

Whitepaper

SECURITY IN THE CLOUD

How further education institutions
can defend their data

YOUR DIGITAL TRANSFORMATION PARTNER FOR GROWTH



The challenge with data

Data is what makes the modern world go round. Businesses, governments and organisations of all shapes and sizes rely on data to ensure the smooth running of their day-to-day operations. But universities are perhaps in a unique situation. Not just because of the information and data sources they hold, but in the way they are expected to operate.

Universities and further education institutions accrue huge amounts of data. As a matter of course, they will gather personal and financial information about students, staff, and faculty members, but they will also gather and hold sensitive data about grant-related research that is not only often politically delicate, but critical to the commercial interests of the institution.

Protecting the intellectual property

The sheer scope and potential value of data held by universities, whether it's academic, operational, financial or personal data about students, makes them an attractive target for cyber criminals. Those looking to make a quick and easy buck often see universities with their treasure troves of student and staff personal information, medical records, and financial data as the perfect target for a simple phishing or malware attack. These attacks can, of course, have a devastating impact on individuals, as well as causing reputational damage to the institutions themselves. But universities also possess uniquely attractive data and infrastructure that makes them vulnerable to more sophisticated attacks: by corporate spies and nation-state-backed hackers looking to steal valuable scientific research, and others who want to hijack the massive bandwidth and power of an institution's servers so that they can redirect attacks and cause mayhem for other, external systems.

The implications for universities of a data breach, loss or theft are enormous and wide-ranging. Reputational damage among faculty and prospective students. Legal and regulatory ramifications. Economic and financial harm. And damage to infrastructure that can cripple the ability of the institution to carry out even its most basic of functions. Just one, catastrophic malware attack could bring a university to its knees for weeks, in just a matter of minutes.

The biggest threats to university data



Spear phishing



User error and social engineering



Macros and ransomware



Old and/or weak security protocols



Browser vulnerabilities



Software vulnerabilities



Poor firewall and/or network configuration



Unsecured USB access



Lack of control over mobile device access



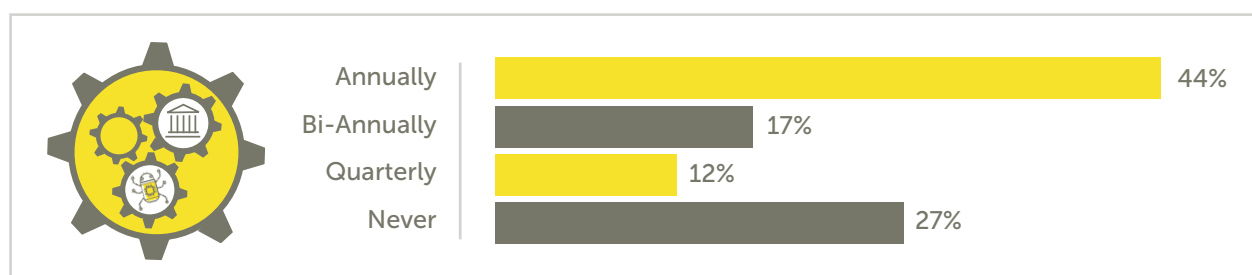
Botnets and DDoS attacks

A rising problem

The statistics on data breaches across the board at UK universities are alarming. In April 2019, security testing firm Jisc deliberately targeted UK universities in a bid to expose the vulnerabilities that seem commonplace across the sector.

In less than two hours, testers were able to penetrate the cyber defences of more than 50 further education providers and gain access to the personal data of students and staff, the institutions' finance systems, and networks that held highly sensitive information concerning research projects. Few of the universities, it seemed, were aware of the vulnerabilities within their own systems, and perhaps even fewer considered protecting data a priority.

How often third-party penetration tests are undertaken by UK universities:*



Jisc's Head of Security Operations Centre, John Chapman, warned that these vulnerabilities in university data defences pose a serious risk of a "disastrous data breach or network outage" and said the test should be a wake-up call for all UK higher education institutions.

While ethical hacking and penetration testing are useful tools for highlighting system vulnerabilities, unfortunately the risks of data being exposed are not just hypothetical: university data is being targeted by genuine cyber criminals at an alarming rate.

According to The Times, cyberattacks on UK universities doubled in the two years to 2017, with many of the 1,152 reported data breaches geared towards stealing financial information and intellectual property.

A report by cyber security firm Redscan found that, in the 12 months to July 2020, 54% of UK universities had suffered at least one data breach of sufficient concern that they reported it to the Information Commissioner's Office (ICO). Redscan further found that universities were particularly vulnerable to phishing attacks, with one institution claiming it had detected as many as 130 million phishing emails across its network in just one 12-month period.

