A FOUNDATION FOR DIGITAL SUCCESS

Secure-by-design networks

Embedding cyber security into the foundations of your network can increase resilience and minimise long term expenditure for your university

Why universities must act

Cyber security is a huge threat to higher education – and it's not one that's going away. Cyber criminals and state-sponsored actors are swarming around institutions. In fact, MI5 has warned universities of the increasingly complex threats they face, which not only look to infiltrate higher education for financial gain but also undermine national security.

While a network security transformation may feel like a big move, it can be a better, cost-effective solution to achieving long-term security, as opposed to patching up problems and bolting-on security as you go. This is especially true when the cost of a data breach now averages £3.4 million, according to IBM Security.

The cost of an attack

Cyber attacks on universities are often at scale, with even bigger consequences. For example, it took The University of Manchester three months of intensive work (and staff holidays cancelled) to contain and eradicate a threat encountered by a complex phishing scam, according to Jisc. Meanwhile, the University of West Scotland reported its financial deficit of £14.4 million had been 'exacerbated' by a similar attack in 2023.

BLOCK

The challenge for CIOs

Ransomware:

Vulnerabilities in remote learning platforms and VPN invite cyber criminals to encrypt your university's data and demand a ransom for its release.

Phishing scams:

Financial aid offices are being impersonated to collect sensitive data from students and staff – sometimes attempting to steal student loans.

DDoS attacks:

Learning management systems and online services are being purposely overwhelmed with traffic to distract IT teams while infecting your university with malware.

Intellectual property theft:

State-sponsored actors are targeting academic research for espionage and financial gain – as MI5 has warned.

BYOD environments:

Network entry points for cyber criminals are numerous and often unmanageable due to so many personal devices on campus.

Problem solved

Block is partnering with universities to implement secure-by-design networks. This architecture limits the impact of inevitable cyber attacks by moving your university towards a zero-trust model.

As a result, IT teams can roll out new services, users, and processes without complex change management, compromises to security, or time-consuming tasks.

We'll survey your existing network, design roadmaps and architectures, and work with your team end-to-end to responsibly implement your new architecture.

"Cyber security is arguably the fastest growing sector in the world right now. However, it is relatively immature in relation to the explosive and unpredictable threat landscape. Addressing this disparity between digital maturity and cyber maturity remains a focus for Block.

"We are passionate about cyber and we relish the opportunity to understand our clients' challenges, working to mitigate inherent and systemic risk. Cyber is a team sport and we're ready to play."

Mark Walton, Chief Technology Officer at Block

Benefits

- Respond faster to threats and reduce attacker dwell time.
- Decrease long term risk and provide cost effective mitigation controls.
- Reduce the blast radius of a breach by segmenting and isolating the network to limit lateral movement.
- Ensure users can connect across campus, and remotely, by extending perimeter defence.
- Expose hidden risks and shadow IT by identifying unknown devices in the estate.