White Paper

Disaster Recovery and Business Continuity in State Legislatures: A Roundtable Discussion

MODERATOR
M. Glenn Newkirk

PARTICIPANTS
Cathy Munson, Washington State Legislative Service Center
Dennis McCarty, North Carolina General Assembly Information Systems Division
Dave Larson, Kansas State Legislature Computer Services
Jim Greenwalt, Minnesota Senate Information Systems

1 August 2003

SENTRY INFO
InfoSENTRY Services, Inc.
www.infosentry.com
919.838.8570

Disaster Recovery and Business Continuity in State Legislatures

August 1, 2003

Over a decade ago, we did a survey for Government Computer News of the nation's 50 state legislatures and found that only two had written disaster recovery plans. Those plans were typical of their times: they protected "the computers in the glass room." A great deal has changed since that survey. Now extended legislative networks often span entire state government complexes. "Mission critical systems" are more pervasive in legislatures, covering much more than just the bill drafting system and the payroll system. They include front desk management systems, chamber voting systems, physical security systems, and Internet-based public access systems.

To gauge how the continuity and recovery climate has changed, we recently asked four veteran legislative information technology leaders to talk with us about their business continuity and disaster recovery processes. While our initial focus was on changes in disaster recovery and business continuity that have come about since 11 September 2001, we found that a transformation was under way well before the shocking events of that day. Legislatures were already "hardening" their systems, developing extensive business continuity plans, and communicating with Members and staff about those plans—because of direct experiences with fires, earthquakes, tornadoes, hurricanes, ice storms, and bomb threats. As one of our roundtable participants noted, legislative business continuity plans have matured because the information systems and the Legislatures have matured.

Now, so have the risks and threats.

Here is the discussion of the driving forces behind business continuity planning in legislatures, the obstacles legislative IT professionals face in implementing their plans, and tips on how to get business continuity plans under way in the unique organizational setting of a State Legislature.

We are particularly appreciative to the four panel participants. We provided them with an initial discussion outline, refined it in several individual telephone calls, and held this conversation with them.

–Glenn Newkirk

Glenn Newkirk: Thanks to everyone for agreeing to take an hour on a Friday afternoon to talk about disaster recovery and business continuity in state legislatures. I know that it is just a really exciting topic for us to discuss on what I hope is a calm day across the country. What I would like to do is start on the West Coast and move eastward and have you give us your name, title, organization, a brief description of your department, and the responsibilities and applications that you work with in the legislature. Cathy, we will start with you in Washington State.

Cathy Munson: I am Cathy Munson and I am the Director of the Legislative Service Center. I report to a joint legislative committee. The service center itself provides information technology to the entire legislature, so we have the House, the Senate, the Actuary, an auditing group, and an accountability group, as well as the Code Revisor. We provide a single system to that whole body, so we are responsible for the systems, network, telephones, application development, customer service training—all of those things.

We basically have two sites: one on the Capitol campus where there are seven buildings and one about two miles away where the rest of us are located. With the exception of our customer group, we are all housed about two miles away from the campus. Our most critical service is telephones. Actually, that is the one service that our members expect to have all the time. And then as far as IT systems, the law making system, email, hotline, and constituent communications—all in about that order.

Glenn Newkirk: Thanks, Cathy. Dave, tell us about your responsibilities in Topeka?

Dave Larson: My name is Dave Larson and I am the Director of Computer Services for the Kansas Legislature. We also are a body that serves both chambers and both parties. My organization is responsible for the network, all the services on the network, and the support of the desktop computers. We deal with other types of technology, too, such as fax machines, telephones, PDAs, and scanners. We also run a training program similar to Cathy's. We operate a first responders program that runs out and performs triage at the site if there is a problem. If necessary, the first responders can escalate an issue up to our senior network technicians and we can support that in-house in most cases. If not, we can contract it out to a private firm. The critical applications are primarily bill drafting, bill status, and a document management system that contains all of our staff-generated documents. Things like fiscal notes, supplemental notes (bill abstracts and analyses), policy analysis, memoranda, and anything else that would be useful to the legislature are stored and indexed in the document management system.

Glenn Newkirk: Thanks, Dave. I guess I should point out here that, Cathy and I knew each other way back in the 1980's through NCSL. I think the first time we really met and did any work together was redistricting in the late 1980's. Is that right?

Cathy Munson: That is right.

Glenn Newkirk: And I have had the pleasure of working with Dave in the Kansas Legislature by way of full disclosure here for a couple of projects going back for a few years now, including project assistance on the document management system. In fact, I think I have been in Topeka so much I am eligible for a Kansas driver's license.

Dave Larson: Well, you have got one of the coffee bean cards.

Glenn Newkirk: Absolutely. They have one of the best coffee shops in the country in Topeka about three blocks from the State Capitol. Jim, how about your work in St. Paul?

Jim Greenwalt: I am Jim Greenwalt. I am Director of Information Systems at the Minnesota Senate. Being a little different from Cathy and Dave, I do not have the overall responsibility in regard to the legislature's information systems. I work solely with the Senate. Primarily, my responsibilities deal with all IS or IT and communications functions here--print and file servers, applications, communications, and faxes. We deal a little bit with our multimedia or Media Services people, with the television folks to get the video and audio streams out over the Internet. We will deal with any sort of support necessary for the Senate. We have our own help desk and we have our own training department. Each of them consists of just one person.

We also do the acquisitions that take care of systems security for the Senate, exclusively dealing with Members and staff. We do not deal with bill drafting itself. That is the Revisor of Statutes, but we do work closely with that department. The one thing is the Legislative IS staffs in the Minnesota sort of works as a group amongst themselves so that we can make everything work. We have a special organization that meets on a regular basis to do just that.

Glenn Newkirk: That sounds great, Jim. Now, Dennis, tell us a little bit about the ISD in North Carolina.

Dennis McCarty: My name is Dennis McCarty; I am Director of the Information Systems Division of the North Carolina General Assembly. We are very similar to Washington and Kansas in that we serve both chambers and both parties.

