Higher Education –
Cyber Security Challenges and Threat Landscape

2020 has changed how we all work, including how Universities are engaging with those within their network. Whilst we hope to get back to some level of normality soon, the impact of COVID-19 will have a lasting imprint. The blended learning, remote access, and the need for security to extend beyond the perimeter of the IT estate all mean that cyber resilience is of utmost importance for the sector.

Relevant solutions need not always be strictly technical. Starting with simple actions, such as those listed here, may be of immense benefits:

- recognising how individual/organisational behaviours and dynamics impact the very fabric of the Universities' IT security.
- recognising the importance of collaboration among HEI stakeholders through cyber threat intelligence sharing,
- understanding how such collaborations can be forged to improve threat recognition in the context of a HEI.

First and foremost, if security does not work for people, it does not work.

But the chosen security framework also needs to address the risk, the exposure, and the technical protection. A potential solution must cover every one of these aspects. Our project:

- focuses on the human factors as well as the technical requirements that will allow the HE sector to be proactive in understanding the threats,
- seeks to map collaborative relations among entities in the context of a HEI,
- defines what good security behaviours looks like in the context of a HEI.

To this end, we aim to:

1. Determine how aware senior leadership teams in UK HEIs are of their organisation's cyber risk and resilience and how they respond to their systemic security risks effectively in protecting their staff, students and valuable data from attacks and data breaches.
2. Determine how senior leadership perceive collaboration and how collaboration and competition act to foster or hinder exchange of knowledge concerning threat intelligence in the HEI sector.

We aim to interview members in the senior leadership teams and people responsible for organisational resilience in the sector.

If you would like to talk to us and contribute to this important research, please contact Dr Srinidhi Vasudevan at s.vasudevan@ucl.ac.uk. Alternatively, you can quickly register your interest here, and we will reach out to you very soon.

Additional background information:

In August 2020, UK Universities and Higher Education Institutions (HEIs) were highlighted as a sector at significant risk of a cyber-attack by the UK's National Cyber Security Centre (NCSC). The NCSC warned that due to the nature of data held and managed by this sector, it has become of interest to global threat actors, from lone wolf activists to nation states and organised criminal gangs. A rising number of attacks against each institution's digital estate should be expected. Indeed, since this warning was issued, the sector has seen an increase in attacks. Many universities and further education colleges have already had to deal with the fallout of ransomware, phishing campaigns, and as of yet unknown level of data exfiltration from inside their networks. For example, in September 2020 alone, there were eight attacks reported by universities that disrupted the start-of-term. The financial, IP theft-related, and reputational damage could be significant, not only to institutions individually, but also to important research and development work such as that currently underway at several UK institutions to develop a COVID-19 vaccine. These warnings and growing number of attacks have led to concerns that increasing cyber-attacks are threatening to fundamentally disrupt the UK's reputation for world-leading education and research.

Universities and HEIs face a set of unique challenges to developing a culture that supports people to practice good cyber security. This is not only because of the large turnover of people every year, but also due to their very nature, i.e., that these institutions of education should be open and collaborative. The security restrictions as placed on businesses would typically limit the development of Universities and the students certainly need to share information and co-operate during their education. It is important that governing bodies and boards at Universities and HEIs understand the risks that cyber brings them, know what their exposure is, and appreciate well the impact these attacks can have on their research and educational mission. Taking responsibility to ensure that effective measures are in place to protect the institution, the staff, the students, and their critical data is imperative. Additionally, having the structures to limit the exposure when an attack happens, must be something that each institution has in place.

Funders:

National Cyber Security Centre
a part of GCHQ

Lloyd's Register Foundation