

Strengthening Technology Resilience

The SC noted a significant increase in cyber-attacks globally in 2022, corresponding with the rise of remote working practices and growth in the adoption of digital technology. These cyber-attacks have also shown that any firm can be compromised, regardless of size or scale.

To strengthen the management of technology and cyber risks for the capital markets, the SC released a consultation paper on the regulatory framework for Technology Risk Management (TRM). Preventive measures were also undertaken to support capital market entities in becoming more proactive in managing cyber security incidents. Various programmes were held to improve cyber risk awareness and hygiene in the capital market. Two major events that took place in 2022 were the Capital Market Cyber Simulation (CMCS) and Capital Market Cyber Incident Tabletop Exercise (CMCIT Exercise). Both serve the purpose of ensuring that cyber risk standards are upheld within the capital market. CMCS was targeted for entities which have higher dependencies on technology in their daily business operation while the CMCIT Exercise aided less technology-dependent companies to initiate planning and be more prepared for cyber-attacks.

Building resilience to cyber risks

- Capital Market Cyber Simulation

The fifth annual cyber simulation for capital market entities was conducted by the SC in collaboration with the National Cyber Security Agency (NACSA) and CyberSecurity Malaysia (CSM).



110 Entities
which have higher dependencies on technology in their daily business operations were invited.



Themed 'Trust But Verify'
with three cyber event scenarios selected to mimic the challenging circumstances in 2022.

Scenarios	Challenges
Supply chain	The SC acknowledges that attackers explore suppliers as new infiltration points into organisations. Resulting from the increased potential for supply chain hacks to penetrate a large number of consumers, these types of attacks are becoming increasingly common. These attacks predominantly target customer data, including Personally Identifiable Information (PII) data and intellectual property.
Data leakage	Employees are the biggest vulnerabilities to a company's data. With large numbers of employees operating outside of secure corporate networks, this vulnerability is growing. Although hackers have developed more sophisticated strategies and tools for stealing data and information, phishing is still common and an inexpensive technique to gain access to organisations' data. Hackers prey on people's fears and manipulate them into handing over data, often via email or website.
Online defacement	The owner of a website that is defaced usually suffers reputational, and in some instances, monetary damage. As a result, trust among customers might be damaged.



Primary Objectives

- Simulate the cyber incident response and recovery process by participating organisations;
- Identify potential gaps in technology capabilities;
- Rehearse the ability to maintain smooth market operations under different cyber incidents; and
- Familiarise participants with the SC Vault Portal⁴ for escalation and submission of incident reports.



Results

- Significant improvement compared to 2021's exercise despite the increased difficulties in the assessment scenarios; and
- Some participants demonstrated maturity in their level of cyber resilience and were better prepared in the event of a cyber-attack.

⁴ The Vault is a case management system which allows intermediaries to report on, and facilitates the SC's tracking of, any cyber or technology incidents that occurred within the intermediary. It also functions as a communication platform where advisories or alerts are released by the SC to intermediaries registered on the Vault platform.




- Capital Market Cyber Incident Tabletop Exercise

To help organisations strengthen their capabilities in facing potential cyber threats, the *SC Guidance Note on Management of Cyber Incidents* was rolled out to all capital market entities in 2022 as a base handbook to guide cyber security incident handling and management. In addition, tabletop exercises were organised to intensify the efficacy of capital market entities' incident response procedures through increasing awareness and understanding of cyber threats. Almost 200 capital market participants who have never been involved in the annual SC CMCS event participated in the CMCIT Exercise.



Read more on *Guidance Note on Management of Cyber Incidents*.

 <https://www.sc.com.my/api/documentms/download.ashx?id=272ca944-ede5-42ec-bd9d-e1e04184c39a>