Cardiff Metropolitan University has a long history dating back to 1865, when it began as Cardiff School of Art. It has five schools specialising in art and design, management, technologies, sport and health sciences, and education and social policy operating across two teaching campuses. Cardiff Met has an extensive network of education partnerships including many transnational ones, offering its degree programmes collaboratively with higher education institutions in 15 countries in Africa, Asia, Europe and the Middle East, and aiming to give overseas learners a seamless experience that's comparable to studying on campus in Cardiff.

Belt and braces approach to cyber threats

As a user of the Janet Network (jisc.ac.uk/janet) Cardiff Metropolitan University uses the Jisc CSIRT (jisc.ac.uk/csirt) team to support active monitoring across its systems and help in resolving cyber security incidents.

"Like all UK universities we are under constant threat from cyber attack," says Sean. "Our firewalls deal with most of these and we have active training programmes for staff and students to try to make sure they are knowledgeable and vigilant."

"But sometimes there are unfamiliar kinds of attack and these are the ones that the CSIRT helps us deal with."

In mid-2020 Cardiff Met detected an unusual type of security breach. This wasn't an attempt to steal or ransom sensitive information and none of the data held by the university was ever compromised; instead, the attackers recognised an opportunity in the university's large, secure data storage systems and devised a way to use these to create a digital safe deposit box for their own data within the university's systems.

As soon as the security breach was detected Jisc's cyber security specialists set to work with Sean's team to evict the illegal tenants. In the first few days the Jisc team was in touch numerous times a day, tailoring the best response and working to close the breach.

The emergency response took several weeks; it often takes weeks or even months to get everything locked back down after a security breach and the fallout can sometimes be felt for even longer.

"The CSIRT response was excellent," says Sean. "I sometimes wonder if David Batho, the security specialist who led Jisc's response for us, can be human. He never stops."
Proactive approach to heading off future attacks
Throughout the 2020 lockdowns cyber attacks on UK universities and colleges increased dramatically in both number and severity – and there’s nothing to indicate that this trend will stop any time soon.

For this reason, the university’s information services team decided they should take additional steps to mitigate future risk.

“Jisc worked with us to produce a report to senior management, documenting what went wrong and how we had resolved it,” says Sean. “The report also made the business case for developing our cyber security plan for the future, what it would cost and what the consequences of inaction might be.”

The plan was in two parts and, with the security breach under control, Jisc’s professional services team helped the university address the most pressing – an exploration of its current security position. Jisc specialists carried out a cyber security assessment, (jisc.ac.uk/cyber-security-assessment) which is an optional extra available for all our members. It offers the opportunity to develop a thorough understanding of your institution’s strengths and vulnerabilities so you can plug security gaps. Implementing the recommendations will protect your ability to deliver services to students and staff, ensure you can comply with funder and regulatory requirements and safeguard your institutional reputation.

“Jisc did a deep dive into all our systems and gave us an amazing level of support and specialist expertise to help us deal with issues that emerged,” says Sean.

The security assessment included penetration testing (jisc.ac.uk/penetration-testing) to identify any weak spots. At Jisc, we always use our own trained and certified specialists for this. With our knowledge of the applications and systems commonly used in education and of the kinds of security threats universities and colleges face we can uncover vulnerabilities and evaluate their potential impact. In every investigation we apply the insights we’ve gained from testing other members’ organisations and this knowledge builds with each subsequent investigation to the benefit of all our members.

Carefully considered investment
The second phase of Cardiff Metropolitan University’s plan is ongoing. It involves the gradual recruitment of additional members to the information services team and regular, quality training to keep staff skills topped up as threats evolve.

“Very deliberately, we will staff up gradually to give ourselves the space to develop the team in an appropriate and timely way,” explains Sean.

“The plan we developed after our cyber security assessment helped us make very fast progress with boosting our security and, longer term, it will make sure we can keep our security levels high.”

To find out how Jisc can support your organisation, please:

Contact: securityservices@jisc.ac.uk
or visit jisc.ac.uk/cyber-security-assessment