

DATA PROTECTION FOR HIGHER EDUCATION

Acronis

Solution Brief

INTRODUCTION

Universities and colleges have a high degree of data to safeguard. First, there is the basic data that contains personal information for students, faculty, the workforce, research human subjects, patients, and so on – with the types of data dependent upon the academic programs an institution offers. For research institutions, faculty members and researchers collect a plethora of data that supports and produces inventions and other scholarly works that benefit the public, the institution, and the scholar. Then there is the data that supports coursework, of which both faculty and students contribute. Last, there is the data that supports the financial, legal, and marketing operations of the institution.

This white paper describes why it is important to protect institution data, the challenges that higher education institutions face with data protection, and why almost 2,000 colleges and universities around the globe use Acronis products to protect their data.

WHY PROTECT INSTITUTION DATA

The following incidents provide different examples as to how institutions can lose data.

Incident #1

The University of X is located near the coast and the data center is destroyed from a Category 4 typhoon. The university's business continuity and disaster recovery plan were still in early stages – not universally implemented, tested, or exercised. While IT backed up the institution's servers, IT did not require training for all data stewards and users. For research data, many of the data stewards were the principal investigators (PIs) and while the senior principal investigators followed policy, other PIs and researchers did not. Regardless, data stewards, PIs, and users backed up their department / personal desktops and laptops unsystematically, almost chaotically. Most backup copies were also stored on campus and were destroyed. The university stored server backups in a remote location 20 miles from campus but unfortunately, that site is destroyed as well.

Figure 1 : The Consequences of Lost Data

- Interruption of university business and on-line classes
- Damage to the university's brand and loss of student and faculty confidence in the institution
- Out of compliance with a variety of regulations such as HIPAA, GLBA, DPA 1998
- Out of compliance with research funding mandates
- Financial losses including potential loss of revenue sources

Figure 1 calls out examples of the possible consequences an institution can suffer when some or all of their critical data is lost. While a natural disaster can result in extreme consequences, a disaster does not happen frequently. However, an institution can lose data in other ways including user errors, viruses and cyber-attacks, hardware failures, software updates/upgrades, and theft / loss of a computer.

DATA PROTECTION FOR HIGHER EDUCATION

Solution Brief

Here are some examples:

Incident #2

A University of British Columbia researcher was studying the effects of global warming on plants when she needed data that was about five decades old to compare with recently gathered information. The data was lost because faculty members were the data stewards and many professors were not reachable or they kept their data on storage devices such as floppy disks. To understand the extent of the problem, the UBC's zoology department examined 516 international zoological studies archived in the school's biodiversity center and found that the data was inaccessible because of faulty contact information and / or obsolete storage devices.

The [study](#) went on to state, "While all data sets were available two years after publication, the odds of obtaining the underlying data dropped by 17 percent per year after that." The bottom line of the study: 80 percent of research data is lost within 2 decades.

Incident #3

In February 2014, an audit revealed that Chicago State University lost equipment holding sensitive data. The audit revealed that 132 computers, servers, CPU's, or other electronic storage devices were lost and that "the [University](#) did not perform a detailed assessment, and therefore was unable to determine whether the missing computers contained confidential information." The audit also noted that "six additional computers... and three others were reported lost." As with the other devices, the audit says the university was unable to determine if those computers contained sensitive information.

“ *When you look at the number of events that can cause data loss, you realize it is not a question of **IF** you will lose data, but **WHEN** you will lose it.* ”

Later in this brief, we will talk to each of these incidents and discuss what these institutions could have done differently to protect their data.

THE CHALLENGES WITH PROTECTING DATA IN A UNIVERSITY SETTING

In many colleges and universities today, the institution's Information technology group defines the data protection policies for the institution and may delegate backup execution to the business, academic unit, or user depending on the type of data.



Because many universities are centralized in their governance of data protection, and decentralized in their processes, there can be gaps that can result in data loss.



