

## IT Executive Exchange

### E-Discovery: IT's Responsibilities for Information Retention & Destruction

#### Executive Summary

This session was a rich examination of the need for a document retention and destruction policy, for understanding new Federal rules pertaining to the discovery and provision of electronically stored information (ESI), and for understanding how those rules may apply in specific cases discussed by the participants. The concepts of “claw back,” “quick peek,” and “safe harbor” were explained. Safe harbor means that if you are following your policy in good faith, you should not be held liable for information that is not recoverable. This changes when a lawsuit starts or is known to be imminent, at which point you should put a “litigation hold” on the destruction of any relevant ESI. The usefulness of a litigation toolkit, which provides templates and procedures for what to do when a lawsuit arises, was also discussed.

After a detailed examination of these issues by invited speaker E. Stewart Moritz, participants discussed many questions and practices surrounding e-discovery, document retention, and backup policies at their firms. Being prepared for litigation means understanding where any and all data are stored, which includes understanding the official and de facto ways that end users are storing data. With storage needs exploding, adding another requirement that suggests defensively storing “everything” could be prohibitive. New technologies may make pinpoint storage and extraction more feasible, leading all the way to a day when retention and destruction gets folded not only into information life cycle management, but knowledge management more generally. Lawyers do not necessarily understand these technical issues, so it behooves IT to be ahead of the game and engage with the lawyers to put policies and practices in place before lawsuits arise.

*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

E-Discovery: IT's Responsibilities for Information Retention & Destruction.....	1
Executive Summary .....	1
Complete Summary of the Session.....	2
Introductory Remarks by E. Stewart Moritz.....	3
Claw Back.....	5
Undue Costs or Burden.....	6
Safe Harbor .....	6
Litigation Hold.....	7
Litigation Toolkit and Data Maps.....	11
Stories and Discussion by All Participants .....	13
Length of Retention, Backup, Central Server vs. User Computer.....	13
Responsibilities for Retention of Clients' Information.....	14
Instant Messages .....	14
International Law .....	14
Encrypted Information.....	14
Other Forms of Data .....	15
A New Paradigm Needed for Pinpoint Backups.....	15
Public Sector; Keyword Watching; Information Life Cycle Management .....	16
SPAM.....	17
Emails, Changes Between Back Ups .....	17
Role of User Discretion; Similarity to Paper .....	18
Purging the LAN and Long Term Retention .....	19
Disaster Recovery vs. Backup; Tape vs. Disk TCO .....	20
Need for Knowledge Life Cycle Management .....	21
Better to Retain More or Less? .....	22
If You Have It Stored, It May Be Subject to Subpoena.....	22
How Well Do Lawyers Understand Where Data Is? .....	23
Assuming You'll Need Images of Personal Drives; Disseminating Policies .....	24
Nuances Related to Hosted Services.....	25
What About Users Working on Company Stuff on Home PCs? .....	25
Obsolete Hardware; Older Software Versions.....	27
Next Meeting .....	27

The purpose of this session was to explore the responsibilities that I/S executives have for the retention and destruction of electronic records in light of new Federal regulations regarding the discovery of electronically stored information. Although this topic sounds narrow, we discovered that it touches on many core CIO activities which may be encapsulated by terms such as Information Life Cycle Management and even Knowledge Management. We began by hearing about the specific provisions of the new regulations, during which many questions arose about specific practices and policies. This led to a broader discussion of the ramifications of these policies and provision of critical infrastructure more generally.

### ***Introductory Remarks by E. Stewart Moritz***

We began the session with an introduction by U. of Akron CIO Jim Sage, who handed out some materials from Gartner relevant to the topic. He noted that the University has a license to share this copyrighted material with “guests.”

There followed a short presentation by E. Stewart Moritz, Associate Professor at the University of Akron School of Law.<sup>1</sup> Prof. Moritz has wide-ranging experience in private practice (California), with the court system (clerking with a Chief Judge in the Court of Appeals for the Sixth Circuit, Nashville), and at several academic law schools. He was selected as outstanding professor of the year in 2006. He serves on several university committees related to information technology (I/T), and typically has been the lawyer in the law firm who actually talks to the I/T people. Prof. Moritz emphasized that he is not licensed to practice law in the state of Ohio, and that nothing that he said during the presentation should be construed as legal advice.

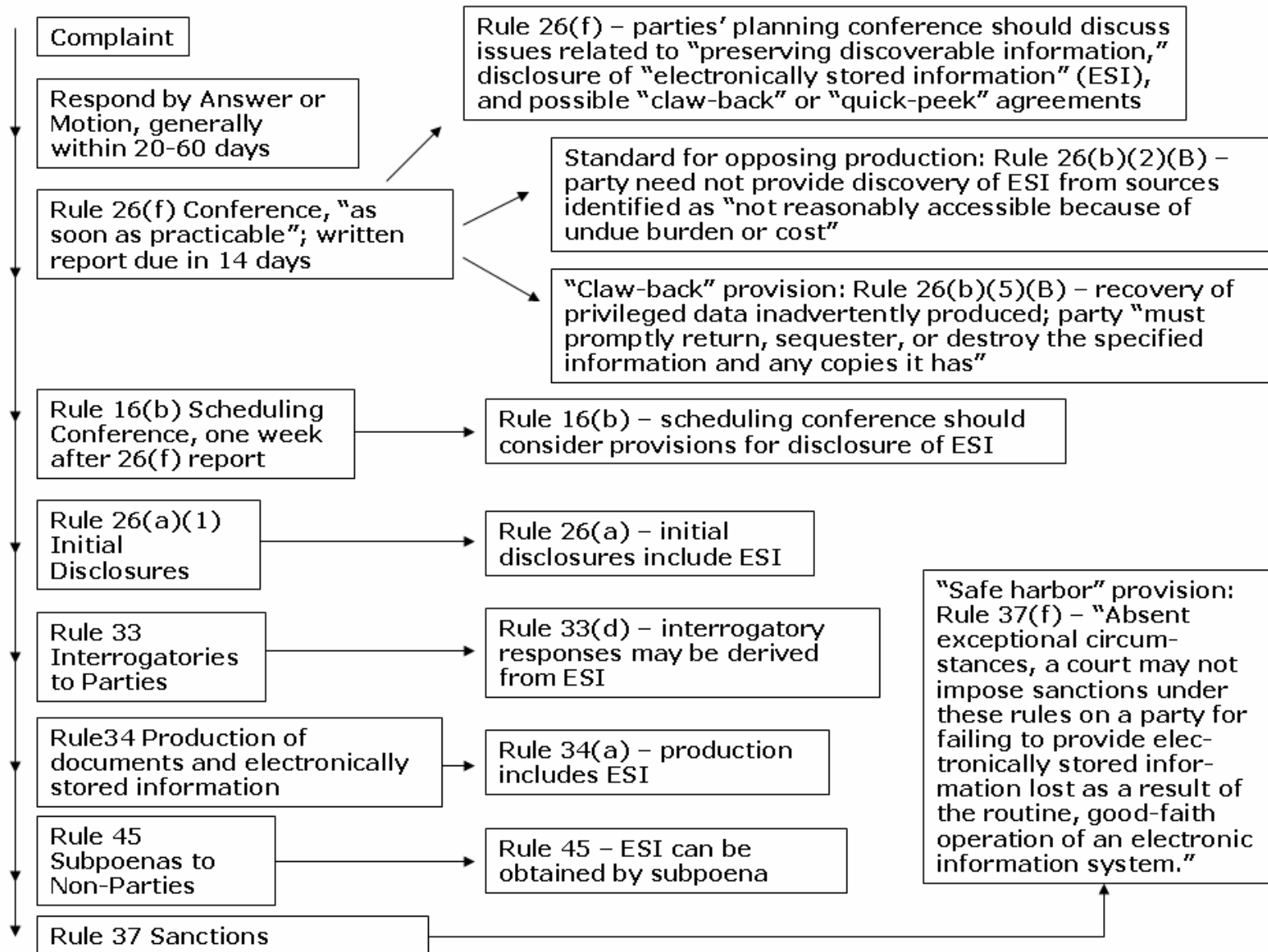
He began by explaining the process of “discovery” (that is, information gathering) in a federal lawsuit. This is laid out in the left-hand column of Exhibit 1. After an initial complaint, a defendant generally must respond within 20-60 days. An informal “Rule 26(f)” conference is then held between the lawyers for both sides (without a judge) at which each side lays out how it sees the case, how the case will be managed and organized, and what information it thinks it will need to discover in order to proceed. The parties issue a joint report, the judge resolves any conflicts in the report, and sets a schedule for what will happen (the “case management plan”). At this point the basic outline of what discovery will happen has been set. In fact, only 1.4% of the federal civil cases ever go to trial, with the rest either being dismissed, settled, or otherwise disposed of ahead of time. Other than cases dismissed “on the pleadings,” however, even cases that do not go to trial have the potential for discovery.