ISD provides the technical infrastructure for the North Carolina General Assembly. The technical infrastructure includes a mixture of personal (desktop and laptop) computers, server-class computers, card access systems, and security cameras connected by both a traditional wired network as well as a wireless network. On the application software side, ISD develops and maintains several legislative application systems. The major ones include: General Assembly Research and Drafting System or GARDS (developed in-house), Bill Status Systems (developed in-house), Electronic Voting

System, DistrictBuilder (in-house developed system for redistricting), Payroll, and finally Internet and Intranet Web sites.

The technical infrastructure is used by approximately 1,000 users with varying levels of technical knowledge and abilities. To help productivity, ISD provides technical training on the use of the infrastructure and its major applications and also maintains a Help Desk to provide support to members and staff.

Finally, ISD provides IT Legislative Analysis and Committee Support for both the Senate and the House.

Something I believe is relevant to our discussion topic that I'd like to mention is security and some of the challenges it presents. We process over 380,000 incoming e-mails each month. Approximately 15% of those have viruses or potential viruses attached to them that our anti-virus software intercepts. We continue to withstand around 182 bona fide attempts to break into our network each day. Any infection or penetration could ultimately force us to activate our business continuity or disaster recovery plans – not a very desired option! ISD is very diligent on keeping our network, servers, and PCs up-to-date with current patches. To date, this has proven to be very effective. Is that a good understanding Glenn?

I just did this presentation for our appropriation so I am rattling off some information from that presentation. [Laughter.]

Glenn Newkirk: Great overview, Dennis. The diversity in your Legislative environments is one of the reasons that I think it is great to get you four folks together—in addition to the fact that I have known all of you for some time. You all come from very different environments in many respects, ranging from basically a chamber system to across-the-legislative support. Then there is a whole arsenal of applications ranging from telephones, as Cathy mentioned, all the way over to other more traditional legislative applications of bill drafting and chamber automation.

To start off the discussion about business continuity and disaster recovery, I would like to mention that in 1990 I did a survey of all 50 state legislatures--just to show I was leading a terribly bored life, Dennis, there in the North Carolina General Assembly with not much to do. [Laughter.]

At that time I found that there were only two states that had any kind of, I guess you would call it, formalized attention being paid to business continuity and disaster recovery. That is to say, they had a plan of any kind on paper—other than a one-way ticket to Rio in the event there was a disaster.

With that in mind, I would like to go back to prior to September 11, 2001. What were some of the steps your legislature had already taken to improve your disaster recovery and business continuity capability without getting into any kind details that you might need to keep confidential for security reasons? How about if we start with you, Dennis? Just talk a little bit about what you had done prior to September 11th.

Dennis McCarty: Okay. Since I have only been the director here for three years a lot of this falls back onto Glenn, so just listen to the bad stuff that is after Glenn and before me. How is that?

Glenn Newkirk: That is great. Just keep in mind that somebody was in there between our tours of duty with the North Carolina General Assembly.

Dennis McCarty: Yes. Actually I started with the legislature five years ago. One of the things I looked at was our disaster recovery plan. At that time, we basically made sure that our tapes are stored off-site. We also had a working disaster recovery plan that had been updated from the one Glenn really put together years ago. I think it was 1923.

Glenn Newkirk: [Laughs] Yes, it feels like that was about in 1923, although I think it was around 1990 or '91.

Dennis McCarty: We had an established disaster recovery team with assignments. Meaning, if there was a disaster everybody knew what he or she had to do. The plan identified our second building (same physical complex) as our recovery site. Upon closer consideration, we decided to re-label the plan as a "Business Continuity" plan. We re-labeled our disaster recovery plan as a business continuity plan. The main reason for the re-labeling was that a… …hurricane could come through Raleigh and take out both of our buildings rendering our plan useless. So at that time we were in the throes of expanding and updating our newly labeled business continuity plan to become a true disaster recovery plan. So that is kind of where we were. Is that what you are after?

…a hurricane could come through Raleigh and take out both of our buildings…

Glenn Newkirk: That is a fine description. Jim, how about in the Minnesota Senate?

Jim Greenwalt: Okay. Let me see. What we had prior to 2001 really was generated from good old Y2K. That seemed to be the big issue back then. Of course, we went through all the hoops and whatnot to take care of that problem. That problem sort of generated the idea that there were additional things to do in regard to business continuity, number one. And number two, once Y2K was over we needed to use our resources for something else, since we found Y2K flopped there. We had people on staff to take care of a problem that turned out to be not so big after all. So we began dealing with what I would say were not so much continuity but security issues in the Minnesota Senate. We started with a security impact analysis. And for that analysis, we brought somebody in from Lucent who did it for us. They pretty much brought us up to speed as to the types of things that we would need to take care of security. But, of course, they also added into that analysis the items that now have

We started with a security impact analysis.

become what we would call a business continuity or disaster recovery plan.

Glenn Newkirk: Great. Dave, how about pre-9/11 in Topeka?

Dave Larson: I am going to take you back to about 1990. Prior to that time the Kansas Legislature and its support staff agencies were all independent entities doing technology and whatever they wanted their way and however the directors thought it should be done. In 1990 they created my position to oversee and unify all of the technology.

We began by first setting out for ourselves some principals that we were going to live by, some architectural principles. We got behind those principles and unified planning and coordination of our operations. We set about to document everything thoroughly. We established primary responsibilities for different systems and the recovery of those systems, training the staff, creating the backup schedules, and moving our critical systems to a secure location. We took them out of people's offices and under desks, moving them into a real computer room with fire protection, water protection, and 24x7 monitored security. We did pretty much the basics that should have been in place already but were not because we were not in any way, shape, or form a unified planning or operating entity.

Glenn Newkirk: Okay. And another thing, Dave, that I think makes Kansas somewhat unique among the four states represented here is that many of the servers in the Kansas legislative system are resident in a separate building actually managed by the Executive Branch's Department of Administration. So, you really have in effect outsourced much of the disaster recovery planning through a Service Level Agreement to an agency outside the Legislature. Is that correct?

