Colleges get a lesson in disaster recovery

Hurricane Sandy was a powerful reminder of the need for smart disaster planning; here's what campus leaders should know

When Hurricane Sandy barreled into the Northeast coast of the United States in late October, it leveled thousands of homes, caused tens of billions of dollars in damage, claimed at least 130 lives, and left millions of people without electricity. It also took numerous businesses offline for hours, or in some cases, days—disrupting operations for services ranging from the New York Stock Exchange and Amtrak to educational institutions.

Many colleges were affected from this storm. The College of Saint Elizabeth in Morristown, N.J., lost access to its data center and voice communications for a few days, according to the Association for Information Communications Technology Professionals in Higher Education (ACUTA). Drew University in Madison, N.J., was among the schools in the New York/New Jersey area that shut down for a week and sent students home.

Lesson, page 12

This Publisher's Report is sponsored by Symantec Corp.

Publisher's Report

Lesson...

continued from page 11

Business continuity experts say the devastating storm served as the latest reminder of the need for careful planning to ensure that critical business functions remain available to stakeholders who need them—even in the wake of a natural disaster or other catastrophic event. And that's just as true for colleges and universities, which increasingly rely on data systems and networks to provide essential services to students and staff.

"Events such as Super Storm Sandy always bring back into sharp focus the need for attention to planning for the impact of disasters," said Brian Voss, chief information officer at the University of Maryland. "The larger storms—like Sandy in 2012 and Katrina in 2005—serve to remind us that disaster response and business continuity planning require attention beyond simply the loss of one's data center, but can extend to the entire campus, the city where the institution is located, and even entire regions."

Today's students use learning management systems to hold class discussions and complete course assignments at all hours of the day. Professors and campus administrators use student information systems and learning analytics programs to store, recall, and analyze data about students and their performance. If a storm or other disaster were to knock these systems offline for long, students' learning would be disrupted. Worse, the loss of data from any of these systems could prove extremely problematic.

But it's not just the education of students that is at stake. Universities have to preserve terabytes of important research. Colleges of all sizes have to protect servers containing sensitive human resources and financial information. In an increasingly competitive market, with schools using sophisticated data systems to recruit and retain students and forge relationships with alumni, the loss of any of these systems could set back enrollment, fundraising, and all kinds of vital operations.

Unfortunately, massive storms like Hurricane Sandy are becoming more common, experts believe—and colleges must be prepared.

In the 1990s, the average cost of weather disasters in the United States was $4 billion a year, former CNN journalist Kathleen Koch said during a Jan. 31 lecture on "Disasters and Resilience" at Hutchinson Community College in Kansas. In 2011, she said, weather disasters cost $14 billion—and this trend is likely to continue as the U.S. faces colder winters, hotter summers, and more severe storms.

Although disasters often occur suddenly, Voss said, CIOs must anticipate and plan ahead to confront disasters head on.

"The frequency of these events means that the reminders are coming at us near-constantly, thus elevating disaster preparedness and business continuity planning off the back burner and into the forefront of campus IT strategies," he said.

Planning for disaster

A sound business continuity plan should address the people, processes, and technologies needed to maintain operations. Disaster recovery is a key component of business continuity, though it's not the only component. While business continuity involves planning for all aspects of campus operations, disaster recovery focuses on the IT systems that support these functions in particular.

Disaster recovery plans should include measures for preventing, detecting, and responding to IT emergencies. Preventative measures can include backing up data (both on and offsite) and safeguarding systems with surge protection, uninterruptible power supplies (UPS), and generators, while responses can include plans for recovering data or servers that are lost during an emergency.

In the days after Hurricane Sandy, Boston's Northeastern University released disaster planning guidance that recommended (1) identifying primary assets for business continuity; (2) securing data storage with regularly tested backups; (3) maintaining an offsite backup and secondary redundancy service location at least 50 miles away from the primary location; and (4) developing staffing plans and resources for relocation or replacement of services.

