies, U. Maryland.

3. Duffie, D., & Younger, J. (2019). Cyber runs. Hutchins Center Working Paper #51. Washington, D.C: The Hutchins Center on Fiscal & Monetary Policy, Brookings Institution.

4. Harry, C., & Gallagher, N. (2018). Classifying cyber events. Journal of Information Warfare, 17(3), 17-31.

5. Goh, J., Kang, M. H., Koh, Z. X., Lim, J. W., Ng, C. W., Sher, G., & Yao, C. (2020). Cyber risk surveillance: A case study of Singapore. IMF Working Papers 2020/028. International Monetary Fund.

6. International Monetary Fund. (2024). Chapter 3: Cyber risk: A growing concern for macrofinancial stability. Global Financial Stability Report.

7. Investment Company Institute (2025). Worldwide regulated open-end fund assets and flows first quarter 2025.

8. Kamiya, S., Kang, J. K., Kim, J., Milidonis, A., & Stulz, R. M. (2021). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. Journal of Financial Economics, 139(3), 719-749.

9. Pseftelis, T., & Chondrokoukis, G. (2025). Understanding cyber incident dynamics in the European union: A study of actor types and sector vulnerabilities. Retrieved from https://www.preprints.org/frontend/manuscript/5d731249e7813941fbcb5f39605508e2/download_pub

10. Uddin, M. H., Ali, M. H., & Hassan, M. K. (2020). Cybersecurity hazards and financial system vulnerability: A synthesis of literature. Risk Management, 22(4), 239-309.

ANNEX A: INFORMATION ON CYBER INCIDENTS DATABASES

The databases typically record cyber incidents across multiple industries with various focuses. CISM and EuRepoC provide more comprehensive records of global cyberattacks, whereas CIT and SCE have specific focuses. CIT, for instance, is designed to assist board directors, executive managers and investors in assessing and managing cybersecurity risks, and it primarily tracks incidents targeting listed companies in the US. SCE, on the other hand, focuses on significant attacks only, such as attacks that target government agencies, defence and high-tech companies, or economic crimes exceeding one million dollars.

Table A1: Information on Cyber Incidents Databases

Database	Data Provider	Data Source	Focus	Data Period
CISM	University of Maryland	News, public reports and social media	Cyberattacks worldwide	2014 - Present
EuRepoC	An independent research consortium	News, public reports and social media	Cyberattacks worldwide	2000 - Present
CIT	Board Cybersecurity, a private Company	SEC reporting	Cyber incidents reported to the US SEC	2019 - Present
SCE	Center for Strategic & International Studies, a non-profit research organization	News, public reports and social media	Significant cyberattacks and significant economic crimes	2006 -Present

ANNEX B: REGRESSION ON FUND FLOWS

To examine the existence of “cyber runs” and the mitigating effect of cybersecurity preparedness, the weekly fund flows of investment funds were regressed on the occurrence of cyber incidents and cybersecurity scores, which can be expressed as Equation (1):

$$
\begin{aligned}
FundFlow_{i,y,t} = {} & \beta_1 Incident_{i,y,t} + \beta_2 Score_{i,y-1} + \beta_3 Incident_{i,y,t} \times Score_{i,y-1} \\
& + \boldsymbol{\delta Fund_{i,y,t-1}} + \boldsymbol{\mu Manager_{i,y-1}} + \boldsymbol{\gamma FF_i} + \boldsymbol{\varphi Week_{y,t}} + \boldsymbol{\theta Index_i} \\
& \times \boldsymbol{Week_{i,\,y,t}} + \varepsilon_{i,y,t}
\end{aligned} \tag{1}
$$

where:

$FundFlow_{i,y,t}$= the fund flow of fund i in week t of year y, which is measured by 100 times the ratio of the weekly fund flow to the total net assets of the fund.

$Score_{i,y-1}$= the composite cybersecurity score of fund i’s manager in year $y-1$.

$Incident_{i,y,t}$= a dummy variable which equals 1 if fund i’s manager experiences any cyber incident (i.e. disrupting the functioning of the fund manager’s investment divisions) in week t of year y and 0 otherwise.

$\boldsymbol{Fund_{i,y,t-1}}$ = a vector of control variables of fund i in week $t-1$ of year y, including the weekly return, the natural logarithm of the fund’s age and the natural logarithm of net assets.

