VEEAM

Freedom of Information Report:

A Lesson in Backup and Disaster Recovery for Universities

01

Introduction

Introduction

Data availability is vital for today's universities. More than ever, they must provide compelling educational experiences that are in-keeping with modern user experiences. Students and teachers expect to access tools, resources and support digitally — anytime, anyplace.

While universities have all the data they need, without the ability to manage and access it, they can't deliver on these expectations. Furthermore, without robust cybersecurity and backup protocols in place, student and teacher data is at risk of being lost or stolen.

Data availability is critical. It ensures data is accessible to all parties, so that they can learn and teach no matter where they are. Furthermore, in the event of an outage, it allows data to be quickly and reliably be recovered.

Ensuring data availability is no mean feat and it's especially important considering the escalating risks of cybercrime. Universities hold more data than ever before. As they break down the walls of silos, they must also ensure they have robust defences. This includes putting rigorous testing processes in place to ensure vulnerabilities are eliminated and systems continue to stay secure.

This report, commissioned by Veeam, assesses the confidence levels of universities in their ability to ensure data remains available, protected and recoverable at all times. By gauging the current state of digital infrastructure, the report outlines key learnings and recommendations for education in the public sector.

02

Methodology

Methodology

To find out, Veeam invited the Times Top 100 UK Universities to take part in a survey. Of this list, 91 institutions provided a response. Veeam asked universities questions about:

- The data they were responsible for handling, use of relevant third parties and suppliers
- Process of backing up data, disaster recovery planning and testing data systems
- The impact and frequency of outages and cyber-attacks, measures in place to mitigate against data loss

This important piece of research shines a light on the data management practices currently employed by the UK's leading universities.

Summary of findings

To fully protect systems and ensure data remains available across universities' digital infrastructure, more work is needed to establish formalized procedures for backing up and testing data systems, as well as producing and updating disaster recovery plans.

Universities almost universally acknowledge their responsibility for storing and processing data, with the vast majority already investing in cloud computing and the ability to backup data to on-premise and cloud-based storage.

The threat of IT outages and cyber-attacks is constant. While universities have not necessarily succumbed to major cyber-breaches, without formalized testing processes the ever-evolving threat landscape will leave them vulnerable in the long term.

03

A degree of confidence

A degree of confidence

The survey responses indicate that universities are fairly confident in their data security measures and are taking ownership of the data they store and process.

Almost all universities (97%) reported responsibility for storing sensitive data — including information on students, research, and IP data. The vast majority also recognise the benefits of cloud technology, with 92% using Office 365, and 96% using some form of cloud computing.

Even more encouraging is that 88% have a digital backup of their data, which suggests universities are aware of the risks of data loss.

Breaking this down further, only 15% manually manage data backups inhouse. The majority (68%) choose to use a specific backup supplier — demonstrating that, in terms of disaster recovery at least, universities are following the recommended industry best practice.

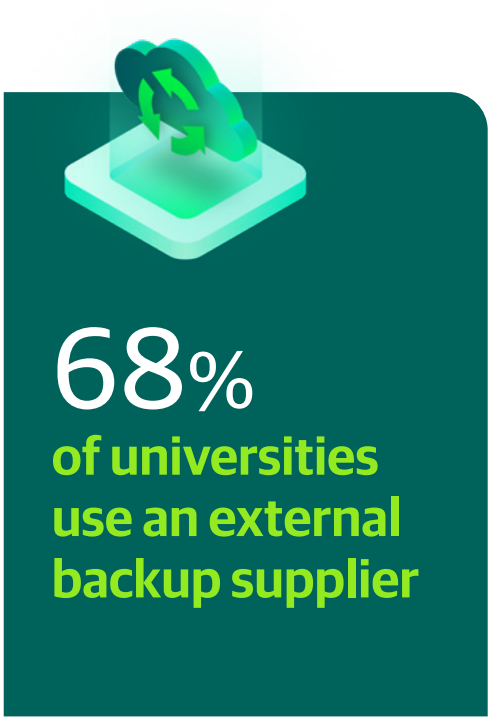
Perhaps the most encouraging outcome was that the vast majority of universities (89%) have a disaster recovery plan in place in case of outage.

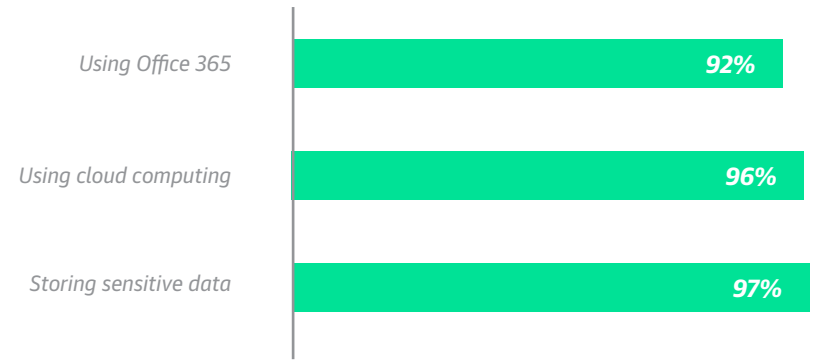
Again, digging deeper into this, four-out-of-five universities (80%) conduct tests on their data backup systems. This falls to three-out-of-four (74%) for those who test their recovery systems.