Data stewards' responsibility for data backup

Many institutions name a data steward in a specific business or academic unit, or a principal investigator in the case of research data, as the individual responsible for data management, including data backup. While there are no recent studies published on the role of data stewardship in higher education, a 2009 EDUCAUSE Center for Higher Research (ECAR) study, "Institutional Data Management in Higher Education", cites that only one-third of institutions report having formal data stewardship policies in place. Although we expect this percentage to be higher today, it is clear that even in cases where formal policies are in place, some data stewards have limited expertise and training in data protection and backup. The lack of policies, training, and expertise can all result in data loss for a particular business or academic unit.

Students' responsibility for data backup

At many institutions, students are responsible for backing up and saving their coursework data such as term papers or project work. They typically store backup copies on CDs, DVDs, flash drives, external hard drives, or on their home computers. If a laptop is stolen and the student was lax with his / her backup procedure, the student can lose hundreds of hours of schoolwork.

With Learning Management Systems starting to proliferate across higher education institutions, many IT organizations are taking steps to preserve this data on behalf of their students. According to a December 2013 article, "The Future of Student Backup Data," Dennis Cromwell, Associated Vice President of Enterprise Infrastructure at Indiana University, states that the old method of students backing up their data is changing. [Cromwell](#) believes that the institution "has an obligation to provide backup services to students not only as a means of preserving that data but to prevent it from being lost in case of accidental deletion of files or some type of disaster."

The Internet of Things (IoT) will make data backup and recovery even more important. In many respects, [the academic world](#) is leading the charge with IoT in both the classroom and through research. The IoT will result in more and more Big Data, challenging academics to find secure ways to store, use, and protect it.

DATA PROTECTION FOR HIGHER EDUCATION

Acronis

Solution Brief

ACRONIS' DATA PROTECTION SOLUTION FOR COLLEGES AND UNIVERSITIES

Regardless of the role the institution's IT team plays in governing data protection and executing backups across an institution, there will always be a level of autonomy afforded to all or selected businesses and academic units. For this reason, universities and colleges should only consider backup solutions that meet the following criteria:

- You do not need to be an IT expert to install and manage the solution, but you have peace of mind knowing that data is protected in the event of any man-made event or natural disaster.
- Backup solutions need to be able to scale up or scale back to accommodate shifting responsibilities for data backup across an institution. For example, today the IT team backs up the institution's servers but has data stewards and users back up their desktops and laptops. Tomorrow, the IT team may take ownership for desktop and laptop backup. Having a single solution that can accommodate this shift in responsibility helps ensure the protection of your backup investment.
- The backup solution must protect the varied server platforms you can find in a university setting, PC and Mac® desktops, and all mobile devices whether institution or personally owned.

Over 1,700 colleges and universities around the world use Acronis products to protect and access their institution data, using a combination of Acronis products.

ACRONIS BACKUP ADVANCED

Acronis Backup Advanced delivers robust, easy-to-use, unified data protection and disaster recovery for multi-system environments. Based on your data protection needs, you can deploy individual solutions to support backup for a specific business or academic unit, or seamlessly blend them together into one efficient backup solution to support multiple departments, academic units, research labs, or all institution data. Powered by the [Acronis AnyData Engine](#), Acronis Backup Advanced uses a single-pass disk imaging technology that takes a snapshot of an entire system on any hardware or virtual machine, including the operating systems, applications, user preferences, data, etc. You can then store this data on disk, tape, SAN, NAS or in the cloud and recover it to any other physical or virtual machine in any location. In addition, Acronis Backup Advanced encrypts data in transit and at rest to ensure privacy and security.

The Acronis Backup Advanced suite of products includes local and cloud backup and recovery for virtual and physical Windows® / Linux environments; VMware®, Microsoft®, Citrix®, Red Hat®, Linux KVM, and Oracle® hypervisors; and Microsoft Exchange, SQL Server, SharePoint® and Active Directory®. Both installation and backups do not require restarting the system or suspending applications, minimizing the impact to user productivity. In minutes, you can recover individual files, application data, a complete system, and hypervisor environment to any location - reducing downtime and ensuring maximum data protection. With key features including dissimilar bare metal hardware restore and Acronis Active Restore, you can reduce recovery time by an average of 50 percent.