Under the rule requiring initial disclosures (Rule 26 (a)(1)), each side must give to the other side the basic information that it is going to use to support its claims or defenses, including electronically stored information (ESI). This happens very early in the lawsuit. Turning over documents that may rebut the other side’s claims comes later. After that the lawyers get to determine the course of discovery, subject to the case management plan, so the exact sequence of events regarding what information is required and when it may be turned over varies from case to case. Usually there are a series of questions

---

<sup>1</sup> <http://www.uakron.edu/law/lawfaculty/moritz.php>

Exhibit 1: Overall Process With Additions for Electronically Stored Information



(“interrogatories,” Rule 33), and they may come to IT regarding what is stored and how to get it out. An example: Moritz worked on a case in the late 1990s involving Novell GroupWise; to get the information out of the archive required rebuilding an image of the actual email structure (hence they called it GroupStupid).<sup>2</sup> IT may get questions at this point about how information is stored and what it will take to get it back. There may also be a request for production of documents or ESI. Even if you are not party to a case, you can still get a “Rule 45 subpoena,” which may require producing ESI for someone else’s case.

About half of the people present had been involved in a lawsuit!

While courts had been making *ad hoc* rulings on the discoverability of electronically stored information (ESI) since the late 1960’s, it was only with the adoption of revised Federal rules in December 2006 that many of these precedents were formalized. ESI has been happening at least since the time of a 1969 anti-trust case involving IBM. When Moritz was in private practice in the 1990’s, it was handled more informally. The columns on the right in Exhibit 1 show specifics about the most important provisions relating to ESI. Each stage of the process now includes specific provisions for discovery and provision of ESI.

## **Claw Back**

One of the chief concerns of lawyers is about revealing privileged information, i.e. information that should remain secret because it falls under client-attorney privilege, represents trade secrets, things the attorneys prepared for a litigation (“work product”), etc. (They don’t care so much about embarrassing emails.) Since ESI can involve massive amounts of information, it becomes more likely that privileged information may inadvertently go out. (With paper, you might have a young associate going through boxes and boxes for months to eliminate anything privileged. For a case with American Honda, they rented a whole building in Boston and spent three years going through more than six million pages of documents to find out which were privileged and which were not. That’s not many terabytes. ESI may involve much more.) If any of this information is inadvertently revealed during discovery, “claw back” rules say that the party that revealed it may get it back, and the party that accidentally received it must give it back, destroy copies of it, and not take it into account (Rule 26 (b)(5)(B)). Both sides agree to this ahead of time because no one knows who may make such a mistake. “Quick peek” (Rule 26) says we’ll let the other side look at all the raw stuff ahead of time, without our review, but if they find anything that is privileged, it must immediately be removed. The concern is that once information leaks that was privileged, it is no longer privileged because it is out there.

Under Rule 33(d), where a response to an interrogatory “may be derived or ascertained from the business records of the party,” the party has the option of just dumping such records to the other side. This now includes electronic information. But good lawyers won’t often do this, because lawyers want to know “the answer” ahead of time; dumping raw materials leaves too much to chance.

---

<sup>2</sup> Prof. McHenry experienced this firsthand when he moved from Georgetown to U. of Akron. Although all his email in GroupWise was provided on DVD, the client he was given that supposedly could read it did not work, and he effectively lost it all.

## Undue Costs or Burden

In some sense, Prof. Moritz said, the new rules favor the defense side. The defense “bar” did a better job of making its case when the new rules were adopted. These rules came out of many years of practice as the courts struggled with how to accommodate changing means of storage and retrieval of information over the past four decades. Electronically stored information at the beginning of discovery is deemed either “accessible” or “inaccessible” *by the party that owns the information*. So the plaintiff can ask for all the documents pertaining, for example, to a product, or that were generated by a department, and some are stored on crumbly disks 100 miles from here and it’s going to cost \$1M to resurrect them, then they may be deemed inaccessible. You only have to respond with accessible stuff. The plaintiff can then say, but we think it’s accessible, and then the parties go before the judge who decides. The judge may order the requesting side to pay the cost of accessing it. You would not want to go forward with a \$100K lawsuit if getting the archived materials will cost \$300K! So with the new rules, this argument is very express now, gives the defense the chance to cull out a lot of information.

[The rules are only five months old. Have there been any precedents yet regarding how judges are ruling about what constitutes undue burden or undue costs?]<sup>3</sup>

There are a bunch of precedents from before the rules went into effect. These rules in a sense codify existing practice. Courts have had to deal with these issues. There is another provision of Rule 26 (before it was renumbered) that had a similar argument about any kind of material. But the new wording for ESI makes it easier to argue that information may be inaccessible. The inaccessible concept is new. As far as I know, there are no suits on that yet. Five years is more likely than five months for forming a body of law about it.

Another one that matters is that if you forget to mention provisions for claw back, the court puts one in for you! This helps the parties being sued, because they are the ones who produce the most information and are thus more likely to produce something privileged. But even though the automatic claw back provision forces the other side to destroy, give back, ignore, etc. this information, it does not deal with the sticky question of whether or not having inadvertently produced it waives its status as privileged (a hard argument to win). This has to be argued before the judge despite the claw back provision. So you are better off creating your own, more comprehensive claw back clause to begin with, with a specific anti-waiver-of-privilege provision.

## Safe Harbor

And this is extraordinary! There is a safe harbor provision that is the most important thing we are talking about here. “Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system.” “May not” is a command—it is not optional. The “electronic information system” is the implementation of

---

<sup>3</sup> In this part of the document, questions or comments from any other participant are in hard brackets, and statements without hard brackets are from Prof. Moritz. Mostly this is paraphrased material; direction quotations are not indicated.

your electronic document retention policy (we always knew it was the document retention and destruction policy, because in practice you also do want to get rid of some documents). So as long as you have a retention plan in place that's regular and you are running it, and something is destroyed in good faith, you are OK. Once you know the litigation is commenced, then it is harder to argue that you destroyed it in good faith. But if someone doesn't get the news or something is left out and gets destroyed, this rule provides a good measure of protection. Prior to the new safe harbor provision, there have been cases that have ended up awarding over \$1M in damages in sanctions when electronic documents have been inadvertently destroyed. Maybe even more important is actually directing verdicts on the merits (there was a \$1.4B case involving destruction of documents in Florida like this where there was an instruction on the merits that led to a jury verdict). It means you have to have a good document retention policy.

[Does the policy have to be in writing?]

Yes—I mean no. Everything in litigation that is interesting does not have an exactly clear answer. I can say, no it does not have to be in writing, but then you have to make a harder case that there was a policy that was known and transmitted orally. I may win, but if you want to know you're going to win, you put it in writing. It's almost never that you completely lose, you could bring in people to testify that this is how we have been doing it. Here's testimony that we have done this this way for ten years and blah blah blah. But better to pull out a paper and hand it to them. You don't want to be the one arguing this before the judge.

## **Litigation Hold**

The process just described of not destroying anything once you know there will be litigation is called a "litigation hold." (This concept and the remaining concepts covered by Prof Moritz are outlined in Exhibit 2.) Once you have a reasonable anticipation that you may be sued, e.g. someone dies, someone is seriously injured, you release confidential information about an employee—you don't have to have a lawsuit filed yet. If you can reasonably anticipate one you have to start working. You suspend the retention program to prevent the loss of information if that information is subject to a preservation obligation. If you don't you may lose your safe harbor, and Rule 37 sanctions may be levied.

[So for example, with the recent Va. Tech. shooting, the IT department would have reasonable expectation of some lawsuits and would put an immediate hold on any emails or other documents that could be related to the case?]

Absolutely. For sure. They have emails backed up on lots of servers.

[So at that point you have to stop your retention policy?]

Well it can be more focused than that, what you have to make sure is that the stuff that might be reasonably needed in this litigation. It does not have to be everything. It is so dependent on the kind of case. If it is an accident case it can be fairly confined. Although emails you never know. Email is a big tough one. But it is easily searchable text, which is an advantage. You try to confine it as much as possible. If you do that in good faith and something gets destroyed, you should be able to argue—of course, even if you do it in good faith, if you are really stupid, it's going to make you look like you did not use good faith.