These results appear to show that universities understand the importance of data and recognise their responsibilities in protecting it.

However, this is a surface-level assessment. While those top-level findings point to a positive state of affairs, scratching beneath the surface raises more pertinent issues and questions. How robust are universities' data backup systems in real terms? How often, but also how rigorously, do they update them? Could there be weaknesses in their systems or processes that aren't being picked up by tests?

More insights are needed to gauge if hidden vulnerabilities could be outages or cybersecurity breaches waiting to happen.





04

Process, process, process

Process, process, process

While universities do have data backup and protection technologies in place, many fail to formalise their processes or conduct testing on a regular basis.

While 89% have a disaster recovery plan in case of an IT failure, only 67% have a formal process detailing their course of action in the event of an outage. When it comes to updating their disaster recovery policy, less than half (41%) do it annually or more frequently.

As you can see, universities don't just struggle with formalising their processes, but also regularly testing and updating the processes they do have. This suggests testing is generally not done often enough, meaning potentially serious weaknesses are being overlooked.

The theme follows through to data backup tests. Only 36% do so once or more a year, and 24% do so on an ad hoc basis. The latter is of particular concern, as all too often 'ad hoc' can mean 'after a problem has been identified'.

When it comes to testing disaster recovery systems, less than half do so once a year or more (41%), and 20% do so on an ad hoc basis. Again, this is concerning. The importance of disaster recovery system cannot be underestimated — yet without regular testing, it is impossible to be certain they are fully secure.

While universities recognise the importance of data security, this apparently is not always translating into robust processes. Invariably, when it comes to backup and data protection, the devil is in the detail.

In an era where technology, regulations, and cyberthreats are constantly shifting, protecting data isn't easy. But the consequences of data loss can be disastrous — so universities need to be fully confident their systems are robust.

Serious outages can come from anywhere — and in fact Uptime Institute estimates that 70% happen because of preventable human error. Something as simple as a typo can knock a data centre out for a significant amount of time. Legacy hardware and software which is no longer fully supported or fit-for-purpose also pose significant continuity risks.

There are forces outside universities' control too such as natural disasters or unplanned power cuts. These outages are mostly unpredictable, and could be potentially crippling if institutions aren't prepared.

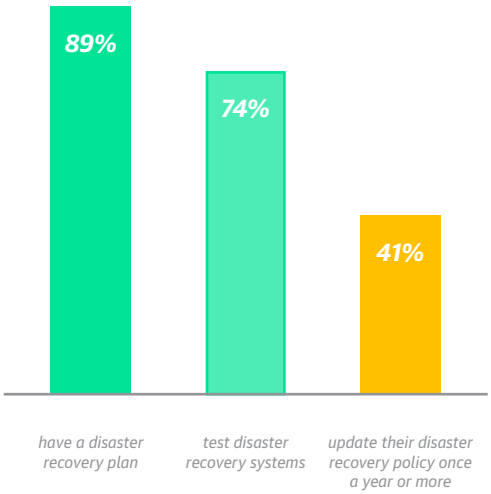
While systems may appear to work well from a cursory glance, often, a more thorough examination can reveal weaknesses that could put data at risk.

That's why it's essential universities backup, test, and update on a continuous basis. Vulnerabilities aren't always easy to detect, and outages can happen anytime. Institutions need to be fully confident their backup systems are working — come what may. That means laying more formalized planning and testing procedures to maximise the chance of issues being detected and solved before they affect business continuity.

88%
producing data backups

80%
test data backup systems

36%
test backups once or more a year



05

Tough examinations

Tough examinations

Ensuring data remains available at all times is a constant challenge for organizations in every sector. According to our survey responses, the volume of IT outages experienced by universities is a potential threat to business continuity.

Out of the 91 universities, 65 provided information on the total number of unplanned outages they had experienced over the past 12 months. On average, there were 1099 unplanned outages across 65 universities — 17.5 per organization each year — or 1.5 per month.

The average length of time for these outages was nine hours and 27 minutes, with the longest period a staggering three days. This means on average universities are experiencing 6 days and 21 hours of unplanned downtime a year.

These figures are concerning. Downtime is when a system is at its most vulnerable. If universities' don't have testing processes or their systems are not up to date, each of these outages could be disastrous and result in data loss.

