Cyber Security

Background

Advance HE, working with other Bodies, offers a programme of Round Table events. The events provide an opportunity for a small number of participants (typically governors, governance professionals and senior managers) to discuss topical or emerging issues relating to the governance of higher education providers (HEPs).

At each event, participants share and exchange views under the strict application of the Chatham House rule. None of the discussion is attributed to either an individual or provider. To facilitate the wider dissemination of some of the key points explored, a summary note of each Round Table is released following the event.

The National Cyber Security Centre (NSCS)

The Round Table was hosted by the National Cyber Security Centre (NCSC). Created in 2016, NCSC brought together GCHQ's technical expertise and a number of cyber-security initiatives spread across government. NCSC's role is to make the United Kingdom the safest place to live and do business online. It is engaged in a range of initiatives, involving detecting and countering cyber-attacks as well as working with key economic sectors – including higher education – to raise cyber resilience and maturity. NCSC produces an annual report of its work.

Cyber threats: the context

Cyber threats are diverse and keep changing. As a consequence, a HEP can never be confident that they have 'ticked-off' the threat.

Surveys by JISC confirm that cyber threats are increasing. Typically, JISC witnesses some 6,000 incidents (i.e. series of events) associated with cyber-attacks on the higher education sector each year.

Although most providers provide security awareness training for staff, fewer do so for their students.

Evidence collated by JISC suggested that while the sector as a whole is reasonably well prepared to deal with cyber threats, there is considerable variation between providers. There is no clear pattern to the type or group of provider as to who is well- or ill-prepared to withstand such attacks.

The NCSC publishes detailed guidance on cyber security on its website, and is planning to release an assessment of the specific threats faced by the higher education sector early in 2019.

The guidance available from the NCSC includes a 'board toolkit' and 'cyber security: a small business guide'. Both documents contain information of value to higher education providers and their governing bodies.

The board toolkit highlights five questions:

- **Q** How do we defend our organisation against phishing attacks?
- **Q** How does our organisation control the use of privileged IT accounts? I.e. access control.
- **Q** How do we ensure that our software and devices are up-to-date? I.e. patching.
- **Q** How do we make sure our partners and supplies protect the information we share with them?
- **Q** What authentication methods are used to control access to systems and data? I.e. passwords.

ROUND TABLE NOTE 5 December 2018

Key messages for Governing Bodies include:

- Cyber security is a serious business risk, and needs to be treated accordingly.
- Governors need to educate themselves in the fundamentals of cyber security.
- Governors should not feel daunted by asking questions about cyber security.
- There is the opportunity to work with other providers or organisations to help improve the provider's cyber security.
- Remember the human element. Do not forget the role of people in enabling cyber security.

Linked to the final point, Governing Bodies should also try and engender a culture which encourages staff to report events even when their actions may have had led to risks with cyber security.

Discussion

Representatives from different of providers indicated that their governing body's audit or audit and risk committee had instigated a 'deep dive' on cyber security. The work had typically been undertaken by the external providers of internal auditor, who had used specialist staff to undertake an assessment of the provider's approach to cyber security and their preparedness to deal with attacks.

Governors sought high-level assurance as to the provider's resilience to withstand cyber-attacks. To maintain the level of assurance there was a question of how often should it be necessary to undertake a 'deep-dive'?

As part of the focus on the people factor, some providers undertook artificial phishing exercises to test how individuals would respond. Such exercises could be useful, and not infrequently had 'found-out' senior members of staff.

Cyber threats could impair business continuity. To avoid such an outcome being realised, it was important that cyber security was not just identified as a risk amongst others on a risk register and that policies to mitigate the risk that had been agreed, had also been fully implemented.

The government-backed 'cyber-essentials' scheme, offered the opportunity to gain certification of government-endorsed standards of cyber hygiene.

Generally, providers gave less attention to the cyber threat and risks to students. The annual intake of new students entering higher education, typically led at the start of each academic year to a significant increase in the cyber-attacks experienced by students.