…you have in effect outsourced much of the disaster recovery planning to an agency outside the Legislature.

Dave Larson: Exactly, that is the part I mentioned about moving to a controlled environment. As their technology gets smaller, it has created space in their mainframe center. Allowing us to move our servers and backup systems into that facility. They were willing to provide the floor space and clean power. They are paying for the guards, the monitoring systems, and other infrastructure. We then wrote a Service Level Agreement that allowed us to have certain expectations for support. Contracting for those services was really a big step for us.

Glenn Newkirk: Okay. Here you see an example of a Legislature that has outsourced, in effect, some of the business continuity and specifically disaster recovery functions to a third party. In this case the outsource agent happens to be the Kansas Department of Administration. That is a crossing of constitutional boundaries to get disaster recovery done. Cathy, how about in Washington State?

Cathy Munson: We have a plan that is called a service interruption preparedness and restoration plan. I know it was in existence by 1995, so it was created sometime between 1990 and 1995. It is essentially divided into three parts.

Preparedness and prevention is the first part.

Preparedness and prevention is the first part. A vulnerability analysis is the second part. A restoration plan is the third part. It has been updated over the years. And as part of that we have implemented a vault that is off-site for our backups. We have redundancy between these two sites that I mentioned earlier. Comcast provides our main connectivity. We have a microwave backup that has been used when Comcast has outages; one memorable occasion occurred during a fire in downtown Olympia.

We have maintenance contracts with a number of vendors. These contracts cover parts for the equipment that we have as well as getting here in a certain number of hours to help us when we have trouble. Several firewalls are involved in our system. We have fire suppression systems. For as long as I have been with the agency we have had these two facilities. They have limited, controlled access as well as water detection systems, backup generators, and fire suppression systems.

Glenn Newkirk: Okay. And, Cathy, I think as far as someone who has had the opportunity to see how some of these things work, you have been somewhat unique in the sense that I recall you experienced a substantial earthquake in Olympia. Was that in 2000 or 2001?

Cathy Munson: 2001.

Glenn Newkirk: 2001, that spring I think?

Cathy Munson: February 28th, right in session.

Glenn Newkirk: Yes. It was a significant earthquake that as I recall cracked the capitol dome and forced an evacuation of parts of the building. Is that right?

Cathy Munson: That is right.

Glenn Newkirk: Cathy, what brought about your recovery and continuity actions in Washington State prior to September 11, 2001? What was the impetus for the Washington State Legislature and your office deciding that you needed to take these steps?

Cathy Munson: Well, it has always been a part of the Legislative Service Center's plan. Since I have been part of the organization we have had this disaster plan. There have been a number of things that have had an impact on that over the ten plus years I have been with the Legislative Service Center. I have only been the Director since January 2001, so I got a real introduction to this whole thing when the Nisqually earthquake occurred at the end of February that year. That certainly brought the whole issue of being prepared and reacting right up to the forefront for us.

I got a real introduction to this whole thing when the Nisqually earthquake occurred.

We had to evacuate the building that day--all of the buildings. There were five buildings that we were responsible for. They were all evacuated. They had to remain evacuated while General Administration, who is actually the owner of those buildings, got a crew in to assess damage. So what we had were a bunch of people standing out in the parking lot for a number of hours.

"People things" became real obvious to us and they were not included necessarily in the plan that LSC had at that point. Individuals got out of the buildings quickly.

"People things" became real obvious to us and they were not necessarily included in the plan at that point.

It was a pretty nice February day. It was cold, and people were outside without keys to their car and without coats. They could not go back in the buildings, and in fact, could not go back in the buildings for three days. So we have had a number of things that we have had to plan for or we are trying to plan for based on that experience. We had to get chambers relocated. It happened on a Wednesday, as I recall, and we were back in session on Monday. But it was a real scramble for those four days in between.

The earthquake happened on a Wednesday and we were back in session on Monday.

Glenn Newkirk: So at least part of the impetus before 9/11 was that you have moved to develop a business continuity planning cycle, based in large part based on your geography. I mean, you are there in an earthquake prone area. So it has always been in the consciousness of the folks in the Northwest that this is something you need to at least think about.

Cathy Munson: Right.

Glenn Newkirk: Okay. Dave, you are in tornado alley, what were some of the main points that brought the Kansas legislature into thinking about business continuity and disaster recovery prior to 9/11?

Dave Larson: I think it probably was just a basic maturing of the legislature's use of IT as IT grew to be more of a critical component. Certainly when we unified our IT planning and began to assess risk across the whole enterprise from the different perspectives, you had people who would look at political, legal, and constitutional requirements for business continuity. They might ask, "If we could not fulfill our constitutional requirements, what would that do to the people of Kansas?" Also, what kind of political ramifications would that have and how would the Kansas Legislature's image look come election time if it was not prepared to handle these things?

When we unified our IT planning, you had people who would look at political, legal, and constitutional requirements for business continuity.

I think having that kind of institutional perspective was important as well as the technical perspective. Business continuity and disaster recovery became more than just worrying about how do I get connections reestablished and how do I make sure my data will be read off of my backup tapes and restored to servers. Those other perspectives really have helped us gauge the total risk. Once we had that maturity and the saturation of technology increased in the Legislature, we were really able then to get serious about the continuity and disaster recovery.

Glenn Newkirk: Okay. Jim, how about in the Minnesota Senate?

Jim Greenwalt: Well, nothing specific really brought about our work before 9/11. Members always were happy with other things they were doing. They were really paying attention to those other legislative matters and not to us. That has always been our sort of ideal. If the Members do not know we exist, that means things are going right. And so, our office kind of tries to ignore them, which we did until we got laptops in the Senate. [Laughter].

But the idea of disaster recovery really came out, as I mentioned, when we started things with Y2K. Y2K raised the idea of security. Security raised the idea of an impact analysis and things that we had to do to prepare. I think another thing that raised the concern was oh, what, about the time Windows 2000 came out. [Laughter]

...the idea of disaster recovery really came out when we started things with Y2K.