This question also revealed some visibility challenges when it comes to recording downtime.

Some 8% of these 65 universities had no record of their IT outages - meaning that, if an IT failure was to occur, they simply wouldn't know. Equally concerning is that 15% had no record of how long their outages lasted over the previous 12 months.

8% of universities have no record of IT outages and 15% have no record of how long outages last

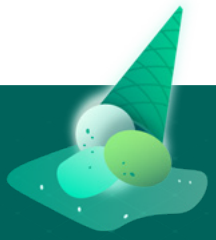
While our survey did not identify any cases of universities experiencing cyber-attacks leading to data loss that was subsequently reported to the ICO, without formalized business continuity processes to reduce downtime and provide better visibility over the effects of outages, the risk of this happening is high.

Malicious agents prey on vulnerabilities within data systems and digital infrastructure, so every precaution must be taken to thwart attacks even from institutions with a clean track record.

While universities are certainly aware of the potentially debilitating effects of cyber-attacks, they're failing to establish formal policies and procedures to protect against them.

Moreover, while most participants have backup and recovery systems in place, they're failing to test these on a regular basis. As cyberthreats evolve, it's only those that have rigorous testing processes that can be fully confident in their cybersecurity and business continuity protocols.

The potential cost of inaction is too great to ignore. Educational institutions need to de-risk, test, and tap into the hidden opportunities their data holds — and for that, they must invest in their Cloud Data Management strategies.



17.5
outages per year

1.5
outages per month

9.5h
average length of downtime

6d 21h
of unplanned downtime a year

06

Next steps

Next steps

Universities need to ensure that data is fully available, protected and secured. A solid digital foundation is needed — with the right backup, disaster recovery and testing processes in place. Here are the steps IT teams need to take.

1. Formalise data-related process and policies

While universities may be confident in their data system testing policies, this confidence is generally misplaced. Current testing is limited, meaning institutions aren't aware of the weakness in their systems — weaknesses that could reduce availability, and have a serve impact on their ability restore data.

Establishing more formalized procedures towards testing data backup and disaster recovery systems will help higher education institutions ensure that data remains available at all times and prepare IT teams for outages and cyber-attacks. Furthermore, disaster recovery planning must be carried out on a regular basis given the vast amounts of data universities process.

Ensuring that these processes are fit-for-purpose includes outlining and enforcing a regular cadence of robust testing.

2. Build a vision for digital transformation

Universities must continue to embrace technologies such as the public cloud, Office365, backup and disaster recovery. While driving cost efficiencies remains a priority, institutions must continually improve the digital user experience they provide students and faculty members.

The first step towards digital transformation is to identify how IT can better support the organization in achieving its strategic business objectives. Whether it's increasing e-learning opportunities, better managing student finance, or ensuring student-faculty member confidentiality, the IT strategy must be rooted in fulfilling tangible business objectives within a suitable timeframe and budget.

3. Prepare for threats to data protection and availability

Minimizing downtime is a key priority for higher education institutions. As well as preventing unplanned downtime, institutions need full digital backups of their data — allowing them to recover systems in minutes.

Any threat to data availability, integrity or security is a threat to digital transformation. Cloud Data Management is of vital strategic importance to any higher education in public sector institution. IT teams must create a strategy that will help deliver against the organization's future objectives.

- Backup and recovery: Invest in a Backup for Cloud Data Management approach.
- Governance and compliance: Develop an approach to maintain visibility of data across multiple platforms — from public cloud to on-premise storage.
- Orchestration and automation: Optimise how data is managed across multi-cloud and on-premise environments.
- Monitoring and analytics: Invest in the necessary IT skills and software to continuously monitor the threat landscape — proactively testing and updating.
- Cloud mobility: Simplify the portability of data across digital infrastructure as the data needs of the institution become more complex.

07

Data availability — anytime, anywhere

Data availability – anytime, anywhere

Veeam is the leader in Backup for Cloud Data Management, helping organizations make their data available and secure across a multitude of industries — including higher education and public sector.

Veeam's industry-leading platform offers complete availability for any app and all data across any cloud. Developed by a team of world-class technical experts, it enables students, teachers, and university staff to interact seamlessly - both on campus and remotely — so they can share resources, research papers and sensitive information in real time.

While universities may believe their data is safe, in reality this may not be the case. An outage could occur at any moment, and as cyberthreats evolve they will pose a bigger and bigger threat. Without formalized testing, institutions cannot be confident their data is fully protected or backed up.

Veeam can give universities that confidence. With Veeam, disaster recovery takes minutes — not weeks. And most importantly, data is protected 24/7. Universities can be confident their data is fully backed up, freeing their resources to do what's really important — educate the professionals of tomorrow.

For more information contact us at:
Veeam.com/sales

VEEAM