[Specifically for professors, but this may apply to any low level employee. Let's say I have a case where I am accusing a student of cheating, and know this may make its way to the university level, there may be a lawsuit, who knows the student may be kicked out. Is it my responsibility to send an email to the University CIO Jim Sage saying hey, there may be a lawsuit going down the road, you have to capture any email that goes with this case with this student? In other words, are individual employees also responsible for alerting people that a lawsuit may be coming?]

(Emphasizing that this is not legal advice...) You would want to talk to the lawyers right away and get IT involved in what needs to be done. This probably would not impinge on the general retention and destruction policy. They may come back to you and say specifically: don't destroy anything on your hard drive or your email or from your or our Outlook server. You need to go up to them right away, that's why you need to have a "litigation hold" toolbox (see Exhibit 2). So you, the professor, should not have to make that decision. The toolbox gives guidance on what to do under various scenarios and provides for ready policy to implement when they arise.

[In an IT environment we're doing backups related to disaster recovery. We have a global backup to record everything and retain everything. I would assume this is not the time to start filtering what I am backing up and what I am deleting. Once I have a hold on anything it implies I have a hold on everything]

It depends on your system. I think that's right. At some point that can get too expensive. Let's say you have tapes and you recycle them every two months. These things are expensive. You might push that out a little longer and buy some more tapes, but at some point it becomes too prohibitive. And if the system kicks back in and there's no efficient way of culling that information out, then (talk to lawyer but) that could be a balance the court strikes because we can't make them do that because it's too expensive, and even if you offer to pay we're not going to do that. Or maybe they will offer to pay and they'll buy a new backup tape.

[So from my team standpoint, the employers would say: this is the destruction cycle that will take place unless you give us any other instructions.]

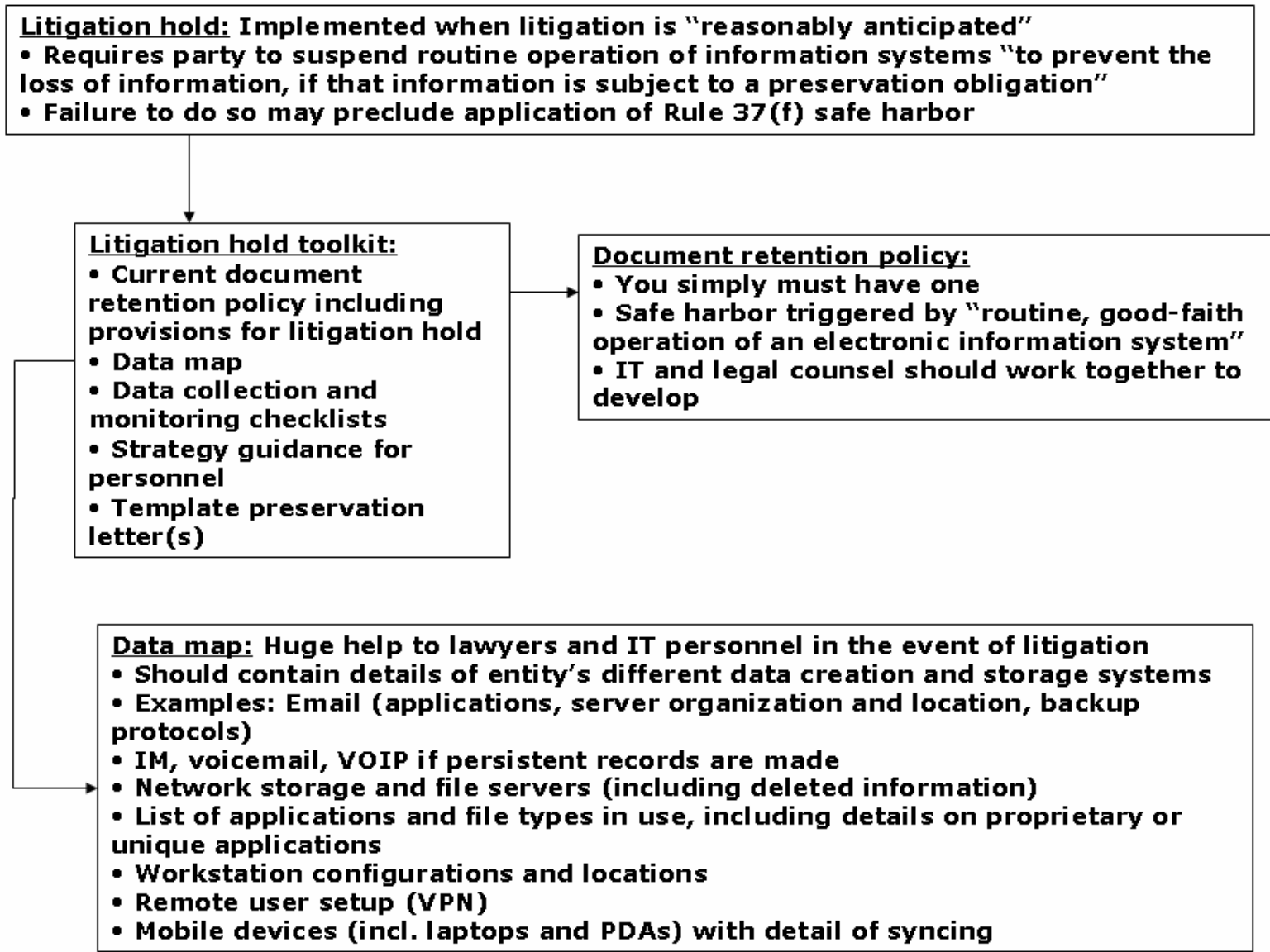
Yeah, it's really important that everyone know exactly what is going on. Sometimes you have to very patiently explain the technological constraints to the lawyers in the most simple terms possible, because then the lawyer has to talk to the judge, a 65-year old man who does not handle this stuff very often. It requires tight coordination. Not that the lawyers should make all the decisions, but have the necessary information.

[Jim Sage (CIO): As another example we have some litigation between two parties on campus, and what we do is capture any activity going in and out of those email boxes, we capture. And set it aside. That came down from legal. The issue went to legal and came down to us. Any activity between these two parties or any in and out of those mailboxes we have to capture.]

You may have to be creative like that. If your regular system is a global backup, you may have to set up something separate—at \$369 per terabyte now for a hard drive you can buy one and set something up fairly cheaply, that might be something that is reasonable to meet the requirement. It is all about adapting to the given situation.

[Does the good faith provision put me as an IT person in the position of having to try to get into the mind of the lawyer and figure out what they may or may not ask for in the future? So I say oh they will want email and delete everything else. And that's not right...]

Exhibit 2: Litigation Toolkit, Retention Policy, and Data Map



You have to have at its base a retention policy that says we delete email after three months, we delete every document after a year, these documents we save. If you just preserve the email and delete everything else and it was not part of your regular policy, then that's a problem. If it's part of regular routine, then it's very much up to your lawyer to be on top of this. A lot of lawyers don't understand this. You may have to make sure they do. Ultimately they're going to determine the scope of the claims, what type of documents are needed, with your help about how to get them. You don't have to litigate it.

[So if we reasonably anticipate that litigation may be imminent, it's our responsibility to prevent lost information...]

It should be your counsel's decision...until you actually hear from your counsel, you should be fine. You don't have to read the newspaper and decide...that's not a decision that has to be made at the IT level. Based on some of the cases out there, it may be more like when counsel should be reasonably anticipating,. But if you know about something you should be on the phone to your lawyer, i.e. an accident or an injury.

### **Litigation Toolkit and Data Maps**

It's important for you to have a toolkit. (See Exhibit 2, based on the Anderson white papers).<sup>4</sup> The suits happen very quickly and you need to get rolling, so you need to make sure you have a document that specifically addresses what are we going to do in the case of litigation. Data maps are so important. You probably have these anyway, but you have to go over with your attorneys about where all this information is. It's underground somewhere, it's in this form, it's not machine readable without this. So you have mapped out where it is and what you have to do to get it. Attorneys should help you prepare what you have to do to collect the data, have a checklist to show you have used good faith, and a checklist for monitoring so you walk around two weeks later to show that the data are still being captured. Because not everybody gets the memo. The lawyers should draft something to let everyone know what is going on, a lawsuit is going on, this is what we are going to do, etc. And then they should tell you what to send out to the employees, what to say to the other side, etc. Templates provide immediate availability of such documents.

Referring to Exhibit 2 again, you have to have a document retention policy that deals with ESI, if you don't have one. Safe harbor is all predicated on that. Your legal council is mainly responsible for it, but you're going to have to help them a lot.

[Is there any case law yet about retention of e-mail? Some people say we're going to delete it as soon as possible and others are keeping it forever.]