There seemed to be a few problems with security with that operating system. And as we continued to look at patches and what we could do, it became sort of obvious that we had to start looking at something beyond wishful thinking. So I think just things that were going on in the marketplace made us think about being able to recover from disasters and major security problems. I think Microsoft itself had a bearing on our beginning to be more aware of and start to do something on continuity planning, which really we had not done very much prior to this time.

Glenn Newkirk: Okay. So in a sense your situation was somewhat similar to Dave's. It was the maturing, the expansion, the use of new techniques and technologies that simply made it necessary to at least think about disaster recovery and business continuity.

Jim Greenwalt: Right. Very necessary because we became far, far more dependent on IT. Every year we continued to become more dependent on IT and the Members and staff could see that. In our office and in some of the other offices, professionals could identify points of failure that could cause considerable disruption in the legislative process. We had to start looking at that possibility.

Glenn Newkirk: Right. Okay. Dennis, what about pre-9/11 for you? Apart from a few bomb threats that you had and other things like that it must have been pretty tame over there on Jones and Lane Streets, huh?

Dennis McCarty: Sure. Bomb threats always help stir creative juices. Really, we looked at business continuity as just a pure system management discipline. We were after a high level availability provided by redundancy, replication, and backups. Again, remember I said that we were doing more of business continuity. But as we looked back in the past reviewing our disaster recovery plans we looked at some things that have happened in the Raleigh area such as Hurricane Fran in the mid-90s and the ice storms of December 2002. Sorry, Kansas, we get bad storms, too!

Hurricane Fran was pretty daunting. There was a lot of damage, but fortunately not to our buildings. Still, that was a wake up call. So if you take the system management practices and best industry practices, and I hate to use that term best practices, we throw into the mix the risks that we have when we do get hurricanes. And then the bottom line is that there was recognition that information technology is not just a nice thing to have in legislatures, it is a necessity. So that is what made us move on to more detailed disaster recovery and business continuity planning.

Information technology is not just a nice thing to have in legislatures. It is a necessity.

Glenn Newkirk: What about 9/11? What steps have you taken after that? And I will say, I will use the phrase, "as a result of 9/11," although we will talk about whether that is really the case or not. But what have you done since 9/11?

Dennis McCarty: Who are you addressing that to, Glenn?

Glenn Newkirk: You.

Dennis McCarty: Okay. After the 9/11 events we accelerated our disaster recovery planning updates. Let us call what we did "hardening" of our facilities. We improved our facilities' physical security with access cards, duress alarms, and cameras—all the deterrents. We improved our network security ten-fold. We reviewed and modified our backup and recovery procedures by looking at the backup cycles, their contents, and the physical location of our off-site storage. The events of 9/11 highlighted the need for us to be able to recover from a "local" disaster and provided the additional justification for establishing a formal out-of-state recovery center. As the result, we… …established a formal agreement with one of the two major Disaster Recovery services providers and conduct three recovery exercises a year. But overall, the largest set of activities was related to disaster avoidance by tightening up our belt on the security side. We have done a lot there. At the end of March we successfully completed an extensive information security assurance review that resulted in us becoming a TruSecure Certified Enterprise. This certification recognized us as making security a priority and certified that we comply with the 101 TruSecure Essential Practices. If nothing else, this shows our commitment to security and disaster preparedness.

Events of 9/11 provided the additional justification for an out-of-state recovery center.

Glenn Newkirk: Great!

Dennis McCarty: So you know, that and maybe a dollar might get you that cup of coffee in Topeka. I am not sure. But it does show that we put some effort in there and now we are prepared. And we have done tests, we have done three major tests off-site and we were able to recover, and we have more to go.

Glenn Newkirk: Okay, great! Jim, how about after 9/11 in St. Paul?

Jim Greenwalt: I would have to say that probably 9/11 did not really affect us that much as far as anything specific happening, other than the fact that it created an awareness. It gave us the opportunity to funnel some dollars into the project. We did that with the Senate, the Revisor, and the Library. Some of us were able to begin dealing with our security issues, which included rebuilding the entire firewall, DMZ, VPN access. We have installed an intrusion detection system. We are just putting together the finishing touches, I hope, on our instant response teams. And as far as our business continuity planning goes, that is still in what I call in draft form.

But 9/11 allowed us to take resources, which were staff and some dollars, and dedicate them towards that work. You asked about the impact of the terrorism threat in your meeting discussion sheet. Did that effect us or have any effect other than scaring us or making the people in our departments of public safety who like to carry guns, feel better about our security? For us, no, but it did bring in the idea that there are all sorts of other opportunities for things to happen, whether it might be something internally or just people messing around with web sites. Terrorism has not been a big issue, but it at least brought a number of issues to the forefront and allowed us to use our resources to add to what we had before.

Glenn Newkirk: Right. So it has brought about some increased awareness.

Jim Greenwalt: Absolutely. Yes.

Glenn Newkirk: I have to say that on September 11, 2001 I was in the Candlewood Suites in Topeka, Kansas, working on a contract with Dave's organization. And I can tell you immediately one effect of September 11, 2001 was that my partner and I could not get into the Kansas State Capitol that morning to go to work. Security became really good and really tight. Everything was blocked off. It took some help from Dave's office to get us back in the building. But, Dave, what has gone on there since that time? I know that you have done some recovery testing. We participated with you and your staff in business continuity and disaster recovery testing for some of your applications. What else has gone on since September 11, 2001?

Dave Larson: Well, I think what made 9/11 pivotal for us was that, finally, it got the upper management's attention even more so than the bombing in Oklahoma City. Oklahoma City did not galvanize upper management like 9/11. One of the effects of 9/11 was that we now have a Kansas homeland security committee. Additionally, before budget items for things like security and disaster recovery were never really examined.