$\boldsymbol{Manager_{i,y-1}}$= a vector of control variables of fund i’s manager in year $y-1$, including the natural logarithm of net assets, the natural logarithm of fund manager’s age, return on assets, Tobin’s Q, leverage ratio, tangible asset ratio.

$\boldsymbol{FF_i}$= fixed effect of fund i.

$\boldsymbol{Week_{y,t}}$= fixed effect of week t in year y.

$\boldsymbol{Index_i} \times \boldsymbol{Week_{i,y,t}}$ = the time-varying fixed effect of the benchmark index of fund i in week t of year y.

$\varepsilon_{i,y,t}$= the error term of the regression model.

The key coefficients measuring the impact of cyber incidents on fund flows are β_1 and β_3. If the sign of β_1 is negative, it indicates that a cyber incident would cause a decrease in fund flows for the affected investment fund, thereby confirming the existence of “cyber runs”. The coefficient β_3 measures how the impact of a cyber incident on fund flows may change with the composite cybersecurity score. If β_3 is positive, it suggests that a higher cybersecurity score could reduce the impact of cyber incidents, thereby implying a mitigation of “cyber runs”.

Regression Results

We found a significant impact on fund flows from incidents that led to material disruptions to the investment operations of fund managers only[17]. The regression results are presented in Table A2.

Table A2: Regression Results of Equation (1)

Dependent Variable: $FundFlow_{i,y,t}$	**Equation (1)**
$Incident_{i,y,t}$	-3.6835***
$Score_{i,y-1}$	-0.0005
$Incident1_{i,y,t} \times Score_{i,y-1}$	0.04897***
$\boldsymbol{Fund_{i,y,t-1}}$	Controlled
$\boldsymbol{Manager_{i,y-1}}$	Controlled
$\boldsymbol{Fixed\ Effects}$	Controlled
	(Number of Funds: 2,064 Number of weeks: 416 Number of Index × Number of week: 91,871)
Number of Observations	466,382
Adj. R-squared	0.0932

Note: *, ** and *** represent the statistical significance at the 10%, 5% and 1% levels, respectively.
Source: HKMA staff estimate.

As expected, the coefficient of $Incident_{i,y,t}$ is negative at the 1% significance level, indicating that cyber incidents can trigger "cyber runs" for investment funds. Specifically, the value of the coefficient was -3.68, signifying that the decrease in fund flow resulting from a cyber incident can be as large as 3.68 ppts, assuming that the fund manager has a cybersecurity score of zero. However, it is worth noting that this magnitude is only hypothetical since the cybersecurity scores observed in our sample are always positive. Furthermore, the coefficient for the interaction term, $Incident1_{i,y,t} \times Score_{i,y-1}$, has a value of 0.049, suggesting that for every 10-point increase in cybersecurity score, the magnitude of "cyber runs" can be reduced by 0.49 ppts. This result confirms the effectiveness of enhanced cybersecurity preparedness in mitigating "cyber runs".

[17] A regression analysis of cyber incidents that did not materially disrupt the investment operations on fund flows has also been conducted. Yet, the estimated impact is found to be statistically insignificant. These findings suggest that only cyber incidents that materially disrupted the investment operations would lead to fund outflows from the affected investment funds.

ANNEX C: REGRESSION ON THE PROBABILITY OF OCCURRENCE OF CYBER INCIDENTS

To examine the effectiveness of cybersecurity preparedness in reducing the probability of fund managers experiencing cyber incidents, a regression analysis was conducted on the occurrence of cyber incidents using a fixed effects probit model, which can be expressed as Equation (2):

$$Prob\big(Incident_{j,y} = 1\big) = \Phi(\alpha Score_{j,y-1} + \boldsymbol{\delta Manager_{j,y-1}} + \boldsymbol{\gamma FF_j}) \qquad (2)$$

Where

$Incident_{j,y}$= a dummy variable which equals 1 if fund manager j experiences any cyber incident in year y and 0 otherwise.

$Score_{j,y-1}$= the composite cybersecurity score of fund manager j in year $y - 1$.

$\boldsymbol{Manager_{j,y-1}}$= a vector of control variables of fund manager j in year $y - 1$, including the natural logarithm of net assets, the natural logarithm of fund manager's age, return on assets, Tobin's Q, leverage ratio, tangible asset ratio.

$\boldsymbol{FF_j}$ = fixed effect of fund manager j.

