Responding to the threat

Cyber security

January 2015

UK Higher Education: Cyber Security so far

In July 2012, UUK advocated the steps that universities should take to reduce their exposure to cyber security risks and increase levels of resilience:

1. Senior management and governing body awareness.
2. Understanding of the institution's primary intellectual property assets and the level of control around these.
3. Application of 20 controls identified by the Centre for the Protection of National Infrastructure (CPNI) for managing cyber security threats.

Universities UK (UUK) issued a self-assessment questionnaire in June 2014. This was based upon a Department for Business, Innovation and Skills (BIS) health check survey with review input from Uniac and Universities and Colleges Information Systems Association (UCISA) amongst others. 63 institutions who responded to the questionnaires will receive individual briefings shortly. HE institutions who did not respond will receive a separate summary briefing without the value of the benchmarking aspect.

Key themes from the questionnaire

There were a variety of respondents to the questionnaire across the institutions. In the main, responses were received from the Head of IT Security or the Chief Information Officer (CIO). There were also instances where responses were sent by the Vice-Chancellor's office, Chief Operating Officer or Registrar. This demonstrated good engagement at senior levels across institutions.

Key theme	Finding	Uniac's view
Cyber risk management and control	70% of respondents' senior executive teams were fairly confident in their risk management and control. 26% of respondents were not very confident at all and only 3% were very confident.	Cyber security is a relatively recent agenda item for senior executive teams but awareness is building of the need for appropriate risk management and control.

	69% of respondents said that cyber security was on their institution's risk register and in the majority of instances assessed as a medium risk. 15 universities did say that cyber was assessed as high risk. In the main respondents were happy with this classification, however 24% of respondents felt it was under-prioritised.	
Main threat areas to institutions	The main threat areas were perceived to be accidental loss or damage or criminal fraud. With the key risks perceived to be business continuity and reputational damage.	In addition, and in line with the original UUK guidance, there are also the risks surrounding institutional IPR.
Has an information audit been performed?	Just over half of the respondents claim to have conducted an information audit with 74% having been undertaken in the last two years. Over 70% of those who had not undertaken an information audit claimed this was either due to lack of resources or the complexity of the exercise.	Our experience shows that this is an absolutely necessary first step to understand the threat that cyber poses to the institution. An information audit needs to be undertaken to identify those areas at greatest risk of cyber-attack to support prioritisation of risk mitigation actions. We have been undertaking these types of audits for our members.
The main challenges to implementing cyber security?	Challenges included awareness of data owners, evaluation of the significance of the threat, difficulties in identifying and monitoring risks, technical capability and reluctance by	Fundamentally awareness is the issue here to bring about a common understanding within institutions of the threat that cyber poses. Only once there is awareness can

	senior executives to commit resources.	institutions begin to evaluate the risk and implement appropriate risk mitigation activity.
What support would institutions most welcome?	When asked what support institutions would welcome there was a theme in respect of training of data owners and SMT along with risk assessment support and identification of controls. An audit of cyber security controls would be valuable. Help with communication of the risk and ensuring that cyber security was on the institution’s risk register were also areas where support would be welcomed.	There is a growing awareness that cyber threats pose to institutions but how to respond to the threat remains less clear. To be able to have the right discussions and to get appropriate buy-in cyber risk needs to be recognised at the highest levels within the institution and accordingly be on the institution’s strategic risk register. Only with senior management commitment can robust risk management activity be taken forward.

For Internal Audit to provide meaningful IT assurance, specialised staff and tools are required to provide the technical level of assurance required by professional standards. If you would benefit from greater expertise or resource in evaluating and responding to cyber security threats, then Uniac can help in a number of ways.

How can we help?

Our team of qualified IT auditors are members of the Information Systems and Control Association (ISACA) with CISA accreditation. They have extensive experience in IT assurance and advisory across a variety of sectors, including Financial Services and Professional Services.

The team understands that universities are knowledge providers, with the ethos of creating, developing and sharing knowledge to internal and external audiences. This understanding is crucial because there is a balance to be struck in securing confidentiality, integrity and availability of information while enabling the institution to operate effectively.

The team’s familiarity with the higher education sector means it is well placed to advise on relevant emerging cyber threats and risks.

Our Services

We offer support to institutions ranging from one-off specialist reviews through to watching brief project assurance and advisory reviews.

Our IT Audit service in this area is delivered with best practice in mind, as such we can formally benchmark the university's performance, if desired against the plethora of IT standards and frameworks such as ISO27001: Information Security Management; ISO20000 & ITIL: IT Service Management; CPNI Controls for Managing Cyber Threats, CPNI & CESG BYOD Guidance and more.

Recognising the challenge to institutions with the Cyber agenda, we can provide the following IT assurance and advisory services:

- Facilitated workshop sessions with SMT and key stakeholders such as data owners to raise awareness of Cyber threats and risks across the institution to ensure the appropriate profile of Cyber risk within the institution.
- Assurance reviews of the Cyber governance and reporting structures within the institution.
- Support with information classification exercises to assess the sensitivity of key information sets held by the university.
- IT assurance reviews against the 20 CPNI controls or other best practice guidance (as detailed above).
- Adhoc technical and risk and control advice to your institution as and when required.
- Periodic briefing papers on current and emerging cyber threats and risks.

Get in Touch

If you would like to discuss how Uniac could help you provide assurance over cyber security risk, please contact:

Ian Musgrave on 0161 247 4697 or imusgrave@uniac.co.uk

Robert Foster on 0161 247 2851 or rfoster@uniac.co.uk