



ASIC
Australian Securities &
Investments Commission

Committee	Parliamentary Joint Committee on Corporations and Financial Services
Inquiry	Oversight of ASIC, the Takeovers Panel and the Corporations Legislation No.1 of the 46th Parliament
Question No.	001
Topic	ASX/cyber
Date	26 November 2021
Reference	Spoken, 26 November 2021, Hansard page 9
Committee member	Mr Hill MP

Question

Mr HILL: Absolutely.

Mr Longo: You actually don't have a choice. There are lots of key pieces of infrastructure that rely on technology, and unless it's upgraded and enhanced, the capacity for—you sort of choose a problem you want to have. If you don't make the investment, the cyber-risk goes up; if you do make the investment, you manage the cyber-risk and hopefully you have other benefits.

Mr HILL: First-mover advantage, potentially, is an upside, but first mover carries more risk. So you're confident it's not going to go horribly wrong?

Mr Longo: I'm confident that we've put in place a supervisory framework that the ASX will deliver. They're one of Australia's oldest institutions. We've met with the board. We have confidence that they will—

Mr HILL: In the interests of time, I'm happy for you to give us, on notice, a short supplementary on the cyber issue, rather than going back—

Mr Longo: That'll be fine. We've done a lot of work with ASX—

CHAIR: I feel for Cathie.

Ms Armour: If it's any help, I was going to say my technology issues—

Mr HILL: You were hacked!

Ms Armour: They seem to be solved.

CHAIR: What we've just said is you can provide some supplementary—

Mr Longo: We'll provide some supplementary—

CHAIR: I think we're trying to communicate that to you. Sometimes we're hearing you and sometimes you're freezing.

Answer

Our work indicates that ASX has a resilient cyber resilience posture that is continually being enhanced in line with a rapidly evolving cyber threat landscape. As can be expected, the ASX is a high-profile target for various types of threat actors but has been resilient throughout a period in which we have seen a significant increase in rates of cyber incidents.

ASIC and the RBA through our respective supervision of ASX's clearing and settlement facilities supervise ASX's cyber strategy and its execution. The ASX shares its emerging cyber risks and threat information and action plans with the regulators. Moreover, the ASX's cyber strategy is aligned with the requirements of the Australian Signals Directorate's (ASD) essential eight, and the Committee on Payments and Market Infrastructures (CPMI) and the International Organization of Securities Commissions (IOSCO) guidance on cyber resilience.

The ASX is implementing Distributed Ledger Technology (DLT) as a core component of its new CHES Replacement platform. Security and resilience have been important facets of its design from the onset – this has been informed and validated by external experts and is an important limb of the overall test strategy that has been developed for the CHES Replacement Program.

ASX is expected to demonstrate that with the implementation of the CHESSE Replacement Program it continues to comply with CPMI-IOSCO's international standards that apply to ASX Clear and ASX Settlement (see QoN 2) including CPMI IOSCO's cyber resilience. ASX's Assurance program for the CHESSE Replacement includes obtaining assurance from an independent third party on the security of the new system. Further, under the additional conditions imposed on ASX an independent expert is to be appointed to assess whether ASX's assurance program for the replacement of CHESSE is fit for purpose and to report regularly to ASIC including a report prior to migrating to the new system.

One important facet to note about the new CHESSE system is that all users will be required to operate within the ASX network, and all users are formally validated (a centralised, permissioned DLT), which removes many of the security concerns that commonly arise with publicly accessible DLT platforms.