The key coefficient α is expected to be negative if a higher composite cybersecurity score can lower the probability of occurrence of cyber incidents. With this estimate, we can calculate the average marginal effect of the composite cybersecurity score, which represents the average change in the probability of occurrence of cyber incidents given a one-point increase in the score.

Moreover, as a robustness check, we also conducted an ordinary least squares (OLS) regression to examine the consistency of the signs of the coefficients across the models. The regression model can be written as Equation (3):

$$Incident_{j,y} = \alpha Score_{j,y-1} + \boldsymbol{\delta Manager_{j,y-1}} + \boldsymbol{\gamma FF_j} + \varepsilon_{i,y,t} \qquad (3)$$

Regression Results

Table A3: Regression Results of Equation (2) and Equation (3)

Dependent Variable: $Incident_{j,y}$	**Equation (2)**	**Equation (3)**
$Score_{i,y-1}$	-0.0200*	-0.0018*
$\boldsymbol{Manager_{j,y-1}}$	Controlled	
$\boldsymbol{Fixed\ Effects}$	Controlled (Number of fund managers: 20)	
Number of Observations:	157	

Notes:

(1) *, ** and *** represent the statistical significance at the 10%, 5% and 1% levels, respectively.

(2) The regression results of the probit model (i.e., Equation (2)) are presented in Column 2, which are the results of interest. For robustness check, the results of the linear model (i.e., Equation (3)) are presented in Column 3.

Source: HKMA staff estimate.

As shown in Table A3, the coefficients of the composite cybersecurity score in both probit and linear models have negative signs, indicating that greater cybersecurity preparedness of fund managers is associated with a lower probability of a cyber incident occurring in the next year. To quantify the magnitude of this impact, we estimated the average marginal effect of $Score_{j,y-1}$, which is presented in Table A4.

Table A4: Average Marginal Effect of Composite Cybersecurity Score

Values of Composite Cyber Score	Average Marginal Effect
Full Sample	-0.00421

Source: HKMA staff estimate.

In Table A4, the average marginal effect of the composite cybersecurity score across all observations is -0.421%. This indicates that, holding other variables constant, a one-point increase in the composite cybersecurity score is associated with an average decrease of 0.421 ppts in the probability of a cyber incident occurring in the next year.[18] To further analyse the impact of the composite cybersecurity score, we calculated its effect at various percentile levels, specifically at the 10th, 25th, 50th and 75th percentiles. The formula used for these calculations can be written as follows:

[18] Due to the non-linearity of the probit model, the marginal effects vary across observations. However, the variance across the marginal effects of our sample is very small (6.08×10^{-6}). Therefore, when we calculated the impact of the composite cybersecurity score on the occurrence of a cyber incident, we assumed that the marginal effects for all observations are consistently equal to the average marginal effect.

$$\text{Impact of Score} = -0.00421 \times \text{Score}$$

The results are summarised in Table A5. Assuming all other variables remain unchanged, when the scores are valued at the 10th, 25th, 50th and 75th percentile, the probability of a cyber incident occurring is estimated to decrease by 6.65 ppts, 12.13 ppts, 21.60 ppts and 30.74 ppts, respectively. Using the score at the 10th percentile as the baseline, an increase in the score to the 25th percentile is associated with a reduction of 5.5 ppts in the probability of a cyber incident occurring. As the score continues to increase to the 50th percentile and the 75th percentile, the estimated reductions in probability become more pronounced, at 14.9 ppts and 24.1 ppts, respectively.

Table A5: Impact of composite cybersecurity score on the probability of a cyber incident occurring

Value of Composite Cyber Score	Impact	Estimated reduction in the probability of a cyber incident occurring compared to that of less-prepared fund managers ($Score = \text{the 10th percentile}$)
$Score = 15.8$ (the 10th percentile)	-6.65 ppts	N.A.
$Score = 28.8$ (the 25th percentile)	-12.13 ppts	-5.5 ppts
$Score = 51.3$ (the 50th percentile)	-21.60 ppts	-14.9 ppts
$Score = 73.0$ (the 75th percentile)	-30.74 ppts	-24.1 ppts

Notes:

(1) Column 2 presents the impact of composite cybersecurity score on the probability of a cyber incident occurring when the scores are valued in different percentiles.

(2) Column 3 presents the estimated reduction in probability of a cyber incident occurring compared to fund managers with composite cyber score in the 10th percentile.

Source: HKMA staff estimate.