But nowadays you are asked, “Have you thought about this and are you prepared for that?” when it comes time for budget examinations. Previously, people who just expected you to be protected and to be able to recover from tornadoes, floods, or whatever. Today, they assume nothing and actively ask you questions that are much broader concerning sources of risk and more and to the point concerning prevention and recovery. So there is, I guess, a much higher awareness. I agree with Jim in that respect. I think management now recognizes the value of business continuity and disaster recovery expenditures.

Management now recognizes the value of business continuity and disaster recovery expenditures.

Glenn Newkirk: Okay. Cathy, how about Washington State?

Cathy Munson: I would agree with the awareness aspect of it. From our perspective, it was mostly awareness of physical security issues. We are also in the middle of renovating our legislative building. That was planned before September 11th, but a security study was going on during that time that has since been published. It is a study for the entire capitol campus, which includes executive branch agencies, the legislature, and the courts.

That study is getting a whole lot more attention as we are renovating the buildings, and security is going to receive more attention as a result of 9/11. The infrastructure necessary to install cameras, control access to buildings, and improve communication was planned but implementation was scheduled for post-renovation. I think that approach is going to change although we are in the middle of discussing that right now. We are in a tight budget situation, so the outcome is still a bit unknown.

It has also brought up the issue of whether our network hub in the legislative building should be located elsewhere. As we were doing the renovation planning we considered moving it and with all of the investment in the infrastructure we were talking about slightly over $1 million to make the move. That did not happen because of that cost. But as an overall plan, we are hoping to look at whether we should remain in that facility.

Glenn Newkirk: Okay. Let me just kind of throw this issue open now. I think Dave in particular mentioned one of the effects of 9/11 was that it increased senior management’s awareness of these issues. How about legislators’ awareness of these issues? Are the events of 9/11 the kind of thing that either made it easier for you to talk to them and present ideas to them? Is it a situation where they would come to you asking you, as Dave indicated senior management had, what are we doing in this legislature regarding security and recovery? Did any of you have those experiences with legislators?

Dennis McCarty: Glenn, I will throw in something that is really interesting. On

9/11, we were in a Legislative Services Commission on Information Technology (our legislative steering committee) meeting on technology. The purpose of this specific meeting was to present our plans for overall equipment, personnel, business continuity, and disaster recovery. We were in the meeting when the incident actually happened and we got a page saying, "You are not going to believe this but the World Trade Center just got hit by an airplane." We thought it was a joke. A TV was wheeled into the meeting room and sure enough it really happened. How appropriate! That spurred a multitude of questions. Now, every time we meet we update them on our security and disaster recovery plans and what our results have been to date. So yes, awareness, absolutely--especially among the Legislators.

Now, every time we meet we update our legislative steering committee on our security and disaster recovery plans…

Glenn Newkirk: Okay. And I know that you also have two or three legislators who work on that committee and some of your other technology committees who are pretty savvy about technology issues. I imagine they would be able to raise some good questions and give some good ideas on occasion.

Dennis McCarty: Well, yes, and they actually have. Several members of the Legislative Services Commission on Information Technology are also on the House and the Senate technology committees. In fact, one of the Senators on the Commission is a former member of the Federal Communications Commission and always poses valuable technical questions and challenges for us to respond to. I guess in Minnesota you have a person, Senator Kelly, who is pretty active as well.

Jim Greenwalt: Yes. Senator Steve Kelly is probably the only person that has raised any issues at all. He is very active in computerization…and not just hardware and stuff, but how it can be utilized for government services, public services, schools, hospitalization, rural development, and areas like that.

But in Minnesota, to be honest with you, with that one exception we have had no other members really raise an issue or raise a concern. As a matter of fact, apparently they have so many other issues that they are worried about this year, we do not have an oversight committee for our operations. We have had one for what, six or eight years, and I would like to tell everybody that we just do such a great job we do not need the oversight committee. [Laughter]

Unfortunately, it makes it tougher sometimes to get money, but we cannot get it anyway because of the budget problems. But we have not really had Members be too concerned. We are fortunate that my boss, Pat Flahaven, the Secretary of the Senate, does a good job of watching those things. I think most of the Members just let him do his job. And that is where we are.

…we have not really had Members be too concerned.

Glenn Newkirk: Thanks, Jim. Dave, Cathy, anything to throw in on that topic?

Cathy Munson: Well, part of this restoration project for the legislative building involves a committee of members of the Legislature. There are two House members and two Senators on the committee. They are very aware of security sorts of issues and planning for disasters and they have been vocal in these meetings about their concern. I think it is a combination of the earthquake and 9/11. There were a number of frightened members during the earthquake because they were in the building. Then 9/11 added to that. We have had a couple of other issues with groups chaining themselves to buildings and that sort of stuff. So security and disaster recovery is very much on their mind.

Glenn Newkirk: Okay. Dave?

Dave Larson: I think the expectation was always there. The expectation from legislators was "You will take care of me" and we had always planned for things like fires, floods, and tornadoes--and even the occasional human error. But since 9/11 I see our legislators rising above previous expectations and actually challenging us to think broadly and innovative about risks. You know, prior to 9/11, airline hijackings were thought of as extortion attempts and not guided missiles. Failures due to human interaction were viewed as stupidity, and now it is looked at as aggression. Mother Nature was always destructive and somewhat fickle, but she was never malicious or cunning about it. Legislators today are asking, "Are we prepared to withstand a technology attack?"

Legislators today are asking, "Are we prepared to withstand a technology attack?"

An ex-military intelligence man heads our homeland security committee. He was picked to head that committee because of his experience. Believe me, he can ask some very penetrating questions.

Glenn Newkirk: Okay. Well, maybe now we can start back again with Cathy and have each of you identify what you would consider to be the one or two hurdles peculiar to the legislative institutions and different maybe from other government organizations. I am referring to hurdles to disaster recovery and business continuity planning. Are there any hurdles that you would say that are peculiar to legislatures?

Cathy Munson: One of the things that we are dealing with in this renovation project is access to buildings, and most of the members want to keep the public access fairly readily available with few obstacles. They do not want to make the buildings difficult to visit. And I think that is unusual as far as other agencies that we see—they have security staff controlling access. So knowing who is in our buildings and what they are doing and then keeping our IT infrastructure secure from threats is important. We have been successful at it so far, that does not mean we will be in the future.

