IT Risk Management Briefing

‘Cyber and Digital Disruption’

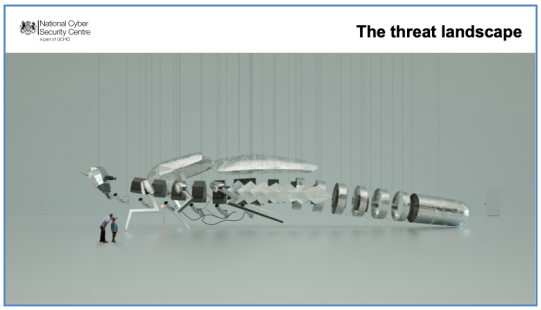
Summary of Uniac Event held on 15th Nov 2019

Introduction

Around 25 HEI staff and non-executive directors attended the Uniac IT risk management event in Senate House, University of London, on Friday 15th November 2019. The twin themes were cyber security and digital disruption with speakers from the National Cyber Security Centre (NCSC), Jisc, Manchester Metropolitan University and Uniac. In a major recent survey* of over 500 European organisations, the Chartered Institute of Internal Auditors has identified cyber and data security as the top risk facing organisations closely followed, in third place, by ‘digitalisation and business model disruption’. This session was therefore a timely reminder of the risks and opportunities offered by these issues.

Cyber Security, Major Issues and Best Practice – Uniac’s View

Joe Johnson and Ian Musgrave of Uniac outlined some of the key findings from Uniac’s recent IT and cyber assurance work with higher education clients. Cyber incidents are continuing to grow, with the education sector globally seen as the least prepared to deal with cyber attacks. Uniac’s cyber approach emphasises the importance of ‘people’ and ‘process’ aspects as well as technology and the need for cyber to be owned by the whole institution not just IT. The ‘human’ aspect of cyber is the main area we are asked to look at by clients and covers user training and awareness, compliance with privacy and security measures, password security and guarding against phishing attacks. Policies and procedures need to be clear and well understood in all of these areas.



NCSC - The Threat Landscape

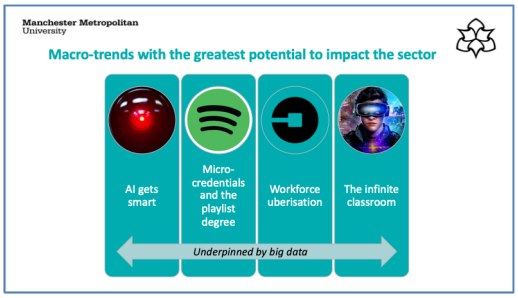
A senior speaker from the NCSC outlined the current threat landscape both within HE and the wider economy and society. Cyber crime probably presents the most evident and disruptive difficulties for universities, although, state-sponsored espionage is likely to cause greater long-term damage. This could damage the value of research, lead to a fall in investment (public or private) in affected universities and harm the UK’s knowledge advantage. The NCSC website www.ncsc.gov.uk is a crucial and helpful resource that incudes discussion of key risk and control vectors such as passwords and phishing, a weekly ‘Threat Report’, ‘Top Tips for Staff’ and links to ‘Cyber Essentials’ accreditation which many universities have undertaken or are considering. The NCSC’s ‘Board Toolkit’ is also a key part of new NCSC guidance and is aimed at helping board members from all sectors become more informed to enable them to carry out their role in understanding risk, assurance and accountability.

* Risk In Focus 2020: Hot Topics for Internal Auditors (CIIA, 2019)

Key Risks and Incidents from Jisc's Security Operations Centre

Simon Cooper manages Jisc's Security Operations Centre which coordinates incident response for all institutions connected to the 'JANET' network and gathers intelligence on potential security issues and advises on mitigation. Simon covered Jisc's latest annual Cyber Security Posture Survey, completed by 122 institutions, including 65 HEIs. This shows that 91% of HEIs have cyber security on their risk register and the number of HE institutions with a dedicated strategic cyber lead shows a steady increase at 66%. The move to gain a security accreditation is also gathering pace across the sector with Cyber Essentials the most popular. The main actions universities should take include improved logging and patch management, penetration testing and better incident response. https://www.jisc.ac.uk/reports/cyber-security-posture-survey-results-2019

Kurt Weideling: 'The Augmented University'



Director of ISDS at Manchester Metropolitan University, Kurt outlined his personal vision of the challenges and opportunities on the horizon. One of the problems in outlining an IT or Digital Strategy is the sheer amount of change and unpredictability. A five-year IT strategy cannot be expected to remain static and will need to be regularly reviewed. Consumers now expect their service providers to work around them (not the other way round) so why should universities be immune to this? Kurt's view of the coming 'macro trends' which will disrupt our sector include: automation of academic tasks such as marking and literature reviews, increased tailoring and flexibility of provision (the 'playlist degree') and the 'Infinite Classroom' with imaginative use of virtual reality technologies. A further challenge is the need to manage data very tightly – not just from a security aspect but from a management perspective given our vital dependency on it.

Staying in Touch

Whether you were able to attend this session or not, we hope you have found this summary of interest. Uniac runs events throughout the year on a variety of subjects related to HE risk, governance and assurance mainly aimed at a joint audience of university staff and board/governing body members. We also publish a range of HE sector briefing notes and benchmarking reports on relevant topics for advice and guidance.

For further information on the above, or any other aspect of Uniac's internal audit and assurance service, please do get in touch.

Ian Musgrave
Head of IT Risk and Assurance
☎ 0161 247 4697 | imusgrave@uniac.co.uk