

IT Executive Exchange

Disaster Recovery and Business Continuity: What Have We Learned?

Executive Summary

A major new issue of concern is regulatory compliance with regimes under Sarbanes-Oxley, HIPPA, and others, which moves the firm from business-driven to business-and-regulation-driven disaster recovery/business continuity (DR/BC). Since regulations change frequently, this seems to lock in the need for expensive consultants on a yearly basis. Outsourcing becomes trickier. Although estimating costs of DR/BC is difficult, regulatory compliance has forced the issue of DR/BC up to the high executive level, where it belongs. DR/BC must be championed at the highest levels of management. Strategies were discussed such as N+1 redundancy; hot, warm, and cold failover; replication; using backup devices for load balancing; and using third party firms for offsite storage, operations monitoring, and short-term operations. Identifying resources that you now hire for short term consulting jobs as people to go to in case your own human resources are diminished was cited as an effective strategy.

Some areas of IT are now coming under more scrutiny for DR/BC. Information on the desktop that is important enough is being subject to enterprise backup, and encryption is being installed on laptops and desktops alike. In specialized cases email may be considered critical, but it is generally not included in the immediate DR/BC plan, and using a third party firm to store and forward the email can eliminate worries altogether. All the firms present use offsite storage through firms such as Iron Mountain.

The IT Executive Exchange (ITEE) is a group of IT Executives and College of Business Administration professors at The University of Akron that meets about every six weeks to discuss pressing and leading edge IT issues faced by IT executives. The purpose of this forum is to have a healthy exchange of ideas that will be useful to all attendees. It is sponsored by the Center for Information Technologies and eBusiness (CITE) of The University of Akron's College of Business Administration. For previous topics and summaries, refer to <http://cite.uakron.edu>

This summary was prepared by Prof. William McHenry, CBA, The University of Akron

Complete Summary of the Session

Disaster Recovery and Business Continuity: What Have We Learned?	1
Executive Summary	1
Complete Summary of the Session	2
SOX and HIPPA	2
Costs and Payoffs.....	4
BC/DR Architecture.....	5
Administration of DR/BC	6
DR at the Desktop Level.....	6
DR for Mobile Devices.....	7
Email Platforms	8
Third Party Providers.....	9
Offsite Backup and Storage	10
The Human Side	11
The University of Akron.....	12
Next Meeting	12

The purpose of this session was to share experience since the first time that the ITEE took up the subject of disaster recovery and business continuity on April 22, 2005. Since different people attended this time, it was more of a session about current practices and questions. Initial question: *How have things been changing for your companies over the past 2-3 years with respect to Disaster Recovery/Business Continuity (DR/BC)?*

SOX and HIPPA

One firm present said that prior to about six months ago, this firm had a company structure that did not make it liable for Sarbanes-Oxley (SOX). This has now changed—it is a wholly-owned subsidiary of a US-based firm, and needs to get up to speed on SOX quickly. This has been “quite a shock” as they begin to grasp what SOX means. (“We were rolling along fine until this monstrosity of regulations came along.”) The first step is pretty much documentation, then the actual continuity, planning and testing falls into place (“or at least that’s what we’ve been told”). Prior to the change, the firm’s BC was purely business-driven. They had documented plans that were tested occasionally, that they thought were good ideas. The groundwork has been laid, but what they have does not cover everything. They had to go into BC mode once. Things did not go exactly as planned (“they never do”). But they kept shipments going out the door, and it only lasted for 24 hours at most. After that they did the evaluation step, and evaluated how they did.

Another firm present was in its third year with SOX. They noted that three things have changed around SOX.