Glenn Newkirk: Okay. Dave, do you have anything that you could reflect on there in Topeka as being unique to the legislative institution?

Dave Larson: One thing that jumps to mind when I hear that question is the peculiar privacy and confidentiality issues that are involved at the legislature. There are preparations that we need to make to preserve the client/attorney privilege between the Revisors attorneys and the Legislators, between the Legislators and the Legislative Research Department staff, and finally between the Legislator and their constituents. It makes me think that I have to have a recovery and continuity process that accounts for that kind of system because the enterprise does not own all the data like it does in a corporate environment. Some of that data is not a public record and it belongs to the Legislator.

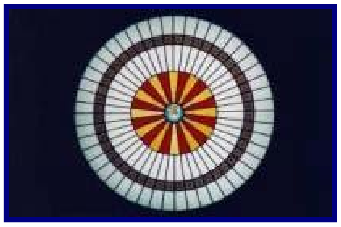
There are particular privacy and confidentiality issues involved in the Legislature.

When you build a business continuity/disaster recovery system of that sort, you have to ask, "What is the real value of the data?" Should I pay thousands of dollars to protect pennies worth of data? In my eyes it might be pennies worth of data, but that view may not be held by the legislator. In corporate America they analyze the recovery and continuity problem in terms of cost and benefit. In the legislature we have a different set of values such as confidentiality, political power, and constituent service—which is another way of saying votes.

In the legislature we have a different set of values such as confidentiality, political power, and constituent service…

Glenn Newkirk: Okay, Dave, excellent observations. Jim?

Jim Greenwalt: I would say the first thing I thought of when I saw this discussion question was that there is such a great amount of variation in the nation's Legislatures. As we know, we have got sizes ranging from California to Wyoming. There is one person, I guess, there are two now in IT in the New Hampshire Legislature. So staff is a little bit different in every state. But the way the Legislature functions and changes, especially the change that seems to be taking place in many places now, is amazing. Some of us—I know Glenn, I think, and myself, I am not sure who else has been around the Legislature since the early 1970's—know that there has been quite a bit of change in the way things happen around Legislatures. Whether the change is term limits or the politics or the pendulum moving this way or that way or the move to more professional legislatures in some cases, the change is always occurring.



…there has been quite a bit of change in the way things happen around Legislatures.

But the facts that we have a tendency to have some turnover here, that we have members coming and going, and that we have leadership changes, do not help us in trying to keep doing what we have to do while talking about business continuity.

And with the issues coming up in the last year and a half, and probably the next year and half, issues that are budget oriented affecting various social welfare programs and tax levels, our staff administrative issues, which include recovery and continuity are going to have a lot of competition in the minds of Legislators.

...administrative issues, which include recovery and continuity are going to have a lot of competition in the minds of Legislators.

So we have a tendency not to be able to have the same support that we have had in the past with Members who have been around longer. They often took a greater interest in the institution then in the particular agendas that the individual members have. You could spend a lot of time talking about the legislative institution and the change in the relationship between Legislators and staff in that regard.

So I think that I have a problem more than simply just having the trained staff. A lot of legislative computer staff in the smaller states comes from the legislative staff. So you do not have "that professional IT person out there." I think it was Dave who mentioned that someone came in from the military who really had a handle on this kind of issue versus a legislative staff person with some computer knowledge who starts working for the computer department. So a big hurdle that we have is simply having the staff size and staff trained to be able to work on issues like business continuity and disaster recovery to keep it going, maintaining the response teams and the business continuity and disaster recovery plans.

...a big hurdle we have is simply having the staff size and staff trained to be able to work on issues like business continuity...

Glenn Newkirk: Okay. Great thoughts, Jim! Dennis?

Dennis McCarty: Those are really good points. It gives me some ammunition back here.

Jim Greenwalt: It is the same in every state, believe it or not.

Dennis McCarty: Here we have slight variation of the problem. We have built a staff that has some very high technical expertise. We have a couple people with their CISSP's (Certified Information System Professional) and several people with all the Microsoft certifications. Now the variation – Although the staff is very technical, they tend to not understand the legislative process and what is/is not important. So when performing a risk assessment, they seem to think "These are just documents--who cares about documents…they can't be all that important." This situation sort of reverses the training requirements for us to emphasize the legislative and business views. On the other side, the legislators and central staff (i.e., fiscal and research staff) do not think that disaster recovery or business continuity applies to them.

The situation reverses training requirements to emphasize the legislative and business views to our technical staff.

If you wrap that up with the last item Jim discussed, the balancing of "technical vs. legislative vs. business" views of security and disaster recovery consumes a lot of time and frequently sends us off to Never-Never Land.

...balancing "technical vs. legislative vs. business" views of security and disaster recovery consumes a lot of time...

A prime example of this conflict was our old policy governing changes to our technical infrastructure during session. Prior to 9/11, our policy was not to do any changes during session. After 9/11 it became apparent that our policy needed to be updated to accommodate for critical changes during session, especially when the change was related to security or disaster recovery. The revised policy also supports good system management practices by controlling the rate of change (no longer a pent-up demand for change followed by a "slam-dunk" implementation).

Glenn Newkirk: And the way the legislative sessions have been going in North Carolina that means you have, let me see, the week between Christmas and New Year's when they are not in session, right?

Dennis McCarty: I think we had almost a month last year to roll in all our changes—and that was a "short session" year.

Glenn Newkirk: Okay. That is a great, thoughtful list, everyone. There are some good observations in there about the differences between Legislatures and other organizations in terms of the environment for business continuity and disaster recovery. Is there any one issue that you think really jumps out as a major hurdle to business continuity planning in Legislatures? When I listen to these points you have made—and, Jim, I imagine you probably have the same reaction, I would say they are all pretty tough issues that you can only work around. I mean, these are big institutional issues. You cannot go in and change the CEO, the COO, or the CIO, or just add money that will solve any of these problems.

