DATAMONITOR

Ensuring business continuity in higher education IT

Preparing for the unexpected

A Datamonitor white paper

Publication Date: April 2007

www.datamonitor.com

Datamonitor USA
245 Fifth Avenue
4th Floor
New York, NY 10016
USA

t: +1 212 686 7400
f: +1 212 686 2626
e: usinfo@datamonitor.com

Datamonitor Europe
Charles House
108-110 Finchley Road
London NW3 5JJ
United Kingdom

t: +44 20 7675 7000
f: +44 20 7675 7500
e: eurinfo@datamonitor.com

Datamonitor Germany
Kastor & Pollux
Platz der Einheit 1
60327 Frankfurt
Deutschland

t: +49 69 9750 3119
f: +49 69 9750 3320
e: deinfo@datamonitor.com

Datamonitor Asia Pacific
Darling Park
Tower 2, Level 21
201 Sussex Street
Sydney NSW 2000
Australia

t: +61 2 9006 1526
f: +61 2 9006 1559
e: apinfo@datamonitor.com

Datamonitor Japan
Wakamatsu Bldg 7F
3-3-6 Nihonbashi-Honcho
Chuo-ku
Tokyo 103-0023
Japan

t: +813 6202 7681
f: +813 5778 7537
e: jpinfo@datamonitor.com

ABOUT DATAMONITOR

Datamonitor plc is a premium business information company specializing in industry analysis.

We help our clients, 5000 of the world's leading companies, to address complex strategic issues.

Through our proprietary databases and wealth of expertise, we provide clients with unbiased expert analysis and in-depth forecasts for six industry sectors: Automotive, Consumer Markets, Energy, Financial Services, Healthcare, Technology.

Datamonitor maintains its headquarters in London and has regional offices in New York, Frankfurt and Hong Kong.

INTRODUCTION

In IT as in personal life, it is tempting to assume that catastrophes are things that happen elsewhere and to other people. IT is increasingly central to education. As solutions such as the student information system (SIS) or learning management system (LMS) become increasingly central to the day-to-day operation of education institutions, ensuring that these solutions keep working regardless of whatever disaster may have befallen the institution becomes a core objective of the IT department. Technology systems become an ever more central part of our lives, it becomes more and more important to overcome the temptation to pretend that we are immune from disaster and make sure that IT departments are prepared for the worst.

In education institutions, as in many other types of organization, the influence of IT systems has gradually crept in to all the functions of the organizations. In all academic subject areas and across administrative functions, IT systems now perform a range of essential roles. However, the gradual creep of our dependence on technology has left many institutions unaware of their reliance upon it. As a result, it is easy to neglect the effect that a catastrophic event might have in IT terms. There are two ways in which an institution's dependence on IT has significant consequences in the event of some kind of catastrophe:

- **IT failure** – IT systems that are damaged in an event will have to be restored for the organization to function adequately.
- **Indirect impact on IT** – Increasing reliance on IT systems mean that these systems may have to adapt to an event that damages another part of the organization. For example, after a building is rendered unusable network access would need to be provided to users at their new location.

Disasters that might require either type of response from the IT department and systems could come in many forms. These potential problems range from the seemingly trivial – such as a leaking pipe – to the completely catastrophic. Damaging events might be natural or man-made. A massive range of eventualities might either cause the IT to be damaged or require help from the IT department.

In all these situations, organizations need to have a clear plan of action that will enable them to make sure that their IT systems are capable of doing all that is

required of them. In this white paper, Datamonitor aims to answer the following questions:

- Why should colleges invest in a business continuity plan?
- What are the components of a business continuity plan?
- What steps should education institutions take today?
- What can a vendor offer you to help with your business continuity strategy?

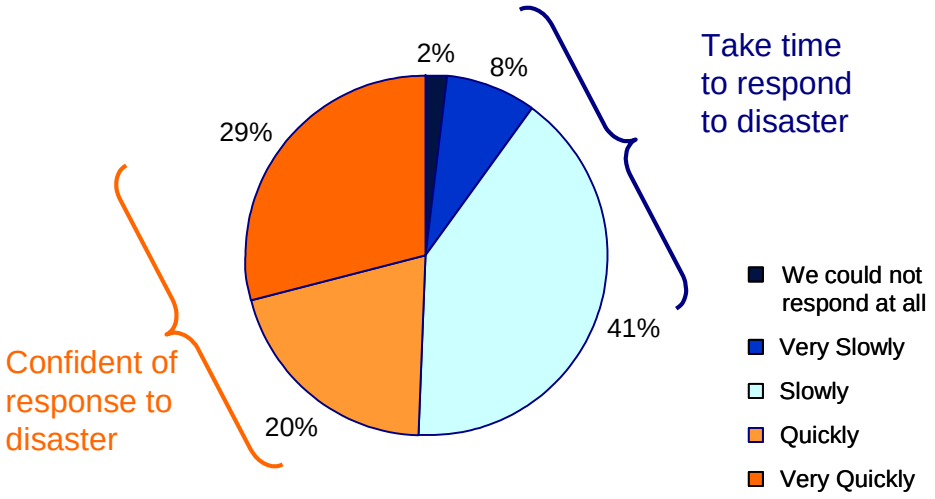
WHY WORRY ABOUT BUSINESS CONTINUITY?