- Requirements of SOX constantly change. Where you thought you were last year may or may not be where you are now because of revision updates. Some areas are more lenient, others more stringent, especially in DR.
- Interpretation of SOX. For financial and DR you have to start by meeting the requirements of 310 and the internal audit. It can be an internal group in the organization or outsourced to an accounting firm that serves as internal audit representing the company as part of the SOX review. You go through the whole requirements and review at the first level for them to tell executive management, yes, you are meeting the requirement. Then the external auditor comes in with a different interpretation—requirements for proof can be completely different from what internal audit group required. So you go through this twice each year, at least.
- Impact of outsourcing when you move pieces that fall under SOX outside the walls. Not all systems you have will fall into SOX compliance. It's relevant when you are using financial and business driven applications. They don't care about an engineering application. As CRM and ERP applications are outsourced, that changes the view of the SOX requirements. In some cases it takes a big load off you, because now you require the supplier to provide the information to meet the requirement of the SOX requirement. The outsourcing firm (OF) provides a SAS 70 form for some of the information, but that's not everything. The OF will submit that and then the audit team will typically come back with more questions related to DR/BC that they want you to fulfill or the supplier to fulfill. In some cases it's a joint answer, e.g. communications, connectivity between the two—then become more involved in that answer. (This firm has an IT office in Asia that has not yet fallen under any requirements, because they use a centralized global application, run from a data center at the provider's space in the U.S.)

Another firm present has a data center in Europe. They have been told they are subject to SOX because the data center supplies services to them in the U.S. This data center does the planning for things such as hardware and software. The database itself is truly resident offshore. But the IT group here is responsible for the bigger picture, for example ensuring that products can still be shipped if the IT system goes down. The firm asks the European center for a SAS 70, and they say, SAS what? But that site does understand that there are requirements on the U.S. side. This center is owned by this firm. (Another comment was that they have to generate their own SAS 70s). This data center has not gone for British certification ISO 27001 (formerly BS7799, a standard about information security), or at least there is nothing about this on the wall there in the center. There are not any British standards about which this representative loses any sleep.

Who makes the revisions in SOX? Is it due to a federal agency, a regulatory body (like the IRS), and court cases?

Yes, yes and yes. The body that controls the regulations and requirements will give the updates, so at least it's channeled through one organization. Normally we don't get hit with localized or individual questions. This body is the Public Company Accounting Oversight Board (PCAOB).

Regulation is not just SOX. There are also similar requirements for HIPPA, but there are different end points. It also comes down to recoverability and security of HIPPA-related information, but the audit process required a different set of documents. This firm does not have a health-related business line. They had to do this audit purely because of the health-related information for their usual employees. HIPPA is government driven. It was not as hard and long as SOX, but it is likely to grow more odious in the next few years. It has to do with provision of personal information. If you have that need or ability, you are subject to it.

Another firm present does have some health-related business and also has been subject to HIPPA audits. They found it fairly similar to SOX.

Couldn't there be one body that could unify all this stuff so only one audit was necessary?

There are a lot of different bodies involved, for one. The opinion here was that there is too much money to be made in this field, and no auditors would propose this form of streamlining the industry. It would be way too obvious to do this. And the impetus for SOX came from abuses by public accounting firms, but now those firms have a perpetual revenue stream doing these audits. The same thing for HIPPA; there are folks making enormous amounts of money on these audits.

Costs and Payoffs

Have you made any estimates of the aggregate cost of these audits? Have you tried to translate that into percentage of revenue so there might be a benchmark for your industry about what percentage of revenue is appropriate to spend on this?

One answer: I haven't seen it. Agreement that this would be a good question to research. CITE could support faculty doing research like this. It would take a lot of digging because it is not a typical line item. It is buried and filtered through a lot of different areas. And would companies want to divulge it? You could add up what you are spending in hard dollars on the external auditors and consultants, but that's about it. Prof. McHenry pointed out that it is sad that this is yet another mandated change for which people do not have to make a business case or calculate an ROI. One firm said that they are not doing a business case for this because "it is not a decision." It is something that has to be done. The business case is being in business or out of business. Prof. McHenry thinks that is a deceptive choice. You can spend more or less and get more or less quality; there are choices between black and white.