Jim Greenwalt: To me the biggest hurdle—and I might have to make a combination of things here—is having the staff trained in how to do business continuity planning and what to do with the plans once we have them. It would be nice if there were some sort of a blueprint that people could use. That would be especially the case in the smaller states that have to get a start on this from the beginning. But they do not have maybe two, three, or four staff people to assist in generating these sorts of plans. I think that would be a huge help along with the other problem we have talked about—and that is Member support for this kind of work.

It would be nice if there were some sort of a blueprint that people could use to assist in generating plans.

I have really found that it is very difficult to do things when you do not have that "project champion" in the leadership or whomever it is that can carry that project with the members. So that awareness, I think, is the one of the biggest problems for us.

...it is very difficult to do things when you do not have a "project champion..."

Glenn Newkirk: Thanks, Jim. Anybody else have any ideas on the hurdles? None? Well, I think I would like to ask now about what are some of the tips and techniques that you can think of or that you have employed that would help legislative IT managers get over some of those hurdles? What are some of the things that you have done, Dave, working with your committees and senior management?

Dave Larson: Well, I am really high on the three-team IT governance structure we have in the Kansas Legislature. Back in the period of time when we were unifying ourselves, we created an Executive Steering Committee, which is the Legislative Leadership. We created what we call a Review Team, which is made up of all of the department heads and four rank-and-file Legislators. Then we have the Information Systems Team, which is made up of professional staff representing all of the different support agencies of the Legislature as well as the Secretary of the Senate and the Chief Clerk of the House.

What I really find helpful about this arrangement is that all of the planning, policy, and budget issues concerned with recovery and continuity are identified by the staff, proposed by the staff, and worked up through the department heads. They in turn analyze what effect the plan or policy is going to have on their departments and on interdepartmental relations. They make refinements to the plan or policies that are necessary to implement business continuity/disaster recovery. Finally, the recommendations are pushed to the Steering Committee who has final approval on budget and policy adoption. By using this three-team approach we have gotten a perspective that covers the entire breadth of the Legislature. Everybody is on the same page and we have an automatic executive buy-in with every project or policy we choose to implement.

Glenn Newkirk: Dave, having worked with you in that three-team approach, I agree with what you mentioned as a key phrase: buy-in. Sometimes it is not easy to get agreement on things, but once you do get that agreement it is pretty much chiseled in stone.

Dave Larson: Yes it is.

Glenn Newkirk: And, Dave, this process works even when it comes to negotiating the service level agreement with your provider of business continuity, disaster recovery, and security services. Without going into any details, I was there at one point when there was a problem with your service provider's performance. I think it is fair to say that once you had to walk across the street and remind them of the contents of the service level agreement. They knew there was no misunderstanding and that they knew clearly that it has been approved all the way up and down the line in the Legislature. There was no doubt whatsoever about what the outcome of that situation was going to be.

Dave Larson: None whatsoever.

Glenn Newkirk: Okay. Anybody else have any tips and techniques they would like to share?

Jim Greenwalt: The one technique I have always wanted to do on the last three days of session is to crash the system intentionally so they know how important it really was. [Laughter]

Glenn Newkirk: You only get one chance to do that test, Jim.

Jim Greenwalt: I know it. I am not that close to retirement yet.

No, but my biggest item is staff training for business continuity and disaster recovery. Also, there is the cooperation and work with the other agencies that you have to deal with on these topics. I think that cooperation is essential, getting everybody involved if you can.

We just talked about three groups of one sort and another. Again, we have a similar group of people that meets regularly here in Minnesota that is involved in security and recovery issues. It is called LSIG, Legislative Security Integration Group. All decisions regarding security and continuity that are made across the board are handled by that group, not just by the Senate or by one agency—if we can avoid it. And the cooperative efforts, buy-in, and cooperative work on that scale or that level are very, very important.

Glenn Newkirk: Okay. Cathy, how about in Washington?

Cathy Munson: Well, our challenge is really to communicate and coordinate our IT business continuity and disaster recovery plan with the security that the Legislature has—as well as with the plans of the executive branch. Because the Legislature shares the Capitol campus with several other agencies, we all need to understand how our individual plans fit into a campus-wide plan.

We also have the challenge of communicating what is in our plan regularly to Legislators and legislative staff. Because we do not have a totally redundant system and we have had outages, it comes home to them somewhat regularly about what we have in that plan and where our vulnerabilities are.

We also have the challenge of communicating what is in our plan regularly to Legislators and legislative staff.

And I had a chuckle on Jim's comment because on the 26th of March we had a cable break, a major cable break as part of this renovation of the legislative building, so we had most of the legislature down for about 16 hours. There is no redundancy where the break occurred. We were in session, were in committees actually, so we did all right. But people

thought we had redundancy there. So it is a matter of communicating information about capabilities on a regular basis so they know what we do have.

Glenn Newkirk: Okay. Dennis, how about your success in North Carolina?

Dennis McCarty: I have already heard most of what I was going to say. Let me just mention, or expand on, a couple of the tips and techniques.

First is getting a sponsor up front. Without a sponsor at the appropriate level, selling the need for disaster recovery and obtaining the funding for it is nearly impossible.

Without a sponsor at the appropriate level, selling the need for disaster recovery and obtaining the funding for it is nearly impossible.

Secondly, boundaries should be set as to which IT services should be expected to be available in the event of a disaster or a business continuity fail over. Supporting this is staying focused--when you get your plan developed, stay focused on it and the objectives that you originally set so that you can execute it successfully.

As a final thought, do not become complacent with the plan you develop. You know, the tendency is there to say, "Whew, my plan is done. I can relax now." No, you cannot! We do hold regular disaster recovery meetings and communications with our staff. That is how we keep our IT staff involved and our Legislative Services Commission involved. Once you have a developed plan, make sure that it is current.

Once you have a developed plan, make sure that it is current.