IT decision-makers in education are faced with meeting the considerable demands for IT services from a diverse set of constituency groups. Students, faculty, staff and administrators who use the organization's IT systems are constantly asking for new features and applications, improved bandwidth, more wireless access points and a host of other enhancements to improve the education environment. These users are naturally interested in applications that will help them learn or teach more effectively. Users may well expect the IT department to help protect them against viruses and other online threats. However, IT professionals in education do not as a rule face worried users who want to know about the business continuity plan.

With all the demands on the computing systems of the institution – not to mention the limited budgets available – it is not surprising that planning for the worst can easily fall to the bottom of the IT to-do list. In a recent Datamonitor survey of education intuitions, less than half of IT decision-makers reported that their organization would be quick or very quick to respond to a natural or man-made disaster, as shown bellow. In addition, the responses only reflected how confident the IT function is about its response rather than any specific measures it has taken. The confidence of many of those who claim a quick recovery time might prove to be unjustified.

IT decision-makers in education do not feel ready for disaster

How quickly and easily do you feel that your organization is able to respond to natural or man-made disasters?



Source: Datamonitor

DATAMONITOR

However, being able to cope should calamity strike is increasingly recognized as vital for education institutions. Datamonitor believes that a number of factors are driving increasing interest in business continuity by education institutions, including:

- **The range of possible disasters** – Extreme weather events across the world help to focus the minds of IT decision-makers on how they would cope if some part of their IT infrastructure were hit by a disaster beyond their control. Events like Hurricane Katrina have helped to turn the thoughts of educational IT decision-makers to the wide variety of catastrophic events with which they might have to wrestle.

- **Increasing dependence on IT** – As discussed in the introduction, all colleges and universities now depend on the technology infrastructure for a significant part of their day-to-day operations. Education decision-makers are waking up to the fact that if central IT functions fail, then their institutions would find it difficult to continue their operations, even in a minimal fashion.

- **Competitive pressure and brand awareness** – The flip side of an awareness of how important IT systems have become to the institution is the recognition of the potential consequences of failure. In an increasingly

competitive higher education environment, institutions must preserve their reputation for stability in a crisis. A minor crisis like a leaking water pipe in the server room can quickly turn into a public relations nightmare if it leads to lost student work or the need to cancel classes.

- **Broader community role** – Universities and colleges are not merely businesses providing an ordinary service, they are often seen as providing a central service to the community as a whole. In the event of a major crisis, education institutions often find themselves at the center of efforts to deal with the situation. The Louisiana State University (LSU) campus in Baton Rouge found itself at the center of the relief effort for Hurricane Katrina. The IT department found itself issuing and supporting phones and computers for the aid workers. Institutions who see themselves as fulfilling this broader role need to keep themselves going in a crisis not just for their own sake but in order to take its place at the center of the community it serves.

The particular stimulus for thinking about business continuity is usually the news of a crisis hitting similar institutions, such as those caught up in the aftermath of Katrina. As a result, interest in business continuity tends to be sporadic. Enthusiasm for investment is cyclical, but the need for solutions remains constant as the images of the last disaster fade in memory.

Awareness of the last major event can also have a distorting effect on the type of event for which institutions plan. It is important that institutions consider the full range of possible events that might significantly damage their ability to function.

WHAT IS A BUSINESS CONTINUITY PLAN?

Business continuity can be described as a strategy that gives an organization the ability to continue to function after or during natural or human-caused disasters that has significantly damaged the organization's operations. Business continuity can be thought of as step forward from disaster recovery – the goal of which is merely to be able to recover systems after an event rather than to continue operations directly. A disaster recovery strategy, while certainly better than having no preparations for disaster, is much less ambitious than a business continuity one.

Even those organizations that have given serious thought to what they would do in the event of a catastrophic event often think in terms of being able to retrieve their data, rather than in terms of keeping IT systems going. As a result, such

organizations have a disaster recovery plan rather than a business continuity plan. While it is indispensable to have a plan to preserve crucial information if a college is to maintain its services in even a minimal fashion it will also need a more comprehensive approach that goes beyond disaster recovery.