Campus leaders should clearly define the roles and responsibilities for IT staff during different types of emergencies. They also should define the required recovery point objective (RPO) and recovery time objective (RTO) for each application and business process. A recovery point objective is the point in time to which an application's data must be recovered before resuming operations. A recovery time objective is the maximum elapsed time before the lack of a business function severely affects an organization.

The RPO and RTO metrics help determine the most suitable recovery strategy for each system. While it would be ideal to have zero data loss and zero time loss for every system, the costs associated with that degree of protection likely would prohibit it. That's why it's essential to prioritize services within a campus IT infrastructure.

"Start with what you'd consider 'essential services,' and then move to 'nice to have,'" advised Frank Forte, director of telecommunications at Rutgers University in New Jersey, which lost power in some buildings during Hurricane Sandy but emerged largely unscathed. "Each comes with a price, both financially and resource-wise. Develop a plan with all key members of each area within the university, and then prepare a methodical rollout plan. Most important is to do regular tests of your plans to ensure they work, and work out any deficiencies."

A sound business continuity plan should address the people, processes, and technologies needed to maintain operations.

Campus networks typically can be categorized in three ways, said Glen Bellomy, a data center architect for Symantec Corporation: management networks, faculty and research networks, and student structures.

Management systems represent the core academic administration and student information infrastructure, and the information they store tends to be confidential and needs high-level security and availability. Faculty and research systems tend to have varying degrees of security and priority, depending on how sensitive and timely the research materials are. Student systems, on the other hand, typically have critical usage levels, but no critical security needs.

Data backup and recovery

Backing up essential data is the cornerstone of any disaster recovery plan. But universities face a particular challenge: having to back up multiple data systems running on different servers and operating systems, across numerous campus departments. Making the task even harder, each system likely has its own needs and varying levels of priority.

To manage this process, universities should invest in powerful, flexible products that can automate data backup across multiple platforms. Symantec's NetBackup is one such product; it's a complete enterprise solution for data backup and recovery that is capable of extending across multiple locations. What's more, it works with tape, disk, snapshot, or cloud-based storage technologies—in either virtual or physical environments.

Cost and complexity often stand in the way of data backup, said Steve Vranyes, chief technical officer for NetBackup. One reason is that backing up data traditionally has required several point solutions, which Vranyes called "little islands of protection," for handling various functions such as backup, deduplication, snapshots, and data replication. NetBackup, however, combines all these functions in a single platform.

"In the past, people have wanted to do [disaster recovery] in the same way they want to eat broccoli—they know they should do it, but they just won't do it," said Vranyes. "With NetBackup, we've done a lot of things to really enable customers to do [disaster recovery more easily]—to eat the broccoli and have it taste good."

NetBackup features a proprietary technology called V-Ray, which Symantec describes as "X-Ray vision into … virtual environments." It allows the software to identify files within virtual machine images, enabling file-level recovery of data from VMware or Hyper-V virtual servers.

This enhanced visibility into virtual servers also helps users avoid backing up huge amounts of wasteful data, because it can detect duplicate files and avoid redundancy. In fact, it's just one of many deduplication tools within NetBackup that streamline the backup process. Another is NetBackup Accelerator, which uses "change detection techniques" on the client side to identify changes that have occurred since the last backup.

With NetBackup Accelerator, the client machine sends only the changed data to the media server, which combines this information with the rest of the machine's data stored from previous backups to create a full, new backup image without having to transfer all of the client's data. In other words, the system provides a full backup—but at the cost and speed of an incremental backup.

"The one thing that makes us truly different from the industry … is we deduplicate at the source, so we can make sure that we're reducing" the amount of data stored, said Carlos Valarezo, national director of systems engineering at Symantec. "You're sending less data through your networks, and it's faster."

