SFC proposes baseline cyber security requirements for internet trading

16 May 2017

The Hong Kong Securities and Futures Commission ("**SFC**") has issued a paper containing proposals to introduce cyber security guidelines under the Securities and Futures Ordinance (the "**SFO**") applicable to internet brokers (the "**Cyber Security Consultation Paper**"). Comments are open through 7 July, 2017.

Background

The Cyber Security Consultation Paper reflects a sharpening of focus by the SFC on cyber security issues. The SFC notes that in the 18 months up to 31 March 2017, 12 licenced corporations reported 27 cyber incidents – the majority involving access to clients' trading accounts. These incidents resulted in unauthorised trades to the value of HK$110 million. The Hong Kong Computer Emergency Response Team Coordination Centre is reported to have handled 6,058 cyber security incidents in 2016, an increase of 23% from 2015.

The Cyber Security Consultation Paper highlights the prevalence of a particular form of "pump and dump" scheme in which hackers gain unauthorised access to internet trading accounts and use the cash and securities in these accounts to fund the purchase of penny stocks targeted by the hackers. The hacked accounts are used to pump up the prices of these penny stocks, following which the hackers dump the stock, causing significant losses to the hacked accounts.

Against this backdrop, the SFC conducted a 2016 cyber security review which consisted of fact finding surveys, on-site inspections of brokers' technology controls, discussions with vendors to evaluate the feasibility, cost and benefits of various systems, and a benchmarking exercise against local and overseas regulations and market practices. Based on its findings, the SFC has proposed a framework of "baseline requirements" which licensed and registered persons are expected to comply with.

Please click here to read the full alert.

Contacts

Mark
Parsons

Partner

Louise
Crawford

Senior
Associate

> Read the full article online