And at the end of 2020, amid the COVID-19 pandemic, one UK university suffered a 'password spraying' attack that resulted in 1,000 student accounts being compromised. This attack took university personnel 80 working days to rectify.

Jisc's Head of Security Operations Centre, John Chapman, warned that these vulnerabilities in university data defences pose a serious risk of a "disastrous data breach or network outage" and said the test should be a wake-up call for all UK higher education institutions.

*Study by Redscan on behaviour in the 12 months to August 2020

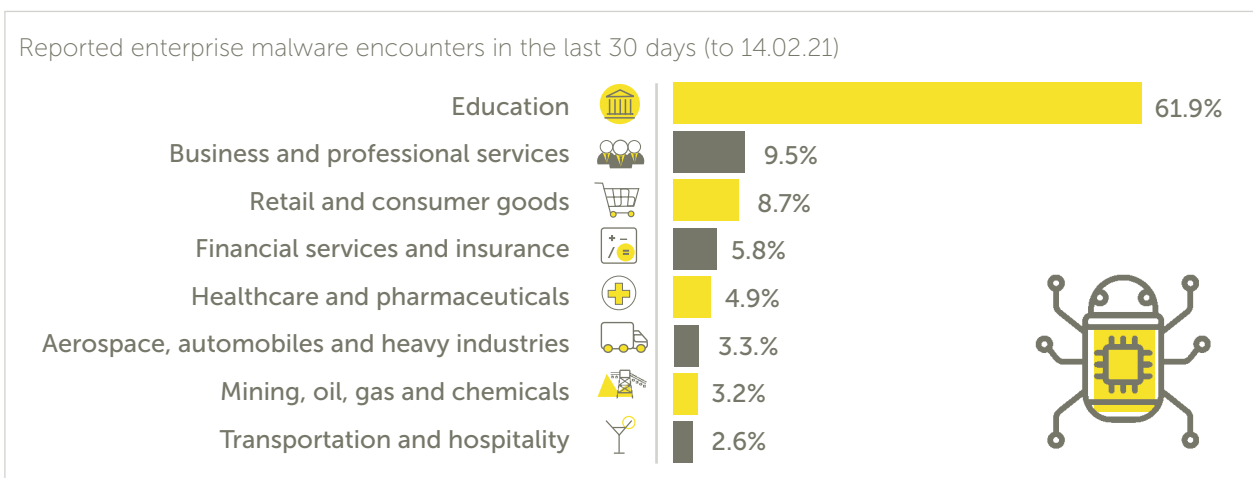
Increased data exposure

The hasty shift to digital and remote learning in the wake of coronavirus has undoubtedly done more to expose valuable data than any other event in history, and cyber criminals have come out in force to exploit the situation.

Between February and June 2020 alone, DDoS attacks on the education sector rose by a staggering 350-500%.

A Microsoft Security Intelligence report in February 2021 highlighted how uniquely exposed educational institutions had become amid the scramble to instate virtual provision, reporting that of the 10.6 million malware encounters experienced in the previous 30 days, 62% had been targeted at the education sector.

Most affected industries



The tools of the virtual lecture hall have become a gateway for hackers, and Google Meet, Microsoft Teams and Zoom have all been targeted with increasing frequency. A report by security software firm Kaspersky said that, of the 168,550 instances of bogus application installations it detected between January and June 2020, 99.5% were associated with fake Zoom apps.

Cybercrime is undoubtedly increasing in frequency and scope across the board, and with the value and vulnerability of the data they hold, universities are among the easiest and most attractive targets.

A unique data landscape for further education establishments

Of course, not all data losses are malicious, and universities are as vulnerable to 'act of God' accidents and human error as any other business. The issue for many further education institutions when it comes to keeping data safe is the unique organisational structure of the education environment.

There is a very real and tangible difference here between universities and the standard corporate network. The historically wide-open campus, and the sprawl of networks, has traditionally made it difficult to implement the sort of tight, security-focussed infrastructure that corporate networks are able to harness without much thought.

Most university networks are made up of many, often geographically dispersed smaller networks. There is a regularly rotating body of users to consider, with students and staff coming and going frequently, as well as an ever-changing roster of visiting academics and the annual influx of students to various halls of residence. There are teams of researchers and graduates collaborating globally and sharing data with individuals and institutions in all corners of the world on a daily basis. And on top of all that, there is the Internet of Things and a necessary bring-your-own-device mentality that leaves networks exposed from all sides.