We update ours whenever there is a major change to the infrastructure (facility, hardware, and software). Also, training for our individuals and providing a "how-to" for recovery has been important. We keep everyone on top of what the new technologies are that we are using, such as different backup systems. Finally, we just keep the communications flowing, especially with our sponsors.

Glenn Newkirk: Okay.

Jim Greenwalt: I would like to make one more observation. Right now our Department of Public Safety is working with our Sergeant's Office on the question of "Okay, what happens if the disaster affects the Capitol Building, such as an earthquake or something that like?" And we have talked about trying to keep things going in that situation. But now they are coming and saying, "Okay, what if we have to pick up and move all of a sudden? What site do we go to?" It has been very interesting to watch that exercise because of folks who are saying, "Oh, we have got to move the Legislature to some other place in the event of some kind of major disaster." Their idea of moving the legislature is we find a room with 201 seats, maybe we find some recording equipment. And that is it as far as they are concerned.

Now, maybe that is the bare minimum. But we all know that sometime, if they are going to try to pass serious legislation, it gets a little bit heavier than that—with more requirements. So, at this point the whole disaster recovery process can take another step beyond just what happens if we have a failure within our system. We start looking at what happens if we have some failure in the facilities themselves and you have to move someplace else—like they did in Washington State.

Glenn Newkirk: That is where you really get into the step up from disaster recovery of computer systems and networks to full business continuity planning for a legislative institution.

Jim Greenwalt: And that is a big thing! It is really interesting because most of the people on the outside of the process do not understand how it works on the inside.

…most of the people on the outside of the process do not understand how it works on the inside.

Glenn Newkirk: Right. You learn quickly that you cannot just go get an auditorium somewhere at Mankato State and start running a session in one day.

Jim Greenwalt: Well, I will tell you, they had some out-state meetings here. Other than somebody finding the bus, they did not know what they were doing down there. It was a little bit on the scary side, to be honest with you.

Glenn Newkirk: [Laughing] Okay. Any other ideas, tips, or tricks to throw in here? This is a great list particularly at the end of a work week for all of you. I really appreciate the comments on the differences of the legislative institution from other organizational settings. Also, you have provided use with some excellent "tips and tricks" for establishing disaster recovery and a business continuity process in legislatures. The issue of being able to get buy-in to support your business continuity planning process was central to your comments. One of the ways that you have all mentioned about getting that buy-in and support is communication with other people, and particularly a sponsor or chief sponsors for your efforts. And, Dennis, you were saying that those sponsors need to be legislative Members and not just legislative management, is that right?

Dennis McCarty: Absolutely. Yes.

Glenn Newkirk: Okay. Let me click off some additional steps you have mentioned as critical to your disaster recovery and business continuity planning processes. Set clear expectations about what you have to do to recover. That is one of the most… …difficult things to do in an environment with constant Member and staff turnover. Hold regular meetings with Members and staff as part of that communication cycle. Keep the plan current. And by keeping the plan current I assume, Dennis, that you are including in that the necessity of testing periodically as well as just keeping it current on paper as your system configuration changes.

Set clear expectations about what you have to do to recover.

Dennis McCarty: Yes. Every time we do a test when we come back we go over the plan and say, okay, "What has to change based on our recent learning experience?"

Glenn Newkirk: Okay. Well, we have stretched just a few minutes over the hour that I promised all of you we would spend in our discussion today.

Just as importantly, we have brought out some key points about the thought, planning, and effort required to keep these unique governmental institutions in operation.

Thank you all very much across the country! As always, it has been a pleasure talking with you and benefiting from your insights on how disaster recovery and business continuity practices have developed in your state legislatures.

Glenn Newkirk is President of InfoSENTRY Services, Inc. He directs all of the firm's major IT consulting engagements, particularly those involving recovery of challenged projects, quality assurance reviews of large IT implementation projects, and business continuity planning projects. Prior to forming InfoSENTRY in 1994, Glenn was Director of the Legislative Automated Systems Division for the North Carolina General Assembly and worked with the National Conference of State Legislatures' Legislative Information System in Denver, Colorado. He is a Certified Business Continuity Professional (CBCP) by the Disaster Recovery Institute International.

Cathy Munson's association with the Washington State Legislature began in 1985 when she was hired by the Senate to assist with the deployment and implementation of personal computers in member offices. In 1990 she moved to the Legislative Service Center as manager of the Customer Support Group. From 1996 to 2001 she managed LSC's Technical Support Group becoming Director of the agency in January 2001. Cathy has an undergraduate degree in computer science and a master's degree in business administration

Dave Larson is the Director of Legislative Computer Services for the Kansas Legislature. He is certified in both public administration and project management. Dave is active in the National Conference of State Legislatures (NCSL) and has served as the Staff Vice Chair on several NCSL information policy and technology committees. Dave is also a member of the NCSL National Association of Legislative Information Technology (NALIT) and is an Associate Member of the NCSL American Society of Legislative Clerks and Secretaries where he has served as chair of their Support Staff and Information Technology committees. He is regularly asked to be a panelist at NCSL conferences. For the State of Kansas, Dave serves on the Information Technology Board (ITAB) and is a member of the email policy, statewide architecture and internet subcommittees. He has published several articles on technology and information systems management.

Dennis McCarty is the Director of the Information Systems Division of the North Carolina General Assembly.

Jim Greenwalt has worked for the Minnesota Senate for over 31 years in several positions, most recently as the Director of Administrative Services Department and Information Systems Department. Jim has been involved with the National Conference of State Legislatures (NCSL) since 1974, as an associate member of the American Society of Legislative Clerks and Secretaries (ASLCS) from 1974 – 1986, and with National Association of Legislative Technology (NALIT) since 1987. He is a past chair of NALIT, past member of the NCSL LSCC and Executive Committees. He has served as chairs of the Information Technology Task Force, the NCSL Web Site and Legisnet Task Force, the Professional Development Task Force and the Special Committee on Information Management. Jim is Staff Chair of the National Conference of State Legislatures for 2003-2004. Jim is a certified project manager and a graduate of St. Cloud State University.