Another feature of NetBackup, called auto image replication (AIR), copies data automatically from one location to another. This enables users to back up information in a remote data center at the same time they're backing it up locally. Whereas Accelerator speeds up data capture, AIR helps export the information to an off-site location.

Lesson, page 13

Publisher's Report

Lesson...

continued from page 12

Managing 'snapshots' of data

NetBackup not only allows you to perform full data backups; it also lets you take periodic "snapshots" of the data on a server. This gives administrators a quick way to make a copy of the data on a machine at a certain point in time and send it to a secondary storage source, so it can be used to rebuild that database in the event of a disaster. The tradeoff to this approach is that it doesn't allow for individual file recovery.

The Replication Director feature of NetBackup version 7.5 enables users to manage the scheduling, policy management, and recovery of data snapshots alongside traditional backup techniques—providing what Symantec calls a "holistic" solution to data recovery.

Users can define and execute lifecycle policies for taking data snapshots, replicating them to a secondary array, or storage level, and having these snapshots "expire" automatically after a pre-defined retention period. They also can back up these replicated copies to a tape or disk for longer storage.

For smaller colleges, Symantec offers a data recovery product called Backup Exec. Like NetBackup, Backup Exec uses V-Ray technology and can protect both physical and virtual servers. However, whereas NetBackup is a very large, multi-task engine that can handle multiple servers and locations at once, Backup Exec is a two-tier (client-server) system that performs backup tasks in sequential order.

Automated recovery

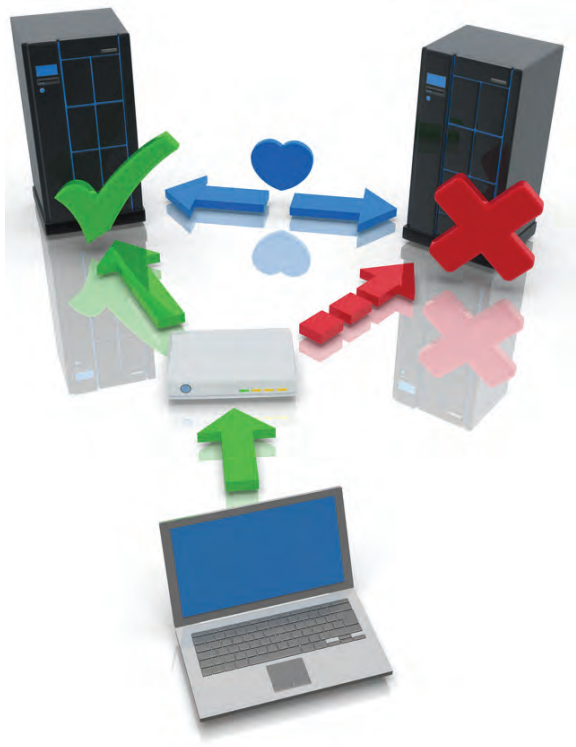
Another significant component of a disaster recovery plan is building redundancy into your IT systems, so if one system fails, its functionality can be switched to another machine quickly. Symantec's Veritas Cluster Server is an industry-leading solution for ensuring application recovery.

Data or application downtime can occur for a number of reasons, and not just from a disaster. In today's highly competitive higher-education market, colleges and universities can't afford to have IT systems like their website, or their online enrollment software, down for long—if at all. Downtime can result in lost revenue, productivity, or student dissatisfaction … which could make the difference between capturing that student as an enrollment or having him enroll somewhere else.

Server clusters, which are groups of independent servers connected by a local network and working together, can protect against server, application, or database downtime by recovering from hardware or software failures automatically. All servers in the cluster remain in constant communication with each other. If one of them becomes unavailable, another begins providing the service in a process known as failover, so users can continue to access the service uninterrupted.

Veritas Cluster Server is an open-architecture clustering solution. It works with a number of different server operating systems and virtualization hypervisors, including Microsoft Windows, Solaris, Linux, UNIX, VMware, and Hyper-V. Schools can mix and match servers and storage types within a single cluster, and the system uses a common, cross-platform console for managing multiple clusters.