The prudent way to go is to do a risk analysis, which is what one firm does when looking at security. One firm says: we look at security posture, risk assessment, and gaps; prioritize; determine needed remediation; and then remediate. We don't remediate everything. We make decision about accepting, insuring, ignoring, and paying. SOX and HIPPA have brought to light the need for BC/DR. Prior to that it was very hard to get executives to

understand why X amount of expenditures should go for nothing more than an insurance policy. That's how CFOs have seen it. They give you the "insurance policy" spiel. The executive level therefore has to drive BC, and DR should be driven from operations (the COO). Doing things like ensuring that manufacturing continues, sales continue, etc. all falls down to the Operations part of the business. That's where ownership of BC/DR has to be. The sales force can still function if the operations go away, but without operations you can't do anything.

This is correct, another person present commented, if you have a strong, formal operations segment. But if you don't... that may not be doable.

More and more companies are putting facilities under the CIO, because it is not just the hardware, it is the buildings, the security of the buildings, etc.

Have there been fewer disasters in the last few years since all this money has been spent on DR/BC, compared to five years ago?

You are asking if hardware has become much more reliable. Yes, it has. But the architecture is more complex. At the granular level we have higher reliability, but because of the complexity of the whole system, the fault tolerance has not grown appreciably. Fifteen years ago you had a mainframe and terminals connected by coaxial cable. DR was pretty easy. Now with workgroup and departmental servers, DASD farms, it is really complex.

Most companies will not publicize if they had a disaster, so you will never know if things are getting better.

One firm said: we have not had disasters so much as serious regional outages, such as when the NE Ohio power grid went out. That has forced us to execute subsections of the plan. We have had serious telecom outages due to construction. That's the kind of thing that has forced us to use the plan, and has raised the bar on the plan, and to test the plans more often. We try to test it 3-4 times per year. Infrastructure things are changing. If you don't test that often, you can have trouble.

BC/DR Architecture

One of the firms present has to supply SAS 70s to other firms because they provide services to them. They have invested in their own redundancy with a second data center, failover, and replication of databases. The T1 lines have to fail over. It is an arduous task to test the plan. They do it on the weekend and publicize it. They do not duplicate equipment down to the actual model. They have a primary piece of hardware with n+1 redundancy on every point. The backup infrastructure does not have n+1 to the nth degree. N+1 means that you have two of everything, so that if one goes out, the other one switches over. It means zero single points of failure. They have two firewalls, three ISPs, and dual generators. A network operations firm monitors everything 24x7 to keep watch for them for any outages. Because the idea of this architecture is complete replication of

the databases, they do not use it as additional capacity. Replication is constant, so they are only running what's on the primary machines. Virtualization helps enormously, which has its own stack of issues. It makes a virtual machine a unit that can be moved around with aplomb.

Another firm present makes use of some of their backup equipment for load balancing purposes. The idea is that equipment that is being used to a certain extent is in better shape, and you know it is better shape, than equipment that just sits cold there waiting to be fired up if a disaster happens. The cold equipment may be a little less stable.

Another firm present has a backup machine for the ERP system, but they use that for testing, development, etc. If they need it for DR, the other applications are stopped and it is utilized only for the primary application.

Administration of DR/BC

Is BC defined from the IT point of view, or is there a bigger perspective?

It's not an option to ignore the bigger point of view. This forces sponsorship of DR/BC out of IT. The last thing you want is to have it in IT. You need to have it at the appropriate executive level, and IT becomes the driver to accomplish what the BC says needs to be done. In prior years too many times IT took that on that entire responsibility and did what they thought was just right for DR/BC and it turned out it was not right by spending too much money on things that were not needed, etc. etc.

DR at the Desktop Level

One firm has had an exercise for more than five years where they try to identify every critical application that sits at the desktop level. The DR plan says how they will recreate the resource if it goes away. Sometimes this means recreating it from files. Sometimes for things that are really important they provide enterprise backup just for those applications. The important resource would get propagated to a central unit where it would then be backed up. This policy is pushed out to every information worker. For every critical item/information worker, it is usually taken to centralized backup.

Another firm is looking at this. DR is at various levels. A minimal DR could be a crash of a hard disk on an engineer's desktop. Aside from the recovery path, who is responsible, the user?, how does all that work? The cost of enterprise backup for all user devices is just tremendous. This is the new area that these service companies are trying to push. That's the new frontier as part of DR plans. Regardless of how hard you try to ensure that business critical information gets put into a centralized area that is backed up, you can't do it. So if you can't beat 'em, join 'em.