DATA PROTECTION FOR HIGHER EDUCATION

Solution Brief

George Brown College in Toronto, Canada uses Acronis Backup Advanced for bare metal restore. Host operating system images are now installed in minutes from a SAN versus the hours once required for manual builds. The IT group also uses Acronis disk imaging technology to deploy new servers. This gives the data center a fully up-to-date, bootable image of each server and its applications, available and ready to go on a rescue disk if a hardware failure takes a server offline. Wayne Kyryluk, College Administrator, Data Center Operations explains, "If a system goes down completely with a hardware failure, we can replace or repair a hard drive, drop in the latest Acronis image from the SAN and make it bootable. Acronis products have simplified recoveries and effectively reduced them to non-events, minimizing time, effort and staff as we grow our server population by several times in the past several years."



Figure 2: Protect Any Data, in Any Location, On Any Device

Let's revisit incident #3 – where sensitive data was lost at Chicago State University because devices were misplaced or stolen – and let's assume that the institution chose Acronis Backup Advanced to protect their data. In this scenario, the institution uses Acronis to backup any server, any desktop, any laptop and store those backups in one to five locations. If the hardware is misplaced, lost, or stolen, the institution has a copy of all data that resides on the missing hardware. Using Acronis' bare metal restore, the institution can easily and quickly restore the data to the same or a different machine. The backup would also help the university determine if any confidential information was stored on the missing machines.

DATA PROTECTION FOR HIGHER EDUCATION

Acronis

Solution Brief

ACRONIS BACKUP AS A SERVICE

Acronis Backup as a Service (BaaS) is a comprehensive, yet simple, complete, and cost-effective local and cloud backup and recovery solution that an institution can deploy in several ways:

- An institution can look to Acronis to store and manage their backups in an Acronis (Cloud) Data Center and quickly roll out the solution. In this scenario, the institution does not have to be concerned with backups – Acronis does everything—installation, backup, and recovery - on behalf of the institution. For example, if a researcher needs a copy of a backup, he / she contacts Acronis for assistance. This will reduce the volume of calls to the institution's help desk.
- An institution can implement their own cloud storage at the university's data center, which gives the institution complete control over their backups and alleviates concerns about data leaks in public clouds.
- Business or academic units can choose to back up their data to their local disk storage, further strengthening their data protection strategy.

For distributed IT organizations looking to offer backup-as-a-service to the businesses and academic units within an institution, Acronis BaaS delivers an extremely scalable, customizable, complete, and reliable service that backs up data from any source, stores data locally or in the cloud – including Acronis Cloud - and recovers data to any destination and system. In this scenario, Acronis BaaS provides usage reports for all service tiers and supports the “internal customer” sign-up process. In fact, the university's IT organization can offer backup-as-a-service to external institutions and agencies as well and develop a revenue stream for services.

The Acronis BaaS solution offers a per-use business model with zero entry costs, eliminating any upfront investment. Acronis BaaS supports workstations and physical / virtual servers and easily automates the deployment and management of software functionalities using a central web-enabled control panel. You can backup and recover data, files, and an entire system, recover a system to bare metal, and encrypt data. BaaS is also an ideal choice for institutions looking to transition from legacy tape backup solutions.

Let's revisit incident #2 – how the University of British Columbia lost research data due to researcher retirement / turnover and obsolete storage devices - and let's assume that this institution chose to have a service provider or their IT department store and manage the university's data in the Acronis Cloud. In this scenario, data is protected on schedule, including disk images of all servers, desktops, and laptops. When a researcher needs to restore data, they can do it themselves, with help of the University's IT department, or it can be restored by the service provider who implemented the Acronis BaaS solution.

DATA PROTECTION FOR HIGHER EDUCATION

Acronis

Solution Brief

ACRONIS DISASTER RECOVER AS A SERVICE (DRAAS)

Acronis Disaster Recovery as a Service (DRaaS) is a fully managed, comprehensive, IT continuity solution that protects institution data and server environments in the event of a natural or man-made disaster. With a university's low tolerance for the unavailability of data and systems, Acronis DRaaS can reliably recover your servers or entire data centers without the need to invest in duplicate systems or additional staff. Providing cold, warm, or hot recovery options, Acronis DRaaS combines the high performance and shortest recovery time of a local appliance with the low cost, predictability, and accessibility of a virtual, private, off-site cloud.