References

1.The Times: University secrets are stolen by cybergangs 2.Securelist.com: Digital education the cyberrisks of the online classroom 3. microsoft.com

Barriers to backing up

While many further education institutions are already operating an increasingly remote and hybrid educational set-up, far too few are taking the necessary parallel steps to enhance security measures, including data backup. Because, as unique as the data landscape is for universities, there is often a similarly unique set of risks guiding reluctance to adopt adequate security measures and data backup.

Technology and transformation costs

Over recent years, further education institutions have seen their budgets decimated following a drop-off in student numbers. Couple this with mothballed student accommodation and conference centres, spiralling pension deficits, and the devastating impact of a global pandemic, and universities are in a precarious financial position. COVID-19 is estimated to have impacted the University of Edinburgh alone to the tune of £150 million.

The UK university sector as a whole is expected to have suffered losses in 2020 of between £3 billion and £19 billion.

It is amid this bleak financial picture that every penny must be accounted for, and every purchase backed up with a strong business case. Protecting data just isn't making the cut while there are dwindling resources and no way of increasing income.

Legacy infrastructure and maintenance costs

Most universities have large, costly bricks-and-mortar estates. There are high, fixed costs associated with housing students, funding research, employing the best professionals, running specialist labs and maintaining myriad other specialist facilities. In 2015-16, UK universities spent approximately 13% of all academic income on maintenance and CapEx projects.

To offset expenditure, institutions are in a race to attract the best candidates and provide the best value-added courses for graduates. Initiatives like the UK Government's Longitudinal Educational Outcomes (LEO) data, which directly links employment and earnings outcomes of graduates with their undergraduate degree and institution, is feeding a growing sense of student entitlement, with prospective students able to filter their choices based on the benefits derived or lost. Amid these increased expectations and massive ongoing costs, it's perhaps no wonder so many universities are choosing to invest in their physical estates rather than prioritise data protection and backup.

But is this sensible? With ongoing, and even increased, threats of ransomware and other cyberattacks, arguably the business case against data protection can no longer be allowed to hold sway. After all, when IT fails, word gets around. Even 99% efficacy will mean one in every 100 students experiencing issues with data, and these days even the smallest breach on a university campus will be all over social media in a matter of seconds. In an increasingly competitive marketplace, with clued-up, tech-savvy 'customers', data breaches can make a huge difference not only in all-important league tables, but for an institution's reputation. When institutions are already struggling to get students through the door, this could sound the death knell for even established 'brand-name' institutions.

Failing IT is demoralising for faculty and worrying for students. So protecting networks and backing up data could be the best business decision any university could make.

The future of estates is digital

There is an argument to be made that universities should be looking to downsize their physical estates and transform their digital estates as quickly as possible. COVID-19 has forced the hand of many further education institutions, and we have seen a tentative move towards virtual lecture halls and online modules. But this could be a transformative opportunity for the future viability of institutions, and university leaders should be looking to go further by considering the benefits of digitalisation in every department. This means leveraging new applications in mobile, AI, cloud computing, blockchain and IOT technologies, all underpinned by affordable, OpEx data security, backup and recovery.

Why data backups are essential

The simple truth is that university IT systems are vulnerable in a number of ways. Wherever data is saved – whether individual laptops, PCs, smartphones or tablets, flash drives, SD cards, external hard drives or mainframe servers – it is vulnerable to physical damage and theft. In the shared space of a university campus, where many of the boundaries of opportunity and proximity are removed, these risks are increased massively.

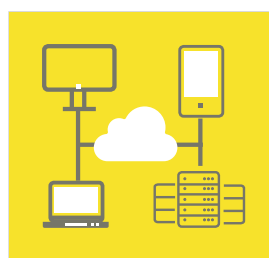
On top of these risks, networked databases can be hacked and infected with Trojans that steal data and cause ransomware attacks, which are particularly prevalent across campuses these days. And, of course, there is always the risk of somebody making a mistake when saving a file, and deleting or overwriting vital data.

Protecting staff, students and intellectual property

Backing up systems and data is insurance for universities against any kind of data loss. The ability to run a rapid recovery from a backup source will save an institution potentially months of damaging downtime, loss of revenue and reputation, and the expense of trying to salvage data from corrupt or compromised systems, as well as dealing with any legal and regulatory implications of data loss.