Is the cost of getting the information workers to identify the critical data, and keep this up-to-date, more than the cost of blanket enterprise backup? Have you made a business case for enterprise backup?

Without a shadow of a doubt, it is less. Backing everything up is far more expensive. As far as the business case, it's more of an intuitive thing. One representative preset said: we have the process down, and the cost is some human effort, a schedule, a cycle, and enterprise backup would be a lot more money. This costs less than a full FTE, whereas enterprise backup would cost more than 10 FTEs.

DR for Mobile Devices

Especially with a remote sales force this is an issue. iPods, iPhones, etc. are becoming important to business continuity. There is stuff on them that is as important as what's on a laptop, desktop, or server. Text messaging with mobile devices is a way to get messages out if other parts of the infrastructure are down (as opposed to fax).

This is another new topic, not only how to do BC/DR, but also the security of IP. With as much information as these devices can hold, it's wide open as far as what can walk out your door, and you have no idea. One representative said: our sales area is starting to ask about this, this, and this. Especially if you are global, and in Asia. With all the reverse engineering, you have to be concerned about the "buddy plan"—people taking your technical knowledge and becoming your "buddy" whether you want them or not.

Do you have a policy on encrypting hard drives on laptops?

One firm stated: yes, part of our recent intense security review over the last 6-12 months was about all our IP. We have started that, and we are almost finished with a full hard disk encryption on all laptop hard drives for the global organization. We are using a firm called Utimaco. Their product also permits you to put LoJack in places where the police can be trusted to help, which is generally not the case in Asia. If it is lost in an area where you cannot count on the police, then you can send commands to destroy the hard disk. The minute the laptop boots and they try to sign on to the Internet, you can send this command, and even if they sign off, when they sign on again, the destruction continues. The good side is that these are becoming commodity products at a cost of \$60-100 per laptop that runs on the BIOS. Even if someone removes the hard drive and puts it into another device, it still will not work. Our engineers do worry about whether it will hurt the performance or how the applications run on the laptop.

The next level to consider is unattended offsite locations, such as sales offices, that do not have security controls (guards, watchmen). You better consider encrypting the desktops there. Everybody and anybody loves to break in offices and steal desktops because they are easily moved on the black market, they bring a pretty good price, and everyone from drugs users on up are more of a threat to you than somebody trying to steal IP. However,

if they put it on eBay, it's now open to whomever wants to buy the unit, and that's where you get into IP questions.

Do you have situations where a disk gets encrypted and then because of some glitch, you cannot get information off it? Or does the backup plan make this moot? We have had some professors even in the Department of Management who have booted their laptops, which have then become stuck after the PointSec encryption is launched, and some have had a tremendously difficult time getting their information back.

You can backup encrypted devices to unencrypted devices. We have three hundred laptops and have not seen this. Lenovo laptops have the fingerprint scans and the encryption software interacts with that, so everything runs off the scan of the fingerprint. It does put in an extra step in the bootup process, but you can go around that, just like LDAP, for single sign-on, if it is at the BIOS level.

Email Platforms

Are email platforms now considered a part of the DR plan?

One firm stated: we would not consider normal email critical, but what we have incorporated with email is that we will run nightly reports from the ERP system and store them in email boxes for retrieval the next morning. That's part of the DR plan. So if we lose the mainframe we go to the email and pull the reports to see what you are supposed to ship and manufacture that day. So that's part of the plan, but normal email we do not worry about for the first 8-24 hours.

Another firm: email was once way off the radar screen for DR, but it is moving closer and closer to something that we have to provide for in the case of a disaster, because so much business gets done over email.

Do you encrypt emails to protect their confidential content?

Not so much in the way of content that is sensitive. We would not send sensitive information unencrypted. But the customer service type information, from all the customers we deal with, when they send an email, they expect us to get it. That expectation is becoming more and more critical. You almost have to re-evaluate the recovery time for the email function. It used to be two days, that was probably OK. That's not getting acceptable any more.

