Higher Education Cyber Webinar

Questions and Answers from the Webinar

The following questions were asked during the webinar. Mark Brannigan, UK Head of Cyber Solutions, and Alison Goodwin, Public Sector Practice Leader, who hosted the webinar answer these below.

Q.Do you think getting accreditation such as ISO27001 is an effective way of involving the whole organisation in the importance of cyber security?

A. Cybersecurity assessments and accreditations such as ISO27001 or the NIST framework provide a standards based approach to help organisations implement and maintain their information security management controls as part of their risk management approach across the organisation.

Q. Do you have any recommendations or tips when it comes to which internal stakeholders to pull into the discussion at the start of the risk analysis? How to engage them and motivate them to share technical IT knowledge to non-IT experts?

A. Given Cyber is a business risk, there are several key stakeholder groups that should contribute to a risk analysis approach including Information Security, IT, Finance, Legal Insurance and Risk. Key for any stakeholder engagement is to make it clear what the overall approach and objective is, how it can affect their role and function and the benefits they will gain through the process. Through Aon's Risk Consultant experience in these engagements, we find that having a universal understand of the Total Cost of Risk (TCoR), and an understanding of the Return on Security Investment (ROSI) are key deliverables for this process and provide that linkage between stakeholder groups.

Q.Please can you clarify what the incident response looks like. Do you have technical staff to troubleshoot?

A. Incident Response is a term that describes the process an organisation uses to handle a data breach or cyber incident, typically focusing on the Detect and Respond Functions, however for a mature organisation, this should also consider Identification, Protect and Respond phases.

Contact us

For further information, please contact one of our team:

Alison Goodwin
Public Sector Practice Leader
+44 (0) 7889 653 033
alison.goodwin@aon.co.uk

Mark Brannigan
UK Head of Cyber Solutions
+44 (0) 7786 545 169
mark.brannigan@aon.co.uk

Empower Results®

An Incident Response team will usually consist of;

- Senior Management – primary decision making
- Incident Response Manager – ensuring that all actions are tracked, the incident is properly and appropriately documented and that communications are escalated and passed down appropriately throughout the team/ stakeholders
- Digital Forensics/ Investigators – analysis of what has happened, how it occurred, and which systems or data has been affected
- IT/ Infrastructure – support of containment and remediation actions, including getting systems or data back online
- Legal – potentially both internal and outside counsel
- PR/ Communications – managing internal and external stakeholder communications
- Business Units – as the business owner of potential affected systems, people or processes
- HR – to play a key role in the management of the people risks and impacts.

Expert technical resource can be provided to your response team from specialist providers such as Aon, or via your cyber insurance providers, if your policy includes this section of cover.

Q.Could other organisations sue a University if it inadvertently releases a virus? Could a virus affect the student clearing/ registration system?

A.With any cyber incident or data breach, there is inherent legal or regulatory risk highlighting the importance of robust and tested planning considering key potential impacts.

In respect of the potential that student clearing/ registration systems being affected by malware or some form of data breach, then yes. All systems have an inherent risk that they can be affected. Good risk management practice considering the vulnerabilities, potential impacts and mitigation options – alongside risk appetite – should be seen as vital.

If you have any other questions, we are always happy to answer them.