AIM 78
Controlling Risk in a Lightning-Speed Trading Environment.

- Explain the importance of speed to high frequency trading.
- Describe ways in which market participants can speed up their trading.
- List the advantages and disadvantages of speed.
- Describe pre-trade and post-trade risk controls used in the marketplace

Explain the importance of speed to high frequency trading

- A main goal of high-frequency trading strategies is to reduce latency, or delays, in placing, filling, and confirming or cancelling orders. This is important because price takers—those who place orders to buy or sell—are exposed to market risk prior to receiving confirmation that their orders have been filled.
- Latency is measured in microseconds (millionths of a second) and has various components, including speed at which market data and signals from the marketplace are processed and geographical distance and response time from the exchange matching engine
- By reducing latency, high-frequency traders are able to send their buy and sell orders to the exchange matching engine at breakneck speeds in the hopes of getting their trades executed first.

Describe ways in which market participants can speed up their trading

- **Unfiltered sponsored access and co-location** Clearing members' customers and nonclearing members typically send their orders to the exchange using the clearing members' trading infrastructure.
- There are two types of arrangements: sponsored access and unfiltered sponsored access.
  - Sponsored access allows clearing members' customers and nonclearing members to access the exchange matching engine directly and includes some pre-trade risk controls, such as price and quantity limits.
  - Unfiltered sponsored access—known as ¯naked access|| in the equities markets and as ¯direct market access|| in the futures markets—enables customers of clearing members and nonclearing members to bypass pre-trade risk controls and to send trades directly to the matching engine.
- Another development in reducing latency is related to how close a trading firm's server is to the exchange matching engine. It is estimated that for each 100 miles the server is located away from the matching engine, 1 millisecond (thousandth of a second) of delay is added.

List the advantages and disadvantages of speed

- Advantages
  - There is evidence that high-frequency algorithmic trading also has some positive benefits for investors by narrowing spreads—the difference between the price at which a buyer is willing to purchase a financial instrument and the price at which a seller is willing to sell it—and by increasing liquidity at each decimal point.
- Disadvantages
  - However, a major issue for regulators and policymakers is the extent to which high-frequency trading, unfiltered sponsored access, and colocation amplify risks, including systemic risk, by increasing the speed at which trading errors or fraudulent trades can occur.
  - Firms with weak internal controls are exposed to risks related to the speed at which trades can be executed and the circumvention of pre-trade risk controls. Moreover, because black boxes sometimes trade with other black boxes, an erroneous price from one could impact the trading strategy of another.
- On January 13, 2010, the SEC proposed a rule change that would prevent broker–dealers from providing customers with unfiltered sponsored access to an exchange.

Describe pre-trade and post-trade risk controls used in the marketplace

- Some exchanges have pre-trade volume and price limits that stop trades outside a certain quantity or price from being executed. Others have trade bust policies that cancel clearly erroneous trades. A well-built algorithm contains risk controls, such as price and quantity limits.
- Broker–dealers and FCMs are responsible for verifying the financial integrity and risk controls of their customers and nonclearing members, whether they are floor, screen-based, or algorithmic traders.
- some clearinghouses, such as the Chicago Mercantile Exchange, provide FCMs with near real-time information on their customers' trades. This post-trade information enables FCMs to monitor customers and nonclearing members with unfiltered sponsored access and to make decisions on whether to allow them to continue trading.
- Therefore, of paramount importance is the speed at which clearing members receive post-trade information from the clearinghouse and incorporate this information into their risk-management systems so 33 that erroneous trades can be detected and stopped.

AIM 79
Report on Cyber Security in the Banking Sector

• Describe factors contributing to the rise of cyber crime against financial institutions.

• Discuss present trends in corporate governance as it relates to cyber security, and explain implications of these trends.

• Assess the greatest challenges financial institutions face in achieving adequate cyber security.

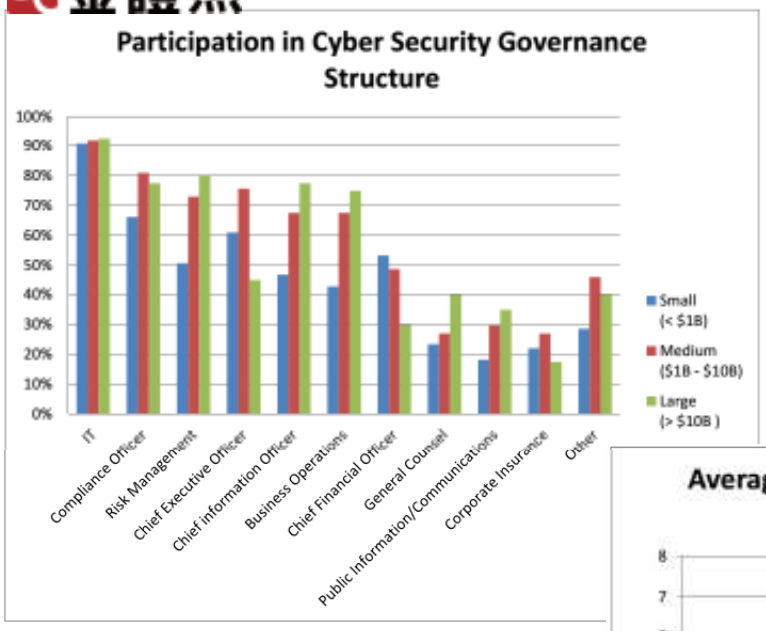
Describe factors contributing to the rise of cyber crime against financial institutions