In our context at the University there are actually state laws that require stuff to be held for a certain period of time. I am not an Ohio lawyer; I am not aware of that in private practice—it's more determined by you based on your investment and what you want to spend on it. You don't have a state records law that says seven years you have to keep everything. I remember

---

<sup>4</sup> <http://www.lexisnexis.com/applieddiscovery/> Whitepapers and articles, including: Christopher Anderson, "Applying the Legal Hold: Tips for Preserving Evidence in High-Stakes Litigation"; "Electronic Discovery Best Practices: The Secret to Success" and "Elements of a Good Document Retention Policy"; Michael R. Arkfeld, *Electronic Discovery and Evidence: Best Practices Guide* (Law Partner Pub. 2006); <http://www.law.cornell.edu/rules/frcp/> (Federal Rules of Civil Procedure); Shira A. Scheindlin, *Moore's Federal Practice, E-Discovery: The Newly Amended Federal Rules of Civil Procedure* (Matt. Bender 2006).

when this started happening and we started litigating these cases, one of the first thing our firm did was to create a policy for ourselves. We made it very quick—if you didn't designate an email for storage by moving it to your own system, it was gone in a couple of weeks. That was perfectly legal. That's kind of tight, when it might destroy some people's email when they are not keeping up with it. That would be a disaster. Some of the professors at the law school have 4,000 emails in their inbox.

[So as long as you are following your stated policy...]

Again talk to a lawyer to make sure that there are no applicable laws in your industry. There could be security laws requirements. In general, that's fair for a private corporation.

[I was involved in a case in Cleveland two years ago and we brought in an expert witness. The firm said basically what you said: people who use their own email clients and store it on their system, that was the permanent storage. They only kept things that had not been taken from the email server yet. So if you went on vacation for a month your stuff would still be there but as soon as you grabbed it, it would be gone. The court decided that was perfectly acceptable.]

Once the litigation hold happens you have to put all of that stuff on hold. But all the stuff that happened beforehand, that sounds right. Some courts are going to order you to pull all those hard drives and get all that stuff off, and that could be expensive. That could be very possible depending on the size of case, in some cases the plaintiff would certainly say "we'll pay for that, no problem at all, we'll just look at the hard drives."

[Prof. McHenry: I don't know if I am violating any policy but I have an external hard drive at home to which I back up the contents of my university laptop. Does that mean that the lawyers could argue that they can go into individual homes to get information? What about the 4<sup>th</sup> Amendment restriction on searches and seizures?]

Well... At some point it might be, but it depends very much on your place in the litigation. The standard for discoverable information is whether it is likely to lead to the discovery of admissible information. So at some point if the lawsuit is not involving you the likelihood that it will lead to discovery of admissible information from you is slim. That's a limitation that is built right into Rule 26(b). That's more fundamental than "it's too hard to get to." It's a fundamental part of what you get to discover and what you don't.

[You mentioned that his personal equipment can be involved? Does it make a difference if it's the person's own equipment?]

Yes, if he is personally involved in the lawsuit, then it's not going to make a difference to the person bringing the suit. If he is a party, or the school is a party and he is a main person in the lawsuit, they can get a subpoena for a non-party or a document request for a party, and they will easily be able to get that, just like they can get your papers. They're not going to get the drive, they're going to ask you and counsel to go through the drive and pull out what is responsive to the request.

[Prof. McHenry: Think about the fact that up until this moment, none of you knew from your data maps that my hard drive existed at home. So you may not be able to have a reasonable data

map for where all your data is, depending on whether or not your employees can move it places that you don't know about.<sup>5</sup>] [USB, Flash, ...]

So the data map shows a lot of different places data may be. Prof. McHenry's hard drive, the Palm in my pocket (I don't even know what's on there)... there's so much stuff that you're responsible for. So you have to brainstorm about all the places the data are.

## **Stories and Discussion by All Participants**

*At this point we made a gradual transition to a general discussion. All discussion threads are shown using bullets, with the original speaker always at the initial level and other comments, by one or more speakers, indented underneath. Rather than summarizing the information given, the more or less raw exchanges are reproduced in order to present the maximum amount of information. Comments by Profs. Moritz, McHenry, and Vijayaraman, and CIO Jim Sage, are explicitly identified. The text is broken up by subheadings, but these subheadings do not necessarily capture all the concepts being discussed in each question-answer-discussion exchange. There is some overlap and redundancy. Most statements are paraphrased, but with enough of the original preserved to get as many nuances as possible.*

### **Length of Retention, Backup, Central Server vs. User Computer**

- In our case we were in litigation 18 months ago and finally came up with a retention policy. I have been there for longer than 10 years and have been saying we needed one for almost all that time. One of the things that came up was about how users can create archives with Lotus Notes, the product we use. We never really trained the users to create archives. Some figured it out. We're like every other company, we have people with 2 GByte email files. We decided not to show people how to do archives. So everything is on the server, and now we have a retention policy, so that quarterly if it's over a year old, it's gone. Legal wanted to do that in 90 days. We said, are you kidding? Users won't go for 90 days, not at our company, because they have had their email forever prior to that. Now you tell them that they can't have it more than 90 days and they can't archive it to the hard drive? I'll be dead from those users.
  - From a knowledge management point of view that's crazy. What if you come back to an idea you had three years ago? But if it's in an email?
- So we have negotiated with the legal department that our retention policy is that it is a year if you haven't marked it for three years, so it can be up to three years for emails the user marks.
  - You are not archiving Lotus archives at all?
- No we're not because I know I can't control it if it's on their hard drives. If it's on the server and is marked I can purge it automatically with my script.
  - We have Lotus Notes also. We set the server policy so that we don't let users archive at all, but we (IT) archive at the server level.
- We don't archive, we purge. Year, three years, it's gone, it's off the server, it literally does not exist. Now does it exist on the six month tape. Yes, for the next six months, but then it is completely gone.

---

<sup>5</sup> Think, in fact, of the existence of archives of personal mail on Google, where several gigabytes may accumulate!

## **Responsibilities for Retention of Clients' Information**

- We record outbound and inbound calls to our customers for our clients. We audio record every phone call, including sometimes credit card information. We have to do that for [??] compliance. Is that a document?
  - Moritz: Yes, the data map would include it, yes, voice mail, or whatever you are using, yes it is a document.
- Is that our property or is that our clients' property? It's our person on the phone with their customer. Who is liable to provide that information if there is a lawsuit. Is it Company A or our company?
  - Moritz: If there is a lawsuit, they are going to try to get the information wherever it is. If you have it, they can get it from you. My thought there would be that you should make provisions in the contract for what the policy will be (you'll tape for quality assurance, etc.), make that a short amount of time, as short as they are willing to take. Because you're sending them the calls anyway. So it's more a contractual thing. But, if you have them, when the lawyers come after them, the lawyers will argue that your tapes are in their control and they can come and get them. If I were the company using you, I would want your retention policy to be very short, like: send them to us, and throw them away. I would not want them to be out there.

## **Instant Messages**

- Vijay: Do you all capture Instant Messages (IM) when your users use that?
  - We don't. They can capture it themselves to their laptops or PC, it's up to them.
  - We haven't enabled logging for that purpose.
- McHenry: Aren't you concerned about leaking intellectual property through IM?
  - Many: It's no more difficult than putting it on a USB drive, or emailing it, or telling it on the phone. It's more a virus vector.

## **International Law**

- Vijay: many of your companies are international. What about European laws?
  - Moritz: so if you are responsive to a suit somewhere else, outside the U.S. what their rules are? Wow! It's going to be all over the map. Some places are ahead of us, some are behind. I am hoping that international companies are having their international lawyers looking at this. I don't personally know about EU law. There will be some obligations. It just gets crazy, how much information there is.

## **Encrypted Information**

- Prof. McHenry: What if the students encrypt their emails with PGP encryption. Are you legally responsible for decrypting it if there is a lawsuit?

- The same could be said for a shredded document. Are you legally responsible for gluing it back together? If you don't have the password for some of those encryption programs, it's out of your control. Some of those are certified by the federal government.
- PGP most likely (could be decrypted), but (not) RSA 128 or TruCrypt.
- You don't have to decrypt PGP for ESI compliance.
- In a very rare situation we have had to do some decryption for credit card information.

