

IT and Cyber Security Threats, Responses and Good Governance



**A briefing session
for HEI staff and
non-executive
directors**

**1st February 2018
Friends Meeting
House,
6 Mount Street
Manchester, M2 5NS**

9am – 12.30pm

This session will be relevant to:

Governing body and audit committee members who have a key oversight and governance role within institutions.

University management and staff with responsibility for managing IT, data and information governance.

The session will explore a range of current IT and cyber risks and how HEIs should respond.

Context

IT and cyber security risks continue to grow and evolve. 2017 has seen a proliferation of phishing, ransomware and 'denial of service' attacks. In addition, there are enhanced data protection requirements arising out of the new 'GDPR' requirements being introduced in May 2018.

This affects all parts of the organisation, and the responses and solutions likewise need to be all-pervasive. Technology is only part of the answer: the emphasis also needs to be on *people* and *processes*. This means it is the responsibility of all users, managers, system owners - and governing bodies. Institutional responses need to be joined up. If they neglect any one of these strands they are destined to fail, with ever more serious consequences for losses and data breaches.

Universities face particular risks whether around research data, student / teaching focused or specialist activities. While universities are moving to more of a 'compliance' culture including mandatory IT security training this presents issues (for example around staff engagement and potential sanctions for non-compliance) which can challenge traditional institutional culture.



Certificate Number 13024
ISO 9001
BS OHSAS 18001
ISO 14001

finalist 
Cyber Security Awards

Uniac
4th Floor, St James' Building
Oxford Street
Manchester
M1 6FQ

Agenda

9.00 – 9.15 Arrival, tea / coffee

9.15 – 9.20 Introduction and welcome - Andrew McConnell, OBE (Director of Finance, University of Huddersfield / Chair of the Uniac Board)

9.20 – 10.00 Cyber security threats - beyond the headlines. Aatish Pattni (Checkpoint Technologies)

Aatish is Head of Threat Prevention, Northern Europe at Checkpoint Technologies. As cyber attacks continue to grow and evolve, Aatish will discuss the nature of current cyber threats and place it in context in terms of the types of attacks, where they come from, and what the responses should be. The session will cover HE and draw in his experience from the wider business environment.

10.00 - 10.30 IT risks within universities - a status report. Ian Musgrave (Uniac) and Andy Holliday (3VRM)

Ian is Uniac's Head of IT Assurance and Andy is an IT security specialist who has worked extensively in HE in addition to banking and retail. Ian and Andy will provide their assessment of the main IT risks and challenges based on Uniac's internal audit and assurance work with clients within the UK higher education sector.

10.30 – 10.45 Tea / coffee

10.45 – 11.30 Information governance - a holistic university approach. Tony Brown (University of Manchester)

Tony is Head of Information Governance at the University of Manchester which established its new Information Governance Office (IGO) in January 2017. This IGO is the hub of a comprehensive framework designed to complement IT and cyber security activities, which includes training, risk assessing all new systems and a network of over 100 Information Governance Guardians across the institution. The vision is to achieve a step change in culture and ensure the successful adoption and embedding of effective security procedures across the University.

11.30 – 12.00 Non-executive directors - how do they meet the cyber challenge? Open forum

However complex the threats, both management and boards need to understand the issues and ensure they act accordingly. University governing bodies and audit committees have a clear oversight duty to ensure management responses are appropriate. Yet it can be difficult to ensure this duty is discharged effectively when there is often a lack of specific non-executive IT / cyber expertise. This is an area we can expect to see grow as threats increase and the potential shift to a compliance-driven culture.

12.00 Closing summary followed by lunch

If you would like to reserve a place, please reply to Amanda Tallon (atallon@uniac.co.uk / Tel 0161 237 1174) by 19th January 2018.



Certificate Number 13024
ISO 9001
BS OHSAS 18001
ISO 14001

finalist 
Cyber Security Awards

Uniac
4th Floor, St James' Building
Oxford Street
Manchester
M1 6FQ