It's also how you deploy email. Is all the store and forward going on in house, or are you using a service. We have a service that holds all the emails in a queue if they cannot be sent on to us, which vastly simplifies our job. Another firm: we do the same thing. That also helps with SPAM control. If your site goes down, the emails will not all bounce back, they will store. That also gives one more level of virus protection, because they use a different platform. That's money well invested.

If someone comes up with a heretofore unknown type of virus, will it cut right through their facility and mow them down, then mow you down? Or would mowing them down stop things so that it would not actually get to you?

If it is undetectable it will get through to us. But the technologies for finding viruses are getting better and better. They are not just signature-based but are capability-based. The days of signature-based only virus detection are over.

Third Party Providers

Is anyone using third providers such as Sunguard? IBM? As a part of the DR program?

One firm: yes, at our European center we have a contract with a hot provider (e.g. if there is flooding). We have a contract to go into the hot site and put everything on a similar machine. We test it there once a year. Tests have gone very well. From UNIX mainframe and Windows apps, they can handle everything. Because that European center is so important to us, we have to have something to bring it back up. We can get that turned around in 8 hours, all the network connections, lines to all the other sites. If we lose one site we can get through it (e.g. by using faxing of documents), but this is the central site and cannot go down.

That's awesome. Are they running warm for you or cold?

That's a good question. Not sure. If they use those for other purposes, I don't know. But we go in there clean.

Does that include any data warehouses? You're not going to load a data warehouse in eight hours.

No, this is critical systems, transactional stuff, to get your business moving. We're not going to worry about peripheral stuff, for example, customer complaints.

What about prioritization of your needs? If there is a disaster in the area a number of firms may have claim to those machines. What guarantee is there that you'll get the equipment? Are they oversubscribed?

Of course they are oversubscribed.

Are you sure you'll get the priority?

We have a contract that says so. We have never had to use it "in anger." But that's a big part of their contract. The Sunguards of the world have footprints around the world. So for any one regional disaster they have to be prepared to handle all the clients in that area.

That question comes up any time there is a disaster. It becomes evident that they have a lot of bandwidth to be able to sustain a pretty large regional disaster. They have to be able to do it.

Another firm: We looked at Sunguard, and then we started building our own infrastructure. We had 18 locations and found it more cost effective to leverage those locations. Our objective was to limit down time to one hour. One hour recovery time with a Sunguard is really, really pricey. You have to have full replication for this, which is really expensive.

Another firm: We use Sunguard for some internals. I tend to lean to your approach because the time to continually review that and make sure that the Sunguard contract is where you are at—since you are constantly changing your infrastructure, servers, etc.—is a large effort and it is easier to have your own infrastructure for this.

How would a firm with centralized IT get order information out to sites that are shipping product during a disaster?

One firm: most is centered out of a single shipping site, so that's pretty easy for us, but this is changing, and we will have to update our method when we widen the places from which we ship. As long as there is electricity, you can fax to other sites. Texting to mobile devices provides a means of getting information there, if the satellite is not down.

Offsite Backup and Storage

One firm says: in our plan this takes place every day for the Windows stuff, and at the ERP data center they store it offsite. We believe that our process will quickly return what we need, but we have rarely ever had to invoke it. If someone loses a file, then how critical is it really?

Two firms mentioned using Iron Mountain as their service. Iron Mountain comes each day and they take a box of tapes, bringing back the box tapes you should use for the next day. One firm says: we've only had to ask for tape one time because we use disk storage as the first line of defense. On disk we have day and month windows. Going to tape hurts. It's really slow and not perfect. Our real critical stuff is replicated every few minutes to another site.

How expensive is Iron Mountain? Can small businesses use it?

One firm: we've been doing it for five years and I can't remember seeing how much it costs. It's small enough to be off the radar screen. It's probably on the order of \$500 per month. Another firm would say their's is not even that high. They pick up and drop off from multiple locations. The tapes are housed in an environmentally protected place. They know what to take and bring according to the schedule.

What if a malicious insider inserted small but significant changes in source systems over an extended period of time that went undetected, until all of the backups going back for months or years, were in essence “infected” with the changes, and no clean copies existed anymore of the source data? Could you handle this? There was a case like this at Encyclopedia Britannica.