## **Other Forms of Data**

- You talked about the data. What about call detail records? System log files. Maybe this would indicate if someone is logging into a system, not in the actual data exchange just that they had access during a given time.
  - Moritz: I would be very interested in that if I were a lawyer and that person were part of a lawsuit. You can have different retention policies for different types of data. You may not need that for very long. You may want to deal with that before it gets into the tapes. I can easily see that being useful for discovery of leakage of information. If you are in a trade secret case with a former employee and you can show they were in the building logging on or coming in through the VPN, so yeah you have to have something. On the other hand you might want to save it forever. You have to think about whether the information is more helpful to you or to the potential plaintiff.
- Isn't that part of a double-edged sword? You offer three year retention, and if I had a conceptual idea 3-4 years ago and we didn't spend much time on it then, but if we are going back to claim patent on it, and we are now purging in a year, haven't we lost the defensive information we need for that patent claim?
  - Moritz: You are hoping that for something that important you're going to have duplicates, i.e. paper copies. But absolutely, from the lawyers point of view, all we want is whatever information you have. Whether it's a lot or a little. We just want to be able to tell the story. As long as we know all the information. What we don't want is someone destroying something off the record and then someone else telling us about it in a deposition later saying, oh yeah, we had all that stuff but we don't know what happened to it... We just want a system in place so that we can tell the judge "your honor, this is all we can get" or "this is what it will cost to get it" and then not come back to the judge 3 months later and say we messed up. That's when you start to get involved with serious sanctions. It's really a business decision.
- For some of our creative work we burn them to DVD. We purge them from the servers on a periodic basis. Often, we won't leave them for 3 years. For example, we leave them 18 months. Before the purges, we find out who made it-especially the creative department, payroll, others—we make them copies they can file in the same place.
  - Is that e-mail or more like LAN files?
- Any email they want to save they have to archive in their own folders. And they have to request those folders to be backed up. They request their Outlook to their .ost or .pst files. We recommend that they save them in a file format, "save as," rather than save as email, then we can back them up. If there is something creative they want to keep... Some companies don't like putting it out on a DVD and giving control back to the user.

## **A New Paradigm Needed for Pinpoint Backups**

- What I am hearing is that, from an IT standpoint we need a whole new paradigm in backup technology as far as to segregate it out. You might give DVDs back to the user that you might have to

help them find. Or if you want to start to create the backup so you can pull two emails for one litigation, or something that R&D deemed beneficial that you need to backup separate, and then be able to restore those separately, related to some issue. That becomes very expensive.

- I am seeing going broke.
- Are you talking about using keywords?
- Getting it from a global backup takes forever to harvest.

## **Public Sector; Keyword Watching; Information Life Cycle Management**

Jim Sage: This is interesting because the requirements imposed on the public sector are different from the private sector. When we knew this was coming back in December we went and pulled out the retention policy. It became apparent quickly that it was missing the ESI components. We added, or are adding, electronic records, for a retention and destruction policy. Destruction is as important as retention. When can we get rid of the stuff? We started with the policy for retention of the state of Ohio. We are involved in creating it, but it is for all universities. Our legal counsel has said that electronic transactions have to have a 1-1 relationship to the original hard copy. If you have an electronic purchasing record, and the purchasing retention policy for paper is five years, then the electronic version has to be retained for five years.

To enable that we have been looking at products that in essence watch the mail server and watch for transactions coming across it. So if a purchasing transaction comes across based on keywords, it gets stuck into the purchasing folder and retained for five years. This happens electronically and is transparent to the user. This takes away the need for the professor or staff member or administrator to worry about it. There are technologies available, or becoming available, to do this. We are looking at EMC for this, who has a whole suite of tools for this. It also can “see” a purchasing transaction and grab the email (also based on the attachment). So if legal wants to do discovery around a category, they can do it. So we updated the policy and then looked for technology to implement it.

This has prompted the need for an Information Life Cycle Management policy for the university. When we look at the mainframe and all the data in PeopleSoft, a large portion of that data doesn't get accessed. We have that sitting on expensive online data storage. We have to take the 80% of our data store that is not being used but sitting on production data stores and move it off to cheaper storage. This is all coming under the umbrella of Information Life Cycle Management (ILCM). Our storage area network (SAN) is growing like crazy. We have to put the data that is not being used most of the time (daily) on “near online” storage, and then after another while, move it to “offline,” to tape when they get old enough. That's ILCM: online, near online, offline. We are working with vendors like EMC to figure out how to enable it.

- Are you running (EMC's product) EmailXtender?
- Jim Sage: No, but we are looking at it
  - We are also looking at it.
  - What is EmailXtender
  - This is an email archiving component for the EMC solution. He is talking about one function. The other function is to help with email quotas (especially if you are a Lotus Notes house). You can archive emails over 90 days old, for example, to pull them out of the Notes mail file. A stub is put there, but to the user it looks like it is there, but technically it is offlined to a cheaper storage. Another problem is backing up all this crap. So you can use a technology called Centera for mirroring. I put another Centera in another physical site and synch them and mirror them, and never back the stuff up. I am highly looking at that right now.
- Exactly what we are going to do.

- One of the huge advantages of that—earlier we were talking about searching technologies, and someone said email is text so it is relatively easy to go through. In the litigation in which I have been involved, the attorneys always come back to email as a panacea and say surely the information we are looking for is in the email. So they make a very broad request for where you should restore the email from. But when you get into searching for things, let's say you are doing an intellectual property or sexual harassment case, you are looking for some very specific things, you may not be dealing with the email, but within an attachment. Email EmailXtender indexes the attachments as well as the email messages.
- We forget it's not just email. It's Word documents and PowerPoint and Excel Spreadsheets.

[New prime speaker]

- Is anyone using Wide EMC? That type of product?
  - We are about as far as the University of Akron is right now. Everybody has users with gigs in their inbox. So much data that is offline that you are responsible for. Storing it offline has to be manageable. That's the promise of products like wide EMC or EmailXtender. The other product we're looking at is DiskXtender, which lets you take care of Excel files and so forth on NTFS or NFS shares.

## **SPAM**

- Do these scanners work on email before they go through the SPAM filters?
  - Jim Sage: It sits between the SPAM filter and the server. There is typically a filter on the way in and maybe one going out. The SPAM never makes it to the server. The listener would not see it.
  - I get so much SPAM there is no way I could ever archive it. I'd have to have a BIG server!
- A lot of it gets kicked out but a large percentage still gets in
  - Sage: About 95% of the inbound email for the University of Akron never makes it in.
  - I am at about 80%+ percent, maybe 90%
  - Sage: Maybe 95% for the University. And we still get millions.
  - So email that is never delivered I am not responsible for.
  - Sage: Exactly. It's not a part of our electronic records.

## **Emails, Changes Between Back Ups**

- Another question is what obligation we have to track changes that happen between backups. I could have a backup every day, but get an email in the middle of the day, read it, and delete it, purge it permanently, and there is no record of that message being delivered. Is there any litigation about that or is IT is responsible for, to ensure there is a record about that?
  - EMC's EmailXtender will log every email coming in and out.
- Yes, we know that. Notes will do that too. Our lawyers are reluctant to let us turn that on. The lawyers themselves get a lot of stuff that is privileged, under client-attorney, etc. For corporate executives, they might not be comfortable with a record of it.
  - My in-house legal is saying the same thing: the sooner you can get rid of it, the better off you will be.
  - If you have to keep it for 3 years, delete it the day after.

- Right, that's their policy
  - Moritz: I worked for a firm not nearly as conservative as that. It's not nearly so black and white. If it were me I'd want you to have it. You have to work that out with your legal counsel.
- What does anyone else do?
  - If it's something privileged then that would fall under the provisions of claw-back. If it's some work done by the attorney that shouldn't be revealed in the case, that should be subject to claw-back.
  - Moritz: Even if you put it out there. I don't know what kind of information you have out there...
  - I assume we all want our users to manage their mail, so if they get stuff they don't want they will delete it. I'd like to think it is all used for company business, it's not. There's spam, personal stuff, people are deleting it when they need to.
  - Our email policy is that we do daily backup, no archiving.
  - Same for us.
  - If it is deleted between backups we have no record of it. We don't want to keep email backups on our server for more than a month. We rotate the tapes.
  - Moritz: that all sounds reasonable. It depends, if you are a company where you have to litigate against your employees for doing stuff you might want to save it longer, trade secret issues, etc. but you are going to have different strategies.
  - We were getting a lot of requests for getting emails back from six month backups. They say "you know I need that email from April of last year." Those kinds of requests can take hours, so we decided not to...
- So from a legal viewpoint there is no obligation as far as...
  - Moritz: No, as long as you have a policy of one kind or the other. Again, once the lawsuit happens if you have a person who is part of the lawsuit, you probably ought to take a careful look at what that person can do. You might want to save all of their email, so it's sort of a different game once you are on notice that there's a problem.
- Our parent company is being purchased and there is an anti-trust discovery process with the DoJ, so we are going through that, though it is not related to litigation.