Veritas Cluster Server provides off-the-shelf support for leading applications and databases from the likes of SAP, Oracle, Microsoft Exchange, PeopleSoft, and SQL, with new software agents being developed continuously—and custom-built agents can be created as well.



Building redundancy into your IT systems is a significant component of a disaster recovery plan.

The system provides high availability of IT assets by monitoring their health and automatically restarting them on a different server in the event of a failure. It also mitigates the effects of planned downtime by allowing IT staff to migrate applications from one server to another during maintenance, or for application testing.

It "allows you to move applications from one system to another," said Eric Hennessey, senior product marketing manager at Symantec. "With the push of a button, it can move applications from Server A to Server B in a predictable, orderly fashion, and [a campus CIO] can do a better job of managing [his] planned downtime." Users can even schedule the movement of their applications for the middle of the night, to disrupt as few students as possible.

In the event of a data center power outage, IT staff would need to recover applications on other machines in what Symantec referred to as "wide-area recovery." Veritas Cluster Server can handle that as well, monitoring the health of the primary data site and alerting IT staff of any problems through email notification. IT managers can decide whether to fail over to another location with the push of a button.

"If a data center is lost, you can use Cluster Server to recover all applications at another data center, and that's through a feature called global clustering," said Hennessey. "We've been doing that for quite some time, [but] what is new is the ability to recover complex, multi-tier applications."

The system also can perform failovers from a physical to a virtual machine, Hennessey said, adding: "This approach allows schools to minimize expenses and their footprint at the recovery site during normal operations."

Data availability

Another way to bring resiliency and high availability to your data center is with Symantec's Veritas Storage Foundation, which maximizes the performance of your storage across multiple operating systems—including physical and virtual environments.

Storage Foundation provides a set of tools to manage data more efficiently. It improves the visibility of data by enabling users to monitor, control, and move around data seamlessly and transparently—in effect, tying together disparate data systems through a single platform and interface. Users can replicate data to another server and create tiered storage systems for different levels of priority.

Hennessey noted that universities experience a somewhat unique pattern in their operations—a cycle of busy starts to semesters, with lulls in the middle of terms.

"There's a predictive rhythm to it," he said. "Storage demands … change as a new semester starts up." With Veritas Storage Foundation, campus IT leaders easily can provision storage as they need it to account for these periods of greater or lesser need.

At the heart of the system is a management console called Veritas Operations Manager. "It provides visibility to the whole [system]," said Hennessey.

Lesson, page 14

Nine steps to preparing for disasters

Massive storms like Hurricane Sandy are becoming more common, experts believe—and colleges must be prepared. Here are nine steps to safeguarding your IT systems.

1. Establish commitment and assign roles.
2. Publish a charter with scope, objectives, and so on.
3. Identify and evaluate threats—and your mitigation posture.
4. Prioritize resources and operations, and define outage tolerances.
5. Evaluate, select, and implement effective tools and strategies.
6. Define response/recovery processes and document plans.
7. Disseminate plans and train staff.
8. Methodically test your plans and strategies, and apply adjustments.
9. Continuously maintain and refine your strategies and plans to sustain your preparedness.

(Source: McGladrey LLP, 2012)

Publisher's Report

Lesson...

continued from page 11

"[You're] able to monitor all storage and applications. It provides dashboard-level views to everything—storage resources and so on."

Colleges and universities produce and store massive amounts of data each day, which can be costly to maintain. Backing up systems and provisioning virtual servers adds to the clutter and can lead to uncontrolled growth in the files containing virtual machines and virtual desktops. Storage Foundation includes compression and deduplication features that work to identify duplicate information on a server and either compress or eliminate it to free up space—which helps institutions save on storage costs.

Hennessey described the system as "a performance enhancer in terms of its ability to keep all the common data in the system's memory, so when a client requests a read of a duplicated block, it'll already be [stored] in the memory."