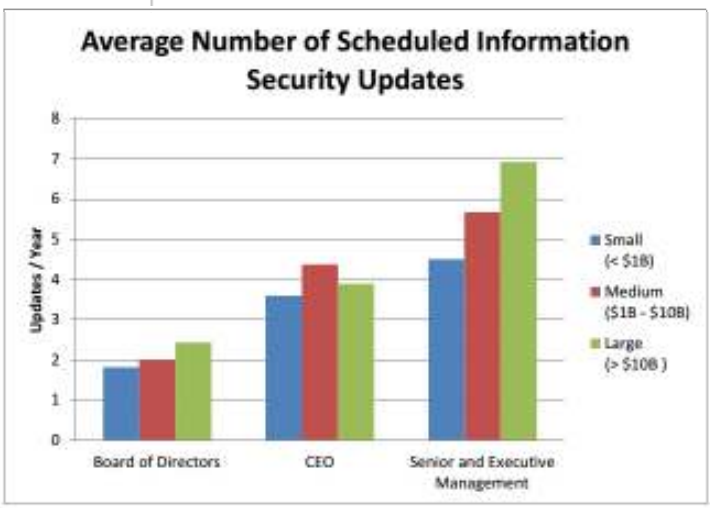
- The rise in frequency and breadth of cyber attacks can be attributed to a number of factors.
  - Unfriendly nation-states breach systems to seek intelligence or intellectual property.
  - Hacktivists aim to make political statements through systems disruptions. Organized crime groups, cyber gangs, and other criminals breach systems for monetary gain—i.e., to steal funds via account takeovers,
  - ATM heists, and other mechanisms. As the cost of technology decreases, the barriers to entry for cyber crime drop, making it easier and cheaper for criminals of all types to seek out new ways to perpetrate cyber fraud. A growing black market for breached data serves to encourage wrongdoers further

Discuss present trends in corporate governance as it relates to cyber security, and explain implications of these trends

- Corporate governance around cyber security tends to be highly IT-centered
- The inclusion of these divisions could only serve to strengthen cyber security governance within an institution and to ensure a holistic approach to managing cyber risk and addressing the consequences of a cyber breach.
- The General Counsel should advise on potential legal liabilities arising from a cyber event, as well as any indemnifications of potential litigants following a breach.
- Corporate Insurance should evaluate the need for (or adequacy of an institution’ s) cyber risk coverage or, alternatively, determine the extent to which Directors and Officers liability policies might apply in the absence of a cyber-specific policy.
- Similarly, an institution’ s Public Information/Communications team should identify potential stakeholders requiring feedback in the aftermath of a cyber attack, as well as anticipate the number and types of inquiries that may arise.

金證照





Assess the greatest challenges financial institutions face in achieving adequate cyber security

- The rapid pace of change makes it more critical than ever that institutions take advantage of the information-sharing and analysis resources available to them. With this in mind, the Department has recommended that all New York State-chartered depository institutions, irrespective of size, become members FS-ISAC.
- Although institutions seem more willing than in the past to share information regarding threats and attacks, many remain hesitant to reveal perceived or actual security weaknesses to competitors.
- In addition, most small and medium institutions outsource functions such as payment processing and most of their web application and online banking systems to external companies. This interconnectedness suggests that an institution’ s cyber risk level depends in large part on the processes and controls put in place by third parties

- Finally, although the issue of limited resources will continue to plague small institutions in particular, the amount of money spent on a cyber program is by no means the best reflection of its strength.
- Costly software that is rarely updated, deployed in an ineffective manner, or fails to take into account social engineering does little to contribute to an institution’ s cyber program. Much more relevant is an institution’ s ability to identify its top cyber risks and design a program around those risks.
- The Department recognizes that cyber security does not have a “one-sizefits-all” solution and that a successful cyber program will be based an institution’ s size, its business model, and sensitivity of data collected. It is essential that an institution’ s view of its cyber risk remains dynamic as those factors change and evolve over time.