[New prime speaker]

- I never had a reason to look and see that Lotus Notes can do that. I think I knew it, I didn't think of using it for that. It's something I would want to do. You get the major marketing pitch from EMC, that just means more storage.
  - But I get nervous because that means there is a standard feature in the software that we are running, and we have elected not to do it, right? So what does that...
  - Moritz: You have to think about it. There is not going to be a clear-cut answer, and you are going to make decisions that have business reasons and you'll be fine.

### **Role of User Discretion; Similarity to Paper**

- I think I heard a couple people reference the idea that based on user discretion or filtering they are archiving based on that. Again if I had some individuals who decided what to mark to save for three years, maybe I wasn't saving anything I should have relevant to some situation—that means we are giving control to the user or to some keywords that have been set up. That still is following policy if that what policy says, so it should be acceptable.

- Moritz: Yes, it's just like paper. In a lot of companies they will store some stuff centrally, but then so-and-so has a really good filing system, and more stuff will be stored there, than with the guy who cleans his desk and only keeps the last month of stuff. I don't think you are responsible for each of your employees having a good system. But at the same time you don't want you entire storage system to rely on their individual hard drives. You're going to have to be keeping some stuff because you need it. But for the stuff you would not be keeping as a matter of course, I don't think it's any different than a regular old company with a big file room. There's going to be a lot of stuff that people throw away, and the company has a business interest in keeping it that way. I am very confident in making that argument.

[New prime speaker]

- I would think electronic data would be very comparable to paper data. We shred everything. CDs and disks when they go out of date, we shred. So we take that same path in IT. So we destroy the data after its past its useful life.
  - Moritz: How do you do that? Do you actually overwrite the data?
- It depends on the media. If it's something like tape and it's deteriorating, we shred it. If it's media we can reuse, we overwrite it.

### **Purging the LAN and Long Term Retention**

- Our retention policy also talks about LAN files, Word files, Excel documents. The back of the retention policy has about four pages listing types of documents (purchasing orders for X, lease contracts for X, thousands of different categories) which would be mirrored to if it were paper. So we went through and created this wild naming convention on the LAN drive so they can rename folders with-it started out to be perm3, perm5, and perm7; because you have to keep payroll records seven years. That has turned into 7, 10, 20, and 99 now. We just pretty much completed our first purge of our LAN files. We had OS/2 LAN server on our NT server. Surprisingly not much got purged and I did not get much space back.
  - It's all in the 99 folder.
- I'll look through that next. It would be interesting to hear, if there is anybody trying; you don't know what the documents are. You don't know if it is a purchase order; in IT we're still on Word purchase orders. So you don't know what that Word document is unless you use filtering logic, and we're not that sophisticated yet. Is anyone else doing anything more sophisticated?
  - I think ours is less. We just went through and got back about 30% of our LAN drives back. We told everybody two months in advance that anything older than this date; we're going to do a full back up and take it off and if you need any of it back, you have so many months until it is gone. There were a few folders like payroll that we kept separate. But we have media designers with 200 MB media files they haven't touched in 3-4 years. They say "oh don't delete that."
- Our legal came up with 3,5, and 7, but they got so much pain it took a year to finally settle back; we have stuff we have to keep forever—stuff on a new product or on the existence of an older product. I think they lost the battle, and that's why perm99 exists.
  - In our industry we have to keep any document related to our products, testing and design for the life of the products, and our products are used for a long time. So we are regulated about what we can get rid of.
- I don't know what regulations we have. Aside from that, the users just were in an uproar. We were supposed to start purging the LAN a year ago. It went into "legal void" as I call it.

- Do you have any restrictions from employees about storing documents and emails on their personal hard drives?
- Oh yeah. I've got people who are out to get around year-round quotas. They'll copy their entire email file to their personal hard drives and then delete everything from the server to be under the quota. They'll have three different versions of the mail file from whenever they copied it. They have everything under the sun. Especially email.

## **Disaster Recovery vs. Backup; Tape vs. Disk TCO**

- Jim Sage: I don't know if the rules are going to change, but when you look at the rules in the public sector that are imposed on us, the backup strategies that we have are inadequate. The backups work really well for disaster recovery but to go in and do any kind of discovery and comply with a retention and destruction policy, they're just not adequate for that. As everyone does, we overwrite tape for backups, and that inherently violates the retention policy. So we've had to look at a different way to address the discovery issue. Aside from what we do to protect the University against a disaster.
  - Is anyone using tape for retention? What I mean is that in the old mainframe days we used to have payroll tapes and we kept those for seven years and you had other tapes you kept for years. With client server that all went away and everyone has a tape with everything on it. How long do you want to keep it? It was forever, I'd say Sarbanes Oxley came along and said don't keep anything over three months. Well I can't do DR (disaster recovery) based on that. So we keep tapes six months, a six month rotation.
- Jim Sage: We've started looking at the cost of tape versus disk storage. We're finding that the cost of disk is dropping so rapidly that it is reaching the cost of tape. It's almost cheaper to buy more disk, set it in a remote location and backup to it, than it is to buy the tape, load the tape, write the tape. So we are actually going to put a disk farm over on our Wayne campus and back up to it over the LAN.
  - Can I borrow that?
  - multiple voices – 14 terabytes is much cheaper than SAN, we're testing that right now
  - We just tried a week ago on a smaller scale of testing, terabyte removable USB disk drives. They pretend to be tapes, the backup software thinks they are a bunch of tapes there. Boy it has speed up backup like ten times. Makes it really easy to transfer to a data space offsite.
  - Using USB drives instead, we're doing something like that...
  - Just for testing so far, not for all of our...
  - We're not doing that for tapes but for our disaster recovery, to keep our [??] logs on a USB drive so I can yank it and get on a plane and go. So I can get back to a recovery point.
  - That could be something to do for the discovery process. You can get a 500 GB removable drive for what, \$130 now? Oh I mean I would assume I would choose that rather than messing with my other retention policy.
  - I have a question about the cost of tape. When you are calculating total cost of ownership for the (TCO), are you looking at that over five years, seven years, because the reason I ask is when I looked at the calculations (I am sure the volume drives you buy are different, the price is different)—but if I take into account that my drive models are changing pretty fast, I am going to have to forklift replace every five years. I am now depending on a spinning platter that consumes electricity, there are maintenance costs, and I'm going to have to time goes on and the storage requirements grow exponentially, I know then that I'll be buying more drives, and each time I do a replacement, I'll be adding more drives, etc. vs. the more traditional either offline tape solution. Once I absorb the cost of that the data on that is now fixed. The cost that I have spent to acquire that tape is done.

- What we tend not to take into consideration is the advantage of disks in implementation. The movement, storage, and protection of the tape—just because you bought a piece of tape and put data on it and stored it somewhere, it still costs you money. I am not saying that the cost of disk is cheap enough yet to replace tape, but it is on its way there. Now the breakeven hasn't been hot yet but it probably will. Tape is made out of oil.
  - A couple other things. If you are frequently being asked for restores, you have to put people's time into that. Assuming with disk the user can go get it and your people are not involved, that's a key dollar figure. Second, it may be a minor cost, but I have to move this tape offsite, so I have iron mountain costs carrying these boxes in and out.
- And if you are storing in iron mountain you pay for storage.
  - I have never tried to do the calculation, but it is getting close. I'm just trying to get stuff so I don't have to back it up at all. Put the old stuff that doesn't change somewhere and mirror it over a T1 I already have in place anyway...
  - At a former place I worked we did something like you're talking about doing, except we did it a few different ways. We had the live backup, you had to keep medical and treatment records forever. We had a backup farm. Then we had another what we called our old data farm. We kept records for however many years of active patients. There's something on our main server and backup servers. If a patient hasn't been there for a year or two, that data got out of those databases, and goes to what we called "the dead file." It was a lot easier than tape. You mentioned the cost of trying to find which tape the patient's records were on and sometime they spanned multiple tapes.
  - That administrative cost is hard to calculate. You can take a stab at it

## **Need for Knowledge Life Cycle Management**

- Prof. McHenry: It seems to me that the lines between backup and disaster recovery policy, retention and destruction policy, and knowledge management—are all blurring. The ability to identify which piece of information is needed for litigation, for long term storage, for later creative use, is in a sense part of the same spectrum. The elusive goal of saying what is the value of any given email or piece of information and it is hard to predict in advance what the value is, in fact it is almost impossible. So that's the conundrum. Don't you think that this is what makes it hard? Are you thinking along these lines, that wow, this is all part of the same spectrum? And you don't just have Information Life Cycle Management problem, you have a Knowledge Life Cycle Management problem?
  - You've made it real complex now!
  - I was going to say, can I avoid that?!
  - I have just gotten my head around Information Life Cycle Management!
  - You are assuming that our emails have knowledge in them?
- Sure, there may be emails that I send to a student or to another colleague that have a spark in them, and I may lose that spark later on. A lot of thinking aloud, brainstorming, etc. takes place in the form of emails. That spark may not be found again.
  - That's where knowledge management really gets wild...
  - Jim Sage: At this point, but I think we will evolve. Today we have a somewhat simplistic system where we store things in simple categories. Payroll, whatever. But in the future it will be around subjects and knowledge. Indexing systems will give us the ability to do that. I am not aware of technology that can do that now. That will capture all the information around this topic, no matter where it's at.
  - That would be a great elective class.
  - If you can figure out how to put the class round it, you are way ahead of us.