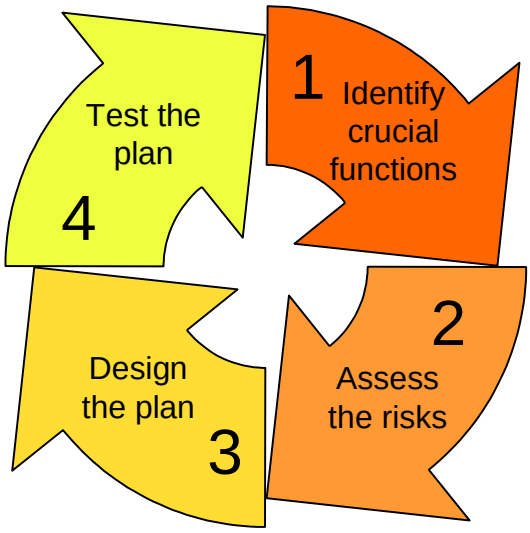
There are two main components of business continuity:

- **Technology and services** – These make up the physical part of the business continuity plan and can be broken down into four sub-components:
  - **Storage and servers** – Education institutions need adequate back-up systems both to preserve data and to provide systems that can take over in the event of a failure.
  - **Software and automation** – A core part of the business continuity strategy is the automation of the process of creating backup data and systems. As well as back up systems, the technology component of business continuity will include software solutions that are able to monitor the IT system's status. These applications give early warning of IT failures and assist in providing a smooth transition to backup systems.
  - **Networking and physical infrastructure** – To create redundant systems there needs to be both a physical space that the organization can make use of and the network to communicate with it.
  - **Skills and services** – Whatever the make up of the hardware and software solution the business continuity strategy will require the skilled IT staff to execute it. Building a successful strategy will require effective cooperation between those staff with responsibility for the all the infrastructure the institution needs to protect.
- **Planning** – Just as important as the technology will be the plan that enables those in the institution to make use of the technological systems that have been put in place. Technology has to be deployed as part of a plan that allows for the types of disaster that might occur and how it will be used in these situations.

WHERE TO START WITH BUSINESS CONTINUITY

There is no one technology product which an institution can purchase that will, by itself, ensure the continuity of its operations during a disruptive event. Creating an effective business continuity strategy involves the coordination not only of several disparate technology products and services, but also of IT staff, administrators, faculty and students. As a result, business continuity is first and foremost an institutional strategy for managing disruption, so institutions need to at least begin to develop their plan before investing in any products or services to provide technological redundancy.

The four stages of the business continuity planning cycle



Source: Datamonitor

DATAMONITOR

Business continuity planning can be viewed as a cycle. As illustrated in the above diagram, Datamonitor suggests that this cycle can be divided into four stages, including:

1. **Identify the crucial functions** – The first stage is to work out which institutional functions it is most important to preserve in the aftermath of a

catastrophic event. By ranking the functions in order of importance it becomes possible to identify which IT systems most need protection.

2. **Assess the risks** – Next intuitions need to determine what kind of events might threaten these functions and make an assessment of how likely these events are. In assessing the risks that the organization is exposed it is important to understand what the core points of failure within the institution are.

3. **Design the plan** – Having picked out the most crucial points in the infrastructure of the institution, be they human or IT systems, you can now formulate a plan. The plan will detail how the technology and other functions of the organization will respond in the event of disaster.

4. **Test the plan** – While conducting a full dry run of the business continuity plan is resource-intensive, it is vital to run through a series of scenarios for how the plan would work in practice. Running the scenarios should give a clear picture of what functions your institution would be left with after the plan is put into effect. You can then address key questions about the effectiveness of the plan, such as:

    a. What systems and functions are not covered by the plan and how long can you do without them?

    b. Equally, do you really need all of the functions that you will have spent scarce resources on protecting?

Once you have reached stage four and tested the plan against reality it is time to reconsider which of the functions your institution really needs in the event of each class of disaster. While the initial round of assessment and planning will be the most difficult it is still important to reexamine how the plan might be made more effective.

Treating business continuity planning as a cycle is important because it helps to ensure that the business continuity strategy is kept “live”. It is very easy for a plan to be drawn up and then filed in the bottom draw never to be seen again. When an incident occurs the plan is either forgotten or so out of date that it is impossible to put into effect. A plan which is not kept live might include references to systems that are no longer in use, depend of facilities that no longer exist and fail to refer to new parts of the institution altogether. Instead business continuity should be a constant part of the IT strategy. To keep the plan live organizations need to persist with the business

continuity planning cycle as part of the normal IT and business planning process of the organization.

Building a plan that can cope with the university's needs in any eventuality can seem very daunting. However, the planning process should help your institution to hone in on the few core technology services that you need to make extra investment in to secure in the event of a catastrophe. Institutions should begin their investments by taking the basic steps to ensure that recovery is possible and then look at more sophisticated options such as the provision of full offsite facilities.