Acronis supports institutions with a team of experts who can help keep IT systems up and running, letting universities focus on education and research contributions and values. The Acronis DRaaS solution is proven in hundreds of mission-critical deployments worldwide and has performed hundreds of "push-of-a-button" recoveries.

- A fully managed, comprehensive, backup and recovery solution ensures operational continuity and on-going availability of data and systems.
- Acronis DRaaS protects your entire environment and all of your data - including files, volumes, servers, and entire data centers. You can recover servers within the local LAN on a physical or virtual appliance, or failover to your virtual private space within the Acronis' cloud data center.
- Choose cold, warm, or hot recovery to address your operational needs and budget.
- Run DR exercises without affecting students, researchers, and staff's productivity.
- Perform all DR tasks using a self-service, web-based recovery console – one single pane of glass.
- Get peace of mind with 24x7 white glove support for failover and fallback.
- Enjoy a broad choice of platform support including physical, virtual, local or cloud, any hypervisor, any storage.

Let's revisit incident #1 - how University X lost all their data because of a disaster – and let's assume that this institution chose Acronis DRaaS recovery. In this scenario, the institution pre-defined the specific service level agreement (SLA) for Recovery Time Objective (RTO) and Recovery Point Objective (RPO) based on their business objectives and budget. If a full disaster happens, the institution notifies the Acronis support team who activates the replica of the IT environment that sits in the Acronis Data Center. The institution's IT team can remotely monitor the recovery process through a web-based recovery console, and see how the servers fail over in the Acronis environment in real time. The systems, applications, and data are then available to internal and external users as per the SLA, and the system replica that sits in the Acronis Data Center will continue to be available to users up until the institution can safely fail back to the original environment.

DATA PROTECTION FOR HIGHER EDUCATION

Acronis

Solution Brief

ACRONIS SNAP DEPLOY®

Acronis Snap Deploy lets you provision hundreds of workstations and servers as fast as you can provision one. Powered by the Acronis AnyData Engine, award-winning disk imaging technology lets you create an exact disk image of any standard configuration you choose - including the operating system, configuration, files, and all applications - and simultaneously deploy the image to multiple machines - even different brands and types of PCs and servers - in one easy step. Acronis Snap Deploy will also automatically manage machine-specific configurations.

Acronis Snap Deploy is ideal for

- Rapid bare-metal initial deployments to a large number of workstations and servers (e.g., when the IT team is rolling out a new fleet of servers or PCs or is performing upgrades on many machines)
- Classroom and lab environments when instructors need to quickly refresh machines back to the original configuration(s)
- Research environments where researchers need to quickly create and re-create a stable technology environment for experimental research; Acronis Snap Deploy establishes a refreshed, consistent technology standard and physical control to minimize the risk of errors with experiments and tests

Acronis Snap Deploy includes Acronis Universal Deploy, which lets you deploy the same image to other brands and types of PCs and servers. The product also manages machine-specific configurations including machine names, IP addresses, domain membership, and other settings. In addition, as soon as you finish a deployment, Acronis Snap Deploy lets you easily modify Windows® settings. Using Acronis Snap Deploy, the University of Aberdeen, located in the North East of Scotland, has halved the time it takes to image existing PCs, saving their Service Delivery Division up to 10 weeks of IT deployment time each year. "Prior to purchasing Snap Deploy, it would take us up to two hours to image a single PC," notes Derek Findlay, Computing Support Officer for the University. "Using Acronis, it now takes us just under one hour."



The classroom team can create individual master images containing the operating system, settings and all the applications required, and place it on any of the 1700 PCs that they maintain.