- I do teach a class about knowledge management, and in that class I talk about the subject of active ontologies. There is experimental work in this area to create the kind of backbone system whereby information gets indexed to the ontology. A taxonomy is a hierarchical representation of knowledge. The ontology takes this one step further in that it is more like a knowledge map (not just hierarchical). An active ontology means that software can be written to alert users to the existence of relevant information, make connections between pieces of information, make inferences (e.g. thereby filling in database fields), do smart indexing (taking into account disambiguation), etc. Students never understand what I am talking about.
  - Sounds like an executive education class that should be offered for us old guys.
- I am not sure that many companies are pursuing active ontologies. I think this is more an experimental topic at present, still being developed. I don't see many companies talking about it in any case.
  - We are not talking about transaction data.
- Even the transaction data may be related to the ontology. People are talking about attaching word files to SAP transactions to understand the context, or attaching emails to transactions. So what we think of as traditional transaction processing may have more of relationship to knowledge management than you think. If you are developing a knowledge management piece, then having the legal end is an important component as well, because you might as well build in your document retention and destruction policy within your knowledge management system.

### **Better to Retain More or Less?**

- Vijay: From a legal point of view, is it good to have a lot of data, or very little data?
  - That's almost a contradiction
  - If you're being sued, you're being sued.
  - Moritz: Sometimes more information can be good. Lawyers are so conservative about this, they would always say that if you are the defendant, you don't want any information. What you realize eventually is that you have to tell the story and it is all going to come out. Just because you don't have a copy of the email doesn't mean that you won't find someone to testify about it. In a way we'd rather have the email so that we can actually say what they did say. People have different risk aversions. I'm on the side I want more. We can always deal with it. We can say we screwed up, they are lying, etc. But I can't deal with information that is a surprise. A lot of lawyers don't think this way
  - In the case of our litigation, that was before we had the retention policy, and there were actually documents that were given by our employees that helped to win the case (for the other side) because we kept the stuff around, we hadn't purged it yet.

### **If You Have It Stored, It May Be Subject to Subpoena**

- One question: we were talking about filtering and all that. Companies have policies about no personal information on company electronic systems and blah blah blah. We all know that is not the case. Do you have any comments or case information about corporations that released their company information to help settle some type of personal issue based on personal content that they unwillingly stored?
  - Moritz: I don't know any specific case. But certainly you could get a subpoena as a third party witness. And most courts will say, oh yeah, you've got the stuff on the hard drive, you'd better come up with it. If it gets really expensive the plaintiff may pay for it, or if it gets too expensive, they may eventually say no.

- It also comes down to what are your retention policies when an employee leaves. When we get a notebook or desktop back in, we wipe it. We don't want any of their person stuff— cause we know people put music programs in or download songs or put personal pictures on it, we don't want to deal with it.

## **How Well Do Lawyers Understand Where Data Is?**

- I was at another session two months ago related to this topic and one of the comments a lawyer had was you need to take disk images of anybody that is potentially involved with this particular litigation. And when we pushed back that if they are following our policy they we're trying to enforce they should not have anything personal on their PC anyway, it's all on the server. No, you have to make images on the drives. And again, how far is IT's responsibility to educate the lawyer that says, what I am doing is irrelevant , there's nothing here, what you want is on the corporate server, which by the way, has everyone else's stuff that you may not want to disclose.
  - Moritz: Communication is very important, obviously. You just have to work with people on a case by case basis to get them to understand. I can't give a global answer on that. In every case there is an individual discovery plan relating to ESI. It's really important to make sure this is strong. A lot of lawyers don't appreciate that enough. They send a paralegal to go, tell them: gather some documents, talk to the IT people. They can't do that. You're the one who is responsible as a lawyer and you need to be involved in talking to the IT people about what actually is there. You ought to be able to explain it to them, although some may be idiots.

[New prime speaker]

- I literally have a laptop that has been in my office for three years because someone left and the lawyers told me that I could not get rid of it. I have extended its warranty, it was only used for a couple of months when that person left. I said all their stuff was on the server and we backed it up, here it is. They said: keep the laptop. I said: don't you want it? Them: no you keep it. It's sitting in my office collecting dust, I just gave up with lawyers.
  - Can't you just take the stuff off it and put it on a removable drive somewhere?
  - We offered. We backed it up. Nothing. It's just one laptop, but it's the principle. So it's not worth it.
  - At some point if it is costing you a lot of money...
- Yeah, there's a threshold of about what the most cost it. It's the principle mainly that we are wasting a whole computer.
  - Was there a lawsuit or someone might sue?
- It was an employee that left. Yes, there was litigation.
  - Can't you just save the hard drive and use the computer?
- The request was clear, do not redeploy, do not alter. Keep it in your office.
  - Moritz: My daughter thinks the computer is in the keyboard...
  - I would let the laptop gather dust in his office. Let him feel some pain.

[New prime speaker]

- A lot of us are getting calls right now from vendors right now. There is a lot of fear-mongering going on. This may be because with reservations by legal right now, maybe I don't understand the scope of this entire change, so I'd better just save it all (or delete everything). There are certain companies that are selling products, they are saying oh this changes everything, you need all this additional stuff. It's almost to that fever pitch with vendors right now. You have to do this or else.
  - And they are direct marketing to the lawyers.

- Moritz: I try to tell this to my students that the hardest thing as a lawyer is to understand what not to file, what not to take. The easiest thing is CYA, and file it all, ask every question. The harder thing is sitting down and figuring out what are the five questions you need to ask. Knowing that you are not going to get in trouble if you don't need to ask all the questions. Experience tells you what you don't have to do. Lawyers are very conservative by nature and will try to cover every possible base. Only when they are experienced enough are they actually confident enough to make that judgment that we don't need that. That's a high skill that they need to gain. And it's difficult. And mistakes are costly.
- In the future you can just say: we have a copy of the data. They can say: don't print something out if you; how you deliver the data is up to you.

[New prime speaker]

- We had a case where we were in litigation about a patent infringement case and the lawyer said: I want the computer that was used to do that design work in 1996. (General laughter.) Is there any company on the planet that would be able to produce that. My response was: you may get it from the landfill. That's where it is. There was no pertinent information on that box when it went into the landfill.
  - Moritz: if they can make that affirmation that there is no computer anymore, and they can make that confidently, that's what they want. What they don't want is for it to turn up later. It's not a question of having it. They don't want it for it to turn up later, e.g. other people dug it out of the landfill and it does have the plans on it.
  - What you are saying is that these lawyers might be more intelligent about this than it might appear. By asking for all of that affirmatively and specifically they are guarantying that they are covering their bases in terms of no equipment which might be out there. Even though they themselves know it is in a landfill.
  - They are expecting a no answer is what that tells me. To just confirm it.
- They had an expert lined up who was going to look at that drive.
  - Oh no way!

### **Assuming You'll Need Images of Personal Drives; Disseminating Policies**

- Jim Sage: We don't have all this e-discovery infrastructure built yet. As a part of our litigation hold process we immediately make a copy of the hard drive. If we anticipate that anyone is involved in litigation or they are, we immediately capture an image of their hard drive.
  - Moritz: I would assume this is a campus owned PC hard drive. If it is personally owned by a student, even though he is involved, you do not have the right to go in and image theirs.
- That is correct. But all the notebooks on campus used by faculty and administrators are.
  - Moritz: But what's your personal information policy? I assume you are allowed to back things up at home and keep things on your local PC.
  - Prof. McHenry: No one actually ever told me that (laughter...), no let me put it this way. I don't really know the policy. If I was told, I was not paying sufficient attention.
  - How well do end users really understand the retention policy, and how well is that communicated to them?
- I know that they do not understand it, because it doesn't exist. We are still working on a retention policy for electronic records. We have one for physical records. But the state yet hasn't completed the electronic records policy.