Using the program's tools, you can make a copy of data for testing purposes, then break it off and mount it on another server. You can also take snapshots of applications while the applications are running, and replicate these on another machine using storage area network (SAN) architecture.

Don't forget security

Threats to business continuity and data availability don't just include natural disasters or hardware failures; they also include security breaches. That's why no disaster plan is complete without a robust security system that protects servers and data from viruses, malware, hackers, and other threats.

"We all know that intrusion is a big problem, that people are constantly trying to get in where they don't belong, and academics are particularly concerned about that," Bellomy said. "For me, security is No. 1, and so establishing a perimeter and making sure that the perimeter defense is strong is so fundamental."

Security breaches and intrusions commonly occur from multiple angles simultaneously, Bellomy said, and campus CIOs need to be prepared for such incidents.

"Typical intrusions are not single-pathed; you need to be able to … analyze [network traffic] and know what you're looking at in a timely manner," he explained. "You have to be actively looking at logs and what's happening and correlate that into a set of events across multiple entry points and servers."

Symantec Security Information Manager is a comprehensive "security information and event management" (SIEM) solution, offering enterprise-wide log collection, management, and retention. This enables organizations to centralize and analyze large amounts of diverse log data.

Another product that can help is Symantec Data Insight, a security solution that puts data access into context using its age, frequency, location, and other factors to expose threats that otherwise might have been missed. "Symantec Data Insight helps organizations improve data governance through data owner identification, and visibility into data usage and access permissions. These insights into the data enable you to manage data growth to reduce costs, protect the data, and manage compliance," Bellomy said.

Elizabethtown College in Elizabethtown, Pa., began using another security product, Symantec Endpoint Protection (SEP), about a decade ago. Campus officials recognized the need for better security as students brought computers that had no antivirus software with them to school.

Threats to business continuity don't just include natural disasters; they also include security breaches.

"We built that in [to our requirements], to know that every machine coming on our campus was secure in some way," said Sam Rothermel, network and communications specialist for the college.

SEP is a stand-alone product that is installed on endpoints such as laptops. It's managed centrally, so campus IT teams can monitor activity across those devices. SEP runs independently on each endpoint, protecting it from viruses, malware, and other security risks and reporting information back to a managing server.

Rothermel said that Elizabethtown receives a campus discount from Symantec that helps to fund its operation. Outside of requiring that SEP be downloaded on to all incoming laptops and PCs, it is run on all campus machines, as well.

One of SEP's newest features, called SONAR, greatly reduces the scanning time of systems. SONAR establishes two distinct application lists, a white list and a black list. The white list includes 70 to 80 percent of a system's applications, which it defines as unnecessary to scan. The black list, in contrast, includes 20 to 30 percent of applications that it defines as important to scan and continue monitoring.

Though the program has proven highly effective at Elizabethtown and other colleges, Rothermel said the school's greatest challenge is the introduction of various mobile devices with disparate operating systems. Gone are the days of simple PC and laptop usage; today's students are accessing information through their tablets, smart phones, and other mobile devices—something that opens the door for greater security risks.

"[There is] definitely a changing landscape," said Rothermel. "You used to see that everyone had a desktop or laptop, but now they might have a smart phone, too, and we still run desktop machines—but we have who knows what else, all kinds of computing devices. The challenge is integrating all of that from a security perspective, and securing all of that is always a tough challenge, getting visibility to all those devices."

A multi-pronged approach is key

The key to a sensible disaster recovery plan, experts agree, is implementing a multi-pronged approach that combines data backup, replication, and application failover technologies. And Symantec has solutions for all of these needs.

Bellomy emphasized that Symantec's products not only work for large-scale universities, but smaller schools as well.

"I can reach high and low; that's the important thing," he said. "Our tools cross your architectures [and will] work with multiple systems, and physical or virtual machines." eCN