BENEFITS

Acronis products deliver significant benefits to institutions looking for data protection and secure access including the ability to

- Reduce recovery time by 50%*
- Reduce long term storage costs by up to 60%*
- Reduce the time to back up a full system by 30%*
- Deploy an image to hundreds of the same or different systems 80% faster*
- Refresh or change configurations in a class, lab, research, or test environment in half the time*
- Easily install, configure and manage with virtually zero training required
- Scale the protection for any data, any operating system, any application
- Choose the best storage option that meets your institution's requirements - Acronis Cloud or your own infrastructure
- Implement quickly with pre-packaged installation and consulting services available from Acronis' network of over 32,000 partners worldwide
- Enjoy peace of mind with a dedicated international technical support team

* According to customer feedback and Acronis survey data

ACRONIS EDUCATION PROGRAMS

In addition to the benefits above, your institution will also benefit by collaborating with Acronis to offer a mix of innovative education programs (see Figure 3). For example, the Moscow Institute of Physics and Technology has partnered with Acronis to offer research projects to students over various topics such as usage of distributed systems, storage systems, mobile solutions, and virtualization technologies. Likewise, Acronis and the Data Storage Institute in Singapore formed a partnership to research and develop innovative data storage technologies that address upcoming Big Data challenges. In addition, Acronis offers a Certification Program to both students and your IT staff. This program includes introductory courses on Acronis products, technologies, and best practices as well as a certified engineer course.

Figure 3: Acronis Education Program

- Acronis mentorship programs
- Student internships in Acronis labs and R&D centers
- Joint research and development projects
- Guest lectures by our IT experts on the hottest IT topics
- Acronis Scholarship Program for outstanding students
- Sponsorships of IT conferences, competitions, and education events

DATA PROTECTION FOR HIGHER EDUCATION

Acronis

Solution Brief

SUMMARY

Most colleges and universities centralize the governance of data backup and protection but delegate day-to-day responsibility and execution to the business, academic units, and users. This egalitarian approach can lead to data loss.

- Many users – specifically those that are not data stewards – do not have experience in data protection and disaster recovery.
- You cannot count on some individuals, such as end users, to back up their data on a regular basis.
- Without training, many individuals can misinterpret the backup policy, which can lead to data loss.

To overcome these challenges, institutions should seek to put in place a cost-effective backup solution that:

- Protects data across all servers, desktops, and mobile devices
- Supports multiple server platforms, desktops, and mobile devices
- Is easy to install and manage
- Can scale up or scale back to accommodate shifting centralized / decentralized ownership of data backup and recovery

Acronis has over 1,700 colleges and universities using Acronis products:

- Acronis Backup Advanced delivers robust, easy-to-use unified data protection and disaster recovery for multi-system environments.
- Acronis Backup as a Service
 - If an institution, business, or academic unit does not want to manage their backups, they can contract with an Acronis service provider in lieu of purchasing Acronis Backup Advanced.
 - Alternatively, an institution's IT organization can offer backup-as-a-service to the businesses and academic units using Acronis Backup as a Service.
- Acronis Disaster Recovery as a Service (DRaaS) is a fully managed, comprehensive, IT continuity solution that protects institution data and server environments in the event of a natural or man-made disaster.
- Acronis Snap Deploy® lets you provision hundreds of workstations and servers and is ideal for rapid bare-metal initial deployments to a large number of workstations and servers, and on-going deployment to the same hardware in education and lab environments.

ABOUT ACRONIS

Acronis sets the standard for New Generation Data Protection through its backup, disaster recovery, and secure access solutions. Powered by the AnyData Engine and set apart by its image technology, Acronis delivers easy, complete and safe file access and sharing as well as backups of all files, applications and OS across any environment—virtual, physical, cloud and mobile.

Founded in 2002, Acronis protects the data of over 5 million consumers and 300,000 businesses in over 130 countries. With its more than 100 patents, Acronis' products have been named best product of the year by Network Computing, TechTarget and IT Professional and cover a range of features, including migration, cloning and replication.

Acronis

For additional information, please visit www.acronis.com

Follow Acronis on Twitter: <http://twitter.com/acronis>

To purchase products, please visit <http://www.acronis.com/en-us/company/contacts.html#international> to find an Acronis office or authorized dealer.

Copyright © 2002-2015 Acronis and the Acronis logo are registered trademarks or trademarks of Acronis International GmbH in the United States and/or other countries. Microsoft, Windows, and Surface are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Linux is the registered trademark of Linus Torvalds in the U.S. and other countries. All other trademarks or registered trademarks are the property of their respective owners. Technical changes and differences from the illustrations are reserved; errors are excepted. 2015-04