Overcoming Cyber Security Challenges in Higher Education

As more students embrace remote learning, universities must carefully consider their approach to cybersecurity, says Neil Bailey, Head of Education at CDW.

The impact of the COVID-19 pandemic has touched every sector and every economy across the globe. The most agile organisations have been able to adapt quickly to maintain operations as normal (or as close to normal as possible), while others have struggled due to practicality or financial constraints.

The education sector has faced unprecedented disruption, with all key stages, further and higher education institutions forced to adapt the way that education is delivered. Hopes that modifications could be short term have dwindled in recent weeks. Many UK universities are now planning a very different first semester with limited or no face-to-face contact time. Some have gone further, sharing that the entire 2020/21 academic year will be taught virtually. These decisions will reshape student campuses, impact the number of graduates and undergraduates starting or recommencing learning, and present technical and pedagogic challenges. The likely outcome is a need to embrace remote learning technologies rapidly and at scale, adapting underlying infrastructure, systems, storage and connectivity, whilst exploring approaches that support social distancing and build COVID-secure environments.

CDW's Higher Education Institution subject matter experts have spent their careers helping universities define, design, source, configure, deploy and support technologies that underpin academic and research performance. The team support half of the UK's universities, and have spent the last the last couple of months identifying and defining solutions to the most prevalent cyber security challenges that universities will face to successfully operate in the "new normal":

- Remote access to lectures, tutorials and data
- Data security: spanning research data, student content, lecturer IPR
- Data centre scaling: access and sizing
- Hybrid cloud environments
- On-campus social distancing: population flows, resource access and scheduling

Taking a holistic approach

At the centre of the potential solutions lies cyber security. Defining and adopting new technologies that provide equitable freedom of choice and access, data protection spanning student and research datasets and GDPR compliance, all whilst ensuring pace, agility and flexibility.

The need for a rigorous cyber security programme, with resilient systems in place, is required to ensure that IT networks are adequately protected. Recent data shows that two thirds of universities have been subjected to cyber-attacks during the last four years, with losses for H1FY18 estimated at £145m. Attacks focus on four key areas:

- Emails
- Bulk personal information on staff and students
- Technical resources (e.g. documentation and standards)
- Sensitive research and intellectual property

To prevent such incidents, universities must ensure that optimised security, governance and compliance is woven into every element of the IT estate, including appliances accessed remotely. This type of holistic approach provides a solid foundation for increased distance learning.

Then it is about ensuring that adequate security systems are in place to protect the students themselves. Most universities will have experience of implementing security solutions spanning the campus IT estate. Still, as distance learning becomes part of the "new normal", universities need to counter the challenge of students accessing networks through personal devices – potentially from all four corners of the globe.

Partnering with IT specialists

Fortunately, there are tried and trusted ways of assessing and dealing with cyber threats. Many universities have already forged successful relationships with expert providers such as CDW, who offer a vendor-neutral view of the cyber security market, while assessing existing IT setups and spotting existing vulnerabilities. Most software security vendors offer free 90-day trials of software packages, giving universities the confidence to 'try before they buy'.

CDW can help select, source, deploy and support the roll-out of cyber security systems, ensuring that implementation is managed unobtrusively. This seamless process leverages unparalleled, long-standing experience of working in the HEI arena, underpinned by a quarter of CDW's global revenues derived from the education sector.

Now is the time for action

Ultimately, the trend towards remote learning is here to stay – and it is forcing universities to rethink their approach to cyber security. This comes at a time of unprecedented acceleration in connectivity, video conferencing, and file-sharing technologies. Every university will seek to ensure seamless productivity, no matter where users are located,

making the need for a partner who provides whole market access and proven expertise more important than ever. Talk to CDW to help plan and deliver solutions that will protect and support your university, this year, next year and into the future.

CDW is a supplier on LUPC's software licence resellers agreement (SLRA) and the Desktops and Notebooks (NDNA) agreement.