- Prof. McHenry: I know I am supposed to keep the exams I give for a year. If there were questions about grades, assignments, etc. I have all that paper in my office and then throw it into recycling once a year.
- Prof. Vijay: I have everything in WebCT, and as soon as WebCT is purged, I have no record of any of it.
- What kind of show are you running here, Jim? (general laughter)
- Does your company have an electronic retention and destruction policy?
  - Not a destruction policy, and not to the level it needs to be. We have some general guidelines.
- When we knew that these changes were coming in the ESI rules, it caused our legal council to ask, what is the retention policy for the university. They pulled it out and said oh darn, we haven't updated this for 15 years. This happened at the state level also. We had a hard copy policy. Since then, 10-15 years ago, all the electronic stuff has occurred.
  - Another thing is that we as IT professionals tended to view data over time as value add to the organization. Now that the lawyers are getting involved we see there is a risk, too. Where does that balance lie?
  - Prof. McHenry: There is also the training cost. When I came to the university I had two mandatory training sessions, one of sexual harassment and the other on fire prevention and safety. I was never required to attend any training regarding my laptop. Professors are not going to be very happy to have to worry about stuff like that. But that's a question of implementation.
- We had a security day last year that everyone attended except you (general, boisterous laughter).

### **Nuances Related to Hosted Services**

- We have not spoken about hosted services. More and more people are using them. I do not recall terms in the contracts or licenses about how to establish retention policies. Anyone dealing with that? That's a whole other repository of stuff
  - We are a hosted service but we also deal with companies that host our stuff as well.
- Do you have a policy about retention that you offer to your customers, i.e. for voice mail, i.e. you will only keep it for six days or 20 days?
  - Per customer it's different, it is negotiated. It is not perfect. We are trying to improve on audio recordings.
- For some of purchasing sites or aggregators you send your data out for purchase orders for quotes or bids. Our employees have put business data out there, and some I don't even know about. There are websites, some standard ones for building products, and they have bids that sit out there that are documents of business. I have no visibility of that.
  - Isn't that similar to what they put on their personal PC?
- I don't know.
  - If someone knew they were out there and needed to be discovered, they would have to out and get those documents. We do a lot of retention for our customers. We do a lot of financial stuff for various companies so we do have a retention policy negotiated on an individual basis client by client for how long we will keep their data. Some want it for 30 days, some for two years.

### **What About Users Working on Company Stuff on Home PCs?**

- Does anyone have something within the usage policy for the PC any limitations around the user taking flash drives, i.e. dropping Excel files onto it, and working on it on a personal machine. Chances

are its going to stay on that hard drive, or anything around that about company data on personal equipment.

- We have 9000 employees across the U.S. Most of them have their own personal machines. We have a very liberal policy about that. In their employment agreement it says that if they are terminated they are to... and we just recently have been looking at the online backup, if we say that employee is terminated, it goes out and deletes any company stuff even if it came from the person's personal PC.
- We have a policy that says no company stuff on the personal PC, but we know it is violated. Any time we have made an issue of it, it turns out that no one looks at it has being something that is critical. It's not fully enforced.
  - We have never allowed it; if you want to work at home we'll give you the equipment. But we have nothing to stop you from putting that Excel spreadsheet on your personal PC. I don't know how you could ever...
  - We have loaner laptops available and if you have to do an assignment, we say take the loaner home. We're not at the point of [??] USB ports yet, we are frowning on that, but we know it has happened.
  - What's the difference between taking home some documents on your briefcase and working at home versus taking home a file? It's the same thing.
  - The only caveat to that is that with a USB device I can take home 1 GB or 2 GBs of something.
  - For example, a customer master file.
  - And I can do it in such a way that I can replicate that very quickly and disseminate it very quickly. If it is on a ream of paper and I went to Kinko's with my credit card, now there is traceability.
  - However, if someone's gonna do that and you have a policy that says no USB devices, how are you going to stop people from doing that anyway?
  - Microsoft answered that question with Vista.
  - For us old guys a 1.5 MB floppy could hold quite a few things, too, so this problem is not new. Now with a Gig, yeah, but your Word document is also bigger.
  - I would think the biggest problem with working from home systems is that they may be hacked. How many home systems are compromised? If they are working on confidential information it could be going out to a server in Russia and then be disseminated
  - yeah, key loggers
  - that's a huge area
  - Moritz: some Senators have just proposed legislation this week that insists on greater privacy protection for personal information after 49 million TJ Maxx customer credit card numbers were hacked. That pushes to total up to 100 million credit card numbers that have been disclosed over the past few years. The University is thinking of putting PointSec security on portable devices as well. We have it on our hard drives now, I backup to an 8 GB card that I stick on my PC at home because I want it there if I need it. That's a huge issue when you talk about your clients. It's the liability you are going to have when it's someone else's information. Data such as social security numbers or credit card numbers of your clients.
  - Work at home for us is an enormous challenge because of credit cards, and it's a great growth opportunity for us, but we are struggling for it. We are on pause on it right now.
- I posed the question about hosted, but we also do work for clients for whom we do work. They may have retention forever of something that we would not.
  - Moritz: There are new technologies to deal with that, with time-limited files. You could put digital rights management (DRM) on files. (None)
  - Sage: we have to deal with that a lot with the students downloading music.
  - Moritz: Amazon just agreed to sell music files without DRM.

## **Obsolete Hardware; Older Software Versions**

- What about cases where you have backups that can only be read by older hardware and then have to get that stuff out? That plays into the discovery, if I have a backup tape I can't read, is it worthless or is it usable? And then the cost of doing that.
  - And does your application read that data?
- That's the question but if your host environment or hardware is no longer compatible, then that's the problem.
  - Moritz: Data forensics is an area that deals with that. They keep old hardware and copies of old programs and will recreate an environment to get that data out. They may have to create a virtual environment to restore 5- or 10-year old stuff.
  - You would only do it if you were legally required, for example, for health records or something. You have to keep them available, otherwise it's just a business decision.
  - Moritz: If it is decided you have an obligation to provide that stuff, and had to hire a forensics firm to do it, the other side might have to pay for that.
  - We actually had a case where we had to restore two backup prior to what we have in production, which the current backup wouldn't restore. So we have actually experienced this.

## **Next Meeting**

Prof. McHenry pointed out that it is great to have people present for these exchanges who are knowledgeable about the topics and have things to share or who have excellent questions to pose. Each person was encouraged to forward information about the ITEE programs to comparable people in their firms who might be interested.

The next meeting will be held from 3:00 PM-5:00 PM on Sept. 7, 2007.

The topic will be Business Continuity/Disaster Recovery: what have we learned in the past few years?

- The ITEE discussed this topic as one of the first sessions several years ago (summaries were not them being written). Surely we have learned important lessons since then?
- We thought this was a particularly timely topic given the role I/S played (or did not play) in the response to the Va. Tech shooting, and in light of recent major disasters such as Katrina. So the topic could include emergency management/crisis management. Do you send emails to students/employees?
- Has anyone had to exercise their plan?
- A particular question was posed: when do you justify setting up your own backup facilities as opposed to outsourcing this function to a DR vendor such as SunGuard or IBM?
- If you are offshoring, or using third parties, are you checking their BC/DR plans (Sarbanes Oxley says you are supposed to have thought about it)?

Other topics that we considered but set aside this time around were:

- Corporate Web 2.0 – use of technologies such as Wikis or social networking within an enterprise framework
  - Evolution of e-business on your websites, external, internal, Cisco's new products, blogging, Wikis
- Greater depth on some issues raised today:
  - remote computing issues, working from home, what are issues from IT side

- the EMC EmailXtender product in particular, storage policies, tape vs. disk, etc.
- Information Life Cycle Management, tiered storage
- syncing old data in synch with new applications (bringing data back), providing applications to read data from old media, data forensics
- Future of the Internet, Internet reliability, implications of Internet-2
  - Akron hooks to the Third Frontier Network which is connected to Internet-2. They have fiber to all the universities and soon will have it to all the high schools.
  - Internet-2 was built by research universities. Public access has not been discussed yet, as far as Jim Sage knows.
  - Prof. McHenry: besides speed increases, there will be protocol changes that may increase security, etc.
- E-training/Using open source software
  - Like WebCT or Blackboard at the University. Jim Sage: the university is hoping to move to an open source solution called SAKAI. There is a group of universities that are building a whole suite of university applications. Commercial software such as PeopleSoft is too expensive. U. of Michigan and Indiana University have built their own financial system. We are going to build our own and replace a lot of it.
  - The Ohio initiative for open CRM was mentioned.
- Using web services
  - Relying on third parties, privacy, xx-70 and all the issues that come out of that. The university is doing more and more of that. And anyone can put a website out there to purport to provide some service.
- E-training