One firm: that’s a tough one. It depends on the backup schedule and how many generations of tapes are out there at any one time. We have a year-old tape offsite, and actually we have four years. Another firm takes a snapshot every quarter and stores it outside the rotation. They say: that would be our only protection. It’s not going to help for the ERP system, because you would never want to go back to the accounts payable from three years ago, but it would work for static files. [In this case the files were not static, since legitimate changes were being introduced at the same time as the illegitimate ones. Thus recovering from the malicious insertions meant giving up the positive changes. The only solution was plea bargaining the guy to where he would find all the changes and reverse them in exchange for a light sentence.]

Encyclopedia Britannica should have had a stricter version control system, where every change was tracked like software code. That IP is what they are, so they should have complete version control. There are layers of separation. Technology exists to help that. [It may not have existed at the time of this case, 20 years ago. The broader question is how to you plan DR for the case of a malicious insider]. It depends on the length of time that the person is doing it for. He would be detected pretty fast. [What about a bumbling insider?] If they are big enough mistakes they will be discovered pretty quickly.

The Human Side

What about the human side of DR? How are you preparing?

From a straight IT perspective we have not really addressed this. At a seminar I attended that pointed this out. The fear factor at that seminar was bird flu. It would affect 80% of your employees with a fatality rate of 50%. (This is projected in the worst case scenario.) If you lose your employees you will be in just as bad a situation.

Prof. McHenry: I can tell you what one of my Russian friends said [actually, it was an American ex-patriot in Moscow who has his own firm doing software offshoring]. Move the people to an old nuclear silo in the Siberia/Arctic area. The cold would kill the virus and all their people would survive.

It does not even have to kill the employees. If there is hurricane or another disaster and the people become so engrossed in putting their personal lives back together, they cannot work either.

One firm: we don’t necessarily have the perfect solution, but in conjunction with HR we have looked at functions, people, etc. in a matrix (functions, skills, knowledge) and try to

ensure that everyone has at least one other person that can do parts of his or her jobs. At the third level we look at third party relationships that can augment our skills, which is in our DR plan. We constantly update that. For example, we may have people trained to a level 5 on a scale of 1-10 on an application. Every so often we need help from someone who is a 5-10. We know who those 7s and 10s are, where are the top three place to go. They help with augmentation or complexity, but we can't afford a 10 all the time. At the time of a disaster, we could recruit some of those people to provide the 1-5 services for us while our other people are not available. We keep current with such people informally, at trade shows, through the grapevine, when we hire them. We do not check up on them in any systematic way. We have a lot of data centers so we have some redundancy as well. The HR side of it is not really part of the DR plan, but the listing of the people is. We don't have a database of our contacts with them, but when we review the DR plan, we review these people, we know with whom we have interacted within the past 12 months.

How often do you visit every corner of the DR plan? You could spend your entire work time just on this.

One firm: it sounds like a lot of time, but after you have been through it a couple of times it really isn't. You have different scheduled events each year that you know you do.

Another firm: As a global manufacturer, I think we would benefit from having a full-time person dedicated for auditing and separation for global DR. We are a large firm, flung far and wide at 25 locations. Every location has its own habits and customs. That creates a lot of complexity. This person would visit these places. Just to keep every PC updated with antivirus software is a thing in itself. Yes we push out the updates, but people may not hook up for two weeks to the network because they are on a sales call. It's like herding squirrels.

The University of Akron

The university environment has also changed in recent years. There have been bomb threats just recently on campus. Student may now sign up for alerts that will be sent via text message to their cell phones. Prof. McHenry pointed out that a story about one of the threats stated that the email about the threat was received on Saturday but not opened until after Labor Day, on Tuesday morning. He expressed distress that such email communications were not being monitored.

Next Meeting

The next topic will be "virtualization." (Virtualization permits the creation of "logical" operating systems/servers, storage devices, and networks from resources in order to free IT architectures from specific physical underpinnings.) Date: November 9. We'll have a networking lunch from 1:00 to 2:00 and discussions from 2:00 to 4:00.