In more general terms, data backup is a valuable tool in a sound data governance strategy, which strives to enact practices that keeps records and archives in good order. Organised and efficient data management can have all sorts of positive knock-on effects for universities, from reducing the time it takes to compile reports to minimising the risk of duplication when it comes to dealing with student results and other data. Productive and effective data management can, in turn, lead to a variety of positive outcomes, from increased stakeholder relations to gaining a competitive edge over other institutions for student attraction and staff retention.

How to backup data



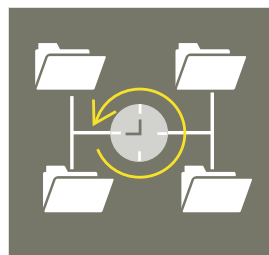
1. Decide what needs to be backed up

The sprawling nature of university networks and infrastructure makes data audit a challenging undertaking, but deciding what data to back up is nevertheless the best place to start. The audit should include an analysis of how data is used, who uses it, and what is and is not essential for the running of the institution. Storing and archiving data that isn't really needed will only add unnecessary cost and complexity.



2. Plan where to store backed up data

This is a crucial consideration, because so-called geographic redundancy (that is storing data in different places to compensate for risks to physical hardware) is a key protection against catastrophic data loss.



3. Determine how often to back up data

If data is lost or there is an outage across the network, any recovery will only roll back to the last time a backup was carried out. Given that universities are gathering, handling and applying data constantly, a weekly backup is unlikely to be good enough. A week of data would be a huge and damaging loss to any institution, so backing up at least once a day is generally recommended.

Data backup options

There are plenty of options for where and how universities can store data, as well as the equipment that can be used. These include on-premise solutions, off-premise solutions for geographical diversity, and cloud-based solutions.



Cloud backups

These days, the most flexible, cost-effective and reliable backup services are those that offer storage in the Cloud. Like bare metal data centre storage, cloud services provide a remote backup option that ensures geographic redundancy. In addition, cloud backup can take advantage of storage efficiencies which come from virtualized pools of resource, to ensure geographic redundancy in the storing of critical and archival data.

Crucially, when dealing with the sort of sensitive data being created and gathered by universities, cloud backup services. This adds a further layer of security for critical data.

Some institutions may opt for a hybrid cloud backup solution, which uses a combination of public and private cloud solutions depending on the sensitivity and use of the data being backed up, and private cloud for the more sensitive data, such as commercially sensitive research and student and faculty personal information.



Disaster Recovery as a Service (DRaaS)

Another sensible option for universities to consider is DRaaS. Disaster recovery should be considered as a part of any business continuity plan, and incorporates system level replication and failover to a secondary location in the event of a catastrophic incident. DRaaS delivers one of the most robust IT failover services available and should be weighed up as part of any business case defining what services a university cannot afford to lose in the event of a disaster.



On-premise and local hardware

This is the default option used whenever anything is saved to a local drive on a particular machine, or on-premise servers. Introducing protocols whereby everything is duplicated to individual machines and servers, or to other media like external hard drives, flash drives or high-capacity digital tapes, provides some protection against small-scale faults or errors on individual machines. However, the protection afforded by local and on-premise backups is limited. In the event of a fire, a major incident of theft, or a large-scale malware violation, backed up data can still be compromised or lost. So while it's a quick and easy bit of reassurance to save copies of files to local hardware as and when they are created, other system level backup procedures should run parallel to ensure more robust protection.



Off-premise and remote hardware

This could be as simple as backing up the on-premise system to a digital tape and taking that tape off the premises every evening, ensuring that if disaster strikes on campus, there is still a safe copy of the university's vital data. This can be a time-consuming and cumbersome task, however, and tapes can often fail. As network technology has increased in speed and reliability, more and more organisations are backing up their systems on remote servers. This might include using a Wide Area Network (WAN) to distribute duplicates of vital data that are then saved on servers dotted around different premises, such as another campus. Alternatively, universities can opt to use a third-party backup service, which saves important data on servers hosted in a secure data centre.


Online backup for the education sector

As research shows, the education sector is exposed to cybersecurity risks on a regular basis and under serious threat of financial loss, with impact on reputation, staff and students alike.


Addressing all the data security challenges can be a cumbersome exercise, from understanding what data is vulnerable to attacks and likely to cause disruption to choosing the right systems and technology that helps overcoming those risks.

To see how you can mitigate cloud security risks, transform your data management approach, and unify data assets across the campus, speak to a member of our specialist team today.

For more information about how M247
can help your institution protect its data,
contact our team today

 0808 301 9688

 info@m247.com

 m247.com

 M247

 M247⁷