FINDING THE RIGHT VENDORS TO HELP WITH YOUR BUINSESS CONTINUITY STRATEGY

When investing to provide the technology components of the business continuity plan – whether that plan preserves only the most vital data and functions or involves having a full hot-site waiting for use – it is essential that you select the right technology partners with which to work. In addition to the suppliers of the redundant hardware and software, vendors can also offer services that can help to make the strategy both more effective and more affordable. In particular, IT services vendors can provide three types of service to assist in the creation of a live business continuity plan:

- Planning services;
- Hosting data;
- Hosting recovery centers.

Planning services

As mentioned earlier in this white paper, the task of building a business continuity plan unaided can seem somewhat daunting. Anticipating all possible misfortunes and understanding how they will impact on the running of your institution will represent a significant challenge.

By turning to an outside organization that has considerable experience with business continuity across technology areas and specifically with higher education, your institution can learn from best practice elsewhere and avoid making costly mistakes in either over or under provision.

For example, AT&T offers a range of business continuity professional services that aims to assist education institutions in making informed decisions about business continuity programs, strategies and investments. AT&T offers services that address each of the stages in the formulation of the business continuity plan including identification, risk assessment, planning and testing. Specifically, AT&T's business continuity professional services portfolio includes:

- **Managed Risk Services** – These provide an appraisal of the functions within the educational environment, including a Business Impact Analysis (BIA) and Risk Assessment.
- **Business Continuity Strategy and Planning** – These design continuity and recovery strategies for your critical processes that focus on planning, testing, training and certification.
- **Business Continuity Program Management** – This assists in the full implementation and management of the plan within the institution.

Hosting data

Offsite backup for institutional data must be a central component of any disaster recovery or business continuity plan. Even if there is no plan in place for how the organization would rebuild its systems, if the data has been preserved at least a plan can be constructed after the fact. Without the institutions most important records and information it will be impossible to recover the IT systems without beginning again from scratch.

Now that most education institutions enjoy a high capacity link to the Internet, there is no longer a volume constraint on the amount of data that can be sensibly backed up to a remote site. It makes sense to make use of a vendor that is able to offer a cost effective price, a robust network with large scale redundancy and the services to make backup as hassle free as possible. In addition a vendor should be able to offer data storage that is located at a sensible distance from your main site. It will be of little use having offsite backup if it is located close enough to your institution to be caught up it whatever is affecting your onsite systems.

AT&T offers two hosted backup solutions that can help colleges to secure their data:

- **AT&T StorageConnect^{SM} Service** – is a multi-location storage transport service that enables clients to extend their remote replication, backup,

Ethernet data and/or mainframe applications between their data centers and/or AT&T Internet Data Centers (IDCs) over any distance with virtually any bandwidth and storage protocol. StorageConnect can be used to replicate the core records of the institution, including data from multiple campuses.

- **Remote Vault[SM]** – is a fully-managed remote backup and restore service. Remote Vault uses your broadband Internet connection to backup data from servers, PCs, or laptops to a secure off-site storage facility, where it is available for recovery at any time and to any location. Users can control the timing and regularity of backups through an easy to use interface.

Fully hosted recovery centers

For those institutions that are serious about continuing their operations through any disaster they will needs some way to provide alternative facilities not just for their data but for their staff. The easiest way to provide a full set of IT facilities can be to rely on a service provider, who has the capacity to offer additional systems and even premises in a crisis.

As part of its Enterprise Recovery Service, AT&T can provide a range of subscription-based services that offer local replacements for systems and user work locations which have become unusable due to an unforeseen event. Because of its size, AT&T is able to offer over 50 mobile facilities in strategic locations and facilities for nearly 20,000 end-user positions worldwide. This also includes support for the full range of hardware platforms, something that will be critical for the heterogeneous IT systems found in many college campuses.

CONCLUSION

There are a wide range of events, from small accidents to natural calamities, which can wreak havoc with the normal functioning of your institution and in particular with its IT systems. Ironically, planning for such eventualities can seem to be both daunting and a low priority. However, all education institutions should have some idea of what they would do in the face of a catastrophe. Institutions should have as a goal creating a business continuity strategy which forms a continuous part of their general planning program.

There are of course limits on the time and budgets available to education intuitions. As with many parts of the IT strategy, business continuity will be the art of the possible, with organizations doing what they can rather than what they would like to do. A business continuity strategy does not have to start out as a comprehensive plan to have every class running smoothly with one hour of a serious incident. Instead a business continuity strategy should be seen as an ongoing process, which adapts and expands over time to provide the best available solution given the needs of the institution at that time.

In coming to grips with your business continuity needs, it is crucial to select the right vendors to support your institution's needs. By choosing to outsource all or part of the business continuity solution that you choose to implement you can save valuable resources and add an extra layers of redundancy to your systems. By selecting the right technology and services partners your institution can give itself peace of mind and should the worst happen help the institution to distinguish itself